Web 应用程序报告

该报告包含有关 web 应用程序的重要安全信息。

安全报告

该报告由 HCL AppScan Standard 创建 10.0.0, 规则： 0
扫描开始时间： 2020/12/29 10:08:57

目录

介绍

- 常规信息
- 登陆设置

摘要

- 问题类型
- 有漏洞的 URL
- 修订建议
- 安全风险
- 原因
- WASC 威胁分类

按问题类型分类的问题

- SQL 盲注 4
- SQL 注入 1
- 跨站点脚本编制 12
- 通过 URL 重定向钓鱼 1
- 跨站点请求伪造 42
- 使用 HTTP 动词篡改的认证旁路 1
- “Content-Security-Policy”头缺失或不安全 5
- JavaScript 劫持 8
- 查询中接受的主体参数 2
- 发现 Web 应用程序源代码泄露模式 1
- 发现数据库错误模式 1
- 跨帧脚本编制防御缺失或不安全 4
- 自动填写未对密码字段禁用的 HTML 属性 1
- HTML 注释敏感信息泄露 33
- 发现电子邮件地址模式 11
- 发现可能的服务器路径泄露模式 7
- 发现内部 IP 泄露模式 1
- 客户端（JavaScript）Cookie 引用 4
- 应用程序错误 2

修订建议

- 查看危险字符注入的可能解决方案
- 禁用基于参数值指向外部站点的重定向
- 将您的服务器配置为仅允许所需 HTTP 方法
- 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce
- 除去 HTML 注释中的敏感信息
- 除去 Web 站点中的电子邮件地址
- 除去 Web 站点中的内部 IP 地址
- 除去 web-server 中的源代码文件并应用任何相关补丁
- 除去客户端中的业务逻辑和安全逻辑
- 将“autocomplete”属性正确设置为“off”
- 将服务器配置为使用安全策略的“Content-Security-Policy”头
- 将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头
- 拒绝恶意请求并防止直接执行 JavaScript 响应
- 请勿接受在查询字符串中发送的主体参数
- 为 Web 服务器或 Web 应用程序下载相关的安全补丁
- 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

咨询

- SQL 盲注
- SQL 注入
- 跨站点脚本编制
- 通过 URL 重定向网络钓鱼
- 跨站点请求伪造
- 使用 HTTP 动词篡改的认证旁路
- “Content-Security-Policy”头缺失或不安全
- JavaScript 劫持
- 查询中接受的主体参数
- 发现 Web 应用程序源代码泄露模式
- 发现数据库错误模式
- 跨帧脚本编制防御缺失或不安全
- 自动填写未对密码字段禁用的 HTML 属性
- HTML 注释敏感信息泄露
- 发现电子邮件地址模式
- 发现可能的服务器路径泄露模式
- 发现内部 IP 泄露模式
- 客户端（JavaScript）Cookie 引用
- 应用程序错误

应用程序数据

- cookie
- JavaScript

- 参数
- 注释
- 已访问的 URL
- 失败的请求
- 已过滤的 URL

介绍

该报告包含由 HCL AppScan Standard 执行的 Web 应用程序安全性扫描的结果。

高严重性问题：	18
中等严重性问题：	43
低严重性问题：	22
参考严重性问题：	58
报告中包含的严重性问题总数：	141
扫描中发现的严重性问题总数：	141

常规信息

扫描文件名称：	未命名
扫描开始时间：	2020/12/29 10:08:57
测试策略：	Default

主机	127.0.0.1
端口	8000
操作系统：	未知
Web 服务器：	未知
应用程序服务器：	JavaAppServer

主机	127.0.0.1
端口	8090
操作系统：	未知
Web 服务器：	未知
应用程序服务器：	JavaAppServer

登陆设置

登陆方法：	自动
并发登陆：	已启用

会话中检测：	已启用
会话中模式：	toclose : true, //自动关闭
跟踪或会话 ID cookie：	JSESSIONID JSESSIONID
跟踪或会话 ID 参数：	time time time
登陆序列：	http://127.0.0.1:8000/xmjg/opus/front/blue/index.html http://127.0.0.1:8000/xmjg/login http://127.0.0.1:8090/opus-front-sso/oauth/authorize?client_id=xmjg&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=jkCUEY http://127.0.0.1:8090/opus-front-sso/authentication/require http://127.0.0.1:8090/opus-front-sso/authentication/form http://127.0.0.1:8090/opus-front-sso/oauth/authorize?client_id=xmjg&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=jkCUEY http://127.0.0.1:8000/xmjg/login?code=1jN0Yy&state=jkCUEY http://127.0.0.1:8000/xmjg/opus/front/blue/index.html http://127.0.0.1:8000/xmjg/opus/front/om/users/currOpusLoginUser?time=1609207775015 http://127.0.0.1:8000/xmjg//xmjg/xmjg-project-info!getScreen.action http://127.0.0.1:8000/xmjg/index/getSystemName http://127.0.0.1:8000/xmjg/opus/front/om/users?loginName=admin&time=1609207775097 http://127.0.0.1:8000/xmjg/opus/front/om/users/user/10000/allMenus?isTree=true&netName=前端网络入口&tmnId=1&topOrgId=A&userId=10000&time=1609207775096 http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879 http://127.0.0.1:8000/xmjg//analysis-info!getPilotCity.action http://127.0.0.1:8000/xmjg//monitorEarlyWarning/earlyWarningRecord/noticeToConfirm.do http://127.0.0.1:8000/xmjg//mapShowConfig.do http://127.0.0.1:8000/xmjg//xmjg-project-info/getProvinceAuthority http://127.0.0.1:8000/xmjg/supervisionInspection/getMergeData.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29 http://127.0.0.1:8000/xmjg/supervisionInspection/getProvinceTopFive.do?province=660000&startDate=2020-01-01&endDate=2020-12-29 http://127.0.0.1:8000/xmjg/supervisionInspection/getYsTotalOfMultidimensional.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29&spysDy0= http://127.0.0.1:8000/xmjg//supervisionInspection/getMapCountryAndProvinceXms.do?xzqhdm=660000&tjfs=xmsl&cityType=province&startDate=2020-01-01&endDate=2020-12-29 http://127.0.0.1:8000/xmjg/supervisionInspection/getYslAndXzblxms.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29 http://127.0.0.1:8000/xmjg//analysis-info!getHaveProjectCitys.action http://127.0.0.1:8000/xmjg//xmjg-project-info!saveFunctionLog.action http://127.0.0.1:8000/xmjg//xmjg-project-info!getMapConfigData.action?bigScreenFolder= http://127.0.0.1:8000/xmjg/xmjg/xndc/map/mapJson/abbrMapJson/province/66.json http://127.0.0.1:8000/xmjg/supervisionInspection/getYslAndXzblxms.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29 http://127.0.0.1:8000/xmjg/supervisionInspection/getMergeData.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29 http://127.0.0.1:8000/xmjg/supervisionInspection/getProvinceTopFive.

```
do?province=660000&startDate=2020-01-01&endDate=2020-12-29
http://127.0.0.1:8000/xmjg/supervisionInspection/getYsTotalOfMultidimensional.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29&spysDy0=
http://127.0.0.1:8000/xmjg//xmjg-project-info!getMapConfigData.action?bigScreenFolder=
```

摘要

问题类型 19

TOC

	问题类型	问题的数量
高	SQL 盲注	4
高	SQL 注入	1
高	跨站点脚本编制	12
高	通过 URL 重定向钓鱼	1
中	跨站点请求伪造	42
中	使用 HTTP 动词篡改的认证旁路	1
低	“Content-Security-Policy”头缺失或不安全	5
低	JavaScript 劫持	8
低	查询中接受的主体参数	2
低	发现 Web 应用程序源代码泄露模式	1
低	发现数据库错误模式	1
低	跨帧脚本编制防御缺失或不安全	4
低	自动填写未对密码字段禁用的 HTML 属性	1
参	HTML 注释敏感信息泄露	33
参	发现电子邮件地址模式	11
参	发现可能的服务器路径泄露模式	7
参	发现内部 IP 泄露模式	1
参	客户端（JavaScript）Cookie 引用	4
参	应用程序错误	2

有漏洞的 URL 69

TOC

	URL	问题的数量
高	http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByXzqhdm2.action	1
高	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getProjectCategoryCountDl.action	4

高	http://127.0.0.1:8090/opus-front-sso/oauth/authorize	5	🟥🟥🟨🟦🟦
高	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do	6	🟥🟥🟥🟧🟨🟦
高	http://127.0.0.1:8000/xmjg/city-page/getCsrk.action	5	🟥🟧🟦🟦🟦
高	http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	6	🟥🟥🟥🟥🟥🟦
高	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do	5	🟥🟥🟥🟧🟨
中	http://127.0.0.1:8000/xmjg/analysis-info!getPilotCity.action	1	🟧
中	http://127.0.0.1:8000/xmjg/bsc/dic/code/lgetItemsByTypeCode.do	2	🟧🟨
中	http://127.0.0.1:8000/xmjg/city-page/getCountyMapData.do	2	🟧🟨
中	http://127.0.0.1:8000/xmjg/city-page/getDataListOfSplcbm.do	2	🟧🟨
中	http://127.0.0.1:8000/xmjg/city-page/getGjdspblqk.do	1	🟧
中	http://127.0.0.1:8000/xmjg/city-page/getJdxms.do	1	🟧
中	http://127.0.0.1:8000/xmjg/city-page/getProjectCount.do	1	🟧
中	http://127.0.0.1:8000/xmjg/city-page/getQqxtCount.do	1	🟧
中	http://127.0.0.1:8000/xmjg/city-page/getSPPJSLCS.do	1	🟧
中	http://127.0.0.1:8000/xmjg/city/getMDAllSpjd.do	2	🟧🟨
中	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	1	🟧
中	http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action	1	🟧
中	http://127.0.0.1:8000/xmjg/opus/front/om/users/currOpusLoginUser	1	🟧
中	http://127.0.0.1:8000/xmjg/opus/front/om/users/user/10000/allMenus	1	🟧
中	http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do	1	🟧
中	http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	5	🟧🟨🟦🟦🟦
中	http://127.0.0.1:8000/xmjg/supervisionInspection/getAllPjysByTjjssj.do	2	🟧🟨
中	http://127.0.0.1:8000/xmjg/supervisionInspection/getJdbjs.do	1	🟧
中	http://127.0.0.1:8000/xmjg/supervisionInspection/getMapCountryAndProvinceXms.do	1	🟧
中	http://127.0.0.1:8000/xmjg/supervisionInspection/getMergeData.do	1	🟧
中	http://127.0.0.1:8000/xmjg/supervisionInspection/getPjysByTjjssj.do	2	🟧🟨
中	http://127.0.0.1:8000/xmjg/supervisionInspection/getProvinceTopFive.do	2	🟧🟨
中	http://127.0.0.1:8000/xmjg/supervisionInspection/getYsTotalOfMultidimensional.do	2	🟧🟨
中	http://127.0.0.1:8000/xmjg/supervisionInspection/getYslAndXzblxms.do	1	🟧
中	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do	1	🟧
中	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getAnalysisCityOverdueRankingData.do	2	🟧🟨
中	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do	1	🟧
中	http://127.0.0.1:8000/xmjg/xmjg-city-map-config!getMapurlByXzqhdm.action	2	🟧🟦
中	http://127.0.0.1:8000/xmjg/xmjg-gzgl-oneform-tabname!getTabName.action	1	🟧
中	http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action	1	🟧
中	http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action	1	🟧

中	http://127.0.0.1:8000/xmjg/xmjg-one-window!getXmjgEditor.action	1
中	http://127.0.0.1:8000/xmjg/xmjg-one-window!getYgck.action	1
中	http://127.0.0.1:8000/xmjg/xmjg-project-info!getMapConfigData.action	1
中	http://127.0.0.1:8000/xmjg/xmjg-project-info/getProvinceAuthority	1
中	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	19
中	http://127.0.0.1:8000/xmjg/xmjg/xmjg-project-info!getScreen.action	2
中	http://127.0.0.1:8090/opus-front-sso/authentication/require	3
低	http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/jquery.cookie.js	3
低	http://127.0.0.1:8090/opus-front-sso/js/jquery.validate.min.js	2
低	http://127.0.0.1:8090/opus-front-sso/js/login.js	1
低	http://127.0.0.1:8090/opus-front-sso/js/md5.js	1
低	http://127.0.0.1:8000/xmjg/analysis-info!getHaveProjectCitys.action	1
参	http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	7
参	http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html	2
参	http://127.0.0.1:8000/xmjg/agcloud/login/js/sm3-sm4-md5-base64-merge.js	1
参	http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-datetimepicker.js	1
参	http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-editable.js	1
参	http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-table-editable.js	1
参	http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-table-zh-CN.js	1
参	http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-table.js	1
参	http://127.0.0.1:8000/xmjg/handsontable-master/dist/handsontable.full.js	1
参	http://127.0.0.1:8000/xmjg/resources/easyui/jquery.easyui.min.js	1
参	http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/vendors.bundle.js	3
参	http://127.0.0.1:8090/opus-front-sso/js/sm4.js	1
参	http://127.0.0.1:8000/xmjg/agcloud/framework/js-lib/element-2/element.js	1
参	http://127.0.0.1:8000/xmjg/agcloud/framework/ui-private/common/element-2/element.js	1
参	http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrapValidator.js	1
参	http://127.0.0.1:8000/xmjg/common/tool/cityselect/js/city_data.js	1
参	http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/element.js	1
参	http://127.0.0.1:8000/xmjg/common/tool/common-core.js	1
参	http://127.0.0.1:8000/xmjg/common/tool/common-merge.js	1

修订建议 16

TOC

修复任务	问题的数量

高	查看危险字符注入的可能解决方案	18
高	禁用基于参数值指向外部站点的重定向	1
中	将您的服务器配置为仅允许所需 HTTP 方法	1
中	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce	42
低	除去 HTML 注释中的敏感信息	33
低	除去 Web 站点中的电子邮件地址	11
低	除去 Web 站点中的内部 IP 地址	1
低	除去 web-server 中的源代码文件并应用任何相关补丁	1
低	除去客户端中的业务逻辑和安全逻辑	4
低	将“autocomplete”属性正确设置为“off”	1
低	将服务器配置为使用安全策略的“Content-Security-Policy”头	5
低	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头	4
低	拒绝恶意请求并防止直接执行 JavaScript 响应	8
低	请勿接受在查询字符串中发送的主体参数	2
低	为 Web 服务器或 Web 应用程序下载相关的安全补丁	7
低	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常	2

安全风险 10

TOC

	风险	问题的数量
高	可能会查看、修改或删除数据库条目和表	6
高	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务	54
高	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息	12
中	可能会升级用户特权并通过 Web 应用程序获取管理许可权	1
中	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置	65
低	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息	1
低	可能会绕开 Web 应用程序的认证机制	1
参	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息	7
参	此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色	4
参	可能会收集敏感的调试信息	2

原因 11

TOC

	原因	问题的数量
高	未对用户输入正确执行危险字符清理	18
高	Web 应用程序执行指向外部站点的重定向	1
中	应用程序使用的认证方法不充分	50
中	Web 应用程序编程或配置不安全	25
低	未安装第三方产品的最新补丁或最新修订程序	1
低	在生产环境中留下临时文件	1
低	程序员在 Web 页面上留下调试信息	34
参	未安装第三方产品的最新补丁或最新修补程序	7
参	Cookie 是在客户端创建的	4
参	未对入局参数值执行适当的边界检查	2
参	未执行验证以确保用户输入与预期的数据类型匹配	2

WASC 威胁分类

TOC

威胁	问题的数量
SQL 注入	6
URL 重定向滥用	1
跨站点脚本编制	12
跨站点请求伪造	42
认证不充分	1
信息泄露	79

按问题类型分类的问题

高 SQL 盲注 4 TOC

问题 1 / 4 TOC

SQL 盲注	
严重性：	高
CVSS 分数：	9.7
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getProjectCategoryCountDl.action
实体：	startDate (Parameter)
风险：	可能会查看、修改或删除数据库条目和表
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `startDate` 从以下位置进行控制： `2020-01-01` 至： `' + '' + '2020-01-01`
参数 `startDate` 从以下位置进行控制： `2020-01-01` 至： `' + ' + '2020-01-01`
参数 `startDate` 从以下位置进行控制： `2020-01-01` 至： `2020-01-01' + ' + '`
参数 `startDate` 从以下位置进行控制： `2020-01-01` 至： `2020-01-01' + '' + '`

推理： 测试结果似乎指示存在漏洞，因为它显示可以在参数值后附加的值，这表明它们嵌入在 SQL 查询中。在该测试中，有 3（有时为 4）个请求已发送。最后一个请求在逻辑上等同于原始请求，而倒数第二个请求则不同。所有其他请求都是为了实现控制目的。最后两个响应与第一个响应的比较（最后一个响应与第一个响应类似，倒数第二个响应则不同）指示应用程序易受攻击。

测试请求和响应：

```
POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412 HTTP/1.1
Content-Length: 53
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US
```

```
xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:08 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "countQ": 0,
 "countR": 0,
 "countO": 0,
 "countP": 0,
 "countS": 0,
 "countT": 0,
 "countA": 0,
 "countB": 0,
 "countE": 0,
 "countF": 0,
 "countC": 0,
 "countD": 0,
 "countI": 0,
 "countJ": 0,
 "countG": 0,
 "countH": 0,
 "countM": 0,
 "countN": 0,
 "countK": 0,
 "countL": 0
}

POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412 HTTP/1.1
Content-Length: 63
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=660100&startDate=' + '' + '2020-01-01&endDate=2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:08 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "countQ": 0,
 "countR": 0,
 "countO": 0,
 "countP": 0,
 "countS": 0,
 "countT": 0,
 "countA": 0,
 "countB": 0,
 "countE": 0,
 "countF": 0,
 "countC": 0,
 "countD": 0,
 "countI": 0,
 "countJ": 0,
 "countG": 0,
 "countH": 0,
 "countM": 0,
 "countN": 0,
 "countK": 0,
 "countL": 0
}

POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412 HTTP/1.1
Content-Length: 62
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=660100&startDate=' + ' + '2020-01-01&endDate=2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:48:11 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "errorCode": "500100",
 "errorMessage": "       服务端异常"
}

POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412 HTTP/1.1
Content-Length: 62
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=660100&startDate=2020-01-01' + ' + '&endDate=2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:48:11 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Enco
...
...
...

Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=660100&startDate=2020-01-01' + '' + '&endDate=2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
...
...
```

```
...
```

问题 2 / 4

TOC

SQL 盲注

严重性：	高
CVSS 分数：	9.7
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getProjectCategoryCountDl.action
实体：	xzqhdm (Parameter)
风险：	可能会查看、修改或删除数据库条目和表
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** xzqhdm 从以下位置进行控制： 660100 至： ' + '' + '660100
参数 xzqhdm 从以下位置进行控制： 660100 至： ' + ' + '660100
参数 xzqhdm 从以下位置进行控制： 660100 至： 660100' + ' + '
参数 xzqhdm 从以下位置进行控制： 660100 至： 660100' + '' + '

推理： 测试结果似乎指示存在漏洞，因为它显示可以在参数值后附加的值，这表明它们嵌入在 SQL 查询中。在该测试中，有 3（有时为 4）个请求已发送。最后一个请求在逻辑上等同于原始请求，而倒数第二个请求则不同。所有其他请求都是为了实现控制目的。最后两个响应与第一个响应的比较（最后一个响应与第一个响应类似，倒数第二个响应则不同）指示应用程序易受攻击。

测试请求和响应：

```
POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412 HTTP/1.1
Content-Length: 53
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:08 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "countQ": 0,
 "countR": 0,
 "countO": 0,
 "countP": 0,
 "countS": 0,
 "countT": 0,
 "countA": 0,
 "countB": 0,
 "countE": 0,
 "countF": 0,
 "countC": 0,
 "countD": 0,
 "countI": 0,
 "countJ": 0,
 "countG": 0,
 "countH": 0,
 "countM": 0,
 "countN": 0,
 "countK": 0,
 "countL": 0
}

POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412 HTTP/1.1
Content-Length: 63
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=' + '' + '660100&startDate=2020-01-01&endDate=2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:08 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "countQ": 0,
 "countR": 0,
 "countO": 0,
 "countP": 0,
 "countS": 0,
 "countT": 0,
 "countA": 0,
 "countB": 0,
 "countE": 0,
 "countF": 0,
 "countC": 0,
 "countD": 0,
 "countI": 0,
 "countJ": 0,
 "countG": 0,
 "countH": 0,
 "countM": 0,
 "countN": 0,
 "countK": 0,
 "countL": 0
}

POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412 HTTP/1.1
Content-Length: 62
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
```

```
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=' + ' + '660100&startDate=2020-01-01&endDate=2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:48:11 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "errorCode": "500100",
 "errorMessage": "       服务端异常"
}

POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412 HTTP/1.1
Content-Length: 62
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=660100' + ' + '&startDate=2020-01-01&endDate=2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:48:11 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Enco
...
...
...

Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=660100' + '' + '&startDate=2020-01-01&endDate=2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
...
...
...
```

问题 3 / 4

TOC

SQL 盲注

严重性：	高
CVSS 分数：	9.7
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getProjectCategoryCountDl.action
实体：	endDate (Parameter)
风险：	可能会查看、修改或删除数据库条目和表
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `endDate` 从以下位置进行控制： `2020-12-29` 至： `' + '' + '2020-12-29`
参数 `endDate` 从以下位置进行控制： `2020-12-29` 至： `' + ' + '2020-12-29`
参数 `endDate` 从以下位置进行控制： `2020-12-29` 至： `2020-12-29' + ' + '`
参数 `endDate` 从以下位置进行控制： `2020-12-29` 至： `2020-12-29' + '' + '`

推理： 测试结果似乎指示存在漏洞，因为它显示可以在参数值后附加的值，这表明它们嵌入在 SQL 查询中。在该测试中，有 3（有时为 4）个请求已发送。最后一个请求在逻辑上等同于原始请求，而倒数第二个请求则不同。所有其他请求都是为了实现控制目的。最后两个响应与第一个响应的比较（最后一个响应与第一个响应类似，倒数第二个响应则不同）指示应用程序易受攻击。

测试请求和响应：

```
POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412 HTTP/1.1
Content-Length: 53
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:08 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "countQ": 0,
 "countR": 0,
 "countO": 0,
 "countP": 0,
 "countS": 0,
 "countT": 0,
 "countA": 0,
 "countB": 0,
 "countE": 0,
 "countF": 0,
 "countC": 0,
 "countD": 0,
 "countI": 0,
 "countJ": 0,
 "countG": 0,
 "countH": 0,
 "countM": 0,
 "countN": 0,
 "countK": 0,
 "countL": 0
}

POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412 HTTP/1.1
Content-Length: 63
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=660100&startDate=2020-01-01&endDate=' + '' + '2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:08 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "countQ": 0,
 "countR": 0,
 "countO": 0,
 "countP": 0,
 "countS": 0,
 "countT": 0,
 "countA": 0,
 "countB": 0,
 "countE": 0,
 "countF": 0,
 "countC": 0,
 "countD": 0,
 "countI": 0,
 "countJ": 0,
 "countG": 0,
 "countH": 0,
 "countM": 0,
 "countN": 0,
 "countK": 0,
 "countL": 0
}

POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412 HTTP/1.1
Content-Length: 62
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=660100&startDate=2020-01-01&endDate=' + ' + '2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:48:11 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
```

```
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "errorCode": "500100",
 "errorMessage": "       服务端异常"
}

POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412 HTTP/1.1
Content-Length: 62
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29' + ' + '

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:48:11 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Enco
...
...
...

Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US

xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29' + '' + '

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
...
...
...
```

问题 4 / 4

TOC

SQL 盲注	
严重性：	高
CVSS 分数：	9.7
URL：	http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByXzqhdm2.action
实体：	xzqhdm (Parameter)
风险：	可能会查看、修改或删除数据库条目和表
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `xzqhdm` 从以下位置进行控制： `660100` 至： `'%20+%20''%20+%20'660100`
参数 `xzqhdm` 从以下位置进行控制： `660100` 至： `'%20+%20'%20+%20'660100`
参数 `xzqhdm` 从以下位置进行控制： `660100` 至： `660100'%20+%20'%20+%20'`
参数 `xzqhdm` 从以下位置进行控制： `660100` 至： `660100'%20+%20''%20+%20'`

推理： 测试结果似乎指示存在漏洞，因为它显示可以在参数值后附加的值，这表明它们嵌入在 SQL 查询中。在该测试中，有 3（有时为 4）个请求已发送。最后一个请求在逻辑上等同于原始请求，而倒数第二个请求则不同。所有其他请求都是为了实现控制目的。最后两个响应与第一个响应的比较（最后一个响应与第一个响应类似，倒数第二个响应则不同）指示应用程序易受攻击。

测试请求和响应：

```
POST /xmjg/xmjg-project-info!getSplcByXzqhdm2.action?xzqhdm=660100 HTTP/1.1
Content-Length: 0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//csrk/oneSystemByMd.do?
city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29&provinceCode=
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:08:32 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "id": null,
         "strId": "68",
         "xzqhdm": "660100",
         "splcbm": "d4ba4952-9be6-4a10-9431-7a099bf5e783",
         "splcmc": "       政府投资房屋建筑类项目",
         "splcbbh": 1.0,
         "splcsxsj": null,
         "splcsm": null,
         "fjmc": null,
         "fjlx": null,
         "fjid": null,
         "sjyxbs": null,
         "sjwxyy": null,
         "splclx": 1,
         "title": null
 },
        {
         "id": null,
         "strId": "69",
         "xzqhdm": "660100",
         "splcbm": "5e6d7d7b-be47-4092-b8d9-c873cd74a8ae",
         "splcmc": "       政府投资城市基础设施工程类...)",
         "splcbbh": 1.0,
         "splcsxsj": null,
         "splcsm": null,
         "fjmc": null,
         "fjlx": null,
         "fjid": null,
         "sjyxbs": null,
         "sjwxyy": null,
         "splclx": 2,
         "title": "       政府投资城市基础设施工程类项目"
 },
        {
         "id": null,
         "strId": "70",
         "xzqhdm": "660100",
         "splcbm": "d21d7468-ca0c-478c-b700-e086340478e0",
         "splcmc": "        一般社会投资项目（不含带方...)",
         "splcbbh": 1.0,
         "splcsxsj": null,
         "splcsm": null,
         "fjmc": null,
         "fjlx": null,
         "fjid": null,
         "sjyxbs": null,
         "sjwxyy": null,
         "splclx": 3,
         "title": "        一般社会投资项目（不含带方案出让用地项目和小型社会投资项目）"
 },
        {
         "id": null,
         "strId": "72",
         "xzqhdm": "660100",
         "splcbm": "0cce535b-bc83-4a61-be72-3d151e1a16e1",
         "splcmc": "        社会投资小型工程项目",
         "splcbbh": 1.0,
         "splcsxsj": null,
         "splcsm": null,
         "fjmc": null,
         "fjlx": null,
         "fjid": null,
         "sjyxbs": null,
         "sjwxyy": null,
         "splclx": 4,
         "title": null
 },
        {
         "id": null,
         "strId": "71",
         "xzqhdm": "660100",
         "splcbm": "92c57c71-4a4a-4768-8888-97efcae9d5c4",
         "splcmc": "        含带方案出让用地的社会投资...)",
         "splcbbh": 1.0,
         "splcsxsj": null,
         "splcsm": null,
         "fjmc": null,
         "fjlx": null,
         "fjid": null,
         "sjyxbs": null,
         "sjwxyy": null,
         "splclx": 5,
         "title": "        含带方案出让用地的社会投资项目"
        }
]

POST /xmjg/xmjg-project-info!getSplcByXzqhdm2.action?xzqhdm='%20+%20''%20+%20'660100 HTTP/1.1
Content-Length: 0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//csrk/oneSystemByMd.do?
city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29&provinceCode=
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:08:32 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "id": null,
         "strId": "68",
         "xzqhdm": "660100",
         "splcbm": "d4ba4952-9be6-4a10-9431-7a099bf5e783",
         "splcmc": "政府投资房屋建筑类项目",
         "splcbbh": 1.0,
         "splcsxsj": null,
         "splcsm": null,
         "fjmc": null,
         "fjlx": null,
         "fjid": null,
         "sjyxbs": null,
         "sjwxyy": null,
         "spl
...
...
...

         "title": "含带方案出让用地的社会投资项目"
        }
]

POST /xmjg/xmjg-project-info!getSplcByXzqhdm2.action?xzqhdm='%20+%20'%20+%20'660100 HTTP/1.1
Content-Length: 0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
...
...
...

 "errorCode": "500100",
 "errorMessage": "服务端异常"
}

POST /xmjg/xmjg-project-info!getSplcByXzqhdm2.action?xzqhdm=660100'%20+%20'%20+%20' HTTP/1.1
Content-Length: 0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
...
...
...

 "errorCode": "500100",
 "errorMessage": "服务端异常"
}

POST /xmjg/xmjg-project-info!getSplcByXzqhdm2.action?xzqhdm=660100'%20+%20''%20+%20' HTTP/1.1
Content-Length: 0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
...
...
...
```

高 SQL 注入 1 TOC

问题 1 / 1 TOC

SQL 注入

严重性：	高
CVSS 分数：	9.7
URL：	http://127.0.0.1:8090/opus-front-sso/oauth/authorize
实体：	client_id (Parameter)
风险：	可能会查看、修改或删除数据库条目和表
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `client_id` 从以下位置进行控制： `xmjg` 至： `xmjg%uFF07`

推理： 测试结果似乎指示存在脆弱性，因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

测试请求和响应：

```
GET /opus-front-
sso/oauth/authorize?client_id=xmjg%uFF07&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_t
ype=code&state=tba1ER HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/form
Cookie: JSESSIONID=24E80C5845F452C87C1B10300BEF316D
Connection: Keep-Alive
Host: 127.0.0.1:8090
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 500
Content-Length: 757
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Connection: close
Date: Tue, 29 Dec 2020 02:55:36 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

<html><body><h1>Whitelabel Error Page</h1><p>This application has no explicit mapping for /error,
so you are seeing this as a fallback.</p><div id='created'>Tue Dec 29 10:55:36 CST 2020</div>
<div>There was an unexpected error (type=Internal Server Error, status=500).</div>
<div>PreparedStatementCallback; bad SQL grammar [select client_id, client_secret from
AGX_RS_CLOUD_SOFT where IS_ACTIVE = &#39;1&#39; AND IS_DELETED = &#39;0&#39; AND client_id = ?AND
IS_ADMIN = &#39;0&#39;]; nested exception is
com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: You have an error in your SQL syntax;
check the manual that corresponds to your MySQL server version for the right syntax to use near
&#39;IS_ADMIN = &#39;0&#39;&#39; at line 1</div></body></html>
```

高 跨站点脚本编制 12

TOC

问题 1 / 12

TOC

### 跨站点脚本编制	
严重性：	高
CVSS 分数：	7.5
URL：	http://127.0.0.1:8000/xmjg/city-page/getCsrk.action
实体：	xzqhdm (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `xzqhdm` 从以下位置进行控制： `660100` 至： `%3D%3Dalert%281660%29%3D%3D1`

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

测试请求和响应：

```
GET /xmjg/city-page/getCsrk.action?
bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=%3D%3Dalert%2
81660%29%3D%3D1&flag=1&startDate=2020-01-01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 04:22:43 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">

 <title>       城市入口</title>
 <script type="text/javascript">
    var ctx= "/xmjg/";
    var xzqhdm="==alert(1660)==1";
    var flag = "1";
    var oldStartDate = "2020-01-01";
    var oldEndDate = "2020-12-29";
    var province="";
    var city="==alert(1660)==1";
    var name="一师阿拉尔市";
    var defaultEndDate="",defaultStartDate="";
    var bigScreenFolder="";
    var provinceCode = "";
    var OrgName = "管理员";
    var districtAdminFlag = "1";
    var initHeartBeat = "";
    //是否是省级用户、管理员用户
 var isAdminUser = "true";
 var isProvinceUser = "false";
    var initStartDate="2018-06-01";//获取配置文件中统计时间的配置参数
 var sfType="";  //       算法类型
</script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

 <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/css/bootstrap.min.css"/>
 <link href="/xmjg/xmjg/supervisionInspection/css/element.css" rel="stylesheet"
type="text/css"/>
 <!--<link rel="stylesheet" type="text/css" th:href="@{/xmjg/csrk/css/xmjg-csrk-main-new-
rem.css}" href="${ctx}/xmjg/csrk/css/xmjg-csrk-main-new-rem.css"/>-->
 <link href="/xmjg/xmjg/xndc/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
 <!--<link rel="stylesheet" type="text/css"
th:href="@{/xmjg/css/{screen}/common_new.css(screen=${session.screen})}"/>-->
 <script src="/xmjg/region/vue.js"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/element.js"></script>
 <script src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" type="text/javascript" charset="utf-
8"></script>
 <!--<script th:src="@{/xmjg/csrk/js/jquery.min.js}"
src="${ctx}/xmjg/csrk/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>-->
 <script src="/xmjg/xmjg/xndc/js/bootstrap.min.js" type="text/javascript" charset="utf-8">
</script>


 <script src="/xmjg/xmjg/xndc/js/bootstrap-datepicker.min.js" type="text/javascript">
</script>
 <script src="/xmjg/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
 <script src="/xmjg/xmjg/csrk/js/echarts.min.js" type="text/javascript" charset="utf-8">
</script>
 <!--
    <script th:src="@{/xmjg/csrk/js/city-csrk-main-new.js}" src="${ctx}/xmjg/csrk/js/city-csrk-
main-new.js" type="text/javascript" charset="utf-8"></script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/city-page.js" type="text/javascript"
charset="utf-8"></script>
```

```
 <!--<script th:src="@{/common/tool/date/js/dateQuery
...
...
...
```

问题 2 / 12

TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do
实体：	stageType (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `stageType` 从以下位置进行控制： `0` 至： `0%0A-alert%28270%29%2F%2F`

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

测试请求和响应：

```
GET /xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?
provinceCode=660000&dataType=8&stageType=0%0A-alert%28270%29%2F%2F&tjkssj=2020-01-01&tjjssj=2020-
12-29&bigScreenFolder=&dateEnd=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 03:00:57 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<html>
 <head>
         <meta charset="utf-8" />
         <title>       各城市各阶段数据</title>
         <script type="text/javascript">
                 var ctx='/xmjg/';
                 var bigScreenFolder="";
                 var tjkssj="2020-01-01";
                 var tjjssj="2020-12-29";
                 var dateEnd = "2020-12-29";
                 var provinceCode="660000";
                 var dataType="8";  //1:       各城市各阶段平均用时（审批用时）; 2:各城市各阶段跨度用时;
3:各城市各阶段最长用时; 4:各城市各阶段平均受理次数;5:本月新增项目数
                 var stageType="0
-alert(270)//"; //0: 总数, 1: 立项用地规划许可; 2: 工程建设许可; 3: 施工许可; 4: 竣工验收
                 var splclx="";
                 var splcmc="";
                 var sfType="";  //       算法类型
         </script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>




                         <link rel="stylesheet" type="text/css"
href="/xmjg/xmjg/supervisionInspection/css/analysis-index-rem.css"/>
                         <link rel="stylesheet" type="text/css"
href="/xmjg/xmjg/supervisionInspection/css/analysis-statistics-rem.css"/>


         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/bootstrap.min.css"/>
         <!--<script  th:src="@{/xmjg/xndc/js/jquery.min.js}"
src="/xmjg/xmjg/xndc/js/jquery.min.js"  type="text/javascript"  charset="utf-8"></script>-->
         <script src="/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js"
type="text/javascript" charset="utf-8"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap.min.js"  type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
         <link href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css"
title="" rel="stylesheet"/>
         <script  src="/xmjg/xmjg/supervisionInspection/js/echarts.min.js"
type="text/javascript"  charset="utf-8"></script>
 <!--        图表柱状图展示操作 -->
```

```
         <script  src="/xmjg/xmjg/xndc/js/common-charts.js" type="text/javascript"
charset="utf-8"></script>
         <!--         城市选择插件  开始 -->
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/cityselect/css/city_select.css"/>
         <script src="/xmjg/common/tool/cityselect/js/city_data.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/cityselect/js/areadata.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/cityselect/js/auto_area.js" type="text/javascript"
charset="utf-8"></script>
         <!--         城市选择插件  结束 -->
         <!--         时间查询控件 开始 -->
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/dateQuery.css"/>
         <script src="/xmjg/common/tool/date/js/dateQuery.js" type="
...
...
...
```

问题 3 / 12

TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do
实体：	name (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `name` 从以下位置进行控制： 至： `%0A-alert%28534%29%2F%2F`

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

测试请求和响应：

```
GET /xmjg/city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=%0A-
alert%28534%29%2F%2F&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-
29&bigScreenFolder=&dateEnd=2020-12-29&splclx= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 03:24:12 GMT
```

```
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN" xmlns="http://www.w3.org/1999/xhtml">
 <head>
         <meta charset="utf-8" />
         <title>       各城市各阶段数据233</title>
         <script type="text/javascript">
          var ctx='/xmjg/';
                 var bigScreenFolder="";
                 var xzqhdms="";
                 var tjkssj="2020-01-01";
                 var tjjssj="2020-12-29";
                 var orderByFlag="";
                 var dataType="8";
                 var sfzb="";
                 var sfbyxz="";
                 var sfjgqqxt="";
                 var spjd="";
                 var blqk="";
                 var splclx="";
                 var splcmc="";
                 var sfyq="";
                 var tjTypeVal="";
                 var qtTypeVal = "";
                 var splcbm="";
                 var dateEnd = "2020-12-29";
                 var provinceCode="";
                 var dataType="8";  //1:       各阶段平均用时（审批用时）; 2:各阶段跨度用时; 3:各阶段最长
用时; 4:各阶段平均受理次数;
                 var stageType="0"; //0       : 总数, 1: 立项用地规划许可; 2: 工程建设许可; 3: 施工许可;
4: 竣工验收
          var oldStartDate = "2020-01-01";
          var oldEndDate = "2020-12-29";
          var flag="1";
          var xzqhdm="660000"; //跳转带过来的行政区划代码 用于钻取标题显示
          var name="
-alert(534)//";//跳转带过来的城市名称 用于钻取标题显示
                 var sfType = "";//       算法类型
         </script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/bootstrap.min.css"/>
         <!--<script  th:src="@{/xmjg/xndc/js/jquery.min.js}"
src="${ctx}/xmjg/xndc/js/jquery.min.js"  type="text/javascript"  charset="utf-8"></script>-->
         <script src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap.min.js"  type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
         <link href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css"
title="" rel="stylesheet"/>
         <link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global-rem.css"
type="text/css"></link>
         <script  src="/xmjg/xmjg/xndc/js/echarts.min.js" type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/resources/js/common/validate.js" type="text/javascript">
</script>
         <script  src="/xmjg/resources/js/common/public.js" type="text/javascript">
</script>
         <!--<script  th:src="@{/xmjg/xndc/js/analysis/analysis-project-stage-list.js}"
src="${ctx}/xmjg/xndc/js/analysis/analysis-project-stage-list.js" type="text/javascript"
charset="utf-8"></script>-->
         <script  src="/xmjg/xmjg/supervisionInspection/js/city-project-stage-list.js"
type="text/javascript"  charset="utf-8"></script>

...
...
...
```

问题 4 / 12

TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do
实体：	xzqhdm (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `xzqhdm` 从以下位置进行控制： `660000` 至： `660000%0A-alert%28529%29%2F%2F`

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

测试请求和响应：

```
GET /xmjg/city-page/getCityProjectList.do?xzqhdm=660000%0A-
alert%28529%29%2F%2F&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-
```

```
29&bigScreenFolder=&dateEnd=2020-12-29&splclx= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 03:24:06 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN" xmlns="http://www.w3.org/1999/xhtml">
 <head>
         <meta charset="utf-8" />
         <title>       各城市各阶段数据233</title>
         <script type="text/javascript">
          var ctx='/xmjg/';
                 var bigScreenFolder="";
                 var xzqhdms="";
                 var tjkssj="2020-01-01";
                 var tjjssj="2020-12-29";
                 var orderByFlag="";
                 var dataType="8";
                 var sfzb="";
                 var sfbyxz="";
                 var sfjgqqxt="";
                 var spjd="";
                 var blqk="";
                 var splclx="";
                 var splcmc="";
                 var sfyq="";
                 var tjTypeVal="";
                 var qtTypeVal = "";
                 var splcbm="";
                 var dateEnd = "2020-12-29";
                 var provinceCode="";
                 var dataType="8";  //1:       各阶段平均用时（审批用时）; 2:各阶段跨度用时; 3:各阶段最长
用时; 4:各阶段平均受理次数;
                 var stageType="0"; //0       ：总数，1：立项用地规划许可；2：工程建设许可；3：施工许可；
4：竣工验收
          var oldStartDate = "2020-01-01";
          var oldEndDate = "2020-12-29";
          var flag="1";
          var xzqhdm="660000
-alert(529)//"; //跳转带过来的行政区划代码 用于钻取标题显示
          var name="";//跳转带过来的城市名称 用于钻取标题显示
                 var sfType = "";//       算法类型
         </script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/bootstrap.min.css"/>
         <!--<script  th:src="@{/xmjg/xndc/js/jquery.min.js}"
src="${ctx}/xmjg/xndc/js/jquery.min.js"  type="text/javascript"  charset="utf-8"></script>-->
         <script src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap.min.js"  type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
         <link href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css"
title="" rel="stylesheet"/>
         <link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global-rem.css"
type="text/css"></link>
         <script  src="/xmjg/xmjg/xndc/js/echarts.min.js" type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/resources/js/common/validate.js" type="text/javascript">
</script>
         <script  src="/xmjg/resources/js/common/public.js" type="text/javascript">
</script>
         <!--<script  th:src="@{/xmjg/xndc/js/analysis/analysis-project-stage-list.js}"
src="${ctx}/xmjg/xndc/js/analysis/analysis-project-stage-list.js" type="text/javascript"
charset="utf-8"></script>-->
         <script  src="/xmjg/xmjg/supervisionInspection/js/city-project-stage-list.js"
type="text/javascript"  charset="utf-8"></script>

...
...
...
```

问题 5 / 12

TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do
实体：	startDate (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `startDate` 从以下位置进行控制： `2020-01-01` 至： `2020-01-01%0Aalert%282599%29%2F%2F`

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

测试请求和响应：

```
GET /xmjg/csrk/oneSystemByMd.do?
city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01%0Aalert%282599%29%2F%2F&endDate=2020-12-29&provinceCode=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:08:47 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <title>一个系统</title>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">

    <script>
        //用于子页面排序的变量
        var orderClickName = "";
        var orderClickCount = 0;
        var orderNameId;

        var ctx = '/xmjg/';
        var oldStartDate = "2020-01-01
alert(2599)//";
        var oldEndDate = "2020-12-29";
        var bigScreenFolder=""; //大屏css 目录，如果是普通屏（默认）则该值为空
        var defaultSelect ="${currentCityName}";
        var dqcs="660100";
        var xzqhdm = "660100";
        var name = decodeURIComponent("%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82");
        var xmlx="";
        var djzt="";//该状态位默认为2，正在办理   ,  -1：代表正在使用及时率、超期率的统计
        var pm_count = ""; //统计排名状态，1： 及时率、2：超期率
        var dqspjd = "";
        var splclxData ;
        var provinceCode = "";
    </script>
    <!--引入样式-->

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/css/bootstrap.min.css"/>
    <link href="/xmjg/xmjg/xndc/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/index-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/jieduan3-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/searchArea-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/global-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/resources/easyui/themes/icon.css"/>
    <link rel="stylesheet" type="text/css"
href="/xmjg/resources/easyui/themes/default/easyui.css"/>
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/dg-xndc-main-rem.css" />
    <script src="/xmjg/xmjg/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>
    <script type="text/javascript" src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" charset="utf-8">
</script>
    <!--<script src="/xmjg/resources/easyui/jquery.min.js" type="text/javascript"></script>-->
    <script src="/xmjg/resources/easyui/jquery.easyui.min.js" type="text/javascript"></script>
    <script src="/xmjg/resources/easyui/locale/easyui-lang-zh_CN.js" type="text/javascript">
</script>
    <script type="text/javascript" src="/xmjg/xmjg/csrk/js/echarts.min.js" charset="utf-8">
</script>
    <script type="text/javascript" src="/xmjg/xmjg/xndc/js/boot
...
...
...
```

问题 6 / 12

TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do
实体：	sfType (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `sfType` 从以下位置进行控制： 至： `%0A-alert%28871%29%2F%2F`

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

测试请求和响应：

```
GET /xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-
01&tjjssj=2020-12-29&dateEnd=2020-12-
29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=210
2&splclx=&sfType=%0A-
alert%28871%29%2F%2F&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=
&pageNo=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//city-page/getCityProjectList.do?
xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-
29&bigScreenFolder=&dateEnd=2020-12-29&splclx=
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 03:44:49 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN" xmlns="http://www.w3.org/1999/xhtml">
 <head>
         <meta charset="utf-8" />
         <title>       各城市各阶段数据233</title>
         <script type="text/javascript">
          var ctx='/xmjg/';
                 var bigScreenFolder="";
                 var xzqhdms="";
                 var tjkssj="2020-01-01";
                 var tjjssj="2020-12-29";
                 var orderByFlag="";
                 var dataType="8";
                 var sfzb="";
                 var sfbyxz="";
                 var sfjgqqxt="";
                 var spjd="";
                 var blqk="";
                 var splclx="";
                 var splcmc="";
                 var sfyq="";
                 var tjTypeVal="";
                 var qtTypeVal = "";
                 var splcbm="";
                 var dateEnd = "2020-12-29";
                 var provinceCode="";
                 var dataType="8";  //1:       各阶段平均用时（审批用时）; 2:各阶段跨度用时; 3:各阶段最长
用时; 4:各阶段平均受理次数;
                 var stageType="0"; //0       : 总数，1：立项用地规划许可；2：工程建设许可；3：施工许可；
4：竣工验收
          var oldStartDate = "2020-01-01";
          var oldEndDate = "2020-12-29";
          var flag="1";
          var xzqhdm="660000"; //跳转带过来的行政区划代码 用于钻取标题显示
          var name="";//跳转带过来的城市名称 用于钻取标题显示
                 var sfType = "
-alert(871)//";//算法类型
         </script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/bootstrap.min.css"/>
         <!--<script  th:src="@{/xmjg/xndc/js/jquery.min.js}"
src="${ctx}/xmjg/xndc/js/jquery.min.js"  type="text/javascript"  charset="utf-8"></script>-->
         <script src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap.min.js"  type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
         <link href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css"
title="" rel="stylesheet"/>
         <link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global-rem.css"
type="text/css"></link>
```

```
          <script  src="/xmjg/xmjg/xndc/js/echarts.min.js" type="text/javascript"
charset="utf-8"></script>
          <script  src="/xmjg/resources/js/common/validate.js" type="text/javascript">
</script>
          <script  src="/xmjg/resources/js/common/public.js" type="text/javascript">
</script>
          <!--<script  th:src="@{/xmjg/xndc/js/anal
...
...
...
```

问题 7 / 12

TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do
实体：	splcmc (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `splcmc` 从以下位置进行控制： 至： `%0A-alert%282255%29%2F%2F`

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

测试请求和响应：

```
GET /xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?
provinceCode=660000&dataType=5&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-
29&bigScreenFolder=&dateEnd=2020-12-29&splcmc=%0A-alert%282255%29%2F%2F&splclx= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:05:40 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<html>
 <head>
```

```
         <meta charset="utf-8" />
         <title>       各城市各阶段数据</title>
         <script type="text/javascript">
                 var ctx='/xmjg/';
                 var bigScreenFolder="";
                 var tjkssj="2020-01-01";
                 var tjjssj="2020-12-29";
                 var dateEnd = "2020-12-29";
                 var provinceCode="660000";
                 var dataType="5";  //1:       各城市各阶段平均用时（审批用时）; 2:各城市各阶段跨度用时;
3:各城市各阶段最长用时; 4:各城市各阶段平均受理次数;5:本月新增项目数
                 var stageType="0"; //0       ：总数，1：立项用地规划许可；2：工程建设许可；3：施工许可；
4：竣工验收
                 var splclx="";
                 var splcmc="
-alert(2255)//";
                 var sfType="";  //       算法类型
         </script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>





                         <link rel="stylesheet" type="text/css"
href="/xmjg/xmjg/supervisionInspection/css/analysis-index-rem.css"/>
                         <link rel="stylesheet" type="text/css"
href="/xmjg/xmjg/supervisionInspection/css/analysis-statistics-rem.css"/>


         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/bootstrap.min.css"/>
         <!--<script  th:src="@{/xmjg/xndc/js/jquery.min.js}"
src="/xmjg/xmjg/xndc/js/jquery.min.js"  type="text/javascript"  charset="utf-8"></script>-->
         <script src="/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js"
type="text/javascript" charset="utf-8"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap.min.js"  type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
```

```
         <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
         <link href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css"
title="" rel="stylesheet"/>
         <script  src="/xmjg/xmjg/supervisionInspection/js/echarts.min.js"
type="text/javascript"  charset="utf-8"></script>
 <!--        图表柱状图展示操作 -->
         <script  src="/xmjg/xmjg/xndc/js/common-charts.js" type="text/javascript"
charset="utf-8"></script>
         <!--        城市选择插件  开始 -->
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/cityselect/css/city_select.css"/>
         <script src="/xmjg/common/tool/cityselect/js/city_data.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/cityselect/js/areadata.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/cityselect/js/auto_area.js" type="text/javascript"
charset="utf-8"></script>
         <!--        城市选择插件  结束 -->
         <!--        时间查询控件 开始 -->
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/dateQuery.css"/>
         <script src="/xmjg/common/tool/date/js/da
...
...
...
```

问题 8 / 12

TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do
实体：	splclx (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** splclx 从以下位置进行控制： 至： %0A-alert%282579%29%2F%2F

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

测试请求和响应：

```
GET /xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?
provinceCode=660000&dataType=5&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-
29&bigScreenFolder=&dateEnd=2020-12-29&splcmc=&splclx=%0A-alert%282579%29%2F%2F HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:07:30 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<html>
 <head>
         <meta charset="utf-8" />
         <title>       各城市各阶段数据</title>
         <script type="text/javascript">
                 var ctx='/xmjg/';
                 var bigScreenFolder="";
                 var tjkssj="2020-01-01";
                 var tjjssj="2020-12-29";
                 var dateEnd = "2020-12-29";
                 var provinceCode="660000";
                 var dataType="5";  //1:       各城市各阶段平均用时（审批用时）; 2:各城市各阶段跨度用时;
3:各城市各阶段最长用时; 4:各城市各阶段平均受理次数;5:本月新增项目数
                 var stageType="0"; //0       ：总数，1：立项用地规划许可；2：工程建设许可；3：施工许可；
4：竣工验收
                 var splclx="
-alert(2579)//";
                 var splcmc="";
                 var sfType="";  //       算法类型
         </script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>
```

```
                         <link rel="stylesheet" type="text/css"
href="/xmjg/xmjg/supervisionInspection/css/analysis-index-rem.css"/>
                         <link rel="stylesheet" type="text/css"
href="/xmjg/xmjg/supervisionInspection/css/analysis-statistics-rem.css"/>


         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/bootstrap.min.css"/>
         <!--<script  th:src="@{/xmjg/xndc/js/jquery.min.js}"
src="/xmjg/xmjg/xndc/js/jquery.min.js"  type="text/javascript"  charset="utf-8"></script>-->
         <script src="/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js"
type="text/javascript" charset="utf-8"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap.min.js"  type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
         <link href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css"
title="" rel="stylesheet"/>
         <script  src="/xmjg/xmjg/supervisionInspection/js/echarts.min.js"
type="text/javascript"  charset="utf-8"></script>
 <!--        图表柱状图展示操作 -->
         <script  src="/xmjg/xmjg/xndc/js/common-charts.js" type="text/javascript"
charset="utf-8"></script>
         <!--        城市选择插件  开始 -->
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/cityselect/css/city_select.css"/>
         <script src="/xmjg/common/tool/cityselect/js/city_data.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/cityselect/js/areadata.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/cityselect/js/auto_area.js" type="text/javascript"
charset="utf-8"></script>
         <!--        城市选择插件  结束 -->
         <!--        时间查询控件 开始 -->
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/dateQuery.css"/>
         <script src="/xmjg/common/tool/date/js/da
...
...
...
```

问题 9 / 12

TOC

跨站点脚本编制	
严重性：	高
CVSS 分数：	7.5
URL：	http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do
实体：	xzqhdm (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `xzqhdm` 从以下位置进行控制： `660100` 至： `660100%0Aalert%282602%29%2F%2F`

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

测试请求和响应：

```
GET /xmjg/csrk/oneSystemByMd.do?
city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100%0Aalert%282602%29%2F%2F&startDate=2020-01-01&endDate=2020-12-29&provinceCode=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:09:23 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <title>一个系统</title>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">

    <script>
        //用于子页面排序的变量
        var orderClickName = "";
        var orderClickCount = 0;
        var orderNameId;

        var ctx = '/xmjg/';
        var oldStartDate = "2020-01-01";
        var oldEndDate = "2020-12-29";
        var bigScreenFolder=""; //大屏css 目录，如果是普通屏（默认）则该值为空
        var defaultSelect ="${currentCityName}";
        var dqcs="660100
alert(2602)//";
        var xzqhdm = "660100
alert(2602)//";
        var name = decodeURIComponent("%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82");
        var xmlx="";
        var djzt="";//该状态位默认为2，正在办理    ,  -1: 代表正在使用及时率、超期率的统计
        var pm_count = ""; //统计排名状态, 1:  及时率、2: 超期率
        var dqspjd = "";
        var splclxData ;
        var provinceCode = "";
    </script>
    <!--引入样式-->

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/css/bootstrap.min.css"/>
    <link href="/xmjg/xmjg/xndc/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/index-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/jieduan3-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/searchArea-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/global-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/resources/easyui/themes/icon.css"/>
    <link rel="stylesheet" type="text/css"
href="/xmjg/resources/easyui/themes/default/easyui.css"/>
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/dg-xndc-main-rem.css" />
    <script src="/xmjg/xmjg/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>
    <script type="text/javascript" src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" charset="utf-8">
</script>
    <!--<script src="/xmjg/resources/easyui/jquery.min.js" type="text/javascript"></script>-->
    <script src="/xmjg/resources/easyui/jquery.easyui.min.js" type="text/javascript"></script>
    <script src="/xmjg/resources/easyui/locale/easyui-lang-zh_CN.js" type="text/javascript">
</script>
    <script type="text/javascript" src="/xmjg/xmjg/csrk/js/echarts.min.js" charset="utf-8">
</script>
    <script type="text/javascript" src="/xmjg/xmj
...
...
...
```

问题 10 / 12

TOC

跨站点脚本编制	
严重性：	高
CVSS 分数：	7.5
URL：	http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do
实体：	provinceCode (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `provinceCode` 从以下位置进行控制： 至： `%0Aalert%282586%29%2F%2F`

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

测试请求和响应：

```
GET /xmjg/csrk/oneSystemByMd.do?
city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29&provinceCode=%0Aalert%282586%29%2F%2F
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:07:43 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <title>一个系统</title>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">

    <script>
        //用于子页面排序的变量
        var orderClickName = "";
        var orderClickCount = 0;
        var orderNameId;

        var ctx = '/xmjg/';
        var oldStartDate = "2020-01-01";
        var oldEndDate = "2020-12-29";
        var bigScreenFolder=""; //大屏css 目录，如果是普通屏（默认）则该值为空
        var defaultSelect ="${currentCityName}";
        var dqcs="660100";
        var xzqhdm = "660100";
        var name = decodeURIComponent("%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82");
        var xmlx="";
        var djzt="";//该状态位默认为2，正在办理   ,  -1: 代表正在使用及时率、超期率的统计
        var pm_count = ""; //统计排名状态, 1:  及时率、2: 超期率
        var dqspjd = "";
        var splclxData ;
        var provinceCode = "
alert(2586)//";
    </script>
    <!--引入样式-->

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/css/bootstrap.min.css"/>
    <link href="/xmjg/xmjg/xndc/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/index-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/jieduan3-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/searchArea-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/global-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/resources/easyui/themes/icon.css"/>
    <link rel="stylesheet" type="text/css"
href="/xmjg/resources/easyui/themes/default/easyui.css"/>
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/dg-xndc-main-rem.css" />
    <script src="/xmjg/xmjg/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>
    <script type="text/javascript" src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" charset="utf-8">
</script>
    <!--<script src="/xmjg/resources/easyui/jquery.min.js" type="text/javascript"></script>-->
    <script src="/xmjg/resources/easyui/jquery.easyui.min.js" type="text/javascript"></script>
    <script src="/xmjg/resources/easyui/locale/easyui-lang-zh_CN.js" type="text/javascript">
</script>
    <script type="text/javascript" src="/xmjg/xmjg/csrk/js/echarts.min.js" charset="utf-8">
</script>
    <script type="text/javascript" src="/xmjg/xmjg/xndc/js/boot
...
...
...
```

问题 11 / 12

TOC

跨站点脚本编制

严重性：	高
CVSS 分数：	7.5
URL：	http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do
实体：	city (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `city` 从以下位置进行控制：

`%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582`

至：

`%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582%0A alert%282582%29%2F%2F`

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

测试请求和响应：

```
GET
/xmjg/csrk/oneSystemByMd.do?city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E
5%25B0%2594%25E5%25B8%2582%0Aalert%282582%29%2F%2F&xzqhdm=660100&startDate=2020-01-
01&endDate=2020-12-29&provinceCode= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:07:42 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <title>一个系统</title>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">

    <script>
        //用于子页面排序的变量
        var orderClickName = "";
        var orderClickCount = 0;
        var orderNameId;

        var ctx = '/xmjg/';
        var oldStartDate = "2020-01-01";
        var oldEndDate = "2020-12-29";
        var bigScreenFolder=""; //大屏css 目录，如果是普通屏（默认）则该值为空
        var defaultSelect ="${currentCityName}";
        var dqcs="660100";
        var xzqhdm = "660100";
        var name = decodeURIComponent("%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82
alert(2582)//");
        var xmlx="";
        var djzt="";//该状态位默认为2，正在办理   ,  -1: 代表正在使用及时率、超期率的统计
        var pm_count = ""; //统计排名状态, 1:  及时率、2: 超期率
        var dqspjd = "";
        var splclxData ;
        var provinceCode = "";
    </script>
    <!--引入样式-->

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/css/bootstrap.min.css"/>
    <link href="/xmjg/xmjg/xndc/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/index-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/jieduan3-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/searchArea-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/global-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/resources/easyui/themes/icon.css"/>
    <link rel="stylesheet" type="text/css"
href="/xmjg/resources/easyui/themes/default/easyui.css"/>
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/dg-xndc-main-rem.css" />
    <script src="/xmjg/xmjg/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>
    <script type="text/javascript" src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" charset="utf-8">
</script>
    <!--<script src="/xmjg/resources/easyui/jquery.min.js" type="text/javascript"></script>-->
    <script src="/xmjg/resources/easyui/jquery.easyui.min.js" type="text/javascript"></script>
    <script src="/xmjg/resources/easyui/locale/easyui-lang-zh_CN.js" type="text/javascript">
</script>
    <script type="text/javascript" src="/xmjg/xmjg/csrk/js/echarts.min.js" charset="utf-8">
</script>
    <script type="text/javascript" src="/xmjg/xmjg/xndc/js/boot
...
...
...
```

问题 12 / 12

跨站点脚本编制	
严重性：	高
CVSS 分数：	7.5
URL：	http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do
实体：	endDate (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `endDate` 从以下位置进行控制： `2020-12-29` 至： `2020-12-29%0Aalert%282587%29%2F%2F`

推理： 测试结果似乎指示存在脆弱性，因为 Appscan 在响应中成功嵌入了脚本，在用户浏览器中装入页面时将执行该脚本。

测试请求和响应：

```
GET /xmjg/csrk/oneSystemByMd.do?
city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29%0Aalert%282587%29%2F%2F&provinceCode=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:07:44 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <title>一个系统</title>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">

    <script>
        //用于子页面排序的变量
        var orderClickName = "";
        var orderClickCount = 0;
        var orderNameId;

        var ctx = '/xmjg/';
        var oldStartDate = "2020-01-01";
        var oldEndDate = "2020-12-29
alert(2587)//";
        var bigScreenFolder=""; //大屏css 目录，如果是普通屏（默认）则该值为空
        var defaultSelect ="${currentCityName}";
        var dqcs="660100";
        var xzqhdm = "660100";
        var name = decodeURIComponent("%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82");
        var xmlx="";
        var djzt="";//该状态位默认为2，正在办理   ,  -1: 代表正在使用及时率、超期率的统计
        var pm_count = ""; //统计排名状态, 1:  及时率、2: 超期率
        var dqspjd = "";
        var splclxData ;
        var provinceCode = "";
    </script>
    <!--引入样式-->

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/css/bootstrap.min.css"/>
    <link href="/xmjg/xmjg/xndc/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/index-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/jieduan3-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/searchArea-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/global-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/resources/easyui/themes/icon.css"/>
    <link rel="stylesheet" type="text/css"
href="/xmjg/resources/easyui/themes/default/easyui.css"/>
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/dg-xndc-main-rem.css" />
    <script src="/xmjg/xmjg/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>
    <script type="text/javascript" src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" charset="utf-8">
</script>
    <!--<script src="/xmjg/resources/easyui/jquery.min.js" type="text/javascript"></script>-->
    <script src="/xmjg/resources/easyui/jquery.easyui.min.js" type="text/javascript"></script>
    <script src="/xmjg/resources/easyui/locale/easyui-lang-zh_CN.js" type="text/javascript">
</script>
    <script type="text/javascript" src="/xmjg/xmjg/csrk/js/echarts.min.js" charset="utf-8">
</script>
    <script type="text/javascript" src="/xmjg/xmjg/xndc/js/boot
...
```

```
...
...
```

高 通过 URL 重定向钓鱼 1 TOC

问题 1 / 1 TOC

通过 URL 重定向钓鱼

严重性：	高
CVSS 分数：	8.5
URL：	http://127.0.0.1:8090/opus-front-sso/oauth/authorize
实体：	redirect_uri (Parameter)
风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序执行指向外部站点的重定向
固定值：	禁用基于参数值指向外部站点的重定向

差异： **参数** `redirect_uri` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg/login` 至： `http://demo.testfire.net`

推理： 测试结果似乎指示存在脆弱性，因为响应包含指向 demo.testfire.net 的重定向，这显示应用程序允许重定向到外部站点，这是网络钓鱼攻击可利用的弱点。

测试请求和响应：

```
GET /opus-front-sso/oauth/authorize?
client_id=xmjg&redirect_uri=http://demo.testfire.net&response_type=code&state=tba1ER HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/form
Cookie: JSESSIONID=24E80C5845F452C87C1B10300BEF316D
Connection: Keep-Alive
Host: 127.0.0.1:8090
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 302
Location: http://demo.testfire.net?code=re30M4&state=tba1ER
X-XSS-Protection: 1; mode=block
Content-Length: 0
X-Content-Type-Options: nosniff
Cache-Control: no-store
Content-Language: en-US
Date: Tue, 29 Dec 2020 02:55:48 GMT
Content-Type: text/html;charset=utf-8
```

中 跨站点请求伪造 42 TOC

问题 1 / 42 TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/analysis-info!getPilotCity.action
实体：	analysis-info!getPilotCity.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Origin` 已从请求除去： `http://127.0.0.1:8000`
标题 `Referer` 从以下位置进行控制：
`http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879`
至： `http://bogus.referer.hcl.com`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
POST /xmjg/analysis-info!getPilotCity.action HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Content-Length: 0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:24 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
    "result": "0",
    "data": [
                   {
                    "XZQHDM": "440100",
                    "NAME": "       广州"
            }       ,
                   {
                    "XZQHDM": "440300",
                    "NAME": "       深圳"
            }       ,
                   {
                    "XZQHDM": "210100",
                    "NAME": "       沈阳"
            }       ,
                   {
                    "XZQHDM": "210200",
                    "NAME": "       大连"
            }       ,
                   {
                    "XZQHDM": "320100",
                    "NAME": "       南京"
            }       ,
                   {
                    "XZQHDM": "330100",
                    "NAME": "       杭州"
            }       ,
                   {
                    "XZQHDM": "330200",
                    "NAME": "       宁波"
            }       ,
                   {
                    "XZQHDM": "330300",
                    "NAME": "       温州"
            }       ,
                   {
                    "XZQHDM": "330400",
                    "NAME": "       嘉兴"
            }       ,
                   {
                    "XZQHDM": "330500",
                    "NAME": "       湖州"
            }       ,
                   {
                    "XZQHDM": "330600",
                    "NAME": "       绍兴"
            }       ,
                   {
                    "XZQHDM": "330700",
                    "NAME": "       金华"
            }       ,
                   {
                    "XZQHDM": "330800",
                    "NAME": "       衢州"
            }       ,
                   {
                    "XZQHDM": "330900",
                    "NAME": "       舟山"
            }       ,
                   {
                    "XZQHDM": "331000",
                    "NAME": "       台州"
            }       ,
                   {
                    "XZQHDM": "331100",
                    "NAME": "       丽水"
            }       ,
                   {
                    "XZQHDM": "350200",
                    "NAME": "       厦门"
            }       ,
                   {
                    "XZQHDM": "420100",
                    "NAME": "       武汉"
            }       ,
                   {
                    "XZQHDM": "510100",
                    "NAME": "       成都"
            }       ,
                    {
                     "XZQHDM": "520100",
                     "NAME": "       贵阳"
            }        ,
                    {
                     "XZQHDM": "610500",
                     "NAME": "       渭南"
            }        ,
                    {
                     "XZQHDM": "610600",
                     "NAME": "       延安"
            }        ,
                    {
                     "XZQHDM": "110000",
                     "NAME": "       北京"
            }        ,
                    {
                     "XZQHDM": "120000",
                     "NAME": "       天津"
            }        ,
                    {
                     "XZQHDM": "310000",
                     "NAME": "       上海"
            }        ,
                    {
                     "XZQHDM": "500000",
                     "NAME": "       重庆"
                    }
           ]
}
```

问题 2 / 42

TOC

跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/city-page/getCsrk.action
实体：	getCsrk.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg/opus/front/blue/index.html`
至： `http://bogus.referer.hcl.com`
标题 `Upgrade-Insecure-Requests` 已从请求除去： `1`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/city-page/getCsrk.action?
bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1
&startDate=2020-01-01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
```

```
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">

 <title>       城市入口</title>
 <script type="text/javascript">
    var ctx= "/xmjg/";
    var xzqhdm="660100";
    var flag = "1";
    var oldStartDate = "2020-01-01";
    var oldEndDate = "2020-12-29";
    var province="";
    var city="660100";
    var name="一师阿拉尔市";
    var defaultEndDate="",defaultStartDate="";
    var bigScreenFolder="";
    var provinceCode = "";
    var OrgName = "管理员";
    var districtAdminFlag = "1";
    var initHeartBeat = "";
    //是否是省级用户、管理员用户
 var isAdminUser = "true";
 var isProvinceUser = "false";
    var initStartDate="2018-06-01";//获取配置文件中统计时间的配置参数
 var sfType="";  //       算法类型
</script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

 <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/css/bootstrap.min.css"/>
 <link href="/xmjg/xmjg/supervisionInspection/css/element.css" rel="stylesheet"
type="text/css"/>
 <!--<link rel="stylesheet" type="text/css" th:href="@{/xmjg/csrk/css/xmjg-csrk-main-new-
rem.css}" href="${ctx}/xmjg/csrk/css/xmjg-csrk-main-new-rem.css"/>-->
 <link href="/xmjg/xmjg/xndc/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
 <!--<link rel="stylesheet" type="text/css"
th:href="@{/xmjg/css/{screen}/common_new.css(screen=${session.screen})}"/>-->
 <script src="/xmjg/region/vue.js"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/element.js"></script>
 <script src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" type="text/javascript" charset="utf-
8"></script>
 <!--<script th:src="@{/xmjg/csrk/js/jquery.min.js}"
src="${ctx}/xmjg/csrk/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>-->
 <script src="/xmjg/xmjg/xndc/js/bootstrap.min.js" type="text/javascript" charset="utf-8">
</script>


 <script src="/xmjg/xmjg/xndc/js/bootstrap-datepicker.min.js" type="text/javascript">
</script>
 <script src="/xmjg/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
 <script src="/xmjg/xmjg/csrk/js/echarts.min.js" type="text/javascript" charset="utf-8">
</script>
 <!--
    <script th:src="@{/xmjg/csrk/js/city-csrk-main-new.js}" src="${ctx}/xmjg/csrk/js/city-csrk-
main-new.js" type="text/javascript" charset="utf-8"></script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/city-page.js" type="text/javascript"
charset="utf-8"></script>
 <!--<script th:src="@{/common/tool/date/js/dateQuery.js}" type="text/javascript"
charset="utf-8"></script>-->
 <!--        城市选择插件  开始 -->
 <link rel="stylesheet" type="text/css" href="/xmjg/common/t
...
...
...
```

问题 3 / 42

TOC

跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8090/opus-front-sso/authentication/require
实体：	require (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：
`http://127.0.0.1:8090/opus-front-sso/authentication/form` 至： `http://bogus.referer.hcl.com`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /opus-front-sso/authentication/require?error=true HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=24E80C5845F452C87C1B10300BEF316D
Connection: Keep-Alive
Host: 127.0.0.1:8090
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 03:50:33 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
 <meta charset="utf-8" />
 <title>       工程建设项目审批管理平台</title>
 <meta name="description" content="Latest updates and statistic charts"/>
 <meta http-equiv="X-UA-Compatible" content="IE=edge"/>
 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/>
 <link rel="shortcut icon"  href="/opus-front-sso/images/guohui.png" type="image/x-icon"/>
 <link rel="icon"  href="/opus-front-sso/images/guohui.png" type="image/x-icon" />
 <link href="/opus-front-sso/css/global.css" rel="stylesheet" type="text/css">
 <link href="/opus-front-sso/css/login_new.css" rel="stylesheet" type="text/css">
 <link href="/opus-front-sso/css/layui.css" rel="stylesheet" type="text/css">
 <script src="/opus-front-sso/js/jquery-3.4.1.min.js"></script>
 <script src="/opus-front-sso/js/jquery.validate.min.js"></script>
 <script src="/opus-front-sso/js/layui.all.js"></script>
 <script>
        var ctx = '/opus-front-sso/';
        var verifyCodeIsOpen = '${verifyCodeIsOpen}';

        //设置高亮(对象,位置)
        function setCaret(textbox,start){
          try{
          if(textbox.createTextRange){
          var r=textbox.createTextRange();
          r.moveStart('character',start);
          r.select();
          }else if(textbox.setSelectionRange){
          textbox.setSelectionRange(0,textbox.value.length);
          textbox.focus();
          }
          }catch(e){}
        }

        function getPic(){

          $('#verifyCodeImg').attr("src", ctx + 'code/image?time1='+ new Date().getTime());
        }

        function checkPwd() {

          var layer ;
          layui.use('layer', function(){
          layer = layui.layer;
          });
          var reg = new RegExp(/^[0-9]+.?[0-9]*$/);//工作密码是否是数字串
          var pwd = $('#password_text').val().trim();
          if  (pwd.length < 8 || reg.test(pwd)){

          layer.msg('密码过于简单，请登录后进行修改！', {time: 2000, icon:6});
          }
        }
 </script>
</head>
<body id="cas">
<div id="main" style="width: 100%;height: 100%;">


<!--系统登录界面-->
<div class="login-logo">
 <div class="ts-logo float-left">
         <img src="/opus-front-sso/images/login_logo.png">
 </div>
</div>
<div class="login-bg"></div>
<div id="login-main">
<form id="login_form" action="/opus-front-sso/authentication/form" method="post">
 <div class="login-content" style="display: none;">
<!--            <div class="m-login__logo">
                 <span class="pro-logo-name">       工程建设项目审批管理平台</span>
         </div> -->
         <div class="login01">
                 <div id="spring_error" style="display: none;">       账号或者密码错误!</div>
                 <div class="login_wel"></div>
                 <ul class="login-input-group">
                         <li       >
                                 <i class="username"></i>
                                 <input id="username_text" class="input" tabindex="1"
onfocus="setCaret(this,0)" placeholder="用户名" accesskey="n" type="text" value="" size="25">
                                 <input id="username" type="hidden" name="username"/>
                         </li>
                         <li       >
                                 <i class="userpassword"></i>
                                 <input id="password_text" class="input" tabindex="2"
onfocus="setCaret(this,0)" accesskey="p" placeholder="密  码" type="password" value="" size="25">
                                 <input id="password" type="hidden" name="password"/>
                                 <input id="proPassword" type="hidden"
name="proPassword"/>
                                 <input id="orgId" type="hidden" name="orgId"/>
                                 <input id="resetPasswordId" type="hidden"
name="resetPasswordId"/>
                                 <input id="deviceType" type="hidden" name="deviceType"
value="pc"/>
                         </li>

                 </ul>
                 <div class="login-btn" style="text-align: center;">

                         <button class="m_login_signin_submit"></button>
                 </div>
         </div>
 </div>
</form>
<form id="editPassword" class="layui-form" action="">
 <div class="layui-form-item" style="margin-top: 30px;">
         <label class="layui-form-label" style="width: 30%">       原密码：</label>
         <div class="layui-input-block" >
                 <input type="password" name="oldPassword" lay-
verify="required|oldPassword"  class="layui-input" style="width: 80%">
         </div>
 </div>
 <div class="layui-form-item">
         <label class="layui-form-label"style="width: 30%" >       新密码：</label>
         <div class="layui-input-block" >
                        <
...
...
...
```

问题 4 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do
实体：	dg-jdkh-main.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg/opus/front/blue/index.html`
至： `http://bogus.referer.hcl.com`
标题 `Upgrade-Insecure-Requests` 已从请求除去： `1`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:03 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
<meta charset="utf-8" />
<title>效能督查</title>
<script type="text/javascript">
    var isWhite = '';
 //pc        版首页
    var ctx='/xmjg/';
    var name = '';
    var xzqhdm= "";
    var loginXzqhdm= "" ? "" : "china";
    var loginProvince = "" ? "" : "china";
   // var oldflag = "";
    var oldflag = "true";
 console.log(oldflag);
    var oldStartDate = "";
    var oldEndDate = "";
    var bigScreenFolder=""; //大屏css 目录，如果是普通屏（默认）则该值为空
    var provinceCode="";
    //var projectManager=parent.projectManager;
    var defaultEndDate="",defaultStartDate="";
    var provinceParam={};
    var params = "";
    var initHeartBeat ="";
    var initStartDate="";//获取配置文件中统计时间的配置参数
</script>
<!--    <th:block th:insert="adsfw/taglibs :: taglibs"/>-->
    <script src="/xmjg/common/tool/common-merge.js" ></script>
    <link href="/xmjg/common/tool/date/css/bootstrap.min.css" rel="stylesheet" type="text/css"/>
 <link href="/xmjg/xmjg/supervisionInspection/css/element.css" rel="stylesheet"
type="text/css"/>
 <!--<link th:href="@{/xmjg/xndc/css/dg-jdkh-main.css}" href="${ctx}/xmjg/xndc/css/dg-
jdkh-main.css" rel="stylesheet" type="text/css"/>-->
 <link href="/xmjg/xmjg/supervisionInspection/css/dg-jdkh-main-rem.css" rel="stylesheet"
type="text/css"/>
 <!--<link rel="stylesheet" href="/framework-
ui/src/main/resources/static/agcloud/framework/ui-private/common/element-2/element.css"
th:href="@{/agcloud/framework/ui-private/common/element-2/element.css}">-->
 <!-- jquery -->
    <!--<script th:src="@{/xmjg/js/jquery.min.js}" type="text/javascript" charset="utf-8">
</script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js"
type="text/javascript" charset="utf-8"></script>
 <script src="/xmjg/common/tool/date/js/bootstrap.min.js" type="text/javascript"
charset="utf-8"></script>
 <link   href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
 <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/numberAnimate.js"
type="text/javascript"></script>
 <!--<script th:src="@{/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js}"
src="${ctx}/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js" type="text/javascript"></script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/dg-jdkh-main.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/echarts.min.js" type="text/javascript"
charset="utf-8"></script>
 <!--<script th:src="@{/common/tool/date/js/dateQuery.js}" type="text/javascript"
charset="utf-8"></script>-->

 <!--        城市选择插件  开始 -->
 <link   href="/xmjg/common/tool/cityselect/css/city_select.css" rel="stylesheet"
type="text/css" />
 <script src="/xmjg/common/tool/cityselect/js/city_data.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/common/tool/cityselect/js/areadata.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/common/tool/cityselect/js/auto_area.js" type="text/javascript"
charset="utf-8"></script>
 <!--        城市选择插件  结束 -->

<script type="text/javascript">
    var date = new Date();
 var dateStr =    date.getFullYear() + "-" + ("0" + (date.getMonth() + 1)).slice(-2) + "-
"+ ("0" + (date.getDate())).slice(-2);
 var startTime = dateStr.substr(0,5)+"01-01";
 var endDateStr = dateStr;
    Date.prototype.format = function(fmt) {
        var o = {
          "M+" : this.getMonth()+1,          //月份
          "d+" : this.getDate(),          //日
          "h+" : this.getHours(),          //小时
          "m+" : this.getMinutes(),          //分
          "s+" : this.getSeconds(),          //秒
          "q+" : Math.floor((this.getMonth()+3)/3), //季度
          "S"  : this.getMilliseconds()          //毫秒
        };
        if(/(y+)/.test(fmt)) {
          fmt=fmt.replace(RegExp.$1, (this.getFullYear()+"").substr(4 - RegExp.$1.length));
        }
        for(var k in o) {
          if(new RegExp("("+ k +")").test(fmt)){
          fmt = fmt.replace(RegExp.$1, (RegExp.$1.length
...
...
...
```

问题 5 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/getProvinceTopFive.do
实体：	getProvinceTopFive.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879
```

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/supervisionInspection/getProvinceTopFive.do?province=660000&startDate=2020-01-
01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:27 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "XZQHDM": "660100",
         "BYXZRKS": 160,
         "NAME": "        一师阿拉尔市"
 },
        {
         "XZQHDM": "660800",
         "BYXZRKS": 92,
         "NAME": "        八师石河子市"
 },
        {
         "XZQHDM": "660300",
         "BYXZRKS": 88,
         "NAME": "       三师图木舒克市"
 },
        {
         "XZQHDM": "661300",
         "BYXZRKS": 83,
         "NAME": "       十三师"
 },
        {
         "XZQHDM": "660400",
         "BYXZRKS": 65,
         "NAME": "       四师可克达拉市"
        }
]
```

问题 6 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/getMapCountryAndProvinceXms.do
实体：	getMapCountryAndProvinceXms.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

`http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879`

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/supervisionInspection/getMapCountryAndProvinceXms.do?
xzqhdm=660000&tjfs=xmsl&cityType=province&startDate=2020-01-01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:35 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
```

```
Transfer-Encoding: chunked

{
 "djProvince": 0,
 "data": [
                {
                 "province": "660000",
                 "city": "660100",
                 "name": "       一师阿拉尔市",
                 "districtType": "city",
                 "fullName": "       一师阿拉尔市",
                 "id": "6601",
                 "value": 160
         }       ,
                {
                 "province": "660000",
                 "city": "660800",
                 "name": "       八师石河子市",
                 "districtType": "city",
                 "fullName": "       八师石河子市",
                 "id": "6608",
                 "value": 92
         }       ,
                {
                 "province": "660000",
                 "city": "660300",
                 "name": "       三师图木舒克市",
                 "districtType": "city",
                 "fullName": "       三师图木舒克市",
                 "id": "6603",
                 "value": 88
         }       ,
                {
                 "province": "660000",
                 "city": "661300",
                 "name": "       十三师",
                 "districtType": "city",
                 "fullName": "       十三师",
                 "id": "6613",
                 "value": 83
         }       ,
                {
                 "province": "660000",
                 "city": "660400",
                 "name": "       四师可克达拉市",
                 "districtType": "city",
                 "fullName": "       四师可克达拉市",
                 "id": "6604",
                 "value": 65
         }       ,
                {
                 "province": "660000",
                 "city": "661200",
                 "name": "       十二师",
                 "districtType": "city",
                 "fullName": "       十二师",
                 "id": "6612",
                 "value": 51
         }       ,
                {
                 "province": "660000",
                 "city": "660700",
                 "name": "       七师胡杨河市",
                 "districtType": "city",
                 "fullName": "       七师胡杨河市",
                 "id": "6607",
                 "value": 49
         }       ,
                {
                 "province": "660000",
                 "city": "660900",
                 "name": "       九师",
                 "districtType": "city",
                 "fullName": "       九师",
                 "id": "6609",
                 "value": 43
         }       ,
                {
                 "province": "660000",
                 "city": "661400",
                 "name": "       十四师昆玉市",
                 "districtType": "city",
                 "fullName": "       十四师昆玉市",
                 "id": "6614",
                 "value": 40
         }       ,
                {
                 "province": "660000",
                 "city": "660500",
                 "name": "       五师双河市",
                 "districtType": "city",
                 "fullName": "       五师双河市",
                 "id": "6605",
                 "value": 38
         }       ,
                {
                 "province": "660000",
                 "city": "661000",
                 "name": "       十师北屯市",
                 "districtType": "city",
                 "fullName": "       十师北屯市",
                 "id": "6610",
                 "value": 37
         }       ,
                {
                 "province": "660000",
                 "city": "660200",
                 "name": "       二师铁门关市",
                 "districtType": "city",
                 "fullName": "       二师铁门关市",
                 "id": "6602",
                 "value": 37
         }       ,
                {
                 "province": "660000",
                 "city": "660600",
                 "name": "       六师五家渠市",
                 "districtType": "city",
                 "fullName": "       六师五家渠市",
                 "id": "6606",
                 "value": 28
                }
 ],
 "djCity": 13,
 "type": "city"
}
```

问题 7 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/getYsTotalOfMultidimensional.do
实体：	getYsTotalOfMultidimensional.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：
`http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879`
至： `http://bogus.referer.hcl.com`
标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/supervisionInspection/getYsTotalOfMultidimensional.do?xzqhdm=660000&startDate=2020-01-
01&endDate=2020-12-29&spysDy0= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 280
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:30 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

[
        {
         "index": 0,
         "spjds": [
                        {
                         "spjd": 1,
                         "pjys": 6,
                         "zcys": 129,
                         "kdys": 32
                 }       ,
                        {
                         "spjd": 2,
                         "pjys": 5,
                         "zcys": 14,
                         "kdys": 20
                 }       ,
                        {
                         "spjd": 3,
                         "pjys": 3,
                         "zcys": 39,
                         "kdys": 23
                 }       ,
                        {
                         "spjd": 4,
                         "pjys": 5,
                         "zcys": 18,
                         "kdys": 12
                 }       ,
                        {
                         "spjd": 5,
                         "pjys": 0,
                         "zcys": 0,
                         "kdys": 0
                        }
         ]       ,
         "bxtj": {
                 "pjys": 0,
                 "zcys": 0,
                 "kdys": 0
         }       ,
         "zpjys": 19,
         "zkdys": 87
```

```
            }
]
```

问题 8 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do
实体：	getSupervisionInspectionDrillData.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Origin` 已从请求除去： `http://127.0.0.1:8000`
标题 `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=8&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29
```

至： `http://bogus.referer.hcl.com`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
POST /xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Content-Length: 104
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

tjkssj=2020-01-01&tjjssj=2020-12-
29&orderByFlag=0&dataType=8&splclx=&splcmc=&provinceCode=660000&sfType=

HTTP/1.1 200
Content-Length: 813
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:03 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

{
 "result": "0",
 "data": [
               {
                 "XZQHDM": "660100",
                 "TOTAL_CNT": 160,
                 "NAME": "       一师阿拉尔市"
         }       ,
                {
                 "XZQHDM": "660800",
                 "TOTAL_CNT": 92,
                 "NAME": "       八师石河子市"
         }       ,
                {
                 "XZQHDM": "660300",
                 "TOTAL_CNT": 88,
                 "NAME": "       三师图木舒克市"
         }       ,
                {
                 "XZQHDM": "661300",
                 "TOTAL_CNT": 83,
                 "NAME": "       十三师"
         }       ,
                {
                 "XZQHDM": "660400",
                 "TOTAL_CNT": 65,
                 "NAME": "       四师可克达拉市"
         }       ,
                {
                 "XZQHDM": "661200",
                 "TOTAL_CNT": 51,
                 "NAME": "       十二师"
         }       ,
                {
                 "XZQHDM": "660700",
                 "TOTAL_CNT": 49,
                 "NAME": "       七师胡杨河市"
         }       ,
                {
                 "XZQHDM": "660900",
                 "TOTAL_CNT": 43,
                 "NAME": "       九师"
         }       ,
                {
                 "XZQHDM": "661400",
                 "TOTAL_CNT": 40,
                 "NAME": "       十四师昆玉市"
         }       ,
                {
                 "XZQHDM": "660500",
                 "TOTAL_CNT": 38,
                 "NAME": "       五师双河市"
         }       ,
                {
                 "XZQHDM": "660200",
                 "TOTAL_CNT": 37,
                 "NAME": "       二师铁门关市"
         }       ,
                {
                 "XZQHDM": "661000",
                 "TOTAL_CNT": 37,
                 "NAME": "       十师北屯市"
         }       ,
                {
                 "XZQHDM": "660600",
                 "TOTAL_CNT": 28,
                 "NAME": "       六师五家渠市"
                }
        ]
}
```

问题 9 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/xmjg-project-info/getProvinceAuthority
实体：	getProvinceAuthority (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Origin` 已从请求除去： `http://127.0.0.1:8000`
标题 `Referer` 从以下位置进行控制：
`http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879`
至： `http://bogus.referer.hcl.com`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
POST /xmjg/xmjg-project-info/getProvinceAuthority HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Content-Length: 0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:36 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "districtCode": "660000",
 "province": "660000",
 "name": "        新疆生产建设兵团",
 "districtType": "province"
}
```

问题 10 / 42 TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/xmjg-project-info!getMapConfigData.action
实体：	xmjg-project-info!getMapConfigData.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

`http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879`

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/xmjg-project-info!getMapConfigData.action?bigScreenFolder= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 88
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:50 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

{
 "configData": [
                {
                 "value": "45%,49%,640,0.7,13,putong",
                 "key": "MAP_CONFIG_DATA_PC_SCREEN"
                }
        ]
}
```

问题 11 / 42 TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/getYslAndXzblxms.do
实体：	getYslAndXzblxms.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879`
至： `http://bogus.referer.hcl.com`
标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/supervisionInspection/getYslAndXzblxms.do?xzqhdm=660000&startDate=2020-01-
01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:39 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "QGYSLXMZS": "811",
 "BYXZXMS": "2102"
}
```

问题 12 / 42 TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/getMergeData.do
实体：	getMergeData.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：
`http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879`
至： `http://bogus.referer.hcl.com`
标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/supervisionInspection/getMergeData.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:42 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "getSPPJSLCS": {
        "JD5SBCS": "2.5",
        "JD4SBCS": "1.6",
        "JD3SBCS": "2.5",
        "JD1SBCS": "1.8",
        "JD2SBCS": "2.4",
        "pjzcs": "2.1"
 },
 "getJdbjs": {
        "JD5YQXMS": 0,
        "JD2YQXMS": 0,
        "JD5XMZS": 464,
        "JD4XMZS": 62,
        "JD2XMZS": 287,
        "JD1YQXMS": 0,
        "JD1XMZS": 947,
        "JD3XMZS": 342,
        "JD4YQXMS": 0,
        "JD3YQXMS": 0
 },
 "getGJDBLQK": {
```

```
            "JD3QTXMS": 22,
            "JD2TJXMS": 10,
            "JD3ZCXMS": 301,
            "JD3TJXMS": 19,
            "JD5QTXMS": 33,
            "JD1ZCXMS": 794,
            "JD2QTXMS": 35,
            "JD1TJXMS": 40,
            "total": 209,
            "JD4TJXMS": 6,
            "JD4ZCXMS": 50,
            "JD4QTXMS": 6,
            "JD2ZCXMS": 242,
            "JD5ZCXMS": 415,
            "JD1QTXMS": 113,
            "JD5TJXMS": 16
    },
    "getCityItemOverTimeSort": {
            "YQLCSMC_2": "       六师五家渠市",
            "YQLYQS_5": "4",
            "YQLCSMC_1": "       三师图木舒克市",
            "YQLYQS_4": "5",
            "YQLCSMC_4": "       五师双河市",
            "YQLCSMC_3": "       二师铁门关市",
            "YQLYQS_1": "23",
            "YQLYQS_3": "5",
            "YQLYQS_2": "7",
            "YQLCSBM_1": "660300",
            "YQLCSBM_2": "660600",
            "YQLCSBM_3": "660200",
            "YQLCSBM_4": "660500",
            "YQLCSBM_5": "660900",
            "YQLBLS_1": "88",
            "YQLBLS_5": "43",
            "YQLBLS_4": "38",
            "YQLCSMC_5": "       九师",
            "YQLBLS_3": "37",
            "YQLBLS_2": "28"
    },
    "getJdzbxms": {
            "JD5XMZS": 53,
            "JD4XMZS": 40,
            "JD2XMZS": 147,
            "JD1XMZS": 365,
            "JD3XMZS": 206
           }
   }
```

问题 13 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action
实体：	excel-export!exportProjectNumber.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg//city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=`
至： `http://bogus.referer.hcl.com`
标题 `Upgrade-Insecure-Requests` 已从请求除去： `1`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
此请求/响应中包含二进制内容，但生成的报告中不包含此内容。
```

问题 14 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do
实体：	getSupervisionInspectionDrillPage.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg/opus/front/blue/index.html`
至： `http://bogus.referer.hcl.com`
标题 `Upgrade-Insecure-Requests` 已从请求除去： `1`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?
provinceCode=660000&dataType=8&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-
29&bigScreenFolder=&dateEnd=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:50 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
```

```
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<html>
 <head>
         <meta charset="utf-8" />
         <title>       各城市各阶段数据</title>
         <script type="text/javascript">
                 var ctx='/xmjg/';
                 var bigScreenFolder="";
                 var tjkssj="2020-01-01";
                 var tjjssj="2020-12-29";
                 var dateEnd = "2020-12-29";
                 var provinceCode="660000";
                 var dataType="8";  //1:       各城市各阶段平均用时（审批用时）; 2:各城市各阶段跨度用时;
3:各城市各阶段最长用时; 4:各城市各阶段平均受理次数;5:本月新增项目数
                 var stageType="0"; //0       : 总数, 1: 立项用地规划许可; 2: 工程建设许可; 3: 施工许可;
4: 竣工验收
                 var splclx="";
                 var splcmc="";
                 var sfType="";  //       算法类型
         </script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>





                         <link rel="stylesheet" type="text/css"
href="/xmjg/xmjg/supervisionInspection/css/analysis-index-rem.css"/>
                         <link rel="stylesheet" type="text/css"
href="/xmjg/xmjg/supervisionInspection/css/analysis-statistics-rem.css"/>


         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/bootstrap.min.css"/>
         <!--<script  th:src="@{/xmjg/xndc/js/jquery.min.js}"
src="/xmjg/xmjg/xndc/js/jquery.min.js"  type="text/javascript"  charset="utf-8"></script>-->
```

```
         <script src="/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js"
type="text/javascript" charset="utf-8"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap.min.js"  type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
         <link href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css"
title="" rel="stylesheet"/>
         <script  src="/xmjg/xmjg/supervisionInspection/js/echarts.min.js"
type="text/javascript"  charset="utf-8"></script>
 <!--        图表柱状图展示操作 -->
         <script  src="/xmjg/xmjg/xndc/js/common-charts.js" type="text/javascript"
charset="utf-8"></script>
         <!--        城市选择插件   开始 -->
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/cityselect/css/city_select.css"/>
         <script src="/xmjg/common/tool/cityselect/js/city_data.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/cityselect/js/areadata.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/cityselect/js/auto_area.js" type="text/javascript"
charset="utf-8"></script>
         <!--        城市选择插件   结束 -->
         <!--        时间查询控件 开始 -->
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/dateQuery.css"/>
         <script src="/xmjg/common/tool/date/js/dateQuery.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8">
</script>
...
...
...
```

问题 15 / 42

TOC

跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	xmjg-statis-show!getSkipPage.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-000000028
79
```

至： `http://bogus.referer.hcl.com`

标题 `Upgrade-Insecure-Requests` 已从请求除去： `1`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
}
.bacckbutton {
    float: right;
    margin: 3px 10px 5px 10px;
    width: 96px;
    height: 32px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
    }
 .dghy-itemWrap {
         float:left;
         margin-left:1%;
         width:19%;
         height:174px;
        }
</style>
<script type="text/javascript">
 var isClickQuery = false; //       是否点击过查询并且没有取消查询

 $(function(){
         //getCountXmfl();
         //getPageData("");
         /       /
...
...
...
```

问题 16 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do
实体：	getCityProjectList.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=
```

至： `http://bogus.referer.hcl.com`

标题 `Upgrade-Insecure-Requests` 已从请求除去： `1`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-
01&tjjssj=2020-12-29&dateEnd=2020-12-
29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=210
2&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pa
geNo=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
```

```
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:26 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN" xmlns="http://www.w3.org/1999/xhtml">
 <head>
         <meta charset="utf-8" />
         <title>       各城市各阶段数据233</title>
         <script type="text/javascript">
          var ctx='/xmjg/';
                 var bigScreenFolder="";
                 var xzqhdms="";
                 var tjkssj="2020-01-01";
                 var tjjssj="2020-12-29";
                 var orderByFlag="";
                 var dataType="8";
                 var sfzb="";
                 var sfbyxz="";
                 var sfjgqqxt="";
                 var spjd="";
                 var blqk="";
                 var splclx="";
                 var splcmc="";
                 var sfyq="";
                 var tjTypeVal="";
                 var qtTypeVal = "";
                 var splcbm="";
                 var dateEnd = "2020-12-29";
                 var provinceCode="";
                 var dataType="8";  //1:       各阶段平均用时（审批用时）; 2:各阶段跨度用时; 3:各阶段最长
用时; 4:各阶段平均受理次数;
                 var stageType="0"; //0       ：总数，1：立项用地规划许可；2：工程建设许可；3：施工许可；
4：竣工验收
          var oldStartDate = "2020-01-01";
          var oldEndDate = "2020-12-29";
          var flag="1";
          var xzqhdm="660000"; //跳转带过来的行政区划代码 用于钻取标题显示
          var name="";//跳转带过来的城市名称 用于钻取标题显示
                 var sfType = "";//       算法类型
         </script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/bootstrap.min.css"/>
         <!--<script  th:src="@{/xmjg/xndc/js/jquery.min.js}"
src="${ctx}/xmjg/xndc/js/jquery.min.js"  type="text/javascript"  charset="utf-8"></script>-->
         <script src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap.min.js"  type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
         <link href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css"
title="" rel="stylesheet"/>
         <link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global-rem.css"
type="text/css"></link>
         <script  src="/xmjg/xmjg/xndc/js/echarts.min.js" type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/resources/js/common/validate.js" type="text/javascript">
</script>
         <script  src="/xmjg/resources/js/common/public.js" type="text/javascript">
</script>
         <!--<script  th:src="@{/xmjg/xndc/js/analysis/analysis-project-stage-list.js}"
src="${ctx}/xmjg/xndc/js/analysis/analysis-project-stage-list.js" type="text/javascript"
charset="utf-8"></script>-->
         <script  src="/xmjg/xmjg/supervisionInspection/js/city-project-stage-list.js"
type="text/javascript"  char
...
...
...
```

问题 17 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getProjectCategoryCountDl.action
实体：	xmjg-statis-show!getProjectCategoryCountDl.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Origin` 已从请求除去： `http://127.0.0.1:8000`
标题 `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29
```

至： `http://bogus.referer.hcl.com`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
POST /xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.6466467024008973 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Content-Length: 53
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:08 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "countQ": 0,
 "countR": 0,
 "countO": 0,
 "countP": 0,
 "countS": 0,
 "countT": 0,
 "countA": 0,
 "countB": 0,
 "countE": 0,
 "countF": 0,
 "countC": 0,
 "countD": 0,
 "countI": 0,
 "countJ": 0,
 "countG": 0,
 "countH": 0,
 "countM": 0,
 "countN": 0,
 "countK": 0,
 "countL": 0
}
```

问题 18 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/city-page/getCountyMapData.do
实体：	getCountyMapData.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

`http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29`

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/city-page/getCountyMapData.do?xzqhdm=660100&tjfs=xmsl&startDate=&endDate= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:30 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "province": "660000",
         "city": "660100",
         "districtType": "area ",
         "name": "        一师阿拉尔市",
         "id": "660100",
         "value": 187
        }
]
```

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/getJdbjs.do
实体：	getJdbjs.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

`http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29`

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/supervisionInspection/getJdbjs.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:39 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "BZJDYQXMS_5": 84,
 "BZJDYQXMS_4": 11,
 "BZJDYQXMS_3": 68,
 "BZJDYQXMS_2": 66,
 "BZJDYQXMS_1": 171
}
```

问题 20 / 42 TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/city-page/getJdxms.do
实体：	getJdxms.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88
%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-1
2-29
```

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/city-page/getJdxms.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:35 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "SPJD_4": 5,
 "SPJD_5": 6,
 "SPJD_1": 59,
 "SPJD_2": 37,
 "SPJD_3": 53
}
```

问题 21 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/city-page/getProjectCount.do
实体：	getProjectCount.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

`http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29`

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/city-page/getProjectCount.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:40 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "XZBJL": "400",
 "YSLXMS": "160"
}
```

问题 22 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/city-page/getGjdspblqk.do
实体：	getGjdspblqk.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

`http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29`

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/city-page/getGjdspblqk.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:45 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "JD3QTXMS": 7,
 "JD2TJXMS": 0,
 "JD3ZCXMS": 59,
 "JD3TJXMS": 2,
 "JD5QTXMS": 5,
 "JD1ZCXMS": 159,
 "JD2QTXMS": 2,
 "JD1TJXMS": 0,
 "total": 27,
 "JD4TJXMS": 0,
 "JD4ZCXMS": 10,
 "JD4QTXMS": 1,
 "JD2ZCXMS": 64,
 "JD5ZCXMS": 78,
 "JD1QTXMS": 12,
 "JD5TJXMS": 1
}
```

问题 23 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/bsc/dic/code/lgetItemsByTypeCode.do
实体：	lgetItemsByTypeCode.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88
%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-1
2-29
```

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/bsc/dic/code/lgetItemsByTypeCode.do?typeCode=TJ_DATE_CONFIG&flag=false HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:34 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "label": "2020       年1月1日-至今",
         "value": "nowYearStart&nowDate",
         "children": null,
         "id": "bf687bbc-f054-461c-b9f5-12d92491c3f7"
 },
        {
         "label": "2018       年6月1日-至今",
         "value": "initStartDate&nowDate",
         "children": null,
         "id": "04c3a943-937d-465d-b9bf-86ee458903c5"
 },
        {
         "label": "2018       年6月1日-2019年12月31日",
         "value": "initStartDate&2019-12-31",
         "children": null,
         "id": "20fdc7d0-a21e-4d64-b77f-be6681b68652"
        }
]
```

问题 24 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/city-page/getSPPJSLCS.do
实体：	getSPPJSLCS.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29
```

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/city-page/getSPPJSLCS.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:41 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "JD5SBCS": "2.6",
 "JD4SBCS": "1.8",
 "JD3SBCS": "2.9",
 "JD1SBCS": "2.2",
 "JD2SBCS": "2",
 "pjzcs": "2.3"
}
```

问题 25 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/city-page/getQqxtCount.do
实体：	getQqxtCount.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88
%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-1
2-29
```

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/city-page/getQqxtCount.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:36 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "XZBJL": "23",
 "YSLXMS": "7"
}
```

问题 26 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/getAllPjysByTjjssj.do
实体：	getAllPjysByTjjssj.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29
```

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/supervisionInspection/getAllPjysByTjjssj.do?xzqhdm=660100&startDate=2020-01-
01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 276
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:41 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

[
        {
         "index": 0,
         "spjds": [
                        {
                         "spjd": 1,
                         "pjys": 7,
                         "zcys": 23,
                         "kdys": 42
                 }       ,
                        {
                         "spjd": 2,
                         "pjys": 6,
                         "zcys": 9,
                         "kdys": 18
                 }       ,
                        {
                         "spjd": 3,
                         "pjys": 2,
                         "zcys": 5,
                         "kdys": 18
                 }       ,
                        {
                         "spjd": 4,
                         "pjys": 2,
                         "zcys": 2,
                         "kdys": 10
                 }       ,
                        {
                         "spjd": 5,
                         "pjys": 5,
                         "zcys": 8,
                         "kdys": 7
                        }
         ]       ,
         "bxtj": {
                 "pjys": 5,
                 "zcys": 8,
                 "kdys": 7
         }       ,
         "zpjys": 22,
         "zkdys": 95
        }
]
```

问题 27 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/city-page/getDataListOfSplcbm.do
实体：	getDataListOfSplcbm.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29
```

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/city-page/getDataListOfSplcbm.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:44 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "PJZYS": 8,
         "SPLCBM": "5e6d7d7b-be47-4092-b8d9-c873cd74a8ae",
         "SPLCMC": "       政府投资城市基础设施工程类项目",
         "YRUXMS": 58,
         "YQXMS": 2
 },
        {
         "PJZYS": 7,
         "SPLCBM": "d4ba4952-9be6-4a10-9431-7a099bf5e783",
         "SPLCMC": "       政府投资房屋建筑类项目",
         "YRUXMS": 34,
         "YQXMS": 1
 },
        {
         "PJZYS": 4,
         "SPLCBM": "d21d7468-ca0c-478c-b700-e086340478e0",
         "SPLCMC": "       一般社会投资项目（不含带方案出让用地项目和小型社会投资项目）",
         "YRUXMS": 61,
         "YQXMS": 1
 },
        {
         "PJZYS": 10,
         "SPLCBM": "0cce535b-bc83-4a61-be72-3d151e1a16e1",
         "SPLCMC": "       社会投资小型工程项目",
         "YRUXMS": 6,
         "YQXMS": 0
 },
        {
         "PJZYS": 2,
         "SPLCBM": "92c57c71-4a4a-4768-8888-97efcae9d5c4",
         "SPLCMC": "       含带方案出让用地的社会投资项目",
         "YRUXMS": 1,
         "YQXMS": 0
        }
]
```

问题 28 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/city/getMDAllSpjd.do
实体：	getMDAllSpjd.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

`http://127.0.0.1:8000/xmjg//csrk/oneSystemByMd.do?city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29&provinceCode=`

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/city/getMDAllSpjd.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-31 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:49:53 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "xmFlag": "YES",
         "spjdXmzs": [
                        {
                         "smzqCount": 4,
                         "SPJD": null,
                         "ybSmzqCount": 19,
                         "ybApprovalCount": 0,
                         "approvalCount": 0
                 }       ,
                        {
                         "smzqCount": 10,
                         "SPJD": 1,
                         "ybSmzqCount": 50,
                         "ybApprovalCount": 0,
                         "approvalCount": 1
                 }       ,
                        {
                         "smzqCount": 7,
                         "SPJD": 2,
                         "ybSmzqCount": 43,
                         "ybApprovalCount": 1,
                         "approvalCount": 0
                 }        ,
                        {
                         "smzqCount": 5,
                         "SPJD": 3,
                         "ybSmzqCount": 38,
                         "ybApprovalCount": 1,
                         "approvalCount": 0
                 }        ,
                        {
                         "smzqCount": 1,
                         "SPJD": 4,
                         "ybSmzqCount": 1,
                         "ybApprovalCount": 0,
                         "approvalCount": 1
                        }
         ]       ,
         "pjysFlag": "YES",
         "bzpjys": [
                        {
                         "BZJDZCYS_4": 2,
                         "BZJDZCYS_2": 9,
                         "BZJDZCYS_3": 5,
                         "BZJDPJYS_2": 2,
                         "BZJDPJYS_1": 3,
                         "BZJDPJYS_4": 1,
                         "BZJDPJYS_3": 1,
                         "BZJDZCYS_1": 23
                        }
                ]
        }
]
```

问题 29 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action
实体：	xmjg-gzgl-upload!getFileName.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Origin` 已从请求除去： `http://127.0.0.1:8000`
标题 `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//xmjg-one-form!getYzbd.action?name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
```

至： `http://bogus.referer.hcl.com`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
POST /xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=d4ba4952-9be6-4a10-9431-
7a099bf5e783&spjdbh=1&bgbh=1&splcbbh=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Content-Length: 0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:51:09 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "fileDescription": null,
         "fileName": "       一阶段办事指南.pdf",
         "filePath": "/yzbd/yishialaer/pdf/7fa992eb-5923-419b-9cbc-612db98522ba       ※一阶段办事
指南.pdf",
         "id": "40392",
         "uploadTime": 1605588826000,
         "fileId": 55889
        }
]
```

问题 30 / 42

TOC

### 跨站点请求伪造	
严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do
实体：	getTotalByMdList.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证"Referer"头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Origin` 已从请求除去： `http://127.0.0.1:8000`
标题 `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//csrk/oneSystemByMd.do?city=%25E4%25B8%2580%25E5%25B8%2588%25E9%25
98%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDa
te=2020-12-29&provinceCode=
```

至： `http://bogus.referer.hcl.com`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
POST /xmjg/city/getTotalByMdList.do HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Content-Length: 1951
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US
Content-Type: application/json;charset=UTF-8

{
 "totals": [
                {
                 "id": null,
                 "strId": "68",
                 "xzqhdm": "660100",
                 "splcbm": "d4ba4952-9be6-4a10-9431-7a099bf5e783",
                 "splcmc":
"\u653f\u5e9c\u6295\u8d44\u623f\u5c4b\u5efa\u7b51\u7c7b\u9879\u76ee",
                 "splcbbh": 1,
                 "splcsxsj": null,
                 "splcsm": null,
                 "fjmc": null,
                 "fjlx": null,
                 "fjid": null,
                 "sjyxbs": null,
                 "sjwxyy": null,
                 "splclx": 1,
                 "title": null
         }       ,
                {
                 "id": null,
                 "strId": "69",
                 "xzqhdm": "660100",
                 "splcbm": "5e6d7d7b-be47-4092-b8d9-c873cd74a8ae",
                 "splcmc":
"\u653f\u5e9c\u6295\u8d44\u57ce\u5e02\u57fa\u7840\u8bbe\u65bd\u5de5\u7a0b\u7c7b...)",
                 "splcbbh": 1,
                 "splcsxsj": null,
                 "splcsm": null,
                 "fjmc": null,
                 "fjlx": null,
                 "fjid": null,
                 "sjyxbs": null,
                 "sjwxyy": null,
                 "splclx": 2,
                 "title":
"\u653f\u5e9c\u6295\u8d44\u57ce\u5e02\u57fa\u7840\u8bbe\u65bd\u5de5\u7a0b\u7c7b\u9879\u76ee"
         }       ,
                {
                 "id": null,
                 "strId": "70",
                 "xzqhdm": "660100",
                 "splcbm": "d21d7468-ca0c-478c-b700-e086340478e0",
                 "splcmc":
"\u4e00\u822c\u793e\u4f1a\u6295\u8d44\u9879\u76ee\uff08\u4e0d\u542b\u5e26\u65b9...)",
                 "splcbbh": 1,
                 "splcsxsj": null,
                 "splcsm": null,
                 "fjmc": null,
                 "fjlx": null,
                 "fjid": null,
                 "sjyxbs": null,
                 "sjwxyy": null,
                 "splclx": 3,
                 "title":
"\u4e00\u822c\u793e\u4f1a\u6295\u8d44\u9879\u76ee\uff08\u4e0d\u542b\u5e26\u65b9\u6848\u51fa\u8ba9
\u7528\u5730\u9879\u76ee\u548c\u5c0f\u578b\u793e\u4f1a\u6295\u8d44\u9879\u76ee\uff09"
         }       ,
                {
                 "id": null,
                 "strId": "72",
                 "xzqhdm": "660100",
                 "splcbm": "0cce535b-bc83-4a61-be72-3d151e1a16e1",
                 "splcmc": "\u793e\u4f1a\u6295\u8d44\u5c0f\u578b\u5de5\u7a0b\u9879\u76ee",
                 "splcbbh": 1,
                 "splcsxsj": null,
                 "splcsm": null,
                 "fjmc": null,
                 "fjlx": null,
                 "fjid": null,
                 "sjyxbs": null,
                 "sjwxyy": null,
                 "splclx": 4,
                 "title": null
         }       ,
                {
                 "id": null,
                 "strId": "71",
                 "xzqhdm": "660100",
                 "splcbm": "92c57c71-4a4a-4768-8888-97efcae9d5c4",
                 "splcmc":
"\u542b\u5e26\u65b9\u6848\u51fa\u8ba9\u7528\u5730\u7684\u793e\u4f1a\u6295\u8d44...)",
                 "splcbbh": 1,
                 "splcsxsj": null,
                 "splcsm": null,
                 "fjmc": null,
                 "fjlx": null,
                 "fjid": null,
                 "sjyxbs": null,
                 "sjwxyy": null,
                 "splclx": 5,
                 "title":
"\u542b\u5e26\u65b9\u6848\u51fa\u8ba9\u7528\u5730\u7684\u793e\u4f1a\u6295\u8d44\u9879\u76ee"
                }
 ],
 "startDate": "2020-01-01",
 "endDate": "2020-12-31"
}

HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:48:09 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "daoqi": null,
         "cuiban": null,
         "guaqi": null,
         "registerTotal": null,
         "acceptTotal": null,
         "fahsCount": null,
         "qbCount": 209,
         "zbCount": 150,
         "ybCount": 0,
         "yqCount": 4,
         "cswbCount": 4,
         "csybCount": 2,
         "xmlxAll": 34,
         "xmlx1": null,
         "xmlx2": null,
         "xmlx3": null,
         "xmlx4": null,
         "xmlx5": null,
         "xmlx6": null,
         "xmlx7": null,
         "xmlx8": null,
         "xmlx9": null,
         "xmlx10": null,
         "xmlx11": null,
         "xmlx12": null,
         "xmlx13": null,
         "xmlx14": null,
         "xmlx15": null,
         "smzq1": null,
         "smzq2": null,
         "smzq3": null,
         "smzq4": null,
         "approval1": null,
         "approval2": null,
         "approval3": null,
         "approval4": null,
         "zbxm": null,
         "bjxm": null,
         "zbyqxm": null,
         "bjyqxm": null,
         "zbQbxmCount": null,
         "zbzcCount": null,
         "zbYqCount": null,
         "bjQbxmCount": null,
         "bjAqCount": null,
         "bjTqCount": null,
         "bjYqCount": null,
         "bjTjCount": null,
         "bjTjCountbak": null,
         "zbwarningCount": null,
         "tjCount": 26,
         "byblsCount": null
 },
        {
         "daoqi": null,
         "cuiban": null,
         "guaqi": null,
         "registerTotal": null,
         "acceptTotal": null,
         "fahsCount": null,
         "qbCount": 209,
         "zbCount": 150,
         "ybCount": 0,
         "yqCount": 4,
         "cswbCount": 4,
         "csybCount": 2,
         "xmlxAll": 58,
         "xmlx1": null,
         "xmlx2": null,
         "xmlx3": null,
         "xmlx4": null,
         "xmlx5": null,
         "xmlx6": null,
         "xmlx7": null,
         "xmlx8": null,
         "xmlx9": null,
         "xmlx10": null,
         "xmlx11": null,
         "xmlx12": null,
         "xmlx13": null,
         "xmlx14": null,
         "xmlx15": null,
         "smzq1": null,
         "smzq2": null,
         "smzq3": null,
         "smzq4": null,
         "approval1": null,
         "approval2": null,
         "approval3": null,
         "approval4": null,
         "zbxm": null,
         "bjxm": null,
         "zbyqxm": null,
         "bjyq
...
...
...
```

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action
实体：	xmjg-one-form!getYzbd.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg/opus/front/blue/index.html` 至： `http://bogus.referer.hcl.com`
标题 `Upgrade-Insecure-Requests` 已从请求除去： `1`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/xmjg-one-form!getYzbd.action?
name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:50:24 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
<title>一张表单</title>
<script type="text/javascript">
    var ctx= "/xmjg/";
 var xzqhdm='660100';
 var name=decodeURIComponent('%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82');
 //var basePath = "<%=basePath%>";//       使用本系统的rest服务
    var basePath = "hello";//使用本系统的rest服务
    var bigScreenFolder="";
    var spjdbh = '';
    var switchBgbh = '';
</script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->
```

```
<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>


<script type="text/javascript" src="/xmjg/bootstrap/js/jquery.min.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/bootstrap.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/bootstrap-common.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/bootstrap-datetimepicker.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/bootstrapValidator.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/bootstrap-table.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/bootstrap-table-zh-CN.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/toastr.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/bootstrap-editable.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/bootstrap-table-editable.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/bootstrap-treeview.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/bootstrap-combotree.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/bootstrap-select.js"></script>
<script type="text/javascript" src="/xmjg/bootstrap/js/jquery.eeyellow.Timeline.js"></script>
<link type="text/css" rel="stylesheet" href="/xmjg/bootstrap/css/bootstrap.css" />
<link type="text/css" rel="stylesheet" href="/xmjg/bootstrap/css/bootstrap.min.css" />
<link type="text/css" rel="stylesheet" href="/xmjg/bootstrap/css/bootstrap-datetimepicker.css" />
<link type="text/css" rel="stylesheet" href="/xmjg/bootstrap/css/bootstrap-
datetimepicker.min.css" />
<link type="text/css" rel="stylesheet" href="/xmjg/bootstrap/css/bootstrapValidator.css" />
<link type="text/css" rel="stylesheet" href="/xmjg/bootstrap/css/bootstrap-table.css" />
<link type="text/css" rel="stylesheet" href="/xmjg/bootstrap/css/toastr.css" />
<link type="text/css" rel="stylesheet" href="/xmjg/bootstrap/css/bootstrap-editable.css" />
<link type="text/css" rel="stylesheet" href="/xmjg/bootstrap/css/bootstrap-treeview.css" />
<link type="text/css" rel="stylesheet" href="/xmjg/bootstrap/css/bootstrap-select.css" />
<link type="text/css" rel="stylesheet" href="/xmjg/bootstrap/css/jquery.eeyellow.T
...
...
...
```

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/xmjg-city-map-config!getMapurlByXzqhdm.action
实体：	xmjg-city-map-config!getMapurlByXzqhdm.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88
%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-1
2-29
```

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/xmjg-city-map-config!getMapurlByXzqhdm.action?
xzqhdm=660100&accessEntry=%E5%9F%8E%E5%B8%82%E9%A6%96%E9%A1%B5 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: text/plain, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 66
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:49:53 GMT
Content-Type: text/plain;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

http://10.4.4.16:8886/agcom/2dMap/interfaceMap.html?userName=admin
```

问题 33 / 42　　TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/xmjg-one-window!getXmjgEditor.action
实体：	xmjg-one-window!getXmjgEditor.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Origin` 已从请求除去： `http://127.0.0.1:8000`
标题 `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//xmjg-one-window!getYgck.action?name=%25E4%25B8%2580%25E5%25B8%258
8%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01
-01&endDate=2020-12-29
```

至： `http://bogus.referer.hcl.com`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
POST /xmjg/xmjg-one-window!getXmjgEditor.action?xzqhdm=660100 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Content-Length: 0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:50:24 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "id": 342,
 "xzqhdm": "660100",
 "xzqhmc": "        一师阿拉尔",
 "content": "<p>                  第一师阿拉尔市按照兵团统一要求，在行政服务中心设置工程建设项目审批制度改革综合
服务窗口，按照“一窗受理”工作机制，按照四个阶段模式，共设置4个工位，其中发改委派驻1人、自然资源和规划局派驻1人、住建
局派驻2人，实现“一窗受理、后台审核、一窗出件”。同时，涉及工程建设项目审批环节的水利局、环保局、应急管理局、城市管理
局等部门，均在行政中心设置服务窗口，建立部门协调、信息共享机制。<img src=\"/xmjg/file/660100/img/bee55036-
81c0-4ee5-a8e9-0b76239a6639-3ce5c3a061ba4854cd098609805323c.jpg\" style=\"max-width: 100%;\"><br>
</p>",
 "images": null,
 "insertdata": 1605801600000,
 "spare1": null,
 "spare2": null
}
```

问题 34 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/xmjg-one-window!getYgck.action
实体：	xmjg-one-window!getYgck.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg/opus/front/blue/index.html`
至： `http://bogus.referer.hcl.com`
标题 `Upgrade-Insecure-Requests` 已从请求除去： `1`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/xmjg-one-window!getYgck.action?
name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:50:21 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport"
           content="width=device-width,initial-scale=1.0">
 <title>       一个窗口</title>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
```

```
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

 <script type="text/javascript">
    var ctx = '/xmjg/';
    var xzqhdm="660100";
    var bigScreenFolder = "";
</script>
 <script src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" type="text/javascript" charset="utf-
8"></script>
 <script type="text/javascript"
                src="/xmjg/resources/easyui/easycore.js"></script>
 <script type="text/javascript"
                src="/xmjg/resources/js/dghy/index.js"></script>
 <script type="text/javascript"
                src="/xmjg/dghyindex/js/dghy-public.js"></script>
 <script type="text/javascript" src="/xmjg/xmjg/xndc/js/DateUtils.js"></script>
 <script
type="text/javascript"src="/xmjg/dghyindex/echarts/build/dist/echarts.min3.8.5.js"></script>
 <script src="/xmjg/xmjg/ygck/js/ygck.js" type="text/javascript" charset="utf-8"></script>
 <link rel="stylesheet" type="text/css"  href="/xmjg/xmjg/ygck/css/common.css" />
 <link rel="stylesheet" type="text/css"  href="/xmjg/xmjg/ygck/css/common-rem.css" />
 <style>
         #back_id {
                position: absolute;
                right: 20px;
                /*left:3265px;*/
                top: 16px;
                width: 96px;
                height: 32px;
                border: 0;
                border-radius: 10px;
                background: #336bbd;
                color: #fff;
                line-height: 32px;
                font-size: 18px;
                text-align: center;
               }


         #box::-webkit-scrollbar {
                display: none;
               }
 </style>
 <link rel="stylesheet" type="text/css"  href="/xmjg/xmjg/css//common_new_rem.css"/>
</head>
<script type="text/javascript">
$(function () {
    var name='%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82';
    $("#cityName").text(decodeURIComponent(name));
 var height = $(document.body).height()-45;
 $(".article-con").css("height",height+'px');
 getXmjgEditor();
 $("#back_id").click(function () {
        commonWindow.returnParentWindow();
    });
 if(bigScreenFolder == 'bigscreenTwo/'){
        $("#titie_div_id").hide();
        $(".article-tit span").show();
        $("#back_id").css({width: '100px',height:'40px','line-height':'40px','font-size':'25px'})
        }
});
function getXmjgEditor(){
 $.ajax({
         type: "POST",
         url: ctx+ '/xmjg-one-window!getXmjgEditor.action?xzqhdm='+xzqhdm,
         dataType: "json",
         success: function (result) {
                 $("#content").html(result.content);
                }
 });
}
</script>
<body style="overflow-x: hidden;overflow-y: hidden;">

  <body>
  <div id="main_div_id" style="width: 99%; margin: 0 10px;">
    <p id = "titie_div_id"style="font-size
...
...
...
```

问题 35 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/xmjg/xmjg-project-info!getScreen.action
实体：	xmjg-project-info!getScreen.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Origin` 已从请求除去： `http://127.0.0.1:8000`
标题 `Referer` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg/opus/front/blue/index.html`
至： `http://bogus.referer.hcl.com`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
POST /xmjg/xmjg/xmjg-project-info!getScreen.action HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Content-Length: 0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 1
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:54:05 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

0
```

问题 36 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do
实体：	qbMdxmList.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

`http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-31`

至： `http://bogus.referer.hcl.com`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/projectInfo/qbMdxmList.do?
name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&currentCityName=&xzqhdm=660100&splclx
=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-
01&endDate=2020-12-
31&orderByName=orderByZBDESC&page.orderBy=%24%7Bpage.orderBy%7D&page.orderDir=%24%7Bpage.orderDir
%7D&pageNum=25 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: Keep-Alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:50:23 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <title>一个系统</title>

    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <!--引入样式-->

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/index-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/global-rem.css" />

    <!--<script th:src="@{/xmjg/js/jquery.min.js}" type="text/javascript" charset="utf-8">
</script>-->
    <script type="text/javascript" src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" charset="utf-8">
</script>
    <script type="text/javascript" src="/xmjg/resources/js/common/public.js" ></script>
    <script type="text/javascript" src="/xmjg/resources/js/common/validate.js" ></script>
    <script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
    <style type="text/css">
        .search_box{
          padding:.15rem 0;
        }
        .search_box a{
          cursor:pointer;
          text-decoration:none;
        }
        .search_box input.text{
          width:2.20rem;
          height:.33rem;
          line-height:.33rem;
          border:1px solid #d4e2f3;
          text-indent:.05rem;
          font-family: Arial,'Microsoft YaHei';
          color:#999;
          font-size:.14rem;
        }
       /* .table tr td, .table tr th{
          font-size: .18rem;
          height:.43rem;
          color: #474747;
          padding: 0 .10rem;
        }*/
        .order-img:hover{
          background-color: rgb(51, 107, 189);
        }
    </style>
    <link rel="stylesheet" type="text/css"  href="/xmjg/xmjg/css//common_new_rem.css"/>
    <script>
        var ctx = '/xmjg/';

        var zb_order = 0; //在办数排序（默认值（0）; 0: 升序; 1: 降序）
        var bj_order = 0; //办结数排序（默认值（0）; 0: 升序; 1: 降序）
        var yj_order = 0; //逾期数排序（默认值（0）; 0: 升序; 1: 降序）
        var bx_order = 0; //并行数排序（默认值（0）; 0: 升序; 1: 降序）
        var tj_order = 0; //退件数排序（默认值（0）; 0: 升序; 1: 降序）

        var xzqhdm= "660100";
        var name = "";
        var currentCityName ="";
        var oldStartDate = "";
        var oldEndDate = "";
    </script>
    <script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
    <script type="text/javascript">
        $(function(){
          if($(window.parent.document).find("#xndc_content_frame").prop("id")=="xndc_content_fra
...
...
...
```

问题 37 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getAnalysisCityOverdueRankingData.do
实体：	getAnalysisCityOverdueRankingData.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Origin` 已从请求除去： `http://127.0.0.1:8000`

标题 `Referer` 从以下位置进行控制：

`http://127.0.0.1:8000/xmjg//supervisionInspectionDrill/analysis-ranking-overdue.do?provinceCode=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29`

至： `http://bogus.referer.hcl.com`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
POST /xmjg/supervisionInspectionDrill/getAnalysisCityOverdueRankingData.do HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Content-Length: 69
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

tjkssj=2020-01-01&tjjssj=2020-12-29&orderByFlag=1&provinceCode=660000

HTTP/1.1 200
Content-Length: 1258
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:54:45 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

{
 "result": "0",
 "data": [
                {
                 "OVERDUE_PER": 26.14,
                 "XZQHDM": "660300",
                 "OVERDUE_CNT": 23,
                 "TOTAL_CNT": 88,
                 "NAME": "        三师图木舒克市"
         }       ,
                {
                 "OVERDUE_PER": 25,
                 "XZQHDM": "660600",
                 "OVERDUE_CNT": 7,
                 "TOTAL_CNT": 28,
                 "NAME": "        六师五家渠市"
         }       ,
                {
                 "OVERDUE_PER": 13.51,
                 "XZQHDM": "660200",
                 "OVERDUE_CNT": 5,
                 "TOTAL_CNT": 37,
                 "NAME": "        二师铁门关市"
         }       ,
                {
                 "OVERDUE_PER": 13.16,
                 "XZQHDM": "660500",
                 "OVERDUE_CNT": 5,
                 "TOTAL_CNT": 38,
                 "NAME": "        五师双河市"
         }       ,
                {
                 "OVERDUE_PER": 9.3,
                 "XZQHDM": "660900",
                 "OVERDUE_CNT": 4,
                 "TOTAL_CNT": 43,
                 "NAME": "        九师"
         }       ,
                {
                 "OVERDUE_PER": 8.16,
                 "XZQHDM": "660700",
                 "OVERDUE_CNT": 4,
                 "TOTAL_CNT": 49,
                 "NAME": "       七师胡杨河市"
         }        ,
                {
                 "OVERDUE_PER": 7.61,
                 "XZQHDM": "660800",
                 "OVERDUE_CNT": 7,
                 "TOTAL_CNT": 92,
                 "NAME": "       八师石河子市"
         }        ,
                {
                 "OVERDUE_PER": 6.15,
                 "XZQHDM": "660400",
                 "OVERDUE_CNT": 4,
                 "TOTAL_CNT": 65,
                 "NAME": "       四师可克达拉市"
         }        ,
                {
                 "OVERDUE_PER": 5,
                 "XZQHDM": "661400",
                 "OVERDUE_CNT": 2,
                 "TOTAL_CNT": 40,
                 "NAME": "       十四师昆玉市"
         }        ,
                {
                 "OVERDUE_PER": 2.5,
                 "XZQHDM": "660100",
                 "OVERDUE_CNT": 4,
                 "TOTAL_CNT": 160,
                 "NAME": "       一师阿拉尔市"
         }        ,
                {
                 "OVERDUE_PER": 1.2,
                 "XZQHDM": "661300",
                 "OVERDUE_CNT": 1,
                 "TOTAL_CNT": 83,
                 "NAME": "       十三师"
         }        ,
                {
                 "OVERDUE_PER": 0,
                 "XZQHDM": "661000",
                 "OVERDUE_CNT": 0,
                 "TOTAL_CNT": 37,
                 "NAME": "       十师北屯市"
         }        ,
                {
                 "OVERDUE_PER": 0,
                 "XZQHDM": "661200",
                 "OVERDUE_CNT": 0,
                 "TOTAL_CNT": 51,
                 "NAME": "       十二师"
                }
        ]
}
```

问题 38 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/xmjg-gzgl-oneform-tabname!getTabName.action
实体：	xmjg-gzgl-oneform-tabname!getTabName.action (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Origin` 已从请求除去： `http://127.0.0.1:8000`
标题 `Referer` 从以下位置进行控制：

`http://127.0.0.1:8000/xmjg//xmjg-one-form!getYzbd.action?name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29`

至： `http://bogus.referer.hcl.com`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
POST /xmjg/xmjg-gzgl-oneform-tabname!getTabName.action?xzqhdm=660100&xmlxbh=1&spjdbh=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Content-Length: 0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:51:03 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "SPJDBH": null,
         "MEMO3": null,
         "MEMO2": null,
         "XZQHDM": null,
         "MEMO5": null,
         "MEMO4": null,
         "MEMO1": "bszn",
         "ID": 1,
         "XMLXBH": null,
         "TABNAME": "       办事指南"
 },
        {
         "SPJDBH": null,
         "MEMO3": null,
         "MEMO2": null,
         "XZQHDM": null,
         "MEMO5": null,
         "MEMO4": null,
         "MEMO1": "bjqd",
         "ID": 2,
         "XMLXBH": null,
         "TABNAME": "       报建清单"
 },
        {
         "SPJDBH": null,
         "MEMO3": null,
         "MEMO2": null,
         "XZQHDM": null,
         "MEMO5": null,
         "MEMO4": null,
         "MEMO1": "sqb",
         "ID": 3,
         "XMLXBH": null,
         "TABNAME": "       申请表"
 },
        {
         "SPJDBH": null,
         "MEMO3": null,
         "MEMO2": null,
         "XZQHDM": null,
         "MEMO5": null,
         "MEMO4": null,
         "MEMO1": "bjlc",
         "ID": 4,
         "XMLXBH": null,
         "TABNAME": "       报建流程"
        }
]
```

问题 39 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/getPjysByTjjssj.do
实体：	getPjysByTjjssj.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制：

`http://127.0.0.1:8000/xmjg//supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?averageTime=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&provinceCode=660000`

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/supervisionInspection/getPjysByTjjssj.do?xzqhdm=660000&startDate=2020-01-
```

```
01&endDate=2020-12-29&spysDy0=0 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 1710
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:54:57 GMT
Content-Type: text/plain;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

[{"index":0,"splclx":1,"splcmc":"政府投资工程建设项目（房屋建筑类）","spjds":
[{"spjd":1,"pjys":7,"zcys":41,"kdys":43},{"spjd":2,"pjys":5,"zcys":14,"kdys":28},
{"spjd":3,"pjys":3,"zcys":8,"kdys":30},{"spjd":4,"pjys":4,"zcys":6,"kdys":8},
{"spjd":5,"pjys":7,"zcys":21,"kdys":33}],"bxtj":
{"pjys":7,"zcys":21,"kdys":33},"zpjys":26,"zkdys":142},{"index":1,"splclx":2,"splcmc":"政府投资工程
建设项目（线性工程类）","spjds":[{"spjd":1,"pjys":6,"zcys":23,"kdys":32},
{"spjd":2,"pjys":4,"zcys":9,"kdys":26},{"spjd":3,"pjys":3,"zcys":7,"kdys":17},
{"spjd":4,"pjys":4,"zcys":11,"kdys":9},{"spjd":5,"pjys":7,"zcys":20,"kdys":28}],"bxtj":
{"pjys":7,"zcys":20,"kdys":28},"zpjys":24,"zkdys":112},{"index":2,"splclx":3,"splcmc":"一般社会投资
项目","spjds":[{"spjd":1,"pjys":5,"zcys":25,"kdys":48},{"spjd":2,"pjys":3,"zcys":9,"kdys":39},
{"spjd":3,"pjys":4,"zcys":9,"kdys":19},{"spjd":4,"pjys":8,"zcys":18,"kdys":15},
{"spjd":5,"pjys":5,"zcys":15,"kdys":36}],"bxtj":
{"pjys":5,"zcys":15,"kdys":36},"zpjys":25,"zkdys":157},{"index":3,"splclx":4,"splcmc":"小型社会投资
项目","spjds":[{"spjd":1,"pjys":3,"zcys":11,"kdys":48},{"spjd":2,"pjys":6,"zcys":13,"kdys":46},
{"spjd":3,"pjys":5,"zcys":12,"kdys":63},{"spjd":4,"pjys":4,"zcys":8,"kdys":21},
{"spjd":5,"pjys":4,"zcys":17,"kdys":49}],"bxtj":
{"pjys":4,"zcys":17,"kdys":49},"zpjys":22,"zkdys":227},{"index":4,"splclx":5,"splcmc":"带方案出让用
地的社会投资项目","spjds":[{"spjd":1,"pjys":3,"zcys":12,"kdys":71},
{"spjd":2,"pjys":0,"zcys":0,"kdys":0},{"spjd":3,"pjys":1,"zcys":1,"kdys":102},
{"spjd":4,"pjys":0,"zcys":0,"kdys":0},{"spjd":5,"pjys":6,"zcys":11,"kdys":32}],"bxtj":
{"pjys":6,"zcys":11,"kdys":32},"zpjys":10,"zkdys":205}]
```

问题 40 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do
实体：	analysis-ranking-overdue.do (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **标题** `Referer` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg/opus/front/blue/index.html`
至： `http://bogus.referer.hcl.com`
标题 `Upgrade-Insecure-Requests` 已从请求除去： `1`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的“Referer”头。

测试请求和响应：

```
GET /xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do?provinceCode=660000&tjkssj=2020-
01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:54:35 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<html>
 <head>
         <meta charset="utf-8" />
         <title>       各城市项目逾期率排名</title>
         <script type="text/javascript">

                 var ctx="/xmjg/";
                 var bigScreenFolder="";
                 //var bigScreenFolder="bigscreenTwo";
                 var tjkssj="2020-01-01";
                 var tjjssj="2020-12-29";
                 var provinceCode="660000";
                 var dateEnd = "2020-12-29";
                 var dataType = "9";
                 var stageType = "0";
                 var provinceDrillXzqhdm ='';
         </script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

         <link rel="stylesheet" type="text/css"
href="/xmjg/xmjg/supervisionInspection/css/analysis-index.css"/>
         <link rel="stylesheet" type="text/css"
href="/xmjg/xmjg/supervisionInspection/css/analysis-statistics.css"/>
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/bootstrap.min.css"/>
         <script src="/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js"
type="text/javascript" charset="utf-8"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap.min.js"  type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
         <link href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css"
title="" rel="stylesheet"/>
         <script  src="/xmjg/xmjg/supervisionInspection/js/echarts.min.js"
type="text/javascript"  charset="utf-8"></script>
         <script  src="/xmjg/xmjg/supervisionInspection/js/analysis-ranking-overdue.js"
type="text/javascript"  charset="utf-8"></script>
         <script  src="/xmjg/xmjg/supervisionInspection/js/common-charts.js"
type="text/javascript"  charset="utf-8"></script>
         <!--        城市选择插件  开始 -->
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/cityselect/css/city_select.css"/>
         <script src="/xmjg/common/tool/cityselect/js/city_data.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/cityselect/js/areadata.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/cityselect/js/auto_area.js" type="text/javascript"
charset="utf-8"></script>
         <!--        城市选择插件  结束 -->
         <!--        时间查询控件 开始 -->
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/dateQuery.css"/>
         <script src="/xmjg/common/tool/date/js/dateQuery.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8">
</script>
         <style>
                 .stage-tab-tit.stage-tab-tit1 {
                         right: 16px;
                        }
                 .cFff{
                         color:#ffffff;
                        }
                 .index-item-table>table tr td.red {
                         color: red;
                        }
         </style>
         <!--
...
...
...
```

问题 41 / 42 TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/opus/front/om/users/currOpusLoginUser
实体：	time (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **参数** time 从以下位置进行控制： 1609210165955 至： 116092101659551

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的 CSRF 令牌。

测试请求和响应：

```
GET /xmjg/opus/front/om/users/currOpusLoginUser?time=116092101659551 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Authorization: bearer null
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded;


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:55:39 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "success": true,
 "message": "       获取成功",
 "content": {
         "user": {
                 "userId": "10000",
                 "userName": "       超级管理员",
                 "loginName": "admin",
                 "loginPwd": null,
                 "isLock": null,
                 "loginFailNum": null,
                 "lockTime": null
         }       ,
         "orgs": [
                        {
                         "orgId": "e3e8a4cb-eab1-475c-8a89-6c580e257a9a",
                         "orgCode": "R001-G10585",
                         "orgName": "       管理员",
                         "orgSeq": null,
                         "isMain": null
                        }
         ]       ,
         "currentOrgId": "A",
         "currentOrgCode": "R001",
         "currentTmn": "pc",
         "appSoftContexts": [
         ]        ,
         "tmnMenuContexts": [

                ]
        }
}
```

问题 42 / 42

TOC

跨站点请求伪造

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/opus/front/om/users/user/10000/allMenus
实体：	time (Parameter)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	应用程序使用的认证方法不充分
固定值：	验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce

差异： **参数** `time` 从以下位置进行控制： `1609210165955` 至： `116092101659551`

推理： 测试结果似乎指示存在漏洞，因为测试响应与原始响应完全相同，而后者指示跨站点请求伪造尝试成功，尽管其中有假想的 CSRF 令牌。

测试请求和响应：

```
GET /xmjg/opus/front/om/users/user/10000/allMenus?
isTree=true&netName=%E5%89%8D%E7%AB%AF%E7%BD%91%E7%BB%9C%E5%85%A5%E5%8F%A3&tmnId=1&topOrgId=A&use
rId=10000&time=116092101659551 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: application/json, text/javascript, */*; q=0.01
Authorization: bearer null
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded;


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:57:22 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "success": true,
 "message": "        获取成功！",
 "content": [
               {
                "creater": "10000",
                "createTime": 1596256085000,
                "modifier": "10000",
                 "modifyTime": 1597471994000,
                 "opusRsType": "MENU",
                 "nodeId": null,
                 "name": null,
                 "pId": null,
                 "pName": null,
                 "open": true,
                 "isHorizontal": false,
                 "type": null,
                 "isParent": false,
                 "iconSkin": null,
                 "nocheck": false,
                 "menuId": "2da101cb-414c-4df4-aa43-3ec3edfc59c9",
                 "menuCode": "opu-rs-menu-00000002879",
                 "menuName": "       运行监控",
                 "menuIconCss": null,
                 "netTmnId": "107f66ee-f2bb-468d-8c10-c88a075919e7",
                 "appSoftId": "0e51914e123e43fe91e1b960eeddc314",
                 "funcId": "61581f1e-a0e5-490b-8a9b-ef5e8a205008",
                 "parentMenuId": "",
                 "menuLevel": 1,
                 "menuSeq": ".2da101cb-414c-4df4-aa43-3ec3edfc59c9.",
                 "menuSortNo": 0,
                 "isActive": "1",
                 "isLeaf": "1",
                 "subCount": 0,
                 "activeSubCount": 0,
                 "pageOpenMode": "default",
                 "smallImgPath": null,
                 "middleImgPath": null,
                 "bigImgPath": "/agcloud/opus/admin/menu/images/32/top_jdkh.png",
                 "menuMemo": null,
                 "menuDeleted": "0",
                 "menuInvokeActivity": null,
                 "menuInvokeType": "h",
                 "isSingleUrl": "0",
                 "autoSwitch": "0",
                 "menuInnerUrl": "http://59.255.8.199:8000/xmjg/supervisionInspection/dg-
jdkh-main.do",
                 "menuGovUrl": "/xmjg/supervisionInspection/dg-jdkh-main.do",
                 "menuOuterUrl": "/xmjg/supervisionInspection/dg-jdkh-main.do",
                 "menuTagUrl": null,
                 "isRecentlyAdd": null,
                 "hugeImgPath": null,
                 "isImgIcon": "1",
                 "handleUrlWay": null,
                 "childrenList": null,
                 "maxMenuLevel": null,
                 "allMenuCount": null,
                 "topMenuCount": null,
                 "menuLevelCount": null,
                 "appSoftName": null,
                 "funcName": null,
                 "isAdmin": null,
                 "keyword": null,
                 "parentMenuName": null,
                 "isNeedChild": null,
                 "isOpenMenuCount": "0",
                 "openMenuCount": false,
                 "menuCountUrl": null,
                 "menuCountInterval": 60000,
                 "id": "MENU_2da101cb-414c-4df4-aa43-3ec3edfc59c9"
         }       ,
                {
                 "creater": "10000",
                 "createTime": 1596258478000,
                 "modifier": "10000",
                 "modifyTime": 1597472051000,
                 "opusRsType": "MENU",
                 "nodeId": null,
                 "name": null,
                 "pId": null,
                 "pName": null,
                 "open": true,
                 "isHorizontal": false,
                 "type": null,
                 "isParent": false,
                 "iconSkin": null,
                 "nocheck": false,
                 "menuId": "20cc1765-4c70-4bf0-8010-8f3c4f621ea6",
                 "menuCode": "opu-rs-menu-00000002882",
                 "menuName": "查询展示",
                 "menuIconCss": null,
                 "netTmnId": "107f66ee-f2bb-468d-8c10-c88a075919e7",
                 "appSoftId": "0e51914e123e43fe91e1b960eeddc314",
                 "funcId": "2e15a43d-35ba-4804-91bd-686d7d0ba4fc",
                 "parentMenuId": "",
                 "menuLevel": 1,
                 "menuSeq": ".20cc1765-4c70-4bf0-8010-8f3c4f621ea6.",
                 "menuSortNo": 2,
                 "isActive": "1",
                 "isLeaf": "1",
                 "subCount": 0,
                 "activeSubCount": 0,
                 "pageOpenMode": "default",
                 "smallImgPath": null,
                 "middleImgPath": null,
                 "bigImgPath": "/agcloud/opus/admin/menu/images/32/top_gzgl.png",
                 "menuMemo": null,
                 "menuDeleted": "0",
                 "menuInvokeActivity": null,
                 "menuInvokeType": "h",
                 "isSingleUrl": "0",
                 "autoSwitch": "0",
                 "menuInnerUrl":
"http://59.255.8.199:8000/xmjg/queryShow/showCxzsMain.do",
                 "menuGovUrl": "/xmjg/queryShow/showCxzsMain.do",
                 "menuOuterUrl": "/xmjg/queryShow/showCxzsMain.do",
                 "menuTagUrl": null,
                 "isRecentlyAdd": null,
                 "hugeImgPath": null,
                 "isImgIcon": "1",
                 "handleUrlWay": null,
                 "childrenList": [
                                {
                                 "creater": "10000",
                                 "createTime": 1596258938000,
                                 "modifier": "10000",
                                 "modifyTime": 1597472091000,
                                 "opusRsType": "MENU",
                                 "nodeId": null,
                                 "name": null,
                                 "pId": null,
                                 "pName": null,
                                 "open": true,
                                 "isHorizontal": false,
                                 "type": null,
                                 "isParent": false,
                                 "iconSkin": null,
                                 "nocheck": false,
                                 "menuId": "ba18ccd8-15ca-4373-95c3-156fcd6cafc8",
                                 "menuCode": "opu-rs-menu-00000002883",
                                 "menuName": "定义查询",
                                 "menuIconCss": null,
                                 "netTmnId": "107f
...
...
...
```

中 使用 HTTP 动词篡改的认证旁路 1 TOC

问题 1 / 1 TOC

使用 HTTP 动词篡改的认证旁路

严重性：	中
CVSS 分数：	6.4
URL：	http://127.0.0.1:8000/xmjg/xmjg/xmjg-project-info!getScreen.action
实体：	xmjg-project-info!getScreen.action (Page)
风险：	可能会升级用户特权并通过 Web 应用程序获取管理许可权 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为仅允许所需 HTTP 方法

差异： **方法** 从以下位置进行控制： POST 至： BOGUS
cookie JSESSIONID 已从请求除去： BAD94CD62CFD05C63C4D2EF079DD5B06

推理： 测试结果似乎指示存在脆弱性，因为“测试响应”与“原始响应”完全相同，这表明动词篡改能够绕过站点认证。

测试请求和响应：

```
CUSTOM_TEST_METHOD /xmjg/xmjg/xmjg-project-info!getScreen.action HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie:
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 1
Set-Cookie: JSESSIONID=2A018D57849FFAB436BE05DE36408094; Path=/xmjg; HttpOnly
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:49:08 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

0
```

低 “Content-Security-Policy”头缺失或不安全 5 TOC

问题 1 / 5 TOC

“Content-Security-Policy”头缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/jquery.cookie.js
实体：	jquery.cookie.js (Page)
风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应：

```
GET /opus-front-sso/framework/ui-themes/common/metronic/js/jquery.cookie.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/require
Cookie: JSESSIONID=D6A5925ADA251562D8C32F08668AA5EE
Connection: keep-alive
Host: 127.0.0.1:8090
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 28 Dec 2020 07:36:44 GMT
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Content-Length: 4467
X-Content-Type-Options: nosniff
Cache-Control: max-age=31556926
Date: Tue, 29 Dec 2020 02:44:19 GMT
Content-Type: application/javascript;charset=utf-8

/**
 * Cookie plugin
 *
 * Copyright (c) 2006 Klaus Hartl (stilbuero.de)
 * Dual licensed under the MIT and GPL licenses:
 * http://www.opensource.org/licenses/mit-license.php
 * http://www.gnu.org/licenses/gpl.html
 *
 */
```

```
/**
 * Create a cookie with the given name and value and other optional parameters.
 *
 * @example $.cookie('the_cookie', 'the_value');
 * @desc Set the value of a cookie.
 * @example $.cookie('the_cookie', 'the_value', { expires: 7, path: '/', domain: 'jquery.com',
secure: true });
 * @desc Create a cookie with all available options.
 * @example $.cookie('the_cookie', 'the_value');
 * @desc Create a session cookie.
 * @example $.cookie('the_cookie', null);
 * @desc Delete a cookie by passing null as value. Keep in mind that you have to use the same
path and domain
 *       used when the cookie was set.
 *
 * @param String name The name of the cookie.
 * @param String value The value of the cookie.
 * @param Object options An object literal containing key/value pairs to provide optional cookie
attributes.
 * @option Number|Date expires Either an integer specifying the expiration date from now on in
days or a Date object.
 *          If a negative value is specified (e.g. a date in the past), the cookie will be
deleted.
 *          If set to null or omitted, the cookie will be a session cookie and will not be
retained
 *          when the the browser exits.
 * @option String path The value of the path atribute of the cookie (default: path of page that
created the cookie).
 * @option String domain The value of the domain attribute of the cookie (default: domain of page
that created the cookie).
 * @option Boolean secure If true, the secure attribute of the cookie will be set and the cookie
transmission will
 *          require a secure protocol (like HTTPS).
 * @type undefined
 *
 * @name $.cookie
 * @cat Plugins/Cookie
 * @author Klaus Hartl/klaus.hartl@stilbuero.de
 */

/**
 * Get the value of a cookie with the given name.
 *
 * @example $.cookie('the_cookie');
 * @desc Get the value of a cookie.
 *
 * @param String name The name of the cookie.
 * @return The value of the cookie.
 * @type String
 *
 * @name $.cookie
 * @cat Plugins/Cookie
 * @author Klaus Hartl/klaus.hartl@stilbuero.de
 */
jQuery.cookie = function(name, value, options) {
    if (typeof value != 'undefined') { // name and value given, set cookie
        options = options || {};
        if (value === null) {
          value = '';
          options = $.extend({}, options); // clone object since it's unexpected behavior if the
expired property were changed
          options.expires = -1;
        }
        var expires = '';
        if (options.expires && (typeof options.expires == 'number' ||
options.expires.toUTCString)) {
          var date;
          if (typeof options.expires == 'number') {
          date = new Date();
          date.setTime(date.getTime() + (options.expires * 24 * 60 * 60 * 1000));
          } else {
          date = options.expires;
          }
          expires = '; expires=' + date.toUTCString(); // use expires attribute, max-age is not
supported by IE
        }
        // NOTE Needed to parenthesize options.path and options.domain
        // in the following expressions, otherwise they evaluate to undefined
        // in the packed version for some reason...
        var path = options.path ? '; path=' + (options.path) : '';
        var domain = options.domain ? '; domain=' + (options.domain) : '';
        var secure = options.secure ? '; secure' : '';
        document.cookie = [name, '=', encodeURIComponent(value), expires, path, domain,
secure].join('');
    } else { // only name given, get cookie
        var cookieValue = null;
        if (document.cookie && document.cookie != '') {
          var cookies = document.cookie.split(';');
          for (var i = 0; i < cookies.length; i++) {
          var cookie = jQuery.trim(cookies[i]);
          // Does this cookie string begin with the name we want?
          if (cookie.substring(0, name.length + 1) == (name + '=')) {

...
...
...
```

问题 2 / 5

TOC

“Content-Security-Policy”头缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8090/opus-front-sso/js/md5.js
实体：	md5.js (Page)
风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应：

```
GET /opus-front-sso/js/md5.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/require
Cookie: JSESSIONID=D6A5925ADA251562D8C32F08668AA5EE
Connection: keep-alive
Host: 127.0.0.1:8090
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 28 Dec 2020 07:36:44 GMT
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Content-Length: 12295
X-Content-Type-Options: nosniff
Cache-Control: max-age=31556926
Date: Tue, 29 Dec 2020 02:44:19 GMT
Content-Type: application/javascript;charset=utf-8
```

```
/*
 * A JavaScript implementation of the RSA Data Security, Inc. MD5 Message
 * Digest Algorithm, as defined in RFC 1321.
 * Version 2.2 Copyright (C) Paul Johnston 1999 - 2009
 * Other contributors: Greg Holt, Andrew Kepert, Ydnar, Lostinet
 * Distributed under the BSD License
 * See http://pajhome.org.uk/crypt/md5 for more info.
 */

/*
 * Configurable variables. You may need to tweak these to be compatible with
 * the server-side, but the defaults work in most cases.
 */
var hexcase = 0;   /* hex output format. 0 - lowercase; 1 - uppercase        */
var b64pad  = "";  /* base-64 pad character. "=" for strict RFC compliance   */

/*
 * These are the functions you'll usually want to call
 * They take string arguments and return either hex or base-64 encoded strings
 */
function hex_md5(s)    { return rstr2hex(rstr_md5(str2rstr_utf8(s))); }
function b64_md5(s)    { return rstr2b64(rstr_md5(str2rstr_utf8(s))); }
function any_md5(s, e) { return rstr2any(rstr_md5(str2rstr_utf8(s)), e); }
function hex_hmac_md5(k, d)
  { return rstr2hex(rstr_hmac_md5(str2rstr_utf8(k), str2rstr_utf8(d))); }
function b64_hmac_md5(k, d)
  { return rstr2b64(rstr_hmac_md5(str2rstr_utf8(k), str2rstr_utf8(d))); }
function any_hmac_md5(k, d, e)
  { return rstr2any(rstr_hmac_md5(str2rstr_utf8(k), str2rstr_utf8(d)), e); }

/*
 * Perform a simple self-test to see if the VM is working
 */
function md5_vm_test()
{
  return hex_md5("abc").toLowerCase() == "900150983cd24fb0d6963f7d28e17f72";
}

/*
 * Calculate the MD5 of a raw string
 */
function rstr_md5(s)
{
  return binl2rstr(binl_md5(rstr2binl(s), s.length * 8));
}

/*
 * Calculate the HMAC-MD5, of a key and some data (raw strings)
 */
function rstr_hmac_md5(key, data)
{
  var bkey = rstr2binl(key);
  if(bkey.length > 16) bkey = binl_md5(bkey, key.length * 8);

  var ipad = Array(16), opad = Array(16);
  for(var i = 0; i < 16; i++)
  {
    ipad[i] = bkey[i] ^ 0x36363636;
    opad[i] = bkey[i] ^ 0x5C5C5C5C;
  }

  var hash = binl_md5(ipad.concat(rstr2binl(data)), 512 + data.length * 8);
  return binl2rstr(binl_md5(opad.concat(hash), 512 + 128));
}

/*
 * Convert a raw string to a hex string
 */
function rstr2hex(input)
{
  try { hexcase } catch(e) { hexcase=0; }
  var hex_tab = hexcase ? "0123456789ABCDEF" : "0123456789abcdef";
  var output = "";
  var x;
  for(var i = 0; i < input.length; i++)
  {
    x = input.charCodeAt(i);
    output += hex_tab.charAt((x >>> 4) & 0x0F)
           +  hex_tab.charAt( x        & 0x0F);
  }
  return output;
}

/*
 * Convert a raw string to a base-64 string
 */
function rstr2b64(input)
{
  try { b64pad } catch(e) { b64pad=''; }
  var tab = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";
  var output = "";
  var len = input.length;
  for(var i = 0; i < len; i += 3)
  {
    var triplet = (input.charCodeAt(i) << 16)
          | (i + 1 < len ? input.charCodeAt(i+1) << 8 : 0)
          | (i + 2 < len ? input.charCodeAt(i+2)      : 0);
    for(var j = 0; j < 4; j++)
    {
      if(i * 8 + j * 6 > input.length * 8) output += b64pad;
      else output += tab.charAt((triplet >>> 6*(3-j)) & 0x3F);
    }
  }
  return output;
}

/*
 * Convert a raw string to an arbitrary string encoding
 */
function rstr2any(input, encoding)
{
  var divisor = encoding.length;
  var i, j, q, x, quotient;

  /* Convert to an array of 16-bit big-endian values, forming the dividend */
  var dividend = Array(Math.ceil(input.length / 2));
  for(i = 0; i < dividend.length; i++)
  {
    dividend[i] = (input.charCodeAt(i * 2) << 8) | input.charCodeAt(i * 2 + 1);
  }

  /*
   * Repeatedly perform a long division. The binary array forms the dividend,
   * the length of the encoding is the divisor. Once computed, the quotient
   * forms the dividend for the next step. All remainders are stored for later
   * use.
   */
  var full_length = Math.ceil(input.length * 8 /
          (Math.log(encoding.length) / Math.log(2)));
  var remainders = Array(full_length);
  for(j = 0; j < full_length; j++)
  {
    quotient = Array();
    x = 0;
    for(i = 0; i < dividend.length; i++)
    {
      x = (x << 16) + dividend[i];
      q = Math.floor(x / divisor);

...
...
...
```

问题 3 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8090/opus-front-sso/js/login.js
实体：	login.js (Page)
风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应：

```
GET /opus-front-sso/js/login.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/require
Cookie: JSESSIONID=D6A5925ADA251562D8C32F08668AA5EE
Connection: keep-alive
Host: 127.0.0.1:8090
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 28 Dec 2020 07:36:44 GMT
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Content-Length: 15367
X-Content-Type-Options: nosniff
Cache-Control: max-age=31556926
Date: Tue, 29 Dec 2020 02:44:19 GMT
Content-Type: application/javascript;charset=utf-8

var rules = {};
var messages = {};
if (verifyCodeIsOpen == 'true') {
    rules = {
        username_text: {
          required: true,
          minlength: 2
        },
        password_text: {
          required: true,
          minlength: 3
        },
        imageCode: {
          required: true,
        }
    };

    messages = {
        username_text: {
          required: "请输入用户名",
          minlength: "用户名不能小于3个字符"
        },
        password_text: {
          required: "请输入密码",
          minlength: "密码不能小于3个字符"
        },
        imageCode: {
          required: "请输入验证码",
        }
    };
} else {
    rules = {
        username_text: {
          required: true,
          minlength: 2
        },
        password_text: {
          required: true,
          minlength: 3
        }
    };

    messages = {
        username_text: {
          required: "请输入用户名",
          minlength: "用户名不能小于3个字符"
        },
        password_text: {
          required: "请输入密码",
          minlength: "密码不能小于3个字符"
        }
    };
}

var _base64 = null;
var sm4 = null;
$(function(){
 //       判断是否启用验证码，启用则输入框纵向排列
 if($(".verify-code").length > 0){
     $(".login_wel").addClass('login_wel_new');
     $(".login-content").addClass('login-content-new');
     $(".login01").addClass('login01-new');
     $(".login-input-group ").addClass("verify-code-Ul");
     $(".login-btn").addClass('login-btn-new ');
        }
 $(".login-content").show();

    var orgId = 'A';
    // var orgId ='b5b092b5-dcad-4524-9631-a73d78e55591';

    _base64 = new Base64();
    sm4 = new SM4Util();
    var spring_error = $("#spring_error").html();

    if (spring_error != undefined) {
        if (spring_error.indexOf("初始化密码") != -1) {

          var form = $("#editPassword");
          var loginName = $.cookie("username");
          if (loginName == "") {
          loginName = $("#username_text").val();
          }
          layer.open({
          type: 1,
          title: '重置初始化密码',
          area: ['490px', '350px'],
          shadeClose: true, //点击遮罩关闭
          content: form,
          btn: ['保存', '取消'],
          btn2: function() {
          layer.closeAll();
          },
          yes: function() {
          if (!form.valid()) {
          return;
          } else {
          $.ajax({
          type: "post",
          url: ctx + 'authentication/user/password',
          data: {
          'loginName': sm4.encryptData_ECB(loginName),
          'oldPassword': sm3(hex_md5($("input[name='oldPassword']").val())),
          'proPassword': sm3(sm4.encryptData_ECB($("input[name='oldPassword']").val())),
          'newPassword': sm3(sm4.encryptData_ECB($("input[name='newPassword']").val()))
          },
          success: function(data) {
          if (data.success) {
```

```
          $("#password_text").val($("input[name='newPassword']").val());
          $("#password").val($("input[name='newPassword']").val());
          if (verifyCodeIsOpen) {
          $("#resetPasswordId").val("1");
          }
          $.cookie("username", $("#username_text").val(), { expires: 7 });
          $("#orgId").val(sm4.encryptData_ECB(orgId));
          $("#username").val(sm4.encryptData_ECB($("#username_text").val()));
          $("#password").val(sm3(hex_md5($("#password_text").val())));
          $("#proPassword").val(sm3(sm4.encryptData_ECB($("#password_text").val())));
          $('#deviceType').val(sm4.encryptData_ECB($("#deviceType").val()));
          $('#login_form').submit();
          layer.closeAll();

...
...
...
```

问题 4 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8090/opus-front-sso/js/jquery.validate.min.js
实体：	jquery.validate.min.js (Page)
风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应：

```
GET /opus-front-sso/js/jquery.validate.min.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/require
Cookie: JSESSIONID=D6A5925ADA251562D8C32F08668AA5EE
Connection: keep-alive
Host: 127.0.0.1:8090
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 28 Dec 2020 07:36:44 GMT
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Content-Length: 24379
X-Content-Type-Options: nosniff
Cache-Control: max-age=31556926
Date: Tue, 29 Dec 2020 02:44:19 GMT
Content-Type: application/javascript;charset=utf-8

/*! jQuery Validation Plugin - v1.19.1 - 6/15/2019
```

```
 * https://jqueryvalidation.org/
 * Copyright (c) 2019 Jörn Zaefferer; Licensed MIT */
!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):"object"==typeof
module&&module.exports?module.exports=a(require("jquery")):a(jQuery)}(function(a){a.extend(a.fn,
{validate:function(b){if(!this.length)return
void(b&&b.debug&&window.console&&console.warn("Nothing selected, can't validate, returning
nothing."));var c=a.data(this[0],"validator");return c?c:
(this.attr("novalidate","novalidate"),c=new
a.validator(b,this[0]),a.data(this[0],"validator",c),c.settings.onsubmit&&
(this.on("click.validate",":submit",function(b)
{c.submitButton=b.currentTarget,a(this).hasClass("cancel")&&(c.cancelSubmit=!0),void
0!==a(this).attr("formnovalidate")&&(c.cancelSubmit=!0)}),this.on("submit.validate",function(b)
{function d(){var d,e;return c.submitButton&&(c.settings.submitHandler||c.formSubmitted)&&(d=a("
<input
type='hidden'/>").attr("name",c.submitButton.name).val(a(c.submitButton).val()).appendTo(c.curren
tForm)),!(c.settings.submitHandler&&!c.settings.debug)||
(e=c.settings.submitHandler.call(c,c.currentForm,b),d&&d.remove(),void 0!==e&&e)}return
c.settings.debug&&b.preventDefault(),c.cancelSubmit?(c.cancelSubmit=!1,d()):c.form()?
c.pendingRequest?(c.formSubmitted=!0,!1):d():(c.focusInvalid(),!1)})),c)},valid:function(){var
b,c,d;return a(this[0]).is("form")?b=this.validate().form():(d=
[],b=!0,c=a(this[0].form).validate(),this.each(function(){b=c.element(this)&&b,b||
(d=d.concat(c.errorList))}),c.errorList=d),b},rules:function(b,c){var
d,e,f,g,h,i,j=this[0],k="undefined"!=typeof
this.attr("contenteditable")&&"false"!==this.attr("contenteditable");if(null!=j&&(!j.form&&k&&
(j.form=this.closest("form")[0],j.name=this.attr("name")),null!=j.form))
{if(b)switch(d=a.data(j.form,"validator").settings,e=d.rules,f=a.validator.staticRules(j),b)
{case"add":a.extend(f,a.validator.normalizeRule(c)),delete f.messages,e[j.name]=f,c.messages&&
(d.messages[j.name]=a.extend(d.messages[j.name],c.messages));break;case"remove":return c?(i=
{},a.each(c.split(/\s/),function(a,b){i[b]=f[b],delete f[b]}),i):(delete e[j.name],f)}return
g=a.validator.normalizeRules(a.extend({},a.validator.classRules(j),a.validator.attributeRules(j),
a.validator.dataRules(j),a.validator.staticRules(j)),j),g.required&&(h=g.required,delete
g.required,g=a.extend({required:h},g)),g.remote&&(h=g.remote,delete g.remote,g=a.extend(g,
{remote:h})),g}}}),a.extend(a.expr.pseudos||a.expr[":"],{blank:function(b)
{return!a.trim(""+a(b).val())},filled:function(b){var c=a(b).val();return
null!==c&&!!a.trim(""+c)},unchecked:function(b)
{return!a(b).prop("checked")}}),a.validator=function(b,c){this.settings=a.extend(!0,
{},a.validator.defaults,b),this.currentForm=c,this.init()},a.validator.format=function(b,c)
{return 1===arguments.length?function(){var c=a.makeArray(arguments);return
c.unshift(b),a.validator.format.apply(this,c)}:void 0===c?b:
(arguments.length>2&&c.constructor!==Array&&
(c=a.makeArray(arguments).slice(1)),c.constructor!==Array&&(c=[c]),a.each(c,function(a,c)
{b=b.replace(new RegExp("\\{"+a+"\\}","g"),function(){return c})}),b)},a.extend(a.validator,
{defaults:{messages:{},groups:{},rules:
{},errorClass:"error",pendingClass:"pending",validClass:"valid",errorElement:"label",focusCleanup
:!1,focusInvalid:!0,errorContainer:a([]),errorLabelContainer:a([]),onsubmit:!0,ignore:":hidden",i
gnoreTitle:!1,onfocusin:function(a){this.lastActive=a,this.settings.focusCleanup&&
(this.settings.unhighlight&&this.settings.unhighlight.call(this,a,this.settings.errorClass,this.s
ettings.validClass),this.hideThese(this.errorsFor(a)))},onfocusout:function(a)
{this.checkable(a)||!(a.name in
this.submitted)&&this.optional(a)||this.element(a)},onkeyup:function(b,c){var d=
[16,17,18,20,35,36,37,38,39,40,45,144,225];9===c.which&&""===this.elementValue(b)||a.inArray(c.ke
yCode,d)!==-1||(b.name in this.submitted||b.name in
this.invalid)&&this.element(b)},onclick:function(a){a.name in this.submitted?
this.element(a):a.parentNode.name in
this.submitted&&this.element(a.parentNode)},highlight:function(b,c,d){"radio"===b.type?
this.findByName(b.name).addClass(c).removeClass(d):a(b).addClass(c).removeClass(d)},unhighlight:f
unction(b,c,d){"radio"===b.type?this.findByName(b.name).removeClass(c).ad
...
...
...
```

问题 5 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8090/opus-front-sso/authentication/require
实体：	require (Page)
风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

差异：

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

测试请求和响应：

```
GET /opus-front-sso/authentication/require HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: JSESSIONID=D6A5925ADA251562D8C32F08668AA5EE
Connection: keep-alive
Host: 127.0.0.1:8090
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:44:19 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
 <meta charset="utf-8" />
 <title>       工程建设项目审批管理平台</title>
 <meta name="description" content="Latest updates and statistic charts"/>
 <meta http-equiv="X-UA-Compatible" content="IE=edge"/>
 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/>
 <link rel="shortcut icon"  href="/opus-front-sso/images/guohui.png" type="image/x-icon"/>
 <link rel="icon"  href="/opus-front-sso/images/guohui.png" type="image/x-icon" />
 <link href="/opus-front-sso/css/global.css" rel="stylesheet" type="text/css">
 <link href="/opus-front-sso/css/login_new.css" rel="stylesheet" type="text/css">
 <link href="/opus-front-sso/css/layui.css" rel="stylesheet" type="text/css">
 <script src="/opus-front-sso/js/jquery-3.4.1.min.js"></script>
 <script src="/opus-front-sso/js/jquery.validate.min.js"></script>
 <script src="/opus-front-sso/js/layui.all.js"></script>
 <script>
        var ctx = '/opus-front-sso/';
        var verifyCodeIsOpen = '${verifyCodeIsOpen}';

        //设置高亮(对象,位置)
        function setCaret(textbox,start){
          try{
          if(textbox.createTextRange){
          var r=textbox.createTextRange();
          r.moveStart('character',start);
          r.select();
          }else if(textbox.setSelectionRange){
```

```
          textbox.setSelectionRange(0,textbox.value.length);
          textbox.focus();
          }
          }catch(e){}
        }

        function getPic(){

          $('#verifyCodeImg').attr("src", ctx + 'code/image?time1='+ new Date().getTime());
        }

        function checkPwd() {

          var layer ;
          layui.use('layer', function(){
          layer = layui.layer;
          });
          var reg = new RegExp(/^[0-9]+.?[0-9]*$/);//工作密码是否是数字串
          var pwd = $('#password_text').val().trim();
          if  (pwd.length < 8 || reg.test(pwd)){

          layer.msg('密码过于简单，请登录后进行修改！', {time: 2000, icon:6});
          }
        }
 </script>
</head>
<body id="cas">
<div id="main" style="width: 100%;height: 100%;">


<!--系统登录界面-->
<div class="login-logo">
 <div class="ts-logo float-left">
         <img src="/opus-front-sso/images/login_logo.png">
 </div>
</div>
<div class="login-bg"></div>
<div id="login-main">
<form id="login_form" action="/opus-front-sso/authentication/form" method="post">
 <div class="login-content" style="display: none;">
<!--            <div class="m-login__logo">
                 <span class="pro-logo-name">       工程建设项目审批管理平台</span>
         </div> -->
         <div class="login01">

                 <div class="login_wel"></div>
                 <ul class="login-input-group">
                         <li       >
                                 <i class="username"></i>
                                 <input id="username_text" class="input" tabindex="1"
onfocus="setCaret(this,0)" placeholder="用户名" accesskey="n" type="text" value="" size="25">
                                 <input id="username" type="hidden" name="username"/>
                         </li>
                         <li       >
                                 <i class="userpassword"></i>
                                 <input id="password_text" class="input" tabindex="2"
onfocus="setCaret(this,0)" accesskey="p" placeholder="密  码" type="password" value="" size="25">
                                 <input id="password" type="hidden" name="password"/>
                                 <input id="proPassword" type="hidden"
name="proPassword"/>
                                 <input id="orgId" type="hidden" name="orgId"/>
                                 <input id="resetPasswordId" type="hidden"
name="resetPasswordId"/>
                                 <input id="deviceType" type="hidden" name="deviceType"
value="pc"/>
                         </li>

                 </ul>
                 <div class="login-btn" style="text-align: center;">

                         <button class="m_login_signin_submit"></button>
                 </div>
         </div>
 </div>
</form>
<form id="editPassword" class="layui-form" action="">
 <div class="layui-form-item" style="margin-top: 30px;">
         <label class="layui-form-label" style="width: 30%">       原密码：</label>
         <div class="layui-input-block" >
                 <input type="password" name="oldPassword" lay-
verify="required|oldPassword"  class="layui-input" style="width: 80%">
         </div>
 </div>
 <div class="layui-form-item">
         <label class="layui-form-label"style="width: 30%" >       新密码：</label>
         <div class="layui-input-block" >
                 <input type="password" name="newPassword" lay-veri
...
...
...
```

低 JavaScript 劫持 8 TOC

问题 1 / 8 TOC

JavaScript 劫持

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/getProvinceTopFive.do
实体：	getProvinceTopFive.do (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	应用程序使用的认证方法不充分
固定值：	拒绝恶意请求并防止直接执行 JavaScript 响应

差异： **标题** `Referer` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879`
至： `http://bogus.referer.hcl.com`
标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Accept` 从以下位置进行控制： `application/json, text/javascript, */*; q=0.01` 至： `*/*`

推理： 测试结果似乎指示存在脆弱性，因为应用程序未正确认证用户，并且响应包含了 JSON 格式。

测试请求和响应：

```
GET /xmjg/supervisionInspection/getProvinceTopFive.do?province=660000&startDate=2020-01-
01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US
```

```
HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:27 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "XZQHDM": "660100",
         "BYXZRKS": 160,
         "NAME": "       一师阿拉尔市"
 },
        {
         "XZQHDM": "660800",
         "BYXZRKS": 92,
         "NAME": "       八师石河子市"
 },
        {
         "XZQHDM": "660300",
         "BYXZRKS": 88,
         "NAME": "       三师图木舒克市"
 },
        {
         "XZQHDM": "661300",
         "BYXZRKS": 83,
         "NAME": "       十三师"
 },
        {
         "XZQHDM": "660400",
         "BYXZRKS": 65,
         "NAME": "       四师可克达拉市"
        }
]
```

问题 2 / 8

TOC

JavaScript 劫持	
严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/getYsTotalOfMultidimensional.do
实体：	getYsTotalOfMultidimensional.do (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	应用程序使用的认证方法不充分
固定值：	拒绝恶意请求并防止直接执行 JavaScript 响应

差异： **标题** `Referer` 从以下位置进行控制：`http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879`
至：`http://bogus.referer.hcl.com`
标题 `X-Requested-With` 已从请求除去：`XMLHttpRequest`
标题 `Accept` 从以下位置进行控制：`application/json, text/javascript, */*; q=0.01` 至：`*/*`

推理： 测试结果似乎指示存在脆弱性，因为应用程序未正确认证用户，并且响应包含了 JSON 格式。

测试请求和响应：

```
GET /xmjg/supervisionInspection/getYsTotalOfMultidimensional.do?xzqhdm=660000&startDate=2020-01-
01&endDate=2020-12-29&spysDy0= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 280
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:37 GMT
Content-Type: text/plain;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

[{"index":0,"spjds":[{"spjd":1,"pjys":6,"zcys":129,"kdys":32},
{"spjd":2,"pjys":5,"zcys":14,"kdys":20},{"spjd":3,"pjys":3,"zcys":39,"kdys":23},
{"spjd":4,"pjys":5,"zcys":18,"kdys":12},{"spjd":5,"pjys":0,"zcys":0,"kdys":0}],"bxtj":
{"pjys":0,"zcys":0,"kdys":0},"zpjys":19,"zkdys":87}]
```

问题 3 / 8

TOC

JavaScript 劫持

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/city-page/getCountyMapData.do
实体：	getCountyMapData.do (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	应用程序使用的认证方法不充分
固定值：	拒绝恶意请求并防止直接执行 JavaScript 响应

差异： **标题** `Referer` 从以下位置进行控制：
`http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29`
至： `http://bogus.referer.hcl.com`
标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Accept` 从以下位置进行控制： `application/json, text/javascript, */*; q=0.01` 至：
`*/*`

推理： 测试结果似乎指示存在脆弱性，因为应用程序未正确认证用户，并且响应包含了 JSON 格式。

测试请求和响应：

```
GET /xmjg/city-page/getCountyMapData.do?xzqhdm=660100&tjfs=xmsl&startDate=&endDate= HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:30 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "province": "660000",
         "city": "660100",
         "districtType": "area ",
         "name": "        一师阿拉尔市",
         "id": "660100",
         "value": 187
        }
]
```

问题 4 / 8

TOC

JavaScript 劫持

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/bsc/dic/code/lgetItemsByTypeCode.do
实体：	lgetItemsByTypeCode.do (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	应用程序使用的认证方法不充分
固定值：	拒绝恶意请求并防止直接执行 JavaScript 响应

差异： **标题** `Referer` 从以下位置进行控制：
`http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29`
至： `http://bogus.referer.hcl.com`
标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Accept` 从以下位置进行控制： `application/json, text/javascript, */*; q=0.01` 至： `*/*`

推理： 测试结果似乎指示存在脆弱性，因为应用程序未正确认证用户，并且响应包含了 JSON 格式。

测试请求和响应：

```
GET /xmjg/bsc/dic/code/lgetItemsByTypeCode.do?typeCode=TJ_DATE_CONFIG&flag=false HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:34 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "label": "2020       年1月1日-至今",
         "value": "nowYearStart&nowDate",
         "children": null,
         "id": "bf687bbc-f054-461c-b9f5-12d92491c3f7"
 },
        {
         "label": "2018       年6月1日-至今",
         "value": "initStartDate&nowDate",
         "children": null,
         "id": "04c3a943-937d-465d-b9bf-86ee458903c5"
 },
        {
         "label": "2018       年6月1日-2019年12月31日",
         "value": "initStartDate&2019-12-31",
         "children": null,
         "id": "20fdc7d0-a21e-4d64-b77f-be6681b68652"
        }
]
```

问题 5 / 8

TOC

JavaScript 劫持

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/getAllPjysByTjjssj.do
实体：	getAllPjysByTjjssj.do (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	应用程序使用的认证方法不充分
固定值：	拒绝恶意请求并防止直接执行 JavaScript 响应

差异： **标题** `Referer` 从以下位置进行控制：

```
http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29
```

至： `http://bogus.referer.hcl.com`

标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

标题 `Accept` 从以下位置进行控制： `application/json, text/javascript, */*; q=0.01` 至：

`*/*`

推理： 测试结果似乎指示存在脆弱性，因为应用程序未正确认证用户，并且响应包含了 JSON 格式。

测试请求和响应：

```
GET /xmjg/supervisionInspection/getAllPjysByTjjssj.do?xzqhdm=660100&startDate=2020-01-
01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 276
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:45 GMT
Content-Type: text/plain;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

[{"index":0,"spjds":[{"spjd":1,"pjys":7,"zcys":23,"kdys":42},
{"spjd":2,"pjys":6,"zcys":9,"kdys":18},{"spjd":3,"pjys":2,"zcys":5,"kdys":18},
{"spjd":4,"pjys":2,"zcys":2,"kdys":10},{"spjd":5,"pjys":5,"zcys":8,"kdys":7}],"bxtj":
{"pjys":5,"zcys":8,"kdys":7},"zpjys":22,"zkdys":95}]
```

问题 6 / 8

TOC

JavaScript 劫持	
严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/city-page/getDataListOfSplcbm.do
实体：	getDataListOfSplcbm.do (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	应用程序使用的认证方法不充分
固定值：	拒绝恶意请求并防止直接执行 JavaScript 响应

差异： **标题** `Referer` 从以下位置进行控制：
`http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29`
至： `http://bogus.referer.hcl.com`
标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Accept` 从以下位置进行控制： `application/json, text/javascript, */*; q=0.01` 至：
`*/*`

推理： 测试结果似乎指示存在脆弱性，因为应用程序未正确认证用户，并且响应包含了 JSON 格式。

测试请求和响应：

```
GET /xmjg/city-page/getDataListOfSplcbm.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:44 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "PJZYS": 8,
         "SPLCBM": "5e6d7d7b-be47-4092-b8d9-c873cd74a8ae",
         "SPLCMC": "       政府投资城市基础设施工程类项目",
         "YRUXMS": 58,
         "YQXMS": 2
 },
        {
         "PJZYS": 7,
         "SPLCBM": "d4ba4952-9be6-4a10-9431-7a099bf5e783",
         "SPLCMC": "       政府投资房屋建筑类项目",
         "YRUXMS": 34,
         "YQXMS": 1
 },
        {
         "PJZYS": 4,
         "SPLCBM": "d21d7468-ca0c-478c-b700-e086340478e0",
         "SPLCMC": "       一般社会投资项目（不含带方案出让用地项目和小型社会投资项目）",
         "YRUXMS": 61,
         "YQXMS": 1
 },
        {
         "PJZYS": 10,
         "SPLCBM": "0cce535b-bc83-4a61-be72-3d151e1a16e1",
         "SPLCMC": "       社会投资小型工程项目",
         "YRUXMS": 6,
         "YQXMS": 0
 },
        {
         "PJZYS": 2,
         "SPLCBM": "92c57c71-4a4a-4768-8888-97efcae9d5c4",
         "SPLCMC": "       含带方案出让用地的社会投资项目",
         "YRUXMS": 1,
         "YQXMS": 0
        }
]
```

问题 7 / 8

TOC

JavaScript 劫持

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/city/getMDAllSpjd.do
实体：	getMDAllSpjd.do (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	应用程序使用的认证方法不充分
固定值：	拒绝恶意请求并防止直接执行 JavaScript 响应

差异： **标题** `Referer` 从以下位置进行控制：
`http://127.0.0.1:8000/xmjg//csrk/oneSystemByMd.do?city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29&provinceCode=`
至： `http://bogus.referer.hcl.com`
标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`
标题 `Accept` 从以下位置进行控制： `application/json, text/javascript, */*; q=0.01` 至：
`*/*`

推理： 测试结果似乎指示存在脆弱性，因为应用程序未正确认证用户，并且响应包含了 JSON 格式。

测试请求和响应：

```
GET /xmjg/city/getMDAllSpjd.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-31 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:49:53 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

[
        {
         "xmFlag": "YES",
         "spjdXmzs": [
                        {
                         "smzqCount": 4,
                         "SPJD": null,
                         "ybSmzqCount": 19,
                         "ybApprovalCount": 0,
                         "approvalCount": 0
                 }       ,
                        {
                         "smzqCount": 10,
                         "SPJD": 1,
                         "ybSmzqCount": 50,
                         "ybApprovalCount": 0,
                         "approvalCount": 1
                 }       ,
                        {
                         "smzqCount": 7,
                         "SPJD": 2,
                         "ybSmzqCount": 43,
                         "ybApprovalCount": 1,
                         "approvalCount": 0
                 }       ,
                        {
                         "smzqCount": 5,
                         "SPJD": 3,
                         "ybSmzqCount": 38,
                         "ybApprovalCount": 1,
                         "approvalCount": 0
                 }       ,
                        {
                         "smzqCount": 1,
                         "SPJD": 4,
                         "ybSmzqCount": 1,
                         "ybApprovalCount": 0,
                         "approvalCount": 1
                        }
         ]       ,
         "pjysFlag": "YES",
         "bzpjys": [
                        {
                         "BZJDZCYS_4": 2,
                         "BZJDZCYS_2": 9,
                         "BZJDZCYS_3": 5,
                         "BZJDPJYS_2": 2,
                         "BZJDPJYS_1": 3,
                         "BZJDPJYS_4": 1,
                         "BZJDPJYS_3": 1,
                         "BZJDZCYS_1": 23
                        }
                ]
        }
]
```

问题 8 / 8

TOC

JavaScript 劫持

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/getPjysByTjjssj.do
实体：	getPjysByTjjssj.do (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	应用程序使用的认证方法不充分
固定值：	拒绝恶意请求并防止直接执行 JavaScript 响应

差异： **标题** `Referer` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg//supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?averageTime=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&provinceCode=660000`
至： `http://bogus.referer.hcl.com`
标题 `X-Requested-With` 已从请求除去： `XMLHttpRequest`

推理： 测试结果似乎指示存在脆弱性，因为应用程序未正确认证用户，并且响应包含了 JSON 格式。

测试请求和响应：

```
GET /xmjg/supervisionInspection/getPjysByTjjssj.do?xzqhdm=660000&startDate=2020-01-
```

```
01&endDate=2020-12-29&spysDy0=0 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://bogus.referer.hcl.com
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 1710
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:54:57 GMT
Content-Type: text/plain;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

[{"index":0,"splclx":1,"splcmc":"政府投资工程建设项目（房屋建筑类）","spjds":
[{"spjd":1,"pjys":7,"zcys":41,"kdys":43},{"spjd":2,"pjys":5,"zcys":14,"kdys":28},
{"spjd":3,"pjys":3,"zcys":8,"kdys":30},{"spjd":4,"pjys":4,"zcys":6,"kdys":8},
{"spjd":5,"pjys":7,"zcys":21,"kdys":33}],"bxtj":
{"pjys":7,"zcys":21,"kdys":33},"zpjys":26,"zkdys":142},{"index":1,"splclx":2,"splcmc":"政府投资工程
建设项目（线性工程类）","spjds":[{"spjd":1,"pjys":6,"zcys":23,"kdys":32},
{"spjd":2,"pjys":4,"zcys":9,"kdys":26},{"spjd":3,"pjys":3,"zcys":7,"kdys":17},
{"spjd":4,"pjys":4,"zcys":11,"kdys":9},{"spjd":5,"pjys":7,"zcys":20,"kdys":28}],"bxtj":
{"pjys":7,"zcys":20,"kdys":28},"zpjys":24,"zkdys":112},{"index":2,"splclx":3,"splcmc":"一般社会投资
项目","spjds":[{"spjd":1,"pjys":5,"zcys":25,"kdys":48},{"spjd":2,"pjys":3,"zcys":9,"kdys":39},
{"spjd":3,"pjys":4,"zcys":9,"kdys":19},{"spjd":4,"pjys":8,"zcys":18,"kdys":15},
{"spjd":5,"pjys":5,"zcys":15,"kdys":36}],"bxtj":
{"pjys":5,"zcys":15,"kdys":36},"zpjys":25,"zkdys":157},{"index":3,"splclx":4,"splcmc":"小型社会投资
项目","spjds":[{"spjd":1,"pjys":3,"zcys":11,"kdys":48},{"spjd":2,"pjys":6,"zcys":13,"kdys":46},
{"spjd":3,"pjys":5,"zcys":12,"kdys":63},{"spjd":4,"pjys":4,"zcys":8,"kdys":21},
{"spjd":5,"pjys":4,"zcys":17,"kdys":49}],"bxtj":
{"pjys":4,"zcys":17,"kdys":49},"zpjys":22,"zkdys":227},{"index":4,"splclx":5,"splcmc":"带方案出让用
地的社会投资项目","spjds":[{"spjd":1,"pjys":3,"zcys":12,"kdys":71},
{"spjd":2,"pjys":0,"zcys":0,"kdys":0},{"spjd":3,"pjys":1,"zcys":1,"kdys":102},
{"spjd":4,"pjys":0,"zcys":0,"kdys":0},{"spjd":5,"pjys":6,"zcys":11,"kdys":32}],"bxtj":
{"pjys":6,"zcys":11,"kdys":32},"zpjys":10,"zkdys":205}]
```

低 查询中接受的主体参数 2 TOC

问题 1 / 2 TOC

查询中接受的主体参数

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/analysis-info!getHaveProjectCitys.action
实体：	analysis-info!getHaveProjectCitys.action (Page)
风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	请勿接受在查询字符串中发送的主体参数

差异： **主体参数** 已从请求除去： 1
查询参数 已添加至请求： 1
方法 从以下位置进行控制： POST 至： GET

推理： 测试结果似乎指示存在脆弱性，因为“测试响应”与“原始响应”类似，这表明应用程序处理了查询总提交的主体参数。

测试请求和响应：

```
GET /xmjg/analysis-info!getHaveProjectCitys.action?flag=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US


HTTP/1.1 200
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:47 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

{
 "result": "0",
 "data": [
                {
                 "XZQHDM": "660100",
                 "CNT": 279
         }       ,
                {
                 "XZQHDM": "660800",
                 "CNT": 162
         }       ,
                {
                 "XZQHDM": "660300",
                 "CNT": 152
         }       ,
                {
                 "XZQHDM": "661300",
                 "CNT": 152
         }       ,
                {
                 "XZQHDM": "660400",
                 "CNT": 112
```

```
          }        ,
                  {
                   "XZQHDM": "660700",
                   "CNT": 91
          }        ,
                  {
                   "XZQHDM": "661200",
                   "CNT": 87
          }        ,
                  {
                   "XZQHDM": "660200",
                   "CNT": 77
          }        ,
                  {
                   "XZQHDM": "660500",
                   "CNT": 69
          }        ,
                  {
                   "XZQHDM": "660900",
                   "CNT": 66
          }        ,
                  {
                   "XZQHDM": "661000",
                   "CNT": 66
          }        ,
                  {
                   "XZQHDM": "661400",
                   "CNT": 64
          }        ,
                  {
                   "XZQHDM": "660600",
                   "CNT": 48
                  }
         ]
}
```

问题 2 / 2

TOC

查询中接受的主体参数

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getAnalysisCityOverdueRankingData.do
实体：	getAnalysisCityOverdueRankingData.do (Page)
风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	请勿接受在查询字符串中发送的主体参数

差异： **主体参数** 已从请求除去： `2020-01-01`
查询参数 已添加至请求： `2020-01-01`
主体参数 已从请求除去： `2020-12-29`
查询参数 已添加至请求： `2020-12-29`
主体参数 已从请求除去： `1`
查询参数 已添加至请求： `1`
主体参数 已从请求除去： `660000`
查询参数 已添加至请求： `660000`

方法 从以下位置进行控制： POST 至： GET

推理： 测试结果似乎指示存在脆弱性，因为“测试响应”与“原始响应”类似，这表明应用程序处理了查询总提交的主体参数。

测试请求和响应：

```
GET /xmjg/supervisionInspectionDrill/getAnalysisCityOverdueRankingData.do?tjkssj=2020-01-
01&tjjssj=2020-12-29&orderByFlag=1&provinceCode=660000 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 127.0.0.1:8000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://127.0.0.1:8000
Referer: http://127.0.0.1:8000/xmjg//supervisionInspectionDrill/analysis-ranking-overdue.do?
provinceCode=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 1258
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:54:45 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

{
 "result": "0",
 "data": [
                {
                 "OVERDUE_PER": 26.14,
                 "XZQHDM": "660300",
                 "OVERDUE_CNT": 23,
                 "TOTAL_CNT": 88,
                 "NAME": "       三师图木舒克市"
         }       ,
                {
                 "OVERDUE_PER": 25,
                 "XZQHDM": "660600",
                 "OVERDUE_CNT": 7,
                 "TOTAL_CNT": 28,
                 "NAME": "       六师五家渠市"
         }       ,
                {
                 "OVERDUE_PER": 13.51,
                 "XZQHDM": "660200",
                 "OVERDUE_CNT": 5,
                 "TOTAL_CNT": 37,
                 "NAME": "       二师铁门关市"
         }       ,
                {
                 "OVERDUE_PER": 13.16,
                 "XZQHDM": "660500",
                 "OVERDUE_CNT": 5,
                 "TOTAL_CNT": 38,
                 "NAME": "       五师双河市"
         }       ,
                {
                 "OVERDUE_PER": 9.3,
                 "XZQHDM": "660900",
                 "OVERDUE_CNT": 4,
                 "TOTAL_CNT": 43,
                 "NAME": "       九师"
         }       ,
                {
                 "OVERDUE_PER": 8.16,
                 "XZQHDM": "660700",
                 "OVERDUE_CNT": 4,
                 "TOTAL_CNT": 49,
                 "NAME": "       七师胡杨河市"
         }       ,
                {
                 "OVERDUE_PER": 7.61,
                 "XZQHDM": "660800",
                 "OVERDUE_CNT": 7,
                 "TOTAL_CNT": 92,
                 "NAME": "       八师石河子市"
         }       ,
                {
                 "OVERDUE_PER": 6.15,
                 "XZQHDM": "660400",
                 "OVERDUE_CNT": 4,
                 "TOTAL_CNT": 65,
                 "NAME": "       四师可克达拉市"
         }       ,
                {
                 "OVERDUE_PER": 5,
                 "XZQHDM": "661400",
                 "OVERDUE_CNT": 2,
                 "TOTAL_CNT": 40,
                 "NAME": "       十四师昆玉市"
         }       ,
                {
                 "OVERDUE_PER": 2.5,
                 "XZQHDM": "660100",
                 "OVERDUE_CNT": 4,
                 "TOTAL_CNT": 160,
                 "NAME": "       一师阿拉尔市"
         }       ,
                {
                 "OVERDUE_PER": 1.2,
                 "XZQHDM": "661300",
                 "OVERDUE_CNT": 1,
                 "TOTAL_CNT": 83,
                 "NAME": "       十三师"
         }       ,
                {
                 "OVERDUE_PER": 0,
                 "XZQHDM": "661000",
                 "OVERDUE_CNT": 0,
                 "TOTAL_CNT": 37,
                 "NAME": "       十师北屯市"
         }       ,
                {
                 "OVERDUE_PER": 0,
                 "XZQHDM": "661200",
                 "OVERDUE_CNT": 0,
                 "TOTAL_CNT": 51,
                 "NAME": "       十二师"
                }
        ]
}
```

低 发现 Web 应用程序源代码泄露模式 1 TOC

问题 1 / 1 TOC

发现 Web 应用程序源代码泄露模式

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	xmjg-statis-show!getSkipPage.action (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	未安装第三方产品的最新补丁或最新修订程序 在生产环境中留下临时文件 程序员在 Web 页面上留下调试信息
固定值：	除去 web-server 中的源代码文件并应用任何相关补丁

差异：

推理： 响应包含可能会泄露有关站点和应用程序逻辑的敏感信息的脚本文件源代码。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
```

```
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    ba
...
...
...

                 </span>

        </div>
       </div>  -->
           <!--<%&#45;&#45; <div class="smzq" style="border: 1px solid #d3e3f3;height:
180px;width:100%;">-->
                 <!--<h2><span>       项目生命周期</span></h2>-->
                 <!--<div style="float:left;margin-left:1%;width:100%;">-->
                         <!--&lt;!&ndash;        工程规划许可 &ndash;&gt;-->
                         <!--<div id="label" style="float:left;height:100px;margin-
top:25px;width:20%;" onclick="clickSmzq('1','立项用地规划许可阶段')"></div>-->
...
...
...

         </div>
 </div>
    <!--main_left End-->

 <!--       <%&#45;&#45; <div class="main_right"-->
         <!--style="width:27%;float: right;min-width       : 700px;margin-top: -35px;margin-
right:1%;">-->
         <!--&lt;!&ndash;content_tab&ndash;&gt;-->
         <!--<div class="content_tab"></div>-->
         <!--&lt;!&ndash;content_box End&ndash;&gt;-->
...
...
...
```

低 发现数据库错误模式 1 TOC

问题 1 / 1 TOC

发现数据库错误模式

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8090/opus-front-sso/oauth/authorize
实体：	client_id (Global)
风险：	可能会查看、修改或删除数据库条目和表
原因：	未对用户输入正确执行危险字符清理
固定值：	查看危险字符注入的可能解决方案

差异： **参数** `client_id` 从以下位置进行控制： `xmjg` 至：

```
/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%
uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/boot.ini
```

推理： 测试结果似乎指示存在脆弱性，因为响应包含 SQL Server 错误。这表明测试设法通过注入危险字符穿透了应用程序并到达 SQL 查询本身。

测试请求和响应：

```
GET /opus-front-
sso/oauth/authorize?client_id=/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%
uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/%uff0e%uff0e/boot.in
i&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=tba1ER HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/form
Cookie: JSESSIONID=24E80C5845F452C87C1B10300BEF316D
Connection: Keep-Alive
Host: 127.0.0.1:8090
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 500
Content-Length: 757
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Connection: close
Date: Tue, 29 Dec 2020 02:55:37 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

<html><body><h1>Whitelabel Error Page</h1><p>This application has no explicit mapping for /error,
so you are seeing this as a fallback.</p><div id='created'>Tue Dec 29 10:55:37 CST 2020</div>
<div>There was an unexpected error (type=Internal Server Error, status=500).</div>
<div>PreparedStatementCallback; bad SQL grammar [select client_id, client_secret from
AGX_RS_CLOUD_SOFT where IS_ACTIVE = &#39;1&#39; AND IS_DELETED = &#39;0&#39; AND client_id = ?AND
IS_ADMIN = &#39;0&#39;]; nested exception is
com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: You have an error in your SQL syntax;
check the manual that corresponds to your MySQL server version for the right syntax to use near
&#39;IS_ADMIN = &#39;0&#39;&#39; at line 1</div></body></html>
```

低 跨帧脚本编制防御缺失或不安全 4 TOC

问题 1 / 4 TOC

跨帧脚本编制防御缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do
实体：	dg-jdkh-main.do (Page)
风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

差异：

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击

测试请求和响应：

```
GET /xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:03 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
<meta charset="utf-8" />
<title>效能督查</title>
<script type="text/javascript">
    var isWhite = '';
 //pc        版首页
    var ctx='/xmjg/';
    var name = '';
    var xzqhdm= "";
    var loginXzqhdm= "" ? "" : "china";
    var loginProvince = "" ? "" : "china";
   // var oldflag = "";
    var oldflag = "true";
 console.log(oldflag);
    var oldStartDate = "";
    var oldEndDate = "";
    var bigScreenFolder=""; //大屏css 目录，如果是普通屏（默认）则该值为空
    var provinceCode="";
    //var projectManager=parent.projectManager;
    var defaultEndDate="",defaultStartDate="";
    var provinceParam={};
    var params = "";
    var initHeartBeat ="";
    var initStartDate="";//获取配置文件中统计时间的配置参数
</script>
<!--    <th:block th:insert="adsfw/taglibs :: taglibs"/>-->
```

```
    <script src="/xmjg/common/tool/common-merge.js" ></script>
    <link href="/xmjg/common/tool/date/css/bootstrap.min.css" rel="stylesheet" type="text/css"/>
 <link href="/xmjg/xmjg/supervisionInspection/css/element.css" rel="stylesheet"
type="text/css"/>
 <!--<link th:href="@{/xmjg/xndc/css/dg-jdkh-main.css}" href="${ctx}/xmjg/xndc/css/dg-
jdkh-main.css" rel="stylesheet" type="text/css"/>-->
 <link href="/xmjg/xmjg/supervisionInspection/css/dg-jdkh-main-rem.css" rel="stylesheet"
type="text/css"/>
 <!--<link rel="stylesheet" href="/framework-
ui/src/main/resources/static/agcloud/framework/ui-private/common/element-2/element.css"
th:href="@{/agcloud/framework/ui-private/common/element-2/element.css}">-->
 <!-- jquery -->
    <!--<script th:src="@{/xmjg/js/jquery.min.js}" type="text/javascript" charset="utf-8">
</script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js"
type="text/javascript" charset="utf-8"></script>
 <script src="/xmjg/common/tool/date/js/bootstrap.min.js" type="text/javascript"
charset="utf-8"></script>
 <link   href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
 <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/numberAnimate.js"
type="text/javascript"></script>
 <!--<script th:src="@{/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js}"
src="${ctx}/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js" type="text/javascript"></script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/dg-jdkh-main.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/echarts.min.js" type="text/javascript"
charset="utf-8"></script>
 <!--<script th:src="@{/common/tool/date/js/dateQuery.js}" type="text/javascript"
charset="utf-8"></script>-->

 <!--        城市选择插件  开始 -->
 <link   href="/xmjg/common/tool/cityselect/css/city_select.css" rel="stylesheet"
type="text/css" />
 <script src="/xmjg/common/tool/cityselect/js/city_data.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/common/tool/cityselect/js/areadata.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/common/tool/cityselect/js/auto_area.js" type="text/javascript"
charset="utf-8"></script>
 <!--        城市选择插件  结束 -->

<script type="text/javascript">
    var date = new Date();
 var dateStr =    date.getFullYear() + "-" + ("0" + (date.getMonth() + 1)).slice(-2) + "-
"+ ("0" + (date.getDate())).slice(-2);
 var startTime = dateStr.substr(0,5)+"01-01";
 var endDateStr = dateStr;
    Date.prototype.format = function(fmt) {
        var o = {
          "M+" : this.getMonth()+1,          //月份
          "d+" : this.getDate(),          //日
          "h+" : this.getHours(),          //小时
          "m+" : this.getMinutes(),          //分
          "s+" : this.getSeconds(),          //秒
          "q+" : Math.floor((this.getMonth()+3)/3), //季度
          "S"  : this.getMilliseconds()          //毫秒
        };
        if(/(y+)/.test(fmt)) {
          fmt=fmt.replace(RegExp.$1, (this.getFullYear()+"").substr(4 - RegExp.$1.length));
        }
        for(var k in o) {
          if(new RegExp("("+ k +")").test(fmt))
...
...
...
```

问题 2 / 4

TOC

跨帧脚本编制防御缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do
实体：	getCityProjectList.do (Page)
风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

差异：

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击

测试请求和响应：

```
GET /xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-
01&tjjssj=2020-12-29&dateEnd=2020-12-
29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=210
2&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pa
geNo=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//city-page/getCityProjectList.do?
xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-
29&bigScreenFolder=&dateEnd=2020-12-29&splclx=
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:26 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN" xmlns="http://www.w3.org/1999/xhtml">
 <head>
         <meta charset="utf-8" />
         <title>       各城市各阶段数据233</title>
         <script type="text/javascript">
          var ctx='/xmjg/';
                 var bigScreenFolder="";
                 var xzqhdms="";
                 var tjkssj="2020-01-01";
                 var tjjssj="2020-12-29";
                 var orderByFlag="";
                 var dataType="8";
                 var sfzb="";
                 var sfbyxz="";
                 var sfjgqqxt="";
                 var spjd="";
                 var blqk="";
                 var splclx="";
                 var splcmc="";
                 var sfyq="";
                 var tjTypeVal="";
                 var qtTypeVal = "";
                 var splcbm="";
                 var dateEnd = "2020-12-29";
                 var provinceCode="";
                 var dataType="8";  //1:       各阶段平均用时（审批用时）; 2:各阶段跨度用时; 3:各阶段最长
用时; 4:各阶段平均受理次数;
                 var stageType="0"; //0       : 总数, 1: 立项用地规划许可; 2: 工程建设许可; 3: 施工许可;
4: 竣工验收
          var oldStartDate = "2020-01-01";
          var oldEndDate = "2020-12-29";
          var flag="1";
          var xzqhdm="660000"; //跳转带过来的行政区划代码 用于钻取标题显示
          var name="";//跳转带过来的城市名称 用于钻取标题显示
                 var sfType = "";//       算法类型
         </script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/bootstrap.min.css"/>
         <!--<script  th:src="@{/xmjg/xndc/js/jquery.min.js}"
src="${ctx}/xmjg/xndc/js/jquery.min.js"  type="text/javascript"  charset="utf-8"></script>-->
         <script src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap.min.js"  type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
         <link href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css"
title="" rel="stylesheet"/>
         <link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global-rem.css"
type="text/css"></link>
         <script  src="/xmjg/xmjg/xndc/js/echarts.min.js" type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/resources/js/common/validate.js" type="text/javascript">
</script>
         <script  src="/xmjg/resources/js/common/public.js" type="text/javascript">
</script>
         <!--<script  th:src="@{/xmjg/xndc/js/analysis/analysis-project-stage-list.js}"
```

```
src="${ctx}/xmjg/xndc/js/analysis/
...
...
...
```

问题 3 / 4

TOC

跨帧脚本编制防御缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do
实体：	getSupervisionInspectionDrillPage.do (Page)
风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

差异：

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击

测试请求和响应：

```
GET /xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?
provinceCode=660000&dataType=8&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-
29&bigScreenFolder=&dateEnd=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:50 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<html>
 <head>
         <meta charset="utf-8" />
         <title>       各城市各阶段数据</title>
         <script type="text/javascript">
                 var ctx='/xmjg/';
                 var bigScreenFolder="";
                 var tjkssj="2020-01-01";
                 var tjjssj="2020-12-29";
                 var dateEnd = "2020-12-29";
                 var provinceCode="660000";
                 var dataType="8";  //1:      各城市各阶段平均用时（审批用时）; 2:各城市各阶段跨度用时;
3:各城市各阶段最长用时; 4:各城市各阶段平均受理次数;5:本月新增项目数
                 var stageType="0"; //0      : 总数，1：立项用地规划许可；2：工程建设许可；3：施工许可；
4：竣工验收
                 var splclx="";
                 var splcmc="";
                 var sfType="";  //      算法类型
         </script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>





                         <link rel="stylesheet" type="text/css"
href="/xmjg/xmjg/supervisionInspection/css/analysis-index-rem.css"/>
                         <link rel="stylesheet" type="text/css"
href="/xmjg/xmjg/supervisionInspection/css/analysis-statistics-rem.css"/>


         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/bootstrap.min.css"/>
         <!--<script  th:src="@{/xmjg/xndc/js/jquery.min.js}"
src="/xmjg/xmjg/xndc/js/jquery.min.js"  type="text/javascript"  charset="utf-8"></script>-->
         <script src="/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js"
type="text/javascript" charset="utf-8"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap.min.js"  type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
         <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
         <link href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css"
title="" rel="stylesheet"/>
         <script  src="/xmjg/xmjg/supervisionInspection/js/echarts.min.js"
type="text/javascript"  charset="utf-8"></script>
 <!--        图表柱状图展示操作 -->
         <script  src="/xmjg/xmjg/xndc/js/common-charts.js" type="text/javascript"
```

```
charset="utf-8"></script>
         <!--         城市选择插件   开始 -->
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/cityselect/css/city_select.css"/>
         <script src="/xmjg/common/tool/cityselect/js/city_data.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/cityselect/js/areadata.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/tool/cityselect/js/auto_area.js" type="text/javascript"
charset="utf-8"></script>
         <!--         城市选择插件   结束 -->
         <!--         时间查询控件 开始 -->
         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/dateQuery.css"/>
         <script src="/xmjg/common/tool/date/js/dateQuery.js" type="text/javascript"
charset="utf-8"></script>
         <script src="/xmjg/common/
...
...
...
```

问题 4 / 4

TOC

跨帧脚本编制防御缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	xmjg-statis-show!getSkipPage.action (Page)
风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

差异：

推理： AppScan 检测到 X-Frame-Options 响应头缺失或具有不安全值，这可能会造成跨帧脚本编制攻击

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
```

```
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
}
.bacckbutton {
    float: right;
    margin: 3px 10px 5px 10px;
    width: 96px;
    height: 32px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
    }
 .dghy-itemWrap {
         float:left;
         margin-left:1%;
         width:19%;
         height:174px;
        }
</style>
<script type="text/javascript">
 var
...
...
...
```

低 自动填写未对密码字段禁用的 HTML 属性 1

TOC

问题 1 / 1

TOC

自动填写未对密码字段禁用的 HTML 属性

严重性：	低
CVSS 分数：	5.0
URL：	http://127.0.0.1:8090/opus-front-sso/authentication/require
实体：	require (Page)
风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

差异：

推理： AppScan 发现密码字段没有强制禁用自动填写功能。

测试请求和响应：

```
GET /opus-front-sso/authentication/require HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Cookie: JSESSIONID=D6A5925ADA251562D8C32F08668AA5EE
Connection: keep-alive
Host: 127.0.0.1:8090
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:44:19 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
 <meta charset="utf-8" />
 <title>       工程建设项目审批管理平台</title>
 <meta name="description" content="Latest updates and statistic charts"/>
 <meta http-equiv="X-UA-Compatible" content="IE=edge"/>
 <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"/>
 <link rel="shortcut icon"  href="/opus-front-sso/images/guohui.png" type="image/x-icon"/>
 <link rel="icon"  href="/opus-front-sso/images/guohui.png" type="image/x-icon" />
 <link href="/opus-front-sso/css/global.css" rel="stylesheet" type="text/css">
 <link href="/opus-front-sso/css/login_new.css" rel="stylesheet" type="text/css">
 <link href="/opus-front-sso/css/layui.css" rel="stylesheet" type="text/css">
 <script src="/opus-front-sso/js/jquery-3.4.1.min.js"></script>
 <script src="/opus-front-sso/js/jquery.validate.min.js"></script>
 <script src="/opus-front-sso/js/layui.all.js"></script>
 <script>
        var ctx = '/opus-front-sso/';
        var verifyCodeIsOpen = '${verifyCodeIsOpen}';

        //设置高亮(对象,位置)
        function setCaret(textbox,start){
          try{
          if(textbox.createTextRange){
          var r=textbox.createTextRange();
          r.moveStart('character',start);
          r.select();
          }else if(textbox.setSelectionRange){
          textbox.setSelectionRange(0,textbox.value.length);
          textbox.focus();
          }
          }catch(e){}
        }

        function getPic(){

          $('#verifyCodeImg').attr("src", ctx + 'code/image?time1='+ new Date().getTime());
        }

        function checkPwd() {

          var layer ;
          layui.use('layer', function(){
          layer = layui.layer;
          });
          var reg = new RegExp(/^[0-9]+.?[0-9]*$/);//工作密码是否是数字串
          var pwd = $('#password_text').val().trim();
          if  (pwd.length < 8 || reg.test(pwd)){

          layer.msg('密码过于简单，请登录后进行修改！', {time: 2000, icon:6});
          }
        }
 </script>
</head>
<body id="cas">
<div id="main" style="width: 100%;height: 100%;">


<!--系统登录界面-->
<div class="login-logo">
 <div class="ts-logo float-left">
         <img src="/opus-front-sso/images/login_logo.png">
 </div>
</div>
<div class="login-bg"></div>
<div id="login-main">
<form id="login_form" action="/opus-front-sso/authentication/form" method="post">
 <div class="login-content" style="display: none;">
<!--            <div class="m-login__logo">
                 <span class="pro-logo-name">       工程建设项目审批管理平台</span>
         </div> -->
         <div class="login01">

                 <       d
...
...
...

                                 <input id="username" type="hidden" name="username"/>
                         </li>
                         <li       >
                                 <i class="userpassword"></i>
                                        <input id="password_text" class="input" tabindex="2"
onfocus="setCaret(this,0)" accesskey="p" placeholder="密  码" type="password" value="" size="25">
                                 <input id="password" type="hidden" name="password"/>
                                 <input id="proPassword" type="hidden"
name="proPassword"/>
                                 <input id="orgId" type="hidden" name="orgId"/>
                                 <input id="resetPasswordId" type="hidden"
name="resetPasswordId"/>
...
...
...

<form id="editPassword" class="layui-form" action="">
 <div class="layui-form-item" style="margin-top: 30px;">
```

```
         <label class="layui-form-label" style="width: 30%">       原密码：</label>
         <div class="layui-input-block" >
                        <input type="password" name="oldPassword" lay-
verify="required|oldPassword"  class="layui-input" style="width: 80%">
         </div>
 </div>
 <div class="layui-form-item">
         <label class="layui-form-label"style="width: 30%" >       新密码：</label>
         <div class="layui-input-block" >
                        <input type="password" name="newPassword" lay-verify="newPassword"
class="layui-input"  style="width: 80%">
         </div>
 </div>

 <div class="layui-form-item">
         <label class="layui-form-label"style="width: 30%;" >       再次输入新密码：</label>
         <div class="layui-input-block" >
                        <input type="password" name="newPasswordCheck" lay-
verify="newPasswordCheck" class="layui-input"  style="width: 80%">
         </div>
 </div>
</form>
</div>
...
...
...
```

参 HTML 注释敏感信息泄露 33 TOC

问题 1 / 33 TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
实体：	<link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-schemes/dark-blue/css/index-... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/opus/front/blue/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/login?code=Hu24Qr&state=tba1ER
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: Keep-Alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:10:15 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!--@Author: ZL-->
<!--@Date:   2019/5/14-->
<!--@Last Modified by:   ZL-->
<!--@Last Modified time: $ $-->
<!DOCTYPE html>
<html lang="zh-CN">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <!--<title>国家工程建设项目审批监管信息系统</title>-->
<!--  <th:block th:insert="adsfw/taglibs :: taglibs"/>-->
  <script>
    var isWhite = '';
  </script>
  <script src="/xmjg/common/tool/common-merge.js" ></script>
  <link rel="shortcut icon" href="/xmjg/agcloud/framework/ui-schemes/dark-
blue/images/system_guohui.png" type="image/x-icon"/>
  <link rel="icon" href="/xmjg/agcloud/framework/ui-schemes/dark-blue/images/system_guohui.png"
type="image/x-icon" />
  <link rel="stylesheet" href="/xmjg/agcloud/framework/js-lib/element-2/element.css"/>
  <!--<link rel="stylesheet" href="../../../../../static/agcloud/framework/icon-lib/agcloud-
fonts/iconfont.css" th:href="@{/agcloud/framework/icon-lib/agcloud-fonts/iconfont.css}">
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css" th:href="@{/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css}">-->
<!--
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/css/index-rem.css" th:href="@{/agcloud/framework/ui-schemes/dark-blue/css/index-rem.css}">
-->

    <style>
        /*
* @Author: ZL
* @Date:   2019/5/14
* @Last Modified by:   ZL
* @Last Modified time: $ $
*/
/*字体字号初始化*/
html,body,.btn,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title .m-
portlet__head-text,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title
.m-portlet__head-text small,.form-control{
    font-family: Microsoft YaHei,Helvetica Neue,Helvetica,PingFang SC,Hiragino Sans
GB,SimSun,sans-serif;
}

html, body{
    font-size: .14rem;
    color: #474747;
    margin: 0;
    padding: 0;
    background: #1b2538;
}
* {
    margin: 0;
    padding: 0;
    box-sizing: border-box;
    text-decoration: none;
}
ul,li {
    list-style: none;
}
a:hover {
    text-decoration: none;
}
.fl {
    float: left;
}
.fr {
    float: right;
}
.clearfix {
    zoom: 1;
}
.clearfix:before, .clearfix:after {
    content: "";
    display: table;
}
.clearfix:after {
    clear: both;
}
[v-cloak] {
    display: none;
}
.el-badge__content {
    border: none;
}
```

```
.protal-header {
    width: 100%;
    height: .69rem;
    line-height: .69rem;
    z-index: 99;
    position: fixed;
    top: 0;
    color: #fff;
    background: -webkit-linear-gradient(top,#243860, #223251);
    background: -o-linear-gradient(top,#243860, #223251);
    background: -moz-linear-gradient(top,#243860, #223251);
    background: linear-gradient(top,#243860, #223251);
    background: -ms-linear-gradient(top,#243860, #223251);/* IE 10 */
    filter: progid:DXImageTransform.Microsoft.gradient(GradientType=0, startColorstr=#243860,
endColorstr=#223251);
    -ms-filter: "progid:DXImageTransform.Microsoft.gradient (GradientType=0,
startColorstr=#243860, endColorstr=#223251)";
    box-shadow: 0 0 10px rgba(0,0,0,.2);
}
.subsystem-logo {
    width: 6.20rem;
    height: .69rem;
    float: left;
    background: url(/xmjg//agcloud/framework/ui-schemes/dark-blue/css/images/system_name.png)
15px center no-repeat;
}
.subsystem-div {
    /*width: 32%;*/
    /*width: 5.9rem;*/
    width: calc(30vw);
    height: .69rem;
    float: left;
    overflow: hidden;
    text-overflow: ellipsis;
    white-space: nowrap;
}
.subsystem-div span {
    color: white;
    font-size: .28rem;
}
.subsystem-guohui-logo {
    width: .70rem;
    height: .69rem;
    float: left;
    background: url(/xmjg//agcloud/framework/ui-schemes/dark-blue/css/images/system_guohui.png)
.15rem center no-repeat;
}
.header-menu {
   /* width: 52%;*/
    width: calc(50vw);/*8.8rem;*/
    height: .69rem;
    overflow: hidden;
}

.header-menu_nav .header-menu_item {
    float: left;
    min-width: calc(5.2vw);
    height: .69rem;
    display: bl
...
...
...
```

问题 2 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
实体：	<img src="../../../../../static/agcloud/framework/ui-schemes/dark-blue/images/help.png" th:src="@{/a... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/opus/front/blue/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/login?code=Hu24Qr&state=tba1ER
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: Keep-Alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:10:15 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!--@Author: ZL-->
<!--@Date:   2019/5/14-->
<!--@Last Modified by:   ZL-->
<!--@Last Modified time: $ $-->
<!DOCTYPE html>
<html lang="zh-CN">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <!--<title>国家工程建设项目审批监管信息系统</title>-->
<!--  <th:block th:insert="adsfw/taglibs :: taglibs"/>-->
  <script>
    var isWhite = '';
  </script>
  <script src="/xmjg/common/tool/common-merge.js" ></script>
  <link rel="shortcut icon" href="/xmjg/agcloud/framework/ui-schemes/dark-
blue/images/system_guohui.png" type="image/x-icon"/>
  <link rel="icon" href="/xmjg/agcloud/framework/ui-schemes/dark-blue/images/system_guohui.png"
type="image/x-icon" />
  <link rel="stylesheet" href="/xmjg/agcloud/framework/js-lib/element-2/element.css"/>
  <!--<link rel="stylesheet" href="../../../../../static/agcloud/framework/icon-lib/agcloud-
fonts/iconfont.css" th:href="@{/agcloud/framework/icon-lib/agcloud-fonts/iconfont.css}">
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css" th:href="@{/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css}">-->
<!--
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/css/index-rem.css" th:href="@{/agcloud/framework/ui-schemes/dark-blue/css/index-rem.css}">
```

```
-->

    <style>
        /*
* @Author: ZL
* @Date:   2019/5/14
* @Last Modified by:   ZL
* @Last Modified time: $ $
*/
/*字体字号初始化*/
html,body,.btn,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title .m-portlet__head-text,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title .m-portlet__head-text small,.form-control{
    font-family: Microsoft YaHei,Helvetica Neue,Helvetica,PingFang SC,Hiragino Sans GB,SimSun,sans-serif;
}

html, body{
    font-size: .14rem;
    color: #474747;
    margin: 0;
    padding: 0;
    background: #1b2538;
}
* {
    margin: 0;
    padding: 0;
    box-sizing: border-box;
    text-decoration: none;
}
ul,li {
    list-style: none;
}
a:hover {
    text-decoration: none;
}
.fl {
    float: left;
}
.fr {
    float: right;
}
.clearfix {
    zoom: 1;
}
.clearfix:before, .clearfix:after {
    content: "";
    display: table;
}
.clearfix:after {
    clear: both;
}
[v-cloak] {
    display: none;
}
.el-badge__content {
    border: none;
}

.protal-header {
    width: 100%;
    height: .69rem;
    line-height: .69rem;
    z-index: 99;
    position: fixed;
    top: 0;
    color: #fff;
    background: -webkit-linear-gradient(top,#243860, #223251);
    background: -o-linear-gradient(top,#243860, #223251);
    background: -moz-linear-gradient(top,#243860, #223251);
    background: linear-gradient(top,#243860, #223251);
    background: -ms-linear-gradient(top,#243860, #223251);/* IE 10 */
    filter: progid:DXImageTransform.Microsoft.gradient(GradientType=0, startColorstr=#243860, endColorstr=#223251);
    -ms-filter: "progid:DXImageTransform.Microsoft.gradient (GradientType=0, startColorstr=#243860, endColorstr=#223251)";
    box-shadow: 0 0 10px rgba(0,0,0,.2);
}
```

```
.subsystem-logo {
    width: 6.20rem;
    height: .69rem;
    float: left;
    background: url(/xmjg//agcloud/framework/ui-schemes/dark-blue/css/images/system_name.png)
15px center no-repea
...
...
...

          <!--<img src="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/images/exit.png" th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/exit.png}"
alt="">-->
          </span>
          <span class="topbar-img" style="background: url(/xmjg/agcloud/framework/ui-
schemes/dark-blue/images/help.png)center center no-repeat ;;background-size:60% 60%">
          <a class="helpDoc" href="/xmjg/xmjg/file/工程建设项目审批管理系统操作手册.doc" download="工程
建设项目审批管理系统操作手册.doc"></a>
          <!--<img src="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/images/help.png" th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/help.png}"
alt="">-->
          </span>
        </div>
      </div>
    </header>
...
...
...
```

问题 3 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
实体：	<img v-if="userSex==0" src="../../../../../static/agcloud/framework/ui-schemes/dark-blue/images/user... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/opus/front/blue/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/login?code=Hu24Qr&state=tba1ER
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: Keep-Alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
```

```
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:10:15 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!--@Author: ZL-->
<!--@Date:   2019/5/14-->
<!--@Last Modified by:   ZL-->
<!--@Last Modified time: $ $-->
<!DOCTYPE html>
<html lang="zh-CN">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <!--<title>国家工程建设项目审批监管信息系统</title>-->
<!--  <th:block th:insert="adsfw/taglibs :: taglibs"/>-->
  <script>
    var isWhite = '';
  </script>
  <script src="/xmjg/common/tool/common-merge.js" ></script>
  <link rel="shortcut icon" href="/xmjg/agcloud/framework/ui-schemes/dark-
blue/images/system_guohui.png" type="image/x-icon"/>
  <link rel="icon" href="/xmjg/agcloud/framework/ui-schemes/dark-blue/images/system_guohui.png"
type="image/x-icon" />
  <link rel="stylesheet" href="/xmjg/agcloud/framework/js-lib/element-2/element.css"/>
  <!--<link rel="stylesheet" href="../../../../../static/agcloud/framework/icon-lib/agcloud-
fonts/iconfont.css" th:href="@{/agcloud/framework/icon-lib/agcloud-fonts/iconfont.css}">
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css" th:href="@{/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css}">-->
<!--
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/css/index-rem.css" th:href="@{/agcloud/framework/ui-schemes/dark-blue/css/index-rem.css}">
-->

    <style>
        /*
* @Author: ZL
* @Date:   2019/5/14
* @Last Modified by:   ZL
* @Last Modified time: $ $
*/
/*字体字号初始化*/
html,body,.btn,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title .m-
portlet__head-text,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title
.m-portlet__head-text small,.form-control{
    font-family: Microsoft YaHei,Helvetica Neue,Helvetica,PingFang SC,Hiragino Sans
GB,SimSun,sans-serif;
}

html, body{
    font-size: .14rem;
    color: #474747;
    margin: 0;
    padding: 0;
    background: #1b2538;
}
* {
    margin: 0;
    padding: 0;
    box-sizing: border-box;
    text-decoration: none;
}
ul,li {
    list-style: none;
}
a:hover {
    text-decoration: none;
}
.fl {
    float: left;
}
```

```
.fr {
    float: right;
}
.clearfix {
    zoom: 1;
}
.clearfix:before, .clearfix:after {
    content: "";
    display: table;
}
.clearfix:after {
    clear: both;
}
[v-cloak] {
    display: none;
}
.el-badge__content {
    border: none;
}

.protal-header {
    width: 100%;
    height: .69rem;
    line-height: .69rem;
    z-index: 99;
    position: fixed;
    top: 0;
    color: #fff;
    background: -webkit-linear-gradient(top,#243860, #223251);
    background: -o-linear-gradient(top,#243860, #223251);
    background: -moz-linear-gradient(top,#243860, #223251);
    background: linear-gradient(top,#243860, #223251);
    background: -m
...
...
...

        <div class="user">
          <div class="fl user-info">
          <div class="fl user-img" v-if="userSex==0" style="background:
url(/xmjg/agcloud/framework/ui-schemes/dark-blue/images/user.png) center center no-repeat
;background-size:100% 70%"></div>
          <div class="fl user-img" v-else style="background: url(/xmjg/agcloud/framework/ui-
schemes/dark-blue/images/user.png) center center no-repeat ;background-size:100% 70%"></div>
          <!--<img v-if="userSex==0" src="../../../../../static/agcloud/framework/ui-
schemes/dark-blue/images/user.png"
          th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/user.png}">
          <img v-else src="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/images/user.png"
          th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/user.png}">
          </div>-->
          <p class="fl user-role" :title="userName">{{userName}}</p>
          </div>
          <span class="topbar-img" @click="editPasswordFlag=true" style="background:
url(/xmjg/agcloud/framework/ui-schemes/dark-blue/images/lock.png) center center no-repeat
;;background-size:60% 60%
...
...
...
```

问题 4 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
实体：	<img src="../../../../../static/agcloud/framework/ui-schemes/dark-blue/images/lock.png" th:src="@{/a... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/opus/front/blue/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/login?code=Hu24Qr&state=tba1ER
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: Keep-Alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:10:15 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!--@Author: ZL-->
<!--@Date:   2019/5/14-->
<!--@Last Modified by:   ZL-->
<!--@Last Modified time: $ $-->
<!DOCTYPE html>
<html lang="zh-CN">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <!--<title>国家工程建设项目审批监管信息系统</title>-->
<!--  <th:block th:insert="adsfw/taglibs :: taglibs"/>-->
  <script>
    var isWhite = '';
  </script>
  <script src="/xmjg/common/tool/common-merge.js" ></script>
  <link rel="shortcut icon" href="/xmjg/agcloud/framework/ui-schemes/dark-
blue/images/system_guohui.png" type="image/x-icon"/>
  <link rel="icon" href="/xmjg/agcloud/framework/ui-schemes/dark-blue/images/system_guohui.png"
type="image/x-icon" />
  <link rel="stylesheet" href="/xmjg/agcloud/framework/js-lib/element-2/element.css"/>
  <!--<link rel="stylesheet" href="../../../../../static/agcloud/framework/icon-lib/agcloud-
fonts/iconfont.css" th:href="@{/agcloud/framework/icon-lib/agcloud-fonts/iconfont.css}">
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css" th:href="@{/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css}">-->
<!--
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/css/index-rem.css" th:href="@{/agcloud/framework/ui-schemes/dark-blue/css/index-rem.css}">
```

```
-->

    <style>
        /*
* @Author: ZL
* @Date:   2019/5/14
* @Last Modified by:   ZL
* @Last Modified time: $ $
*/
/*字体字号初始化*/
html,body,.btn,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title .m-
portlet__head-text,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title
.m-portlet__head-text small,.form-control{
    font-family: Microsoft YaHei,Helvetica Neue,Helvetica,PingFang SC,Hiragino Sans
GB,SimSun,sans-serif;
}

html, body{
    font-size: .14rem;
    color: #474747;
    margin: 0;
    padding: 0;
    background: #1b2538;
}
* {
    margin: 0;
    padding: 0;
    box-sizing: border-box;
    text-decoration: none;
}
ul,li {
    list-style: none;
}
a:hover {
    text-decoration: none;
}
.fl {
    float: left;
}
.fr {
    float: right;
}
.clearfix {
    zoom: 1;
}
.clearfix:before, .clearfix:after {
    content: "";
    display: table;
}
.clearfix:after {
    clear: both;
}
[v-cloak] {
    display: none;
}
.el-badge__content {
    border: none;
}

.protal-header {
    width: 100%;
    height: .69rem;
    line-height: .69rem;
    z-index: 99;
    position: fixed;
    top: 0;
    color: #fff;
    background: -webkit-linear-gradient(top,#243860, #223251);
    background: -o-linear-gradient(top,#243860, #223251);
    background: -moz-linear-gradient(top,#243860, #223251);
    background: linear-gradient(top,#243860, #223251);
    background: -ms-linear-gradient(top,#243860, #223251);/* IE 10 */
    filter: progid:DXImageTransform.Microsoft.gradient(GradientType=0, startColorstr=#243860,
endColorstr=#223251);
    -ms-filter: "progid:DXImageTransform.Microsoft.gradient (GradientType=0,
startColorstr=#243860, endColorstr=#223251)";
    box-shadow: 0 0 10px rgba(0,0,0,.2);
}
```

```
.subsystem-logo {
    width: 6.20rem;

...
...
...

          <p class="fl user-role" :title="userName">{{userName}}</p>
          </div>
          <span class="topbar-img" @click="editPasswordFlag=true" style="background:
url(/xmjg/agcloud/framework/ui-schemes/dark-blue/images/lock.png) center center no-repeat
;;background-size:60% 60%">
          <!--<img src="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/images/lock.png" th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/lock.png}"
alt="">-->
          </span>
          <span class="topbar-img" @click="logout" style="background:
url(/xmjg/agcloud/framework/ui-schemes/dark-blue/images/exit.png) center center no-repeat
;;background-size:60% 60%">
          <!--<img src="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/images/exit.png" th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/exit.png}"
alt="">-->
          </span>
...
...
...
```

问题 5 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
实体：	<img src="../../../../../static/agcloud/framework/ui-schemes/dark-blue/images/exit.png" th:src="@{/a... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/opus/front/blue/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/login?code=Hu24Qr&state=tba1ER
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: Keep-Alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
```

```
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:10:15 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!--@Author: ZL-->
<!--@Date:   2019/5/14-->
<!--@Last Modified by:   ZL-->
<!--@Last Modified time: $ $-->
<!DOCTYPE html>
<html lang="zh-CN">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <!--<title>国家工程建设项目审批监管信息系统</title>-->
<!--  <th:block th:insert="adsfw/taglibs :: taglibs"/>-->
  <script>
    var isWhite = '';
  </script>
  <script src="/xmjg/common/tool/common-merge.js" ></script>
  <link rel="shortcut icon" href="/xmjg/agcloud/framework/ui-schemes/dark-
blue/images/system_guohui.png" type="image/x-icon"/>
  <link rel="icon" href="/xmjg/agcloud/framework/ui-schemes/dark-blue/images/system_guohui.png"
type="image/x-icon" />
  <link rel="stylesheet" href="/xmjg/agcloud/framework/js-lib/element-2/element.css"/>
  <!--<link rel="stylesheet" href="../../../../../static/agcloud/framework/icon-lib/agcloud-
fonts/iconfont.css" th:href="@{/agcloud/framework/icon-lib/agcloud-fonts/iconfont.css}">
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css" th:href="@{/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css}">-->
<!--
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/css/index-rem.css" th:href="@{/agcloud/framework/ui-schemes/dark-blue/css/index-rem.css}">
-->

    <style>
        /*
* @Author: ZL
* @Date:   2019/5/14
* @Last Modified by:   ZL
* @Last Modified time: $ $
*/
/*字体字号初始化*/
html,body,.btn,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title .m-
portlet__head-text,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title
.m-portlet__head-text small,.form-control{
    font-family: Microsoft YaHei,Helvetica Neue,Helvetica,PingFang SC,Hiragino Sans
GB,SimSun,sans-serif;
}

html, body{
    font-size: .14rem;
    color: #474747;
    margin: 0;
    padding: 0;
    background: #1b2538;
}
* {
    margin: 0;
    padding: 0;
    box-sizing: border-box;
    text-decoration: none;
}
ul,li {
    list-style: none;
}
a:hover {
    text-decoration: none;
}
.fl {
    float: left;
}
.fr {
    float: right;
```

```
}
.clearfix {
    zoom: 1;
}
.clearfix:before, .clearfix:after {
    content: "";
    display: table;
}
.clearfix:after {
    clear: both;
}
[v-cloak] {
    display: none;
}
.el-badge__content {
    border: none;
}

.protal-header {
    width: 100%;
    height: .69rem;
    line-height: .69rem;
    z-index: 99;
    position: fixed;
    top: 0;
    color: #fff;
    background: -webkit-linear-gradient(top,#243860, #223251);
    background: -o-linear-gradient(top,#243860, #223251);
    background: -moz-linear-gradient(top,#243860, #223251);
    background: linear-gradient(top,#243860, #223251);
    background: -ms-l
...
...
...
        <span class="topbar-img" @click="editPasswordFlag=true" style="background:
url(/xmjg/agcloud/framework/ui-schemes/dark-blue/images/lock.png) center center no-repeat
;;background-size:60% 60%">
          <!--<img src="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/images/lock.png" th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/lock.png}"
alt="">-->
          </span>
          <span class="topbar-img" @click="logout" style="background:
url(/xmjg/agcloud/framework/ui-schemes/dark-blue/images/exit.png) center center no-repeat
;;background-size:60% 60%">
          <!--<img src="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/images/exit.png" th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/exit.png}"
alt="">-->
          </span>
          <span class="topbar-img" style="background: url(/xmjg/agcloud/framework/ui-
schemes/dark-blue/images/help.png)center center no-repeat ;;background-size:60% 60%">
          <a class="helpDoc" href="/xmjg/xmjg/file/工程建设项目审批管理系统操作手册.doc" download="工程
建设项目审批管理系统操作手册.doc"></a>
          <!--<img src="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/images/help.png" th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/help.png}"
alt="">-->
...
...
...
```

问题 6 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	<div style="float:left;"> (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
```

```
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
}
.bacckbutton {
    float: right;
    margin: 3px 10px 5px 10px;
    width: 96px;
    height: 32px;
    background-color: #006ecc;
    borde
...
...
...

 <div id="show">
         <div style="width:100%;margin-top:7px;"></div>
         <img src="/xmjg/dghyindex/img/loding.gif" />
         <!--<div style="float:left;">
                 <img th:src="@{/dghyindex/img       /loding.gif}" src="../../img/loding.gif" />
         </div>-->
         <div style="width:100%;margin-top:15px;"></div>
         <div class="loadingText">       正在加载,请稍候...</div>
 </div>
...
...
...
```

问题 7 / 33

TOC

HTML 注释敏感信息泄露	
严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
实体：	<link rel="stylesheet" href="../../../../../static/agcloud/framework/icon-lib/agcloud-fonts/iconfont... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/opus/front/blue/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/login?code=Hu24Qr&state=tba1ER
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: Keep-Alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:10:15 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!--@Author: ZL-->
<!--@Date:   2019/5/14-->
<!--@Last Modified by:   ZL-->
<!--@Last Modified time: $ $-->
<!DOCTYPE html>
<html lang="zh-CN">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <!--<title>国家工程建设项目审批监管信息系统</title>-->
<!--  <th:block th:insert="adsfw/taglibs :: taglibs"/>-->
  <script>
    var isWhite = '';
  </script>
  <script src="/xmjg/common/tool/common-merge.js" ></script>
  <link rel="shortcut icon" href="/xmjg/agcloud/framework/ui-schemes/dark-
blue/images/system_guohui.png" type="image/x-icon"/>
  <link rel="icon" href="/xmjg/agcloud/framework/ui-schemes/dark-blue/images/system_guohui.png"
type="image/x-icon" />
  <link rel="stylesheet" href="/xmjg/agcloud/framework/js-lib/element-2/element.css"/>
  <!--<link rel="stylesheet" href="../../../../../static/agcloud/framework/icon-lib/agcloud-
fonts/iconfont.css" th:href="@{/agcloud/framework/icon-lib/agcloud-fonts/iconfont.css}">
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css" th:href="@{/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css}">-->
<!--
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/css/index-rem.css" th:href="@{/agcloud/framework/ui-schemes/dark-blue/css/index-rem.css}">
-->

    <style>
        /*
* @Author: ZL
* @Date:   2019/5/14
* @Last Modified by:   ZL
* @Last Modified time: $ $
*/
/*字体字号初始化*/
html,body,.btn,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title .m-
portlet__head-text,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title
.m-portlet__head-text small,.form-control{
    font-family: Microsoft YaHei,Helvetica Neue,Helvetica,PingFang SC,Hiragino Sans
GB,SimSun,sans-serif;
}

html, body{
    font-size: .14rem;
    color: #474747;
    margin: 0;
    padding: 0;
    background: #1b2538;
}
* {
    margin: 0;
    padding: 0;
    box-sizing: border-box;
    text-decoration: none;
}
ul,li {
    list-style: none;
}
a:hover {
    text-decoration: none;
}
.fl {
    float: left;
}
.fr {
    float: right;
}
.clearfix {
    zoom: 1;
}
.clearfix:before, .clearfix:after {
    content: "";
    display: table;
}
.clearfix:after {
    clear: both;
}
[v-cloak] {
    display: none;
}
.el-badge__content {
    border: none;
}

.protal-header {
    width: 100%;
    height: .69rem;
    line-height: .69rem;
    z-index: 99;
    position: fixed;
    top: 0;
    color: #fff;
    background: -webkit-linear-gradient(top,#243860, #223251);
    background: -o-linear-gradient(top,#243860, #223251);
    background: -moz-linear-gradient(top,#243860, #223251);
    background: linear-gradient(top,#243860, #223251);
    background: -ms-linear-gradient(top,#243860, #223251);/* IE 10 */
    filter: progid:DXImageTransform.Microsoft.gradient(GradientType=0, startColorstr=#243860,
endColorstr=#223251);
    -ms-filter: "progid:DXImageTransform.Microsoft.gradient (GradientType=0,
startColorstr=#243860, endColorstr=#223251)";
    box-shadow: 0 0 10px rgba(0,0,0,.2);
}
.subsystem-logo {
    width: 6.20rem;
    height: .69rem;
    float: left;
    background: url(/xmjg//agcloud/framework/ui-schemes/dark-blue/css/images/system_name.png)
15px center no-repeat;
}
.subsystem-div {
    /*width: 32%;*/
    /*width: 5.9rem;*/
    width: calc(30vw);
    height: .69rem;
    float: left;
    overflow: hidden;
    text-overflow: ellipsis;
    white-space: nowrap;
}
.subsystem-div span {
    color: white;
    font-size: .28rem;
}
.subsystem-guohui-logo {
    width: .70rem;
    height: .69rem;
    float: left;
    background: url(/xmjg//agcloud/framework/ui-schemes/dark-blue/css/images/system_guohui.png)
.15rem center no-repeat;
}
.header-menu {
   /* width: 52%;*/
    width: calc(50vw);/*8.8rem;*/
    height: .69rem;
    overflow: hidden;
}
```

```
.header-menu_nav .header-menu_ite
...
...
...
```

问题 8 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
实体：	<script src="/framework-ui/src/main/resources/static/agcloud/login/js/md5.js" th:src="@{/agcloud/log... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/opus/front/blue/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/login?code=Hu24Qr&state=tba1ER
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: Keep-Alive
Host: 127.0.0.1:8000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:10:15 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!--@Author: ZL-->
<!--@Date:   2019/5/14-->
<!--@Last Modified by:   ZL-->
<!--@Last Modified time: $ $-->
<!DOCTYPE html>
<html lang="zh-CN">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <!--<title>国家工程建设项目审批监管信息系统</title>-->
<!--  <th:block th:insert="adsfw/taglibs :: taglibs"/>-->
  <script>
    var isWhite = '';
  </script>
  <script src="/xmjg/common/tool/common-merge.js" ></script>
  <link rel="shortcut icon" href="/xmjg/agcloud/framework/ui-schemes/dark-
blue/images/system_guohui.png" type="image/x-icon"/>
  <link rel="icon" href="/xmjg/agcloud/framework/ui-schemes/dark-blue/images/system_guohui.png"
type="image/x-icon" />
  <link rel="stylesheet" href="/xmjg/agcloud/framework/js-lib/element-2/element.css"/>
  <!--<link rel="stylesheet" href="../../../../../static/agcloud/framework/icon-lib/agcloud-
fonts/iconfont.css" th:href="@{/agcloud/framework/icon-lib/agcloud-fonts/iconfont.css}">
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css" th:href="@{/agcloud/framework/ui-
private/common/plugins/agcloud-fonts/iconfont.css}">-->
<!--
    <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-schemes/dark-
blue/css/index-rem.css" th:href="@{/agcloud/framework/ui-schemes/dark-blue/css/index-rem.css}">
-->

    <style>
        /*
* @Author: ZL
* @Date:   2019/5/14
* @Last Modified by:   ZL
* @Last Modified time: $ $
*/
/*字体字号初始化*/
html,body,.btn,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title .m-
portlet__head-text,.m-portlet .m-portlet__head .m-portlet__head-caption .m-portlet__head-title
.m-portlet__head-text small,.form-control{
    font-family: Microsoft YaHei,Helvetica Neue,Helvetica,PingFang SC,Hiragino Sans
GB,SimSun,sans-serif;
}

html, body{
    font-size: .14rem;
    color: #474747;
    margin: 0;
    padding: 0;
    background: #1b2538;
}
* {
    margin: 0;
    padding: 0;
    box-sizing: border-box;
    text-decoration: none;
}
ul,li {
    list-style: none;
}
a:hover {
    text-decoration: none;
}
.fl {
    float: left;
}
.fr {
    float: right;
}
.clearfix {
    zoom: 1;
}
.clearfix:before, .clearfix:after {
    content: "";
    display: table;
}
.clearfix:after {
    clear: both;
}
[v-cloak] {
    display: none;
}
.el-badge__content {
    border: none;
}

.protal-header {
    width: 100%;
    height: .69rem;
    line-height: .69rem;
    z-index: 99;
    position: fixed;
    top: 0;
    color: #fff;
    background: -webkit-linear-gradient(top,#243860, #223251);
    background: -o-linear-gradient(top,#243860, #223251);
    background: -moz-linear-gradient(top,#243860, #223251);
    background: linear-gradient(top,#243860, #223251);
    background: -ms-linear-gradient(top,#243860, #223251);/* IE 10 */
    filter: progid:DXImageTransform.Microsoft.gradient(GradientType=0, startColorstr=#243860,
endColorstr=#223251);
    -ms-filter: "progid:DXImageTransform.Microsoft.gradient (GradientType=0, s
...
...
...

  <script src="/xmjg/agcloud/framework/js-lib/vue-v2/vue.js"></script>
  <script src="/xmjg/agcloud/framework/js-lib/element-2/element.js"></script>
  <script src="/xmjg/agcloud/framework/js-lib/agcloud-lib/js/common.js"></script>
  <script src="/xmjg/agcloud/framework/ui-schemes/dark-blue/js/index.js"></script>
<!--  <script src="/framework-ui/src/main/resources/static/agcloud/login/js/md5.js"
th:src="@{/agcloud/login/js/md5.js}"></script>
  <script src="/framework-ui/src/main/resources/static/agcloud/login/js/base64.js"
th:src="@{/agcloud/login/js/base64.js}"></script>
  <script src="/framework-ui/src/main/resources/static/agcloud/login/js/sm4.js"
th:src="@{/agcloud/login/js/sm4.js}"></script>-->
  <script src="/xmjg/agcloud/login/js/sm3-sm4-md5-base64-merge.js"></script>
  <!--END:js文件-->
  <script>
      initWhite();
...
...
...
```

问题 9 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html
实体：	Copyright 2012 Mozilla Foundation (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg/csrk/pdfShow/web/viewer.html?file=%20/xmjg/file/yzbd/yishialaer/pdf/7fa992eb-5923-
419b-9cbc-
612db98522ba%E2%80%BB%E4%B8%80%E9%98%B6%E6%AE%B5%E5%8A%9E%E4%BA%8B%E6%8C%87%E5%8D%97.pdf HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//xmjg-one-form!getYzbd.action?
name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
```

```
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 22080
Last-Modified: Mon, 21 Sep 2020 04:41:14 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 05:12:16 GMT
Content-Type: text/html;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

<!DOCTYPE html>
<!--
Copyright 2012 Mozilla Foundation

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

Adobe CMap resources are covered by their own copyright but the same license:

    Copyright 1990-2015 Adobe Systems Incorporated.

See https://github.com/adobe-type-tools/cmap-resources
-->
<html dir="ltr" mozdisallowselectionprint>
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
    <meta name="google" content="notranslate">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>PDF.js viewer</title>


    <link rel="stylesheet" href="viewer.css">


<!-- This snippet is used in production (included from viewer.html) -->
<link rel="resource" type="application/l10n" href="locale/locale.properties">
<script src="../build/pdf.js"></script>


    <script src="viewer.js"></script>

  </head>

  <body tabindex="1" class="loadingInProgress">
    <div id="outerContainer">

      <div id="sidebarContainer">
        <div id="toolbarSidebar">
          <div class="splitToolbarButton toggled">
          <button id="viewThumbnail" class="toolbarButton toggled" title="Show Thumbnails"
tabindex="2" data-l10n-id="thumbs">
          <span data-l10n-id="thumbs_label">Thumbnails</span>
          </button>
          <button id="viewOutline" class="toolbarButton" title="Show Document Outline (double-
click to expand/collapse all items)" tabindex="3" data-l10n-id="document_outline">
          <span data-l10n-id="document_outline_label">Document Outline</span>
          </button>
          <button id="viewAttachments" class="toolbarButton" title="Show Attachments"
tabindex="4" data-l10n-id="attachments">
```

```
          <span data-l10n-id="attachments_label">Attachments</span>
          </button>
          </div>
        </div>
        <div id="sidebarContent">
          <div id="thumbnailView">
          </div>
          <div id="outlineView" class="hidden">
          </div>
          <div id="attachmentsView" class="hidden">
          </div>
        </div>
        <div id="sidebarResizer" class="hidden"></div>
      </div>  <!-- sidebarContainer -->

      <div id="mainContainer">
        <div class="findbar hidden doorHanger" id="findbar">
          <div id="findbarInputContainer">
          <input id="findInput" class="toolbarField" title="Find" placeholder="Find in document…"
tabindex="91" data-l10n-id="find_input">
          <div class="splitToolbarButton">
          <button id="findPrevious" class="toolbarButton findPrevious" title="Find the previous
occurrence of the phrase" tabindex="92" data-l10n-id="find_previous">
          <span data-l10n-id="find_previous_label">Previous</span>
          </button>
          <div class="splitToolbarButtonSeparator"></div>
          <button id="findNext" class="toolbarButton findNext" title="Find the next occurrence of
the phrase" tabindex="93" data-l10n-id="find_next">
          <span data-l10n-id="find_next_label">Next</span>
          </button>
          </div>
          </div>

          <div id="findbarOptionsOneContainer">
          <input type="checkbox" id="findHighlightAll" class="toolbarField" tabindex="94
...
...
...
```

问题 10 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do
实体：	<link th:href="@{/xmjg/xndc/css/dg-jdkh-main.css}" href="${ctx}/xmjg/xndc/css/dg-jdkh-main.css" rel =... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879 HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:03 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
<meta charset="utf-8" />
<title>效能督查</title>
<script type="text/javascript">
    var isWhite = '';
 //pc       版首页
    var ctx='/xmjg/';
    var name = '';
    var xzqhdm= "";
    var loginXzqhdm= "" ? "" : "china";
    var loginProvince = "" ? "" : "china";
   // var oldflag = "";
    var oldflag = "true";
 console.log(oldflag);
    var oldStartDate = "";
    var oldEndDate = "";
    var bigScreenFolder=""; //大屏css 目录，如果是普通屏（默认）则该值为空
    var provinceCode="";
    //var projectManager=parent.projectManager;
    var defaultEndDate="",defaultStartDate="";
    var provinceParam={};
    var params = "";
    var initHeartBeat ="";
    var initStartDate="";//获取配置文件中统计时间的配置参数
</script>
<!--    <th:block th:insert="adsfw/taglibs :: taglibs"/>-->
    <script src="/xmjg/common/tool/common-merge.js" ></script>
    <link href="/xmjg/common/tool/date/css/bootstrap.min.css" rel="stylesheet" type="text/css"/>
 <link href="/xmjg/xmjg/supervisionInspection/css/element.css" rel="stylesheet"
type="text/css"/>
 <!--<link th:href="@{/xmjg/xndc/css       /dg-jdkh-main.css}" href="${ctx}/xmjg/xndc/css/dg-
jdkh-main.css" rel="stylesheet" type="text/css"/>-->
 <link href="/xmjg/xmjg/supervisionInspection/css/dg-jdkh-main-rem.css" rel="stylesheet"
type="text/css"/>
 <!--<link rel="stylesheet" href="/framework-
ui/src/main/resources/static/agcloud/framework/ui-private/common/element-2/element.css"
th:href="@{/agcloud/framework/ui-private/common/element-2/element.css}">-->
 <!-- jquery -->
    <!--<script th:src="@{/xmjg/js/jquery.min.js}" type="text/javascript" charset="utf-8">
</script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js"
type="text/javascript" charset="utf-8"></script>
 <script src="/xmjg/common/tool/date/js/bootstrap.min.js" type="text/javascript"
charset="utf-8"></script>
 <link   href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
 <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/numberAnimate.js"
type="text/javascript"></script>
 <!--<script th:src="@{/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js}"
src="${ctx}/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js" type="text/javascript"></script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/dg-jdkh-main.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/echarts.min.js" type="text/javascript"
```

```
charset="utf-8"></script>
 <!--<script th:src="@{/common/tool/date/js/dateQuery.js}" type="text/javascript"
charset="utf-8"></script>-->

 <!--        城市选择插件  开始 -->
 <link   href="/xmjg/common/tool/cityselect/css/city_select.css" rel="stylesheet"
type="text/css" />
 <script src="/xmjg/common/tool/cityselect/js/city_data.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/common/tool/cityselect/js/areadata.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/common/tool/cityselect/js/auto_area.js" type="text/javascript"
charset="utf-8"></script>
 <!--        城市选择插件  结束 -->

<script type="text/javascript">
    var date = new Date();
 var dateStr =    date.getFullYear() + "-" + ("0" + (date.getMonth() + 1)).slice(-2) + "-
"+ ("0" + (date.getDate())).slice(-2);
 var startTime = dateStr.substr(0,5)+"01-01";
 var endDateStr = dateStr;
    Date.prototype.format = function(fmt) {
        var o = {
          "M+" : this.getMonth()+1,          //月份
          "d+" : this.getDate(),          //日
          "h+" : this.getHours(),          //小时
          "m+" : this.getMinutes(),          //分
          "s+" : this.getSeconds(),          //秒
          "q+" : Math.floor((this.getMonth()+3)/3), //季度
          "S"  : this.getMilliseconds()          //毫秒
        };
        if(/(y+)/.test(fmt)) {
          fmt=fmt.replace(RegExp.$1, (this.getFullYear()+"").substr(4 - RegExp.$1.length));
        }
        for(var k in o) {

...
...
...
```

问题 11 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do
实体：	<link rel="stylesheet" href="/framework-ui/src/main/resources/static/agcloud/framework/ui-private/co... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:03 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
<meta charset="utf-8" />
<title>效能督查</title>
<script type="text/javascript">
    var isWhite = '';
 //pc       版首页
    var ctx='/xmjg/';
    var name = '';
    var xzqhdm= "";
    var loginXzqhdm= "" ? "" : "china";
    var loginProvince = "" ? "" : "china";
   // var oldflag = "";
    var oldflag = "true";
 console.log(oldflag);
    var oldStartDate = "";
    var oldEndDate = "";
    var bigScreenFolder=""; //大屏css 目录，如果是普通屏（默认）则该值为空
    var provinceCode="";
    //var projectManager=parent.projectManager;
    var defaultEndDate="",defaultStartDate="";
    var provinceParam={};
    var params = "";
    var initHeartBeat ="";
    var initStartDate="";//获取配置文件中统计时间的配置参数
</script>
<!--    <th:block th:insert="adsfw/taglibs :: taglibs"/>-->
    <script src="/xmjg/common/tool/common-merge.js" ></script>
    <link href="/xmjg/common/tool/date/css/bootstrap.min.css" rel="stylesheet" type="text/css"/>
 <link href="/xmjg/xmjg/supervisionInspection/css/element.css" rel="stylesheet"
type="text/css"/>
 <!--<link th:href="@{/xmjg/xndc/css/dg-jdkh-main.css}" href="${ctx}/xmjg/xndc/css/dg-
jdkh-main.css" rel="stylesheet" type="text/css"/>-->
 <link href="/xmjg/xmjg/supervisionInspection/css/dg-jdkh-main-rem.css" rel="stylesheet"
type="text/css"/>
 <!--<link rel="stylesheet" href="/framework-
ui/src/main/resources/static/agcloud/framework/ui-private/common/element-2/element.css"
th:href="@{/agcloud/framework/ui-private/common/element-2/element.css}">-->
 <!-- jquery -->
    <!--<script th:src="@{/xmjg/js/jquery.min.js}" type="text/javascript" charset="utf-8">
</script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js"
type="text/javascript" charset="utf-8"></script>
 <script src="/xmjg/common/tool/date/js/bootstrap.min.js" type="text/javascript"
charset="utf-8"></script>
 <link   href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
 <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/numberAnimate.js"
type="text/javascript"></script>
 <!--<script th:src="@{/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js}"
src="${ctx}/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js" type="text/javascript"></script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/dg-jdkh-main.js" type="text/javascript"
charset="utf-8"></script>
```

```
 <script src="/xmjg/xmjg/supervisionInspection/js/echarts.min.js" type="text/javascript"
charset="utf-8"></script>
 <!--<script th:src="@{/common/tool/date/js/dateQuery.js}" type="text/javascript"
charset="utf-8"></script>-->

 <!--        城市选择插件   开始 -->
 <link   href="/xmjg/common/tool/cityselect/css/city_select.css" rel="stylesheet"
type="text/css" />
 <script src="/xmjg/common/tool/cityselect/js/city_data.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/common/tool/cityselect/js/areadata.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/common/tool/cityselect/js/auto_area.js" type="text/javascript"
charset="utf-8"></script>
 <!--        城市选择插件   结束 -->

<script type="text/javascript">
    var date = new Date();
 var dateStr =    date.getFullYear() + "-" + ("0" + (date.getMonth() + 1)).slice(-2) + "-
"+ ("0" + (date.getDate())).slice(-2);
 var startTime = dateStr.substr(0,5)+"01-01";
 var endDateStr = dateStr;
    Date.prototype.format = function(fmt) {
        var o = {
          "M+" : this.getMonth()+1,          //月份
          "d+" : this.getDate(),          //日
          "h+" : this.getHours(),          //小时
          "m+" : this.getMinutes(),          //分
          "s+" : this.getSeconds(),          //秒
          "q+" : Math.floor((this.getMonth()+3)/3), //季度
          "S"  : this.getMilliseconds()          //毫秒
        };
        if(/(y+)/.test(fmt)) {
          fmt=fmt.replace(RegExp.$1, (this.getFullYear()+"").substr(4 - RegExp.$1.length));
        }
        for(var k in o) {

...
...
...
```

问题 12 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do
实体：	<script th:src="@{/common/tool/date/js/dateQuery.js}" type="text/javascript" charset="utf-8"></scrip... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:45:03 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
<meta charset="utf-8" />
<title>效能督查</title>
<script type="text/javascript">
    var isWhite = '';
 //pc       版首页
    var ctx='/xmjg/';
    var name = '';
    var xzqhdm= "";
    var loginXzqhdm= "" ? "" : "china";
    var loginProvince = "" ? "" : "china";
   // var oldflag = "";
    var oldflag = "true";
 console.log(oldflag);
    var oldStartDate = "";
    var oldEndDate = "";
    var bigScreenFolder=""; //大屏css 目录，如果是普通屏（默认）则该值为空
    var provinceCode="";
    //var projectManager=parent.projectManager;
    var defaultEndDate="",defaultStartDate="";
    var provinceParam={};
    var params = "";
    var initHeartBeat ="";
    var initStartDate="";//获取配置文件中统计时间的配置参数
</script>
<!--    <th:block th:insert="adsfw/taglibs :: taglibs"/>-->
    <script src="/xmjg/common/tool/common-merge.js" ></script>
    <link href="/xmjg/common/tool/date/css/bootstrap.min.css" rel="stylesheet" type="text/css"/>
 <link href="/xmjg/xmjg/supervisionInspection/css/element.css" rel="stylesheet"
type="text/css"/>
 <!--<link th:href="@{/xmjg/xndc/css/dg-jdkh-main.css}" href="${ctx}/xmjg/xndc/css/dg-
jdkh-main.css" rel="stylesheet" type="text/css"/>-->
 <link href="/xmjg/xmjg/supervisionInspection/css/dg-jdkh-main-rem.css" rel="stylesheet"
type="text/css"/>
 <!--<link rel="stylesheet" href="/framework-
ui/src/main/resources/static/agcloud/framework/ui-private/common/element-2/element.css"
th:href="@{/agcloud/framework/ui-private/common/element-2/element.css}">-->
 <!-- jquery -->
    <!--<script th:src="@{/xmjg/js/jquery.min.js}" type="text/javascript" charset="utf-8">
</script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js"
type="text/javascript" charset="utf-8"></script>
 <script src="/xmjg/common/tool/date/js/bootstrap.min.js" type="text/javascript"
charset="utf-8"></script>
 <link   href="/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
 <script src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/numberAnimate.js"
type="text/javascript"></script>
 <!--<script th:src="@{/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js}"
src="${ctx}/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js" type="text/javascript"></script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/dg-jdkh-main.js" type="text/javascript"
charset="utf-8"></script>
```

```
 <script src="/xmjg/xmjg/supervisionInspection/js/echarts.min.js" type="text/javascript"
charset="utf-8"></script>
 <!--<script th:src="@{/common/tool/date/js        /dateQuery.js}" type="text/javascript"
charset="utf-8"></script>-->

 <!--        城市选择插件   开始 -->
 <link   href="/xmjg/common/tool/cityselect/css/city_select.css" rel="stylesheet"
type="text/css" />
 <script src="/xmjg/common/tool/cityselect/js/city_data.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/common/tool/cityselect/js/areadata.js" type="text/javascript"
charset="utf-8"></script>
 <script src="/xmjg/common/tool/cityselect/js/auto_area.js" type="text/javascript"
charset="utf-8"></script>
 <!--        城市选择插件   结束 -->

<script type="text/javascript">
    var date = new Date();
 var dateStr =    date.getFullYear() + "-" + ("0" + (date.getMonth() + 1)).slice(-2) + "-
"+ ("0" + (date.getDate())).slice(-2);
 var startTime = dateStr.substr(0,5)+"01-01";
 var endDateStr = dateStr;
    Date.prototype.format = function(fmt) {
        var o = {
          "M+" : this.getMonth()+1,          //月份
          "d+" : this.getDate(),          //日
          "h+" : this.getHours(),          //小时
          "m+" : this.getMinutes(),          //分
          "s+" : this.getSeconds(),          //秒
          "q+" : Math.floor((this.getMonth()+3)/3), //季度
          "S"  : this.getMilliseconds()          //毫秒
        };
        if(/(y+)/.test(fmt)) {
          fmt=fmt.replace(RegExp.$1, (this.getFullYear()+"").substr(4 - RegExp.$1.length));
        }
        for(var k in o) {
          if(new RegExp("("+ k +")").test(fmt))
...
...
...
```

问题 13 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	<img id="ckyimg" th:src="@{/dghyindex/img/xmjg/shhz.png}" src="${ctx}/dghyindex/img/xmjg/shhz.png" ... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-borde
...
...
...

                         <!--</div>-->
                         <!--&lt;!&ndash;        一般社会投资项目(公开出让用地) &ndash;&gt;-->
                         <!--<div style="float:left;/*margin-
left:2%;*/width:10%;height:166px;text-align:center;">-->
                                 <!--<div style="margin-top:0px;width:100%;height:1px;">
</div>-->
                                 <!--<img id="ckyimg"
th:src="@{/dghyindex/img/xmjg/shhz.png}"  src="${ctx}/dghyindex/img/xmjg/shhz.png"
style="cursor:pointer;" onclick="clickXmfl('4')"-->
                                         <!--onmouseover="setImgSrc(this,'over')"
onmouseout="setImgSrc(this,'out')" />-->
                                 <!--<div id="ybsh"></div>-->
                         <!--</div>-->
                         <!--&lt;!&ndash;        带方案出让用地的社会投资项目 &ndash;&gt;-->
...
...
...
```

问题 14 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	src="${ctx}/xmzh/project/img/tjpm.png" onmouseover="overcyy()" (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
```

```
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
```

```
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
}
.bacckbutton {
    float: right;
    margin: 3px 10px 5px 1
...
...
...

                                                 <!--align="center" onmouseout="outcyy()"
/> <br />-->
                                         <!--</div>-->
                                         <!--<div style="float:left;margin-
left:3px;width:30%;margin-top:20px;" align="center">-->
                                                 <!--<img style="cursor:pointer;"
onclick="clickPmtj()" id="pmtjimg"-->
                                                 <!-       -
src="${ctx}/xmzh/project/img/tjpm.png" onmouseover="overcyy()"-->
                                                 <!--align="center" onmouseout="outcyy()"
/> <br />-->
                                         <!--</div>&ndash;&gt;-->
                                 <!--</div>-->
                         <!--</div>-->
...
...
...
```

问题 15 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	<script type="text/javascript" src="js/ajaxfileupload.js"></script> (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
}
.bacckbutton {
    float: right;
    margin: 3px 10px 5px 10px;
    width: 96px;
    height: 32px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-r
...
...
...
```

```
        function zhQuery(){
                window.location.href="${ctx}/dghyindex/common-content.jsp?method=zhcx";
        }
</script>
<!-- <script type="text/javascript" src="js/ajaxfileupload.js"></script> -->
</head>
<body style="background-color:rgb(27 37 56); height:88%;">
 <div id="bg"></div>
 <div id="show">
...
...
...
```

问题 16 / 33

TOC

HTML 注释敏感信息泄露	
严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	src="${ctx}/xmzh/project/img/cyy.png" onmouseover="overcyy()" (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
```

```
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid tra
...
...
...

                                          <!--</div>-->
                                          <!--<div style="float:left;margin-
left:0px;width:30%;margin-top:20px;"-->
                                                  <!--align="center">-->
                                                  <!--<img style="cursor:pointer;"
onclick="clickCYY()" id="cyyimg"-->
                                                  <!--src="${ctx}/xmzh/project/img       /cyy.png"
onmouseover="overcyy()"-->
                                                  <!--align="center" onmouseout="outcyy()"
/> <br />-->
                                          <!--</div>-->
                                          <!--<div style="float:left;margin-
left:3px;width:30%;margin-top:20px;" align="center">-->
                                                  <!--<img style="cursor:pointer;"
onclick="clickPmtj()" id="pmtjimg"-->
...
...
...
```

问题 17 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	src="${ctx}/xmzh/project/img/cyl.png" onmouseover="overcyl()" (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
```

```
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
}
.bacckbutton {
    float: right;
    margin: 3px 10px 5px 10px;
    width: 96px;
    height: 32px;

...
...
...

                                                  <!--align="center" onmouseout="outzbls()"
/> <br />-->
                                          <!--</div>-->
                                          <!--<div style="float:left;margin-
left:0px;width:30%;" align="center">-->
                                                  <!--<img style="cursor:pointer;"
onclick="clickCYL()" id="cylimg"-->
                                                  <!--src="${ctx}/xmzh/project/img       /cyl.png"
onmouseover="overcyl()"-->
                                                  <!--align="center" onmouseout="outcyl()"
/> <br />-->
                                          <!--</div>-->
                                  <!--</div>-->

...
...
...
```

问题 18 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do
实体：	<script th:src="@{/xmjg/xndc/js/analysis/analysis-project-stage-list.js}" src="${ctx}/xmjg/xndc/js/... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-
01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:10:26 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN" xmlns="http://www.w3.org/1999/xhtml">
 <head>
         <meta charset="utf-8" />
         <title>       各城市各阶段数据233</title>
         <script type="text/javascript">
          var ctx='/xmjg/';
                 var bigScreenFolder="";
                 var xzqhdms="";
                 var tjkssj="2020-01-01";
                 var tjjssj="2020-12-29";
                 var orderByFlag="";
                 var dataType="8";
                 var sfzb="";
                 var sfbyxz="";
                 var sfjgqqxt="";
                 var spjd="";
                 var blqk="";
                 var splclx="";
                 var splcmc="";
                 var sfyq="";
                 var tjTypeVal="";
                 var qtTypeVal = "";
                 var splcbm="";
                 var dateEnd = "2020-12-29";
                 var provinceCode="";
                 var dataType="8";  //1:       各阶段平均用时（审批用时）；2:各阶段跨度用时；3:各阶段最长
用时；4:各阶段平均受理次数；
                 var stageType="0"; //0       ：总数，1：立项用地规划许可；2：工程建设许可；3：施工许可；
4：竣工验收
          var oldStartDate = "2020-01-01";
          var oldEndDate = "2020-12-29";
          var flag="1";
          var xzqhdm="660000"; //跳转带过来的行政区划代码 用于钻取标题显示
          var name="";//跳转带过来的城市名称 用于钻取标题显示
                 var sfType = "";//       算法类型
         </script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {
```

```
          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

         <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/date/css/bootstrap.min.css"/>
         <!--<script  th:src="@{/xmjg/xndc/js/jquery.min.js}"
src="${ctx}/xmjg/xndc/js/jquery.min.js"  type="text/javascript"  charset="utf-8"></script>-->
         <script src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap.min.js"  type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/common/tool/date/js/bootstrap-datepicker.min.js"
type="text/javascript"></script>
         <script  src="/xm
...
...
...

         <link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global-rem.css"
type="text/css"></link>
         <script  src="/xmjg/xmjg/xndc/js/echarts.min.js" type="text/javascript"
charset="utf-8"></script>
         <script  src="/xmjg/resources/js/common/validate.js" type="text/javascript">
</script>
         <script  src="/xmjg/resources/js/common/public.js" type="text/javascript">
</script>
         <!--<script  th:src="@{/xmjg/xndc/js/analysis       /analysis-project-stage-list.js}"
src="${ctx}/xmjg/xndc/js/analysis/analysis-project-stage-list.js" type="text/javascript"
charset="utf-8"></script>-->
         <script  src="/xmjg/xmjg/supervisionInspection/js/city-project-stage-list.js"
type="text/javascript"  charset="utf-8"></script>
         <script type="text/javascript" charset="utf-8" src="/xmjg/common/tool/common.js">
</script>
         <!--        城市选择插件  开始 -->
         <script  src="/xmjg/common/tool/cityselect/js/city_data.js"
type="text/javascript" charset="utf-8"></script>
...
...
...
```

问题 19 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}" src. .. (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
```

```
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
}
.bacckbutton {
    float: right;
    margin: 3px 10px 5px 10px;
    width: 96px;
    height: 32px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
    }
 .dghy-itemWrap {
         float:left;
         margin-left:1%;
         width:19%;
         height:174px;
        }
</s
...
...
...
```

问题 20 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/city-page/getCsrk.action
实体：	<link rel="stylesheet" type="text/css" th:href="@{/xmjg/css/{screen}/common_new.css(screen=${session... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/city-page/getCsrk.action?
bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1
```

```
&startDate=2020-01-01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">

 <title>       城市入口</title>
 <script type="text/javascript">
    var ctx= "/xmjg/";
    var xzqhdm="660100";
    var flag = "1";
    var oldStartDate = "2020-01-01";
    var oldEndDate = "2020-12-29";
    var province="";
    var city="660100";
    var name="一师阿拉尔市";
    var defaultEndDate="",defaultStartDate="";
    var bigScreenFolder="";
    var provinceCode = "";
    var OrgName = "管理员";
    var districtAdminFlag = "1";
    var initHeartBeat = "";
    //是否是省级用户、管理员用户
 var isAdminUser = "true";
 var isProvinceUser = "false";
    var initStartDate="2018-06-01";//获取配置文件中统计时间的配置参数
 var sfType="";  //       算法类型
</script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

 <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/css/bootstrap.min.css"/>
 <link href="/xmjg/xmjg/supervisionInspection/css/element.css" rel="stylesheet"
type="text/css"/>
 <!--<link rel="stylesheet" type="text/css" th:href="@{/xmjg/csrk/css/xmjg-csrk-main-new-
rem.css}" href="${ctx}/xmjg/csrk/css/xmjg-csrk-main-new-rem.css"/>-->
 <link href="/xmjg/xmjg/xndc/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
 <!--<link rel="stylesheet" type="text/css"
th:href="@{/xmjg/css/{screen}/common_new.css(screen=${session.screen})}"/>-->
 <script src="/xmjg/region/vue.js"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/element.js"></script>
 <script src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" type="text/javascript" charset="utf-
8"></script>
 <!--<script th:src="@{/xmjg/csrk/js/jquery.min.js}"
src="${ctx}/xmjg/csrk/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>-->
 <script src="/xmjg/xmjg/xndc/js/bootstrap.min.js" type="text/javascript" charset="utf-8">
</script>


 <script src="/xmjg/xmjg/xndc/js/bootstrap-datepicker.min.js" type="text/javascript">
</script>
 <script src="/xmjg/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
 <script src="/xmjg/xmjg/csrk/js/echarts.min.js" type="text/javascript" charset="utf-8">
</script>
 <!--
    <script th:src="@{/xmjg/csrk/js/city-csrk-main-new.js}" src="${ctx}/xmjg/csrk/js/city-csrk-
main-new.js" type="text/javascript" charset="utf-8"></script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/city-page.js" type="text/javascript"
charset="utf-8"></script>
 <!--<script th:src="@{/common/tool/date/js/dateQuery.js}" type="text/javascript"
charset="utf-8"></script>-->
 <!--        城市选择插件  开始
...
...
...
```

问题 21 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	<img id="zzyimg" th:src="@{/dghyindex/img/xmjg/czjz.png}" src="${ctx}/dghyindex/img/xmjg/czjz.png" ... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
```

```
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-bo
...
...
...

                 <!--<div style="float:left;margin-top:0px;width:100%;" align="center">-->
                         <!--&lt;!&ndash;        财政性投融资工程建设项目(房屋建筑类)&ndash;&gt;-->
                         <!--<div style="float:left;width:21%;height:166px;text-
align:center;">-->
                                 <!--<div style="margin-top:0px;width:100%;height:1px;">
</div>-->
                                 <!--<img id="zzyimg"
th:src="@{/dghyindex/img/xmjg/czjz.png}"  src="${ctx}/dghyindex/img/xmjg/czjz.png"
style="cursor:pointer;" onclick="clickXmfl('1')"-->
                                         <!--onmouseover="setImgSrc(this,'over')"
onmouseout="setImgSrc(this,'out')" />-->
                                 <!--<div id="czjz"></div>-->
                         <!--</div>-->
                         <!---->
...
...
...
```

问题 22 / 33

TOC

HTML 注释敏感信息泄露	
严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	<img id="drrsimg" th:src="@{/dghyindex/img/xmjg/czxx.png}" src="${ctx}/dghyindex/img/xmjg/czxx.png"... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US
```

```
HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
```

```
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius:
...
...
...

                         <!---->
                         <!--&lt;!&ndash;        财政性投融资工程建设项目(线性工程类)&ndash;&gt;-->
                         <!--<div style="float:left;/*margin-
left:1%;*/width:10%;height:166px;text-align:center;">-->
                                 <!--<div style="margin-top:0px;width:100%;height:1px;">
</div>-->
                                 <!--<img id="drrsimg"
th:src="@{/dghyindex/img/xmjg/czxx.png}"  src="${ctx}/dghyindex/img/xmjg/czxx.png"
style="cursor:pointer;" onclick="clickXmfl('2')"-->
                                         <!--onmouseover="setImgSrc(this,'over')"
onmouseout="setImgSrc(this,'out')" />-->
                                 <!--<div id="czxx"></div>-->
                         <!--</div>-->
                         <!--&lt;!&ndash;        小型社会投资项目 &ndash;&gt;-->
...
...
...
```

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	<div style="float:left;margin-top:53px;width:1%;margin-left:1%;"><img th:src="@{/dghyindex/img/arrow... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
```

```
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
...
...
...

                <!--<h2><span>       项目生命周期</span></h2>-->
                <!--<div style="float:left;margin-left:1%;width:100%;">-->
                        <!--&lt;!&ndash;        工程规划许可 &ndash;&gt;-->
                        <!--<div id="label" style="float:left;height:100px;margin-
top:25px;width:20%;" onclick="clickSmzq('1','立项用地规划许可阶段')"></div>-->
                        <!--<div style="float:left;margin-top:53px;width:1%;margin-
left:1%;"><img th:src="@{/dghyindex/img/arrow.png}" src="${ctx}/dghyindex/img/arrow.png" />
</div>-->
                        <!--&lt;!&ndash;        工程建设许可 &ndash;&gt;-->
                        <!--<div id="label2" style="float:left;height:100px;margin-
top:25px;width:20%;margin-left:2%;" onclick="clickSmzq('2','工程建设许可')"></div>-->
                        <!--<div style="float:left;margin-top:53px;width:1%;margin-
left:1%;"><img th:src="@{/dghyindex/img/arrow.png}" src="${ctx}/dghyindex/img/arrow.png" />
</div>-->
                        <!--&lt;!&ndash;        施工许可 &ndash;&gt;-->
                        <!--<div id="label3" style="float:left;height:100px;margin-
top:25px;width:20%;margin-left:2%;" onclick="clickSmzq('3','施工许可')"></div>-->
                        <!--<div style="float:left;margin-top:53px;width:1%;margin-
left:1%;"><img th:src="@{/dghyindex/img/arrow.png}" src="${ctx}/dghyindex/img/arrow.png" />
</div>-->
                        <!--&lt;!&ndash;        竣工验收 &ndash;&gt;-->
```

```
                         <!--<div id="label4" style="float:left;height:100px;margin-
top:25px;width:20%;margin-left:2%;" onclick="clickSmzq('4','竣工验收')"></div>-->
                 <!--</div>-->
         <!--</div>-->
...
...
...
```

问题 24 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}" src="... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
```

```
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
```

```
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
}
.bacckbutton {
    float: right;
    margin: 3px 10px 5px 10px;
    width: 96px;
    height: 32px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
    }
 .dghy-itemWrap {
         float:left;
         margin-left:1%;
         width:19%;
         height:174px;
        }
</s
...
...
...
```

问题 25 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/city-page/getCsrk.action
实体：	<script th:src="@{/xmjg/csrk/js/city-csrk-main-new.js}" src="${ctx}/xmjg/csrk/js/city-csrk-main-new.... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/city-page/getCsrk.action?
bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1
&startDate=2020-01-01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">

 <title>       城市入口</title>
 <script type="text/javascript">
    var ctx= "/xmjg/";
    var xzqhdm="660100";
    var flag = "1";
    var oldStartDate = "2020-01-01";
    var oldEndDate = "2020-12-29";
    var province="";
    var city="660100";
    var name="一师阿拉尔市";
    var defaultEndDate="",defaultStartDate="";
    var bigScreenFolder="";
    var provinceCode = "";
    var OrgName = "管理员";
    var districtAdminFlag = "1";
    var initHeartBeat = "";
    //是否是省级用户、管理员用户
 var isAdminUser = "true";
 var isProvinceUser = "false";
```

```
    var initStartDate="2018-06-01";//获取配置文件中统计时间的配置参数
 var sfType="";  //       算法类型
</script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

 <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/css/bootstrap.min.css"/>
 <link href="/xmjg/xmjg/supervisionInspection/css/element.css" rel="stylesheet"
type="text/css"/>
 <!--<link rel="stylesheet" type="text/css" th:href="@{/xmjg/csrk/css/xmjg-csrk-main-new-
rem.css}" href="${ctx}/xmjg/csrk/css/xmjg-csrk-main-new-rem.css"/>-->
 <link href="/xmjg/xmjg/xndc/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
 <!--<link rel="stylesheet" type="text/css"
th:href="@{/xmjg/css/{screen}/common_new.css(screen=${session.screen})}"/>-->
 <script src="/xmjg/region/vue.js"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/element.js"></script>
 <script src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" type="text/javascript" charset="utf-
8"></script>
 <!--<script th:src="@{/xmjg/csrk/js/jquery.min.js}"
src="${ctx}/xmjg/csrk/js/jquery.min.js" type="text
...
...
...

 <script src="/xmjg/xmjg/xndc/js/bootstrap-datepicker.min.js" type="text/javascript">
</script>
 <script src="/xmjg/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
 <script src="/xmjg/xmjg/csrk/js/echarts.min.js" type="text/javascript" charset="utf-8">
</script>
 <!--
    <script th:src="@{/xmjg/csrk/js/city-csrk-main-new.js}" src="${ctx}/xmjg/csrk/js/city-csrk-
main-new.js" type="text/javascript" charset="utf-8"></script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/city-page.js" type="text/javascript"
charset="utf-8"></script>
 <!--<script th:src="@{/common/tool/date/js/dateQuery.js}" type="text/javascript"
charset="utf-8"></script>-->
 <!--        城市选择插件   开始 -->
 <link rel="stylesheet" type="text/css"
href="/xmjg/common/tool/cityselect/css/city_select.css"/>
```

```
...
...
...
```

问题 26 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	<img id="nlmyyimg" th:src="@{/dghyindex/img/xmjg/shba.png}" src="${ctx}/dghyindex/img/xmjg/shba.png... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
```

```
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-ra
...
...
...

                         <!--</div>-->
                         <!--&lt;!&ndash;        小型社会投资项目 &ndash;&gt;-->
                         <!--<div style="float:left;/*margin-
left:1%;*/width:22%;height:166px;text-align:center;">-->
                                 <!--<div style="margin-top:0px;width:100%;height:1px;">
</div>-->
                                 <!--<img id="nlmyyimg"
th:src="@{/dghyindex/img/xmjg/shba.png}"  src="${ctx}/dghyindex/img/xmjg/shba.png"
style="cursor:pointer;" onclick="clickXmfl('3')"-->
                                         <!--onmouseover="setImgSrc(this,'over')"
onmouseout="setImgSrc(this,'out')" />-->
                                 <!--<div id="xxsh"></div>-->
                         <!--</div>-->
                         <!--&lt;!&ndash;        一般社会投资项目(公开出让用地) &ndash;&gt;-->
...
...
...
```

问题 27 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/city-page/getCsrk.action
实体：	<link rel="stylesheet" type="text/css" th:href="@{/xmjg/csrk/css/xmjg-csrk-main-new-rem.css}" href= "... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/city-page/getCsrk.action?
bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1
&startDate=2020-01-01&endDate=2020-12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:47:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">

 <title>       城市入口</title>
 <script type="text/javascript">
    var ctx= "/xmjg/";
    var xzqhdm="660100";
    var flag = "1";
    var oldStartDate = "2020-01-01";
    var oldEndDate = "2020-12-29";
    var province="";
    var city="660100";
    var name="一师阿拉尔市";
    var defaultEndDate="",defaultStartDate="";
    var bigScreenFolder="";
    var provinceCode = "";
    var OrgName = "管理员";
    var districtAdminFlag = "1";
    var initHeartBeat = "";
    //是否是省级用户、管理员用户
 var isAdminUser = "true";
 var isProvinceUser = "false";
    var initStartDate="2018-06-01";//获取配置文件中统计时间的配置参数
 var sfType="";  //       算法类型
</script>

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

 <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/css/bootstrap.min.css"/>
 <link href="/xmjg/xmjg/supervisionInspection/css/element.css" rel="stylesheet"
type="text/css"/>
 <!--<link rel="stylesheet" type="text/css" th:href="@{/xmjg/csrk/css       /xmjg-csrk-main-new-
rem.css}" href="${ctx}/xmjg/csrk/css/xmjg-csrk-main-new-rem.css"/>-->
 <link href="/xmjg/xmjg/xndc/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
 <!--<link rel="stylesheet" type="text/css"
th:href="@{/xmjg/css/{screen}/common_new.css(screen=${session.screen})}"/>-->
 <script src="/xmjg/region/vue.js"></script>
 <script src="/xmjg/xmjg/supervisionInspection/js/element.js"></script>
 <script src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" type="text/javascript" charset="utf-
8"></script>
 <!--<script th:src="@{/xmjg/csrk/js/jquery.min.js}"
src="${ctx}/xmjg/csrk/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>-->
 <script src="/xmjg/xmjg/xndc/js/bootstrap.min.js" type="text/javascript" charset="utf-8">
</script>


 <script src="/xmjg/xmjg/xndc/js/bootstrap-datepicker.min.js" type="text/javascript">
</script>
 <script src="/xmjg/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js"
type="text/javascript"></script>
 <script src="/xmjg/xmjg/csrk/js/echarts.min.js" type="text/javascript" charset="utf-8">
</script>
 <!--
    <script th:src="@{/xmjg/csrk/js/city-csrk-main-new.js}" src="${ctx}/xmjg/csrk/js/city-csrk-
main-new.js" type="text/javascript" charset="utf-8"></script>-->
 <script src="/xmjg/xmjg/supervisionInspection/js/city-page.js" type="text/javascript"
charset="utf-8"></script>
 <!--<script th:src="@{/common/tool/date/js/dateQuery.js}" type="text/javascript" cha
...
...
...
```

问题 28 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	src="${ctx}/xmzh/project/img/tztj.png" onmouseover="overtztj()" (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
```

```
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: middle;
    border: 1px solid transparent;
}
.bacckbutton {
    float: right;

...
...
...
                                 <!--<div style="float:left;width:100%;">-->
                                         <!--<div style="float:left;width:32%;margin-
left:0px;margin-top:20px;"-->
                                                 <!--align="center">-->
                                                 <!--<img style="cursor:pointer;"
onclick="clickTZTJ()" id="tztjimg"-->
                                                 <!-       -
src="${ctx}/xmzh/project/img/tztj.png" onmouseover="overtztj()"-->
                                                 <!--onmouseout="outtztj()" />-->
                                         <!--</div>-->
                                         <!--<div style="float:left;margin-
left:0px;width:30%;margin-top:20px;"-->
                                                 <!--align="center">-->
...
...
...
```

问题 29 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	th:src="@{/xmzh/project/img/tjpm.png}" src="${ctx}/xmzh/project/img/tjpm.png" onmouseover="overc yy()... (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
```

```
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-borde
...
...
...

                                                 <!--&lt;!&ndash; <img
style="cursor:pointer;" onclick="clickSSZD()" id="sszdimg"-->
                                                 <!-       -
src="${ctx}/xmzh/project/img/sszd.png" onmouseover="oversszd()"-->
                                                 <!--onmouseout="outsszd()" /> <br
/>&ndash;&gt;-->
                                                 <!--<img style="cursor:pointer;"
onclick="clickPmtj()" id="pmtjimg"-->
                                                  <!-       -
th:src="@{/xmzh/project/img/tjpm.png}" src="${ctx}/xmzh/project/img/tjpm.png"
onmouseover="overcyy()"-->
                                                 <!--align="center" onmouseout="outcyy()"
/> <br />-->
                                         <!--</div>-->
                                         <!--&lt;!&ndash; <div style="float:left;margin-
left:0px;width:32%;" align="center">-->
                                                 <!--<img style="cursor:pointer;"
onclick="clickZBLS()" id="zblsimg"-->
...
...
...
```

问题 30 / 33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	src="${ctx}/xmzh/project/img/zbls.png" onmouseover="overzbls()" (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
```

```
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-radius: 2px;
    border-radius: 2px;
    -khtml-border-radius: 2px;
    text-align: center;
    vertical-align: mi
...
...
...
                                                 <!--align="center" onmouseout="outcyy()"
/> <br />-->
                                         <!--</div>-->
                                         <!--&lt;!&ndash; <div style="float:left;margin-
left:0px;width:32%;" align="center">-->
                                                 <!--<img style="cursor:pointer;"
onclick="clickZBLS()" id="zblsimg"-->
                                                 <!-       -
src="${ctx}/xmzh/project/img/zbls.png" onmouseover="overzbls()"-->
                                                 <!--align="center" onmouseout="outzbls()"
/> <br />-->
                                         <!--</div>-->
                                         <!--<div style="float:left;margin-
left:0px;width:30%;" align="center">-->
                                                 <!--<img style="cursor:pointer;"
onclick="clickCYL()" id="cylimg"-->
...
...
...
```

问题　31　/　33

TOC

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action
实体：	src="${ctx}/xmzh/project/img/sszd.png" onmouseover="oversszd()" (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-
12-29 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
```

```
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:46:17 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
 <meta charset="utf-8">
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
 <meta http-equiv="viewport" content="width=device-width,initial-scale=1.0">
 <title>       多规行业首页</title>
<script type="text/javascript">
 var ctx="/xmjg/";
 var xzqhdm ="660000";
 var startDate ="2020-01-01";
 var endDate ="2020-12-29";
</script>
<script type="text/javascript" src="/xmjg/resources/js/jquery/jquery.js"></script>
<script type="text/javascript" src="/xmjg/resources/easyui/easycore.js"></script>
<script type="text/javascript" src="/xmjg/resources/js/dghy/index.js"></script>
<!--
<script type="text/javascript" th:src="@{/resources/components/raphael_jquery/js/raphael.js}"
src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/js/index-dghy-main.js"></script>
<script type="text/javascript" src="/xmjg/dghyindex/js/dghy-public.js"></script>
<!--
<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}"
src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
-->
<script type="text/javascript" src="/xmjg/dghyindex/echarts/build/dist/echarts.js"></script>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/frame.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/global.css" type="text/css"/>
<link rel="stylesheet" href="/xmjg/resources/css/dghyindex/css/index.css" type="text/css"/>
<style type="text/css">
.progresstext {
    width: 60px;
    height: 60px;
    line-height: 60px;
    position: absolute;
    margin-top: -60px;
    text-align: center;
    color: #9e9fa3;
    font-size: 18px;
    font-family: Arial;
}
.showEllipsis{
 width:170px;
 display:block;
 overflow:hidden;
 word-break:keep-all;
 white-space:nowrap;text-overflow:ellipsis;
}
.menu_img_right_count{
 position:relative;
 top:-70px;
 left:52px;
 z-index:1;
 border-radius: 10px;
 behavior: url(ie-css3.htc);
 padding:1px 5px;
 color: #fff;
 font-size: 12px;
 font-weight:700;
 line-height:18px;
 text-align:center;
 background-color: #e86d00;
}
.zr-element{cursor:pointer;}
.smzq h2 span {
 background: url("../dghyindex/img/h2_bg.png") no-repeat 0 0;
 width: 172px;
 height: 33px;
 line-height: 33px;
 font-size: 16px;
 color: #fff;
 text-indent: 16px;
 display: block;
 margin-top: 0px;
 margin-left: -1px;
}
.smzq h2 {
 height: 32px;
 background-color: #f1f8ff;
 border-bottom: 1px solid #d3e3f3;
}
#bg{ display: none; position: absolute; top: 0%; left: 0%; width: 100%; height: 1540px;
background-color: black; z-index:1001; -moz-opacity: 0.4; opacity:.40; filter:
alpha(opacity=40);}
#show{display: none; position: absolute; width: 100%;height: 100%;background:
rgba(0,0,0,.5);left:0}
#show img {
 width: 100px;
 height: 100px;
 margin: 20% 0 0 45%;

 /*top: 40%; left: 45%; width: 166px; height: 50px; padding: 5px; border: 5px solid
#E8E9F7;border-radius:3px; background-color: white; z-index:1002; overflow: auto;*/
}
.loadingText {
 width: 148px;
 margin: 11px 0 0 44%;
 color:#fff;
}
.searchbutton{
    margin: 3px 10px 5px 10px;
    width: 60px;
    height: 25px;
    background-color: #006ecc;
    border-color: #357ebd;
    color: #fff;
    -moz-border-radius: 2px;
    -webkit-border-ra
...
...
...

                         <!--<div style="float:left;margin-top:10%;margin-left:2%;margin-
bottom: 10%">-->
                                 <!--<div style="float:left;width:100%;">-->
                                         <!--<div style="float:left;width:32%;"
align="center">-->
                                                 <!--&lt;!&ndash; <img
style="cursor:pointer;" onclick="clickSSZD()" id="sszdimg"-->
                                                 <!-       -
src="${ctx}/xmzh/project/img/sszd.png" onmouseover="oversszd()"-->
                                                 <!--onmouseout="outsszd()" /> <br
/>&ndash;&gt;-->
                                                 <!--<img style="cursor:pointer;"
onclick="clickPmtj()" id="pmtjimg"-->
                                                  <!-       -
th:src="@{/xmzh/project/img/tjpm.png}" src="${ctx}/xmzh/project/img/tjpm.png"
onmouseover="overcyy()"-->
                                                 <!--align="center" onmouseout="outcyy()"
/> <br />-->
...
...
...
```

HTML 注释敏感信息泄露

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do
实体：	chageClass(this.id); (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/csrk/oneSystemByMd.do?
city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29&provinceCode= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 05:12:15 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Transfer-Encoding: chunked

<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <title>一个系统</title>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">

    <script>
        //用于子页面排序的变量
        var orderClickName = "";
        var orderClickCount = 0;
        var orderNameId;

        var ctx = '/xmjg/';
        var oldStartDate = "2020-01-01";
        var oldEndDate = "2020-12-29";
        var bigScreenFolder=""; //大屏css 目录，如果是普通屏（默认）则该值为空
        var defaultSelect ="${currentCityName}";
        var dqcs="660100";
        var xzqhdm = "660100";
        var name = decodeURIComponent("%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82");
        var xmlx="";
        var djzt="";//该状态位默认为2，正在办理   ，  -1：代表正在使用及时率、超期率的统计
        var pm_count = ""; //统计排名状态，1：  及时率、2：超期率
        var dqspjd = "";
        var splclxData ;
        var provinceCode = "";
    </script>
    <!--引入样式-->

<!-- 项目名称 -->
<!--<c:set var="ctx" value="${pageContext.request.contextPath}"/>-->
<!-- 风格样式 -->
<!--<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>-->

<script src="/xmjg/common/tool/common.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/common-core.js" type="text/javascript" charset="utf-8"></script>
<script src="/xmjg/common/tool/projectManager.js" type="text/javascript" charset="utf-8">
</script>
<script>
    var isWhite = '';
    var screen = (isWhite=="white"?3:0);
    function initWhite(){
        $.ajax({
          type: "POST",
          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',
          dataType: "json",
          async:false,

          success: function (result) {

          screen = result;
          if("3"==result){
          var doc=document;
          var link=doc.createElement("link");
          link.setAttribute("rel", "stylesheet");
          link.setAttribute("type", "text/css");
          link.setAttribute("href", ctx+"/xmjg/css/white/common_new.css");
          var heads = doc.getElementsByTagName("head");
          if(heads.length)
          heads[0].appendChild(link);
          else
          doc.documentElement.appendChild(link);
          }
          }
        });
    }
</script>

    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/css/bootstrap.min.css"/>
    <link href="/xmjg/xmjg/xndc/css/bootstrap-datepicker3.standalone.css" title=""
rel="stylesheet"/>
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/index-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/jieduan3-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/searchArea-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/global-rem.css" />
    <link rel="stylesheet" type="text/css" href="/xmjg/resources/easyui/themes/icon.css"/>
    <link rel="stylesheet" type="text/css"
href="/xmjg/resources/easyui/themes/default/easyui.css"/>
    <link rel="stylesheet" type="text/css" href="/xmjg/xmjg/xndc/css/dg-xndc-main-rem.css" />
    <script src="/xmjg/xmjg/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>
    <script type="text/javascript" src="/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js" charset="utf-8">
</script>
    <!--<script src="/xmjg/resources/easyui/jquery
...
...
...

          <div onclick="changeTab('0')" id="xmspjdtab" class="jstabselected">项目审批阶段</div>

          </div>
          <div id="optionDiv" style="display:none" >
          <input id="ApprovedId" type="button" class="c-ApprovedId"
onclick="showProInfo_xmlx('','备案类');" value="备案类"><!-- chageClass(this.id); -->
          </div>
          <div id="tabCon" style="height:100%">
          <div id="tabCon_0" class="c-tabCon_0" >
          </div>
```

```
...
...
...
```

问题 33 / 33

TOC

HTML 注释敏感信息泄露	
严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html
实体：	This snippet is used in production (included from viewer.html) (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	程序员在 Web 页面上留下调试信息
固定值：	除去 HTML 注释中的敏感信息

差异：

推理： AppScan 发现了包含看似为敏感信息的 HTML 注释。

测试请求和响应：

```
GET /xmjg/xmjg/csrk/pdfShow/web/viewer.html?file=%20/xmjg/file/yzbd/yishialaer/pdf/7fa992eb-5923-
419b-9cbc-
612db98522ba%E2%80%BB%E4%B8%80%E9%98%B6%E6%AE%B5%E5%8A%9E%E4%BA%8B%E6%8C%87%E5%8D%97.pdf HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//xmjg-one-form!getYzbd.action?
name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 22080
Last-Modified: Mon, 21 Sep 2020 04:41:14 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 05:12:16 GMT
Content-Type: text/html;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

<!DOCTYPE html>
<!--
Copyright 2012 Mozilla Foundation

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
```

```
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

Adobe CMap resources are covered by their own copyright but the same license:

    Copyright 1990-2015 Adobe Systems Incorporated.

See https://github.com/adobe-type-tools/cmap-resources
-->
<html dir="ltr" mozdisallowselectionprint>
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
    <meta name="google" content="notranslate">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>PDF.js viewer</title>


    <link rel="stylesheet" href="viewer.css">


<!-- This snippet is used in production (included from viewer.html) -->
<link rel="resource" type="application/l10n" href="locale/locale.properties">
<script src="../build/pdf.js"></script>


    <script src="viewer.js"></script>

  </head>

  <body tabindex="1" class="loadingInProgress">
    <div id="outerContainer">

      <div id="sidebarContainer">
        <div id="toolbarSidebar">
          <div class="splitToolbarButton toggled">
          <button id="viewThumbnail" class="toolbarButton toggled" title="Show Thumbnails"
tabindex="2" data-l10n-id="thumbs">
          <span data-l10n-id="thumbs_label">Thumbnails</span>
          </button>
          <button id="viewOutline" class="toolbarButton" title="Show Document Outline (double-
click to expand/collapse all items)" tabindex="3" data-l10n-id="document_outline">
          <span data-l10n-id="document_outline_label">Document Outline</span>
          </button>
          <button id="viewAttachments" class="toolbarButton" title="Show Attachments"
tabindex="4" data-l10n-id="attachments">
          <span data-l10n-id="attachments_label">Attachments</span>
          </button>
          </div>
        </div>
        <div id="sidebarContent">
          <div id="thumbnailView">
          </div>
          <div id="outlineView" class="hidden">
          </div>
          <div id="attachmentsView" class="hidden">
          </div>
        </div>
        <div id="sidebarResizer" class="hidden"></div>
      </div>  <!-- sidebarContainer -->

      <div id="mainContainer">
        <div class="findbar hidden doorHanger" id="findbar">
          <div id="findbarInputContainer">
          <input id="findInput" class="toolbarField" title="Find" placeholder="Find in document…"
tabindex="91" data-l10n-id="find_input">
          <div class="splitToolbarButton">
          <button id="findPrevious" class="toolbarButton findPrevious" title="Find the previous
occurrence of the phrase" tabindex="92" data-l10n-id="find_previous">
          <span data-l10n-id="find_previous_label">Previous</span>
          </button>
          <div class="splitToolbarButtonSeparator"></div>
          <button id="findNext" class="toolbarButton findNext" title="Find the next occurrence of
the phrase" tabindex="93" data-l10n-id="find_next">
          <span data-l10n-id="find_next_label">Next</span>
          </button>
```

```
            </div>
            </div>

            <div id="findbarOptionsOneContainer">
            <input type="checkbox" id="findHighlightAll" class="toolbarField" tabindex="94">
            <label for="findHighlightAll
...
...
...
```

参 发现电子邮件地址模式 11 TOC

问题 1 / 11 TOC

发现电子邮件地址模式	
严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/jquery.cookie.js
实体：	jquery.cookie.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。

测试请求和响应：

```
GET /opus-front-sso/framework/ui-themes/common/metronic/js/jquery.cookie.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/require
Cookie: JSESSIONID=D6A5925ADA251562D8C32F08668AA5EE
Connection: keep-alive
Host: 127.0.0.1:8090
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 28 Dec 2020 07:36:44 GMT
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Content-Length: 4467
X-Content-Type-Options: nosniff
Cache-Control: max-age=31556926
Date: Tue, 29 Dec 2020 02:44:19 GMT
Content-Type: application/javascript;charset=utf-8

/**
 * Cookie plugin
 *
 * Copyright (c) 2006 Klaus Hartl (stilbuero.de)
 * Dual licensed under the MIT and GPL licenses:
 * http://www.opensource.org/licenses/mit-license.php
 * http://www.gnu.org/licenses/gpl.html
 *
 */

/**
 * Create a cookie with the given name and value and other optional parameters.
 *
 * @example $.cookie('the_cookie', 'the_value');
 * @desc Set the value of a cookie.
 * @example $.cookie('the_cookie', 'the_value', { expires: 7, path: '/', domain: 'jquery.com',
secure: true });
 * @desc Create a cookie with all available options.
 * @example $.cookie('the_cookie', 'the_value');
 * @desc Create a session cookie.
 * @example $.cookie('the_cookie', null);
 * @desc Delete a cookie by passing null as value. Keep in mind that you have to use the same
path and domain
 *       used when the cookie was set.
 *
 * @param String name The name of the cookie.
 * @param String value The value of the cookie.
 * @param Object options An object literal containing key/value pairs to provide optional cookie
attributes.
 * @option Number|Date expires Either an integer specifying the expiration date from now on in
days or a Date object.
 *          If a negative value is specified (e.g. a date in the past), the cookie will be
deleted.
 *          If set to null or omitted, the cookie will be a session cookie and will not be
retained
 *          when the the browser exits.
 * @option String path The value of the path atribute of the cookie (default: path of page that
created the cookie).
 * @option String domain The value of the domain attribute of the cookie (default: domain of page
that created the cookie).
 * @option Boolean secure If true, the secure attribute of the cookie will be set and the cookie
transmission will
 *          require a secure protocol (like HTTPS).
 * @type undefined
 *
 * @name $.cookie
 * @cat Plugins/Cookie
 * @author Klaus Hartl/klaus.hartl@stilbuero.de
 */

/**
 * Get the value of a cookie with the given name.
 *
 * @example $.cookie('the_cookie');
 * @desc Get the value of a cookie.
 *
 * @param String name The name of the cookie.
 * @return The value of the cookie.
 * @type String
 *
 * @name $.cookie
 * @cat Plugins/Cookie
 * @author Klaus Hartl/klaus.hartl@stilbuero.de
 */
jQuery.cookie = function(name, value, options) {
    if (typeof value != 'undefined') { // name and value given, set cookie
        options = options || {};
        if (value === null) {
          value = '';
          options = $.extend({}, options); // clone object since it's unexpected behavior if the
expired property were changed
          options.expires = -1;
        }
        var expires = '';
        if (options.expires && (typeof options.expires == 'number' ||
options.expires.toUTCString)) {
          var date;
          if (typeof options.expires == 'number') {
          date = new Date();
          date.setTime(date.getTime() + (options.expires * 24 * 60 * 60 * 1000));
          } else {
```

```
          date = options.expires;
          }
          expires = '; expires=' + date.toUTCString(); // use expires attribute, max-age is not
supported by IE
        }
        // NOTE Needed to parenthesize options.path and options.domain
        // in the following expressions, otherwise they evaluate to undefined
        // in the packed version for some reason...
        var path = options.path ? '; path=' + (options.path) : '';
        var domain = options.domain ? '; domain=' + (options.domain) : '';
        var secure = options.secure ? '; secure' : '';
        document.cookie = [name, '=', encodeURIComponent(value), expires, path, domain,
secure].join('');
    } else { // only name given, get cookie
        var cookieValue = null;
        if (document.cookie && document.cookie != '') {
          var cookies = document.cookie.split(';');
          for (var i = 0; i < cookies.length; i++) {
          var cookie = jQuery.trim(cookies[i]);
          // Does this cookie string begin with the name we want?
          if (cookie.substring(0, name.length
...
...
...
```

问题 2 / 11

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8090/opus-front-sso/js/sm4.js
实体：	sm4.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。

测试请求和响应：

```
GET /opus-front-sso/js/sm4.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/require
Cookie: JSESSIONID=D6A5925ADA251562D8C32F08668AA5EE
Connection: keep-alive
Host: 127.0.0.1:8090
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 28 Dec 2020 07:36:44 GMT
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Content-Length: 13826
X-Content-Type-Options: nosniff
Cache-Control: max-age=31556926
```

```
Date: Tue, 29 Dec 2020 02:44:20 GMT
Content-Type: application/javascript;charset=utf-8

/**
 * base64js
 */
/**
 * base64js
 * base64js.toByteArray(d.input)
 * base64js.fromByteArray(c);
 * @author c.z.s
 * @email 1048829253@qq.com
 * @company
 * @date 2018-07
 *
 */
(function(r){if(typeof exports==="object"&&typeof module!=="undefined")
{module.exports=r()}else{if(typeof define===
    "function"&&define.amd){define([],r)}else{var e;if(typeof window!=="undefined")
{e=window}else{if(typeof global
    !=="undefined"){e=global}else{if(typeof self!=="undefined")
{e=self}else{e=this}}e.base64js=r()}}})(function(){
  var r,e,t;return function r(e,t,n){function o(i,a){if(!t[i]){if(!e[i]){var u=typeof
require=="function"&&require;if(!a&&u){
    return u(i,!0)}if(f){return f(i,!0)}var d=new Error("Cannot find module '"+i+"'");throw
d.code="MODULE_NOT_FOUND",d}
    var c=t[i]={exports:{}};e[i][0].call(c.exports,function(r){var t=e[i][1][r];return o(t?
t:r)},c,c.exports,r,e,t,n)}return t[i].exports}
    var f=typeof require=="function"&&require;for(var i=0;i<n.length;i++){o(n[i])}return o}({"/":
[function(r,e,t){t.byteLength=c;
      t.toByteArray=v;t.fromByteArray=s;var n=[];var o=[];var f=typeof Uint8Array!=="undefined"?
Uint8Array:Array;
      var i="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";for(var
a=0,u=i.length;a<u;++a){n[a]=i[a];
        o[i.charCodeAt(a)]=a}o["-".charCodeAt(0)]=62;o["_".charCodeAt(0)]=63;function d(r){var
e=r.length;if(e%4>0){
        throw new Error("Invalid string. Length must be a multiple of 4")}return r[e-2]==="="?
2:r[e-1]==="="?1:0}
      function c(r){return r.length*3/4-d(r)}function v(r){var e,t,n,i,a;var
u=r.length;i=d(r);a=new f(u*3/4-i);t=i>0?u-4:u;
        var c=0;for(e=0;e<t;e+=4){n=o[r.charCodeAt(e)]<<18|o[r.charCodeAt(e+1)]
<<12|o[r.charCodeAt(e+2)]<<6|o[r.charCodeAt(e+3)];
          a[c++]=n>>16&255;a[c++]=n>>8&255;a[c++]=n&255}if(i===2){n=o[r.charCodeAt(e)]
<<2|o[r.charCodeAt(e+1)]>>4;a[c++]=n&255}
        else{if(i===1){n=o[r.charCodeAt(e)]<<10|o[r.charCodeAt(e+1)]
<<4|o[r.charCodeAt(e+2)]>>2;a[c++]=n>>8&255;a[c++]=n&255}}return a}
      function l(r){return n[r>>18&63]+n[r>>12&63]+n[r>>6&63]+n[r&63]}function h(r,e,t){var n;var
o=[];for(var f=e;f<t;f+=3){
        n=(r[f]<<16)+(r[f+1]<<8)+r[f+2];o.push(l(n))}return o.join("")}function s(r){var e;var
t=r.length;var o=t%3;var f="";var i=[];
        var a=16383;for(var u=0,d=t-o;u<d;u+=a){i.push(h(r,u,u+a>d?d:u+a))}if(o===1){e=r[t-
1];f+=n[e>>2];f+=n[e<<4&63];f+="=="}else{if(o===2){
          e=(r[t-2]<<8)+r[t-1];f+=n[e>>10];f+=n[e>>4&63];f+=n[e<<2&63];f+="="}}i.push(f);return
i.join("")}},{}]},{},[])("/")});


/**
 * 国密SM4加密算法
 * @author c.z.s
 * @email 1048829253@qq.com
 * @company GDT-ZWZX-DEV-PT
 * @date 2018-07
 */
function SM4_Context() {
  this.mode=1;
  this.isPadding = true;
  this.sk = new Array(32);
}

function SM4() {
  this.SM4_ENCRYPT=1;
  this.SM4_DECRYPT = 0;

  var SboxTable =
[0xd6,0x90,0xe9,0xfe,0xcc,0xe1,0x3d,0xb7,0x16,0xb6,0x14,0xc2,0x28,0xfb,0x2c,0x05,
    0x2b,0x67,0x9a,0x76,0x2a,0xbe,0x04,0xc3,0xaa,0x44,0x13,0x26,0x49,0x86,0x06,0x99,
    0x9c,0x42,0x50,0xf4,0x91,0xef,0x98,0x7a,0x33,0x54,0x0b,0x43,0xed,0xcf,0xac,0x62,
    0xe4,0xb3,0x1c,0xa9,0xc9,0x08,0xe8,0x95,0x80,0xdf,0x94,0xfa,0x75,0x8f,0x3f,0xa6,
    0x47,0x07,0xa7,0xfc,0xf3,0x73,0x17,0xba,0x83,0x59,0x3c,0x19,0xe6,0x85,0x4f,0xa8,
    0x68,0x6b,0x81,0xb2,0x71,0x64,0xda,0x8b,0xf8,0xeb,0x0f,0x4b,0x70,0x56,0x9d,0x35,
    0x1e,0x24,0x0e,0x5e,0x63,0x58,0xd1,0xa2,0x25,0x22,0x7c,0x3b,0x01,0x21,0x78,0x87,
    0xd4,0x00,0x46,0x57,0x9f,0xd3,0x27,0x52,0x4c,0x36,0x02,0xe7,0xa0,0xc4,0xc8,0x9e,
    0xea,0xbf,0x8a,0xd2,0x40,0xc7,0x38,0xb5,0xa3,0xf7,0xf2,0xce,0xf9,0x61,0x15,0xa1,
    0xe0,0xae,0x5d,0xa4,0x9b,0x34,0x1a,0x55,0xad,0x93,0x32,0x30,0xf5,0x8c,0xb1,0xe3,
    0x1d,0xf6,0xe2,0x2e,0x82,0x66,0xca,0x60,0xc0,0x29,0x23,0xab,0x0d,0x53,0x4e,0x6f,
    0xd5,0xdb,0x37,0x45,0xde,0xfd,0x8e,0x2f,0x03,0xff,0x6a,0x72,0x6d,0x6c,0x5b,0x51,
    0x8d,0x1b,0xaf,0x92,0xbb,0xdd,0xbc,0x7f,0x11,0xd9,0x5c,0x41,0x1f,0x10,0x5a,0xd8,
    0x0a,0xc1,0x31,0x88,0xa5,0xcd,0x7b,0xbd,0x2d,0x74,0xd0,0x12,0xb8,0xe5,0xb4,0xb0,
    0x89,0x69,0x97,0x4a,0x0c,0x96,0x77,0x7e,0x65,0xb9,0xf1,0x09,0xc5,0x6e,0xc6,0x84,
    0x18,0xf0,0x7d,0xec,0x3a,0xdc,0x4d,0x20,0x79,0xee,0x5f,0x3e,0xd7,0xcb,0x39,0x48];

  var
...
...
...
```

问题 3 / 11

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/vendors.bundle.js
实体：	vendors.bundle.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。

测试请求和响应：

```
GET /opus-front-sso/framework/ui-themes/common/metronic/js/vendors.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/require
Cookie: JSESSIONID=D6A5925ADA251562D8C32F08668AA5EE
Connection: keep-alive
Host: 127.0.0.1:8090
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 28 Dec 2020 07:36:44 GMT
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Content-Length: 3899883
X-Content-Type-Options: nosniff
Cache-Control: max-age=31556926
Date: Tue, 29 Dec 2020 02:44:21 GMT
Content-Type: application/javascript;charset=utf-8

/*!
 * jQuery JavaScript Library v3.2.1
 * https://jquery.com/
 *
 * Includes Sizzle.js
 * https://sizzlejs.com/
 *
 * Copyright JS Foundation and other contributors
 * Released under the MIT license
 * https://jquery.org/license
 *
 * Date: 2017-03-20T18:59Z
 */
( function( global, factory ) {

 "use strict";

 if ( typeof module === "object" && typeof module.exports === "object" ) {

         // For CommonJS and CommonJS-like environments where a proper `window`
         // is present, execute the factory and get jQuery.
         // For environments that do not have a `window` with a `document`
         // (such as Node.js), expose a factory as module.exports.
         // This accentuates the need for the creation of a real `window`.
         // e.g. var jQuery = require("jquery")(window);
         // See ticket #14549 for more info.
         module.exports = global.document ?
                 factory( global, true ) :
                 function( w ) {
                         if ( !w.document ) {
                                 throw new Error( "jQuery requires a window with a
document" );
                                }
                         return factory( w );
                 }       ;
 } else {
         factory( global );
        }

// Pass this if window is not defined yet
} )( typeof window !== "undefined" ? window : this, function( window, noGlobal ) {

// Edge <= 12 - 13+, Firefox <=18 - 45+, IE 10 - 11, Safari 5.1 - 9+, iOS 6 - 9.1
// throw exceptions when non-strict code (e.g., ASP.NET 4.5) accesses strict mode
// arguments.callee.caller (trac-13335). But as of jQuery 3.0 (2016), strict mode should be
common
// enough that all such attempts are guarded in a try block.
"use strict";

var arr = [];

var document = window.document;

var getProto = Object.getPrototypeOf;

var slice = arr.slice;

var concat = arr.concat;

var push = arr.push;

var indexOf = arr.indexOf;

var class2type = {};

var toString = class2type.toString;

var hasOwn = class2type.hasOwnProperty;

var fnToString = hasOwn.toString;

var ObjectFunctionString = fnToString.call( Object );

var support = {};



 function DOMEval( code, doc ) {
         doc = doc || document;

         var script = doc.createElement( "script" );
         script.text = code;
         doc.head.appendChild( script ).parentNode.removeChild( script );
        }
/* global Symbol */
// Defining this global in .eslintrc.json would create a danger of using the global
// unguarded in another place, it seems safer to define global only for this module



var
 version = "3.2.1",

 // Define a local copy of jQuery
 jQuery = function( selector, context ) {

         // The jQuery object is actually just the init constructor 'enhanced'
         // Need init if jQuery is called (just allow error to be thrown if not included)
         return new jQuery.fn.init( selector, context );
 },

 // Support: Android <=4.0 only
 // Make sure we trim BOM and NBSP
 rtrim = /^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,

 // Matches dashed string for camelizing
 rmsPrefix = /^-ms-/,
 rdashAlpha = /-([a-z])/g,

 // Used by jQuery.camelCase as callback to replace()
 fcamel
...
...
...


// jquery.input version 0.0.0
// https://github.com/DubFriend/jquery.input
// (MIT) 09-04-2014
// Brian Detering <BDeterin@gmail.com> (http://www.briandetering.net/)
(function ($) {
'use strict';

var createBaseInput = function (fig, my) {
...
...
...

License: MIT License (MIT)
*/

/*
Copyright Manos Malihutsakis (email: manos@malihu.gr)

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
...
...
...

  * bootstrap-switch - Turn checkboxes and radio buttons into toggle switches.
  *
  * @version v3.3.4
  * @homepage https://bttstrp.github.io/bootstrap-switch
  * @author Mattia Larentis <mattia@larentis.eu> (http://larentis.eu)
  * @license Apache-2.0
  */

(function (global, factory) {
...
...
...


// Released under MIT license
// Copyright (c) 2009-2010 Dominic Baggott
// Copyright (c) 2009-2010 Ash Berlin
// Copyright (c) 2011 Christoph Dorn <christoph@christophdorn.com> (http://www.christophdorn.com)
```

```
/*jshint browser:true, devel:true */

(function( expose ) {
...
...
...
```

问题 4 / 11

TOC

发现电子邮件地址模式	
严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-table-editable.js
实体：	bootstrap-table-editable.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。

测试请求和响应：

```
GET /xmjg/bootstrap/js/bootstrap-table-editable.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//xmjg-one-form!getYzbd.action?
name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 3915
Last-Modified: Mon, 21 Sep 2020 04:41:10 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:50:42 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

/**
 * @author zhixin wen <wenzhixin2010@gmail.com>
 * extensions: https://github.com/vitalets/x-editable
 */

!function ($) {

    'use strict';

    $.extend($.fn.bootstrapTable.defaults, {
```

```
    editable: true,
    onEditableInit: function () {
      return false;
    },
    onEditableSave: function (field, row, oldValue, $el) {
      return false;
    },
    onEditableShown: function (field, row, $el, editable) {
      return false;
    },
    onEditableHidden: function (field, row, $el, reason) {
      return false;
    }
});

$.extend($.fn.bootstrapTable.Constructor.EVENTS, {
    'editable-init.bs.table': 'onEditableInit',
    'editable-save.bs.table': 'onEditableSave',
    'editable-shown.bs.table': 'onEditableShown',
    'editable-hidden.bs.table': 'onEditableHidden'
});

var BootstrapTable = $.fn.bootstrapTable.Constructor,
    _initTable = BootstrapTable.prototype.initTable,
    _initBody = BootstrapTable.prototype.initBody;

BootstrapTable.prototype.initTable = function () {
    var that = this;
    _initTable.apply(this, Array.prototype.slice.apply(arguments));

    if (!this.options.editable) {
      return;
    }

    $.each(this.columns, function (i, column) {
      if (!column.editable) {
      return;
      }

      var _formatter = column.formatter;
      column.formatter = function (value, row, index) {
      var result = _formatter ? _formatter(value, row, index) : value;

      return ['<a href="javascript:void(0)"',
      ' data-name="' + column.field + '"',
      ' data-pk="' + row[that.options.idField] + '"',
      ' data-value="' + result + '"',
      '>' + '</a>'
      ].join('');
      };
    });
};

BootstrapTable.prototype.initBody = function () {
    var that = this;
    _initBody.apply(this, Array.prototype.slice.apply(arguments));

    if (!this.options.editable) {
      return;
    }

    $.each(this.columns, function (i, column) {
      if (!column.editable) {
      return;
      }

      that.$body.find('a[data-name="' + column.field + '"]').editable(column.editable)
      .off('save').on('save', function (e, params) {
      var data = that.getData(),
      index = $(this).parents('tr[data-index]').data('index'),
      row = data[index],
      oldValue = row[column.field];

      row[column.field] = params.submitValue;
      that.trigger('editable-save', column.field, row, oldValue, $(this));
      });
      that.$body.find('a[data-name="' + column.field + '"]').editable(column.editable)
      .off('shown').on('shown', function (e, editable) {
          var data = that.getData(),
          index = $(this).parents('tr[data-index]').data('index'),
          row = data[index];

          that.trigger('editable-shown', column.field, row, $(this), editable);
          });
          that.$body.find('a[data-name="' + column.field + '"]').editable(column.editable)
          .off('hidden').on('hidden', function (e, reason) {
          var data = that.getData(),
          index = $(this).parents('tr[data-index]').data('index'),
          row = data[index];

          that.trigger('editable-hidden', column.field, row, $(this), reason);
          });
        });
        this.trigger('editable-init');
    };

}(jQuery);
```

问题 5 / 11

TOC

发现电子邮件地址模式	
严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-table.js
实体：	bootstrap-table.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。

测试请求和响应：

```
GET /xmjg/bootstrap/js/bootstrap-table.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?
bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1
&startDate=2020-01-01&endDate=2020-12-29
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 96734
Last-Modified: Mon, 21 Sep 2020 04:41:10 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:47:33 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
```

```
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

/**
 * @author zhixin wen <wenzhixin2010@gmail.com>
 * version: 1.9.0
 * https://github.com/wenzhixin/bootstrap-table/
 */

!function ($) {
    'use strict';

    // TOOLS DEFINITION
    // ======================

    var cachedWidth = null;

    // it only does '%s', and return '' when arguments are undefined
    var sprintf = function (str) {
        var args = arguments,
          flag = true,
          i = 1;

        str = str.replace(/%s/g, function () {
          var arg = args[i++];

          if (typeof arg === 'undefined') {
          flag = false;
          return '';
          }
          return arg;
        });
        return flag ? str : '';
    };

    var getPropertyFromOther = function (list, from, to, value) {
        var result = '';
        $.each(list, function (i, item) {
          if (item[from] === value) {
          result = item[to];
          return false;
          }
          return true;
        });
        return result;
    };

    var getFieldIndex = function (columns, field) {
        var index = -1;

        $.each(columns, function (i, column) {
          if (column.field === field) {
          index = i;
          return false;
          }
          return true;
        });
        return index;
    };

    // http://jsfiddle.net/wenyi/47nz7ez9/3/
    var setFieldIndex = function (columns) {
        var i, j, k,
          totalCol = 0,
          flag = [];

        for (i = 0; i < columns[0].length; i++) {
          totalCol += columns[0][i].colspan || 1;
        }

        for (i = 0; i < columns.length; i++) {
          flag[i] = [];
          for (j = 0; j < totalCol; j++) {
          flag[i][j] = false;
          }
        }

        for (i = 0; i < columns.length; i++) {
          for (j = 0; j < columns[i].length; j++) {
```

```
          var r = columns[i][j],
          rowspan = r.rowspan || 1,
          colspan = r.colspan || 1,
          index = $.inArray(false, flag[i]);

          if (colspan === 1) {
          r.fieldIndex = index;
          // when field is undefined, use index instead
          if (typeof r.field === 'undefined') {
          r.field = index;
          }
          }

          for (k = 0; k < rowspan; k++) {
          flag[i + k][index] = true;
          }
          for (k = 0; k < colspan; k++) {
          flag[i][index + k] = true;
          }
          }
        }
    };

    var getScrollBarWidth = function () {
        if (cachedWidth === null) {
          var inner = $('<p/>').addClass('fixed-table-scroll-inner'),
          outer = $('<div/>').addClass('fixed-table-scroll-outer'),
          w1, w2;

          outer.append(inner);
          $('body').append(outer);

          w1 = inner[0].offsetWidth;
          outer.css('overflow', 'scroll');
          w2 = inner[0].offsetWidth;

          if (w1 === w2) {
          w2 = outer[0].clientWidth;
          }

          outer.remove();
          cachedWidth = w1 - w2;
        }
        return cachedWidth;
    };

    var calculateObjectValue = function (self, name, args, defaultValue) {
        var func = name;

        if (typeof name === 'string') {
          // support obj.func1.func2
          var names = name.split('.');

          if (names.length > 1) {
          func = window;
          $.each(names, function (i, f) {
          func = func[f];
          });
          } else {
          func = window[name];
          }
        }
        if (typeof func === 'object') {
          return func;
        }
        if (typeof func === 'function') {
          return func.apply(self, args);
        }
        if (!func && typeof name === 'string' && sprintf.apply(this, [name].concat(args))) {
...
...
...
```

问题 6 / 11

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-editable.js
实体：	bootstrap-editable.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。

测试请求和响应：

```
GET /xmjg/bootstrap/js/bootstrap-editable.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//xmjg-one-form!getYzbd.action?
name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 238098
Last-Modified: Mon, 21 Sep 2020 04:41:10 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:50:39 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

/*! X-editable - v1.5.1
* In-place editing with Twitter Bootstrap, jQuery UI or pure jQuery
* http://github.com/vitalets/x-editable
* Copyright (c) 2013 Vitaliy Potapov; Licensed MIT */
/**
Form with single input element, two buttons and two states: normal/loading.
Applied as jQuery method to DIV tag (not to form tag!). This is because form can be in loading
state when spinner shown.
Editableform is linked with one of input types, e.g. 'text', 'select' etc.

@class editableform
@uses text
@uses textarea
**/
(function ($) {
    "use strict";

    var EditableForm = function (div, options) {
        this.options = $.extend({}, $.fn.editableform.defaults, options);
        this.$div = $(div); //div, containing form. Not form tag. Not editable-element.
        if(!this.options.scope) {
          this.options.scope = this;
        }
        //nothing shown after init
    };

    EditableForm.prototype = {
        constructor: EditableForm,
        initInput: function() {  //called once
          //take input from options (as it is created in editable-element)
          this.input = this.options.input;

          //set initial value
          //todo: may be add check: typeof str === 'string' ?
          this.value = this.input.str2value(this.options.value);

          //prerender: get input.$input
          this.input.prerender();
        },
        initTemplate: function() {
          this.$form = $($.fn.editableform.template);
        },
        initButtons: function() {
          var $btn = this.$form.find('.editable-buttons');
          $btn.append($.fn.editableform.buttons);
          if(this.options.showbuttons === 'bottom') {
          $btn.addClass('editable-buttons-bottom');
          }
        },
        /**
        Renders editableform

        @method render
        **/
        render: function() {
          //init loader
          this.$loading = $($.fn.editableform.loading);
          this.$div.empty().append(this.$loading);

          //init form template and buttons
          this.initTemplate();
          if(this.options.showbuttons) {
          this.initButtons();
          } else {
          this.$form.find('.editable-buttons').remove();
          }

          //show loading state
          this.showLoading();

          //flag showing is form now saving value to server.
          //It is needed to wait when closing form.
          this.isSaving = false;

          /**
          Fired when rendering starts
          @event rendering
          @param {Object} event event object
          **/
          this.$div.triggerHandler('rendering');

          //init input
          this.initInput();

          //append input to form
          this.$form.find('div.editable-input').append(this.input.$tpl);

          //append form to container
          this.$div.append(this.$form);

          //render input
          $.when(this.input.render())
          .then($.proxy(function () {
          //setup input to submit automatically when no buttons shown
          if(!this.options.showbuttons) {
          this.input.autosubmit();
          }

          //attach 'cancel' handler
          this.$form.find('.editable-cancel').click($.proxy(this.cancel, this));
          if(this.input.error) {
          this.error(this.input.error);
          this.$form.find('.editable-submit').attr('disabled', true);
          this.input.$input.attr('disabled', true);

...
...
...

@extends text
@final
@since 1.3.0
@example
<a href="#" id="email" data-type="email" data-pk="1">admin@example.com</a>
<script>
$(function(){
    $('#email').editable({
        url: '/post',
...
...
...
```

问题 7 / 11

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/resources/easyui/jquery.easyui.min.js
实体：	jquery.easyui.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。

测试请求和响应：

```
GET /xmjg/resources/easyui/jquery.easyui.min.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//xmjg-statis-show!getSkipPage.action?
sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 379438
Last-Modified: Mon, 21 Sep 2020 04:41:11 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:47:09 GMT
Content-Type: application/javascript;charset=utf-8
```

```
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

/**
 * jQuery EasyUI 1.4.2
 *
 * Copyright (c) 2009-2015 www.jeasyui.com. All rights reserved.
 *
 * Licensed under the GPL license: http://www.gnu.org/licenses/gpl.txt
 * To use it on other terms please contact us at info@jeasyui.com
 *
 */
(function($){
$.parser={auto:true,onComplete:function(_1){
},plugins:
["draggable","droppable","resizable","pagination","tooltip","linkbutton","menu","menubutton","spl
itbutton","progressbar","tree","textbox","filebox","combo","combobox","combotree","combogrid","nu
mberbox","validatebox","searchbox","spinner","numberspinner","timespinner","datetimespinner","cal
endar","datebox","datetimebox","slider","layout","panel","datagrid","propertygrid","treegrid","da
talist","tabs","accordion","window","dialog","form"],parse:function(_2){
var aa=[];
for(var i=0;i<$.parser.plugins.length;i++){
var _3=$.parser.plugins[i];
var r=$(".easyui-"+_3,_2);
if(r.length){
if(r[_3]){
r[_3]();
}else{
aa.push({name:_3,jq:r});
}
}
}
if(aa.length&&window.easyloader){
var _4=[];
for(var i=0;i<aa.length;i++){
_4.push(aa[i].name);
}
easyloader.load(_4,function(){
for(var i=0;i<aa.length;i++){
var _5=aa[i].name;
var jq=aa[i].jq;
jq[_5]();
}
$.parser.onComplete.call($.parser,_2);
});
}else{
$.parser.onComplete.call($.parser,_2);
}
},parseValue:function(_6,_7,_8,_9){
_9=_9||0;
var v=$.trim(String(_7||""));
var _a=v.substr(v.length-1,1);
if(_a=="%"){
v=parseInt(v.substr(0,v.length-1));
if(_6.toLowerCase().indexOf("width")>=0){
v=Math.floor((_8.width()-_9)*v/100);
}else{
v=Math.floor((_8.height()-_9)*v/100);
}
}else{
v=parseInt(v)||undefined;
}
return v;
},parseOptions:function(_b,_c){
var t=$(_b);
var _d={};
var s=$.trim(t.attr("data-options"));
if(s){
if(s.substring(0,1)!="{"){
s="{"+s+"}";
}
_d=(new Function("return "+s))();
}
$.map(["width","height","left","top","minWidth","maxWidth","minHeight","maxHeight"],function(p){
var pv=$.trim(_b.style[p]||"");
if(pv){
if(pv.indexOf("%")==-1){
pv=parseInt(pv)||undefined;
```

```
}
_d[p]=pv;
}
});
if(_c){
var _e={};
for(var i=0;i<_c.length;i++){
var pp=_c[i];
if(typeof pp=="string"){
_e[pp]=t.attr(pp);
}else{
for(var _f in pp){
var _10=pp[_f];
if(_10=="boolean"){
_e[_f]=t.attr(_f)?(t.attr(_f)=="true"):undefined;
}else{
if(_10=="number"){
_e[_f]=t.attr(_f)=="0"?0:parseFloat(t.attr(_f))||undefined;
}
}
}
}
}
$.extend(_d,_e);
}
return _d;
}};
$(function(){
var d=$("<div style=\"position:absolute;top:-1000px;width:100px;height:100px;padding:5px\">
</div>").appendTo("body");
$._boxModel=d.outerWidth()!=100;
d.remove();
if(!window.easyloader&&$.parser.auto){
$.parser.parse();
}
});
$.fn._outerWidth=function(_11){
if(_11==undefined){
if(this[0]==window){
return this.width()||document.body.clientWidth;
}
return this.outerWidth()||0;
}
return this._size("width",_11);
};
$.fn._outerHeight=function(_12){
if(_12==undefined){
if(this[0]==window){
return this.height()||document.body.clientHeight;
}
return this.outerHeight()||0;
}
return this._size("height",_12);
};
$.fn._scrollLeft=function(_13){
if(_13==undefined){
return this.scrollLeft();
}else{
return this.each(function(){
$(this).scrollLeft(_13);
});
}
};
$.fn._propAttr=$.fn.prop||$.fn.attr;
$.fn._size=function(_14,_15){
if(typeof _14=="string"){
if(_14=="clear"){
return this.each(function(){
$(this).css({width:"",minWidth:"",maxWidth:"",height:"",minHeight:"",maxHeight:""});
});
}else{
if(_14=="fit"){
return this.each(function(){
_16(this,this.tagName=="BODY"?$("body"):$(this).parent(),true);
});
}else{
if(_14=="unfit"){
return this.each(function(){
```

```
_16(this,$(this).parent(),false);
});
}else{
if(_15==undefined){
return _17(this[0],_14);
}else{
return this.each(function(){
_17(this,_14,_15);
});
}
}
}
}
}else{
return this.each(function(){
_15=_15||$(this).parent();
$.extend(_14,_16(this,_15,_14.fit)||{});
var r1=_18(this,"width",_15,_14);
var r2=_18(this,"height",_15,_14);
if(r1||r2){
$(this).addClass("easyui-fluid");
}else{
$(this).removeClass("easyui-fluid");
}
});
}
function _16(_19,_1a,fit){
if(!_1a.length){
return false;
}
var t=$(_19)[0];
var p=_1a[0];
va
...
...
...
```

问题 8 / 11

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-table-zh-CN.js
实体：	bootstrap-table-zh-CN.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。

测试请求和响应：

```
GET /xmjg/bootstrap/js/bootstrap-table-zh-CN.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?
bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1
&startDate=2020-01-01&endDate=2020-12-29
```

```
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 1248
Last-Modified: Mon, 21 Sep 2020 04:41:10 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:47:30 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

/**
 * Bootstrap Table Chinese translation
 * Author: Zhixin Wen<wenzhixin2010@gmail.com>
 */
(function ($) {
    'use strict';

    $.fn.bootstrapTable.locales['zh-CN'] = {
        formatLoadingMessage: function () {
          return '正在加载,请稍候……';
        },
        formatRecordsPerPage: function (pageNumber) {
          return '每页显示 ' + pageNumber + ' 条记录';
        },
        formatShowingRows: function (pageFrom, pageTo, totalRows) {
          return '显示第 ' + pageFrom + ' 到第 ' + pageTo + ' 条记录，总共 ' + totalRows + ' 条记录';
        },
        formatSearch: function () {
          return '搜索';
        },
        formatNoMatches: function () {
          return '没有找到匹配的记录';
        },
        formatPaginationSwitch: function () {
          return '隐藏/显示分页';
        },
        formatRefresh: function () {
          return '刷新';
        },
        formatToggle: function () {
          return '切换';
        },
        formatColumns: function () {
          return '列';
        }
    };

    $.extend($.fn.bootstrapTable.defaults, $.fn.bootstrapTable.locales['zh-CN']);

})(jQuery);
```

问题 9 / 11

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-datetimepicker.js
实体：	bootstrap-datetimepicker.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。

测试请求和响应：

```
GET /xmjg/bootstrap/js/bootstrap-datetimepicker.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//xmjg-one-form!getYzbd.action?
name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 86544
Last-Modified: Mon, 21 Sep 2020 04:41:10 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:50:38 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

/* =========================================================
 * bootstrap-datetimepicker.js
 * =========================================================
 * Copyright 2012 Stefan Petre
 *
 * Improvements by Andrew Rowls
 * Improvements by Sébastien Malot
 * Improvements by Yun Lai
 * Improvements by Kenneth Henderick
 * Improvements by CuGBabyBeaR
 * Improvements by Christian Vaas <auspex@auspex.eu>
 *
 * Project URL : http://www.malot.fr/bootstrap-datetimepicker
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 * http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 * ========================================================= */

(function(factory){
    if (typeof define === 'function' && define.amd)
        define(['jquery'], factory);
    else if (typeof exports === 'object')
        factory(require('jquery'));
    else
        factory(jQuery);

}(function($, undefined){

    // Add ECMA262-5 Array methods if not supported natively (IE8)
    if (!('indexOf' in Array.prototype)) {
        Array.prototype.indexOf = function (find, i) {
          if (i === undefined) i = 0;
          if (i < 0) i += this.length;
          if (i < 0) i = 0;
          for (var n = this.length; i < n; i++) {
          if (i in this && this[i] === find) {
          return i;
          }
          }
          return -1;
        }
    }

    // Add timezone abbreviation support for ie6+, Chrome, Firefox
    function timeZoneAbbreviation() {
        var abbreviation, date, formattedStr, i, len, matchedStrings, ref, str;
        date = (new Date()).toString();
        formattedStr = ((ref = date.split('(')[1]) != null ? ref.slice(0, -1) : 0) ||
date.split(' ');
        if (formattedStr instanceof Array) {
          matchedStrings = [];
          for (var i = 0, len = formattedStr.length; i < len; i++) {
          str = formattedStr[i];
          if ((abbreviation = (ref = str.match(/\b[A-Z]+\b/)) !== null) ? ref[0] : 0) {
          matchedStrings.push(abbreviation);
          }
          }
          formattedStr = matchedStrings.pop();
        }
        return formattedStr;
    }

    function UTCDate() {
        return new Date(Date.UTC.apply(Date, arguments));
    }

    // Picker object
    var Datetimepicker = function (element, options) {
        var that = this;

        this.element = $(element);

        // add container for single page application
        // when page switch the datetimepicker div will be removed also.
        this.container = options.container || 'body';

        this.language = options.language || this.element.data('date-language') || 'en';
        this.language = this.language in dates ? this.language : this.language.split('-')[0]; //
fr-CA fallback to fr
        this.language = this.language in dates ? this.language : 'en';
        this.isRTL = dates[this.language].rtl || false;
        this.formatType = options.formatType || this.element.data('format-type') || 'standard';
        this.format = DPGlobal.parseFormat(options.format || this.element.data('date-format') ||
dates[this.language].format || DPGlobal.getDefaultFormat(this.formatType, 'input'),
this.formatType);
        this.isInline = false;
        this.isVisible = false;
        this.isInput = this.element.is('input');
        this.fontAwesome = options.fontAwesome || this.element.data('font-awesome') || false;

        this.bootcssVer = options.bootcssVer || (this.isInput ? (this.element.is('.form-control')
? 3 : 2) : ( this.bootcssVer = this.element.is('.inpu
...
...
...
```

问题 10 / 11

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/handsontable-master/dist/handsontable.full.js
实体：	handsontable.full.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。

测试请求和响应：

```
GET /xmjg/handsontable-master/dist/handsontable.full.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//xmjg-one-form!getYzbd.action?
name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 2290099
Last-Modified: Mon, 21 Sep 2020 04:41:11 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:50:53 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

/*!
 * (The MIT License)
 *
 * Copyright (c) 2012-2014 Marcin Warpechowski
 * Copyright (c) 2015 Handsoncode sp. z o.o. <hello@handsoncode.net>
 *
 * Permission is hereby granted, free of charge, to any person obtaining
 * a copy of this software and associated documentation files (the
 * 'Software'), to deal in the Software without restriction, including
 * without limitation the rights to use, copy, modify, merge, publish,
 * distribute, sublicense, and/or sell copies of the Software, and to
 * permit persons to whom the Software is furnished to do so, subject to
 * the following conditions:
 *
 * The above copyright notice and this permission notice shall be
 * included in all copies or substantial portions of the Software.
 *
 * THE SOFTWARE IS PROVIDED 'AS IS', WITHOUT WARRANTY OF ANY KIND,
 * EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
 * MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
 * IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
 * CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
 * TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
 * SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
 *
 * Version: 6.0.0
 * Release date: 27/09/2018 (built at 26/09/2018 12:54:09)
 */
(function webpackUniversalModuleDefinition(root, factory) {
 if(typeof exports === 'object' && typeof module === 'object')
         module.exports = factory();
 else if(typeof define === 'function' && define.amd)
         define("Handsontable", [], factory);
 else if(typeof exports === 'object')
         exports["Handsontable"] = factory();
 else
         root["Handsontable"] = factory();
})(typeof self !== 'undefined' ? self : this, function() {
return /******/ (function(modules) { // webpackBootstrap
/******/        // The module cache
/******/        var installedModules = {};
/******/
/******/        // The require function
/******/        function __webpack_require__(moduleId) {
/******/
/******/                // Check if module is in cache
/******/                if(installedModules[moduleId]) {
/******/                        return installedModules[moduleId].exports;
/******/                }
/******/                // Create a new module (and put it into the cache)
/******/                var module = installedModules[moduleId] = {
/******/                        i: moduleId,
/******/                        l: false,
/******/                        exports: {}
/******/                };
/******/
/******/                // Execute the module function
/******/                modules[moduleId].call(module.exports, module, module.exports,
__webpack_require__);
/******/
/******/                // Flag the module as loaded
/******/                module.l = true;
/******/
/******/                // Return the exports of the module
/******/                return module.exports;
/******/        }
/******/
/******/
/******/        // expose the modules object (__webpack_modules__)
/******/        __webpack_require__.m = modules;
/******/
/******/        // expose the module cache
/******/        __webpack_require__.c = installedModules;
/******/
/******/        // define getter function for harmony exports
/******/        __webpack_require__.d = function(exports, name, getter) {
/******/                if(!__webpack_require__.o(exports, name)) {
/******/                        Object.defineProperty(exports, name, {
/******/                                configurable: false,
/******/                                enumerable: true,
/******/                                get: getter
/******/                        });
/******/                }
/******/        };
/******/
/******/        // getDefaultExport function for compatibility with non-harmony modules
/******/        __webpack_require__.n = function(module) {
/******/                var getter = module && module.__esModule ?
/******/                        function getDefault() { return module['default']; } :
/******/                        function getModuleExports() { return module; };
/******/                __webpack_require__.d(getter, 'a', getter);
/******/                return getter;
/******/        };
/******/
/******/        // Object.prototype.hasOwnProperty.call
/******/        __webpack_require__.o = function(object, property) { return
Object.prototype.hasOwnProperty.call(object, property); };
```

```
/******/
/******/        // __webpack_public_path__
/******/        __webpack_require__.p = "";
/******/
/******/        // Load entry module and return exports
/******/        r
...
...
...
```

问题 11 / 11

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/agcloud/login/js/sm3-sm4-md5-base64-merge.js
实体：	sm3-sm4-md5-base64-merge.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

差异：

推理： 响应包含可能是专用的电子邮件地址。

测试请求和响应：

```
GET /xmjg/agcloud/login/js/sm3-sm4-md5-base64-merge.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 36028
Last-Modified: Thu, 29 Oct 2020 15:39:15 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:54:09 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

/*
 * JavaScript SM3
 * https://github.com/jiaxingzheng/JavaScript-SM3
 *
 * Copyright 2017, Zheng Jiaxing
 *
 * Licensed under the MIT license:
 * http://www.opensource.org/licenses/MIT
 *
 * Refer to
 * http://www.oscca.gov.cn/UpFile/20101222141857786.pdf
 */


// 左补0到指定长度
function leftPad(str, totalLength) {
  const len = str.length;
  return Array(totalLength > len ? ((totalLength - len) + 1) : 0).join(0) + str;
}

// 二进制转化为十六进制
function binary2hex(binary) {
  const binaryLength = 8;
  let hex = '';
  for (let i = 0; i < binary.length / binaryLength; i += 1) {
    hex += leftPad(parseInt(binary.substr(i * binaryLength, binaryLength), 2).toString(16), 2);
  }
  return hex;
}

// 十六进制转化为二进制
function hex2binary(hex) {
  const hexLength = 2;
  let binary = '';
  for (let i = 0; i < hex.length / hexLength; i += 1) {
    binary += leftPad(parseInt(hex.substr(i * hexLength, hexLength), 16).toString(2), 8);
  }
  return binary;
}

// 普通字符串转化为二进制
function str2binary(str) {
  let binary = '';
  for (const ch of str) {
    binary += leftPad(ch.codePointAt(0).toString(2), 8);
  }
  return binary;
}

// 循环左移
function rol(str, n) {
  return str.substring(n % str.length) + str.substr(0, n % str.length);
}

// 二进制运算
function binaryCal(x, y, method) {
  const a = x || '';
  const b = y || '';
  const result = [];
  let prevResult;
  // for (let i = 0; i < a.length; i += 1) { // 小端
  for (let i = a.length - 1; i >= 0; i -= 1) { // 大端
    prevResult = method(a[i], b[i], prevResult);
    result[i] = prevResult[0];
  }
  // console.log(`x     :${x}\ny     :${y}\nresult:${result.join('')}\n`);
  return result.join('');
}

// 二进制异或运算
function xor(x, y) {
  return binaryCal(x, y, (a, b) => [(a === b ? '0' : '1')]);
}

// 二进制与运算
function and(x, y) {
  return binaryCal(x, y, (a, b) => [(a === '1' && b === '1' ? '1' : '0')]);
}

// 二进制或运算
function or(x, y) {
  return binaryCal(x, y, (a, b) => [(a === '1' || b === '1' ? '1' : '0')]);// a === '0' && b ===
'0' ? '0' : '1'
}

// 二进制与运算
function add(x, y) {
  const result = binaryCal(x, y, (a, b, prevResult) => {
    const carry = prevResult ? prevResult[1] : '0' || '0';
    if (a !== b) return [carry === '0' ? '1' : '0', carry];// a,b不等时,carry不变，结果与carry相反
    // a,b相等时，结果等于原carry，新carry等于a
    return [carry, a];
  });
  // console.log('x: ' + x + '\ny: ' + y + '\n=  ' + result + '\n');
  return result;
}

// 二进制非运算
function not(x) {
  return binaryCal(x, undefined, a => [a === '1' ? '0' : '1']);
}

function calMulti(method) {
  return (...arr) => arr.reduce((prev, curr) => method(prev, curr));
}

// function xorMulti(...arr) {
//   return arr.reduce((prev, curr) => xor(prev, curr));
// }

// 压缩函数中的置换函数 P1(X) = X xor (X <<< 9) xor (X <<< 17)
function P0(X) {
  return calMulti(xor)(X, rol(X, 9), rol(X, 17));
}

// 消息扩展中的置换函数 P1(X) = X xor (X <<< 15) xor (X <<< 23)
function P1(X) {
  return calMulti(xor)(X, rol(X, 15), rol(X, 23));
}

// 布尔函数，随j的变化取不同的表达式
function FF(X, Y, Z, j) {
  return j >= 0 && j <= 15 ? calMulti(xor)(X, Y, Z) : calMulti(or)(and(X, Y), and(X, Z), and(Y,
Z));
}

// 布尔函数，随j的变化取不同的表达式
function GG(X, Y, Z, j) {
  return j >= 0 && j <= 15 ? calMulti(xor)(X, Y, Z) : or(and(X, Y), and(not(X), Z));
}

// 常量，随j的变化取不同的值
function T(j) {
  return j >= 0 && j <= 15 ? hex2binary('79cc4519') : hex2binary('7a879d8a');
}

// 压缩函数
function CF(V, Bi) {
  // 消息扩展
  const wordLength = 32;
  const W = [];
  const M = [];// W'

  // 将消息分组B划分为16个字W0， W1，…… ，W15 （字为长度为32的比特串）
  for (let i = 0; i < 16; i += 1) {
    W.push(Bi.substr(i * wordLength, wordLength));
  }

  // W[j] <- P1(W[j-16] xor W[j-9] xor (W[j-3] <<< 15)) xor (W[j-13] <<< 7) xor W[j-6]
  for (let j = 16; j < 68; j += 1) {
    W.push(calMulti(xor)(
      P1(calMulti(xor)(W[j - 16], W[j - 9], ro
...
...
...

 * base64js
 * base64js.toByteArray(d.input)
 * base64js.fromByteArray(c);
 * @author c.z.s
 * @email 1048829253@qq.com
 * @company
 * @date 2018-07
 *
 */
...
```

```
...
...


/**
 * 国密SM4加密算法
 * @author c.z.s
 * @email 1048829253@qq.com
 * @company GDT-ZWZX-DEV-PT
 * @date 2018-07
 */
function SM4_Context() {
...
...
...
```

参 发现可能的服务器路径泄露模式 7 TOC

问题 1 / 7 TOC

发现可能的服务器路径泄露模式	
严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/vendors.bundle.js
实体：	vendors.bundle.js (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修补程序
固定值：	为 Web 服务器或 Web 应用程序下载相关的安全补丁

差异：

推理： 响应包含服务器上文件的绝对路径和/或文件名。

测试请求和响应：

```
GET /opus-front-sso/framework/ui-themes/common/metronic/js/vendors.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/require
Cookie: JSESSIONID=D6A5925ADA251562D8C32F08668AA5EE
Connection: keep-alive
Host: 127.0.0.1:8090
Accept: */*
Accept-Language: en-US


...
...
...

 // Regular expressions
 // http://www.w3.org/TR/css3-selectors/#whitespace
 whitespace = "       [\\x20\\t\\r\\n\\f]",

 // http://www.w3.org/TR/CSS21/syndata.html#value-def-identifier
 identifier = "(?:\\\\.|[\\w-]|[^\0       -\\xa0])+",

 // Attribute selectors: http://www.w3.org/TR/selectors/#attribute-selectors
 attributes = "\\[" + whitespace + "*(" + identifier + ")(?:" + whitespace +
         // Operator (capture 2)
...
...
...
:{future:"in %s",past:"%s ago",s:"a few seconds",ss:"%d seconds",m:"a minute",mm:"%d
minutes",h:"an hour",hh:"%d hours",d:"a day",dd:"%d days",M:"a month",MM:"%d months",y:"a
year",yy:"%d years"},months:Gt,monthsShort:Vt,week:
{dow:0,doy:6},weekdays:Et,weekdaysMin:zt,weekdaysShort:At,meridiemParse:/[ap]\.?m?\.?/i},Xt=
{},Kt={},en=/^\s*((?:[+-]\d{6}|\d{4})-(?:\d\d-\d\d|W\d\d-\d|W\d\d|\d\d\d|\d\d))(?:(T| )
(\d\d(?::\d\d(?::\d\d(?:[.,]\d+)?)?)?)([\+\-]\d\d(?::?\d\d)?|\s*Z)?)?$/,tn=/^\s*((?:[+-
]\d{6}|\d{4})(?:\d\d\d\d|W\d\d\d|W\d\d|\d\d\d|\d\d))(?:(T| )(\d\d(?:\d\d(?:\d\d(?:[.,]\d+)?)?)?)
([\+\-]\d\d(?::?\d\d)?|\s*Z)?)?$/,nn=/Z|[+-]\d\d(?::?\d\d)?/,sn=[["YYYYYY-MM-DD",/[+-]\d{6}-\d\d-
\d\d/],["YYYY-MM-DD",/\d{4}-\d\d-\d\d/],["GGGG-[W]WW-E",/\d{4}-W\d\d-\d/],["GGGG-[W]WW",/\d{4}-
W\d\d/,!1],["YYYY-DDD",/\d{4}-\d{3}/],["YYYY-MM",/\d{4}-\d\d/,!1],["YYYYYYMMDD",/[+-]\d{10}/],
["YYYYMMDD",/\d{8}/],["GGGG[W]WWE",/\d{4}W\d{3}/],["GGGG[W]WW",/\d{4}W\d{2}/,!1],
["YYYYDDD",/\d{7}/]],rn=[["HH:mm:ss.SSSS",/\d\d:\d\d:\d\d\.\d+/],
["HH:mm:ss,SSSS",/\d\d:\d\d:\d\d,\d+/],["HH:mm:ss",/\d\d:\d\d:\d\d/],["HH:mm",/\d\d:\d\d/],
["HHmmss.SSSS",/\d\d\d\d\d\d\.\d+/],["HHmmss,SSSS",/\d\d\d\d\d\d,\d+/],["HHmmss",/\d\d\d\d\d\d/],
["HHmm",/\d\d\d\d/],["HH",/\d\d/]],an=/^\/?Date\((\-?\d+)/i,on=/^(?:
(Mon|Tue|Wed|Thu|Fri|Sat|Sun),?\s)?
(\d{1,2})\s(Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec)\s(\d{2,4})\s(\d\d):(\d\d)(?::
(\d\d))?\s(?:(UT|GMT|[ECMP][SD]T)|([Zz])|([+-]\d{4}))$/,un={UT:0,GMT:0,EDT:-240,EST:-300,CDT:-
300,CST:-360,MDT:-360,MST:-420,PDT:-420,PST:-480};e.createFromInputFallback=v("value provided is
not in a recognized RFC2822 or ISO format. moment construction falls back to js Date(), which is
not reliable across all browsers and versions. Non RFC2822/ISO date formats are discouraged and
will be removed in an upcoming major release. Please refer to
http://momentjs.com/guides/#/warnings/js-date/ for more info.",function(e){e._d=new Date(e._i+
(e._useUTC?" UTC":""))}),e.ISO_8601=function(){},e.RFC_2822=function(){};var ln=v("moment().min
is deprecated, use m
...
...
...

     return this.wrap([fn, type ? '.' + type + '(' : '(', params, ')']);
   },

   quotedString: function quotedString(str) {
     return '"' + (str + '').replace(/\\/g, '\\\\').replace(/"/g, '\\"').replace(/\n/g,
'\\n').replace(/\r/g, '\\r').replace(/\u2028/g, '\\u2028') // Per Ecma-262 7.3 + 7.8.4
     .replace(/\u2029/g,        '\\u2029') + '"';
   },

   objectLiteral: function objectLiteral(obj) {
     var pairs = [];
...
...
...
          validator: ".",
          cardinality: 1
          }
          },
          mask: "(\\http://)|(\\http\\s://)|(ftp://)|(ftp\\s:/)i{+}",
          insertMode: !1,
          autoUnmask: !1,
          inputmode: "url"
          },
...
...
...


    for ( var b = 0; b < blocks.length; ++b ) {
      var m = blocks[ b ].match( tight ),
          terms = m[ 1 ].replace( /\n$/, "" ).split( /\n/ ),
          defns = m[ 2 ].split( /\n:\s+/ );

      // print( uneval( m ) );

      for ( i = 0; i < terms.length; ++i ) {
```

```
...
...
...

                 if ( type === "file" ) {

                         // Modern browser (chrome & safari)
                         if ( val.substr( 0, 12 ) ===        "C:\\fakepath\\" ) {
                                 return val.substr( 12 );
                                }

                         // Legacy browsers
...
...
...

];

// iso time formats and regexes
var isoTimes = [
    ['HH:mm:ss.SSSS', /\d\d:\d\d:\d\d\.\d+/],
    ['HH:mm:ss,SSSS', /\d\d:\d\d:\d\d,\d+/],
    ['HH:mm:ss', /\d\d:\d\d:\d\d/],
    ['HH:mm', /\d\d:\d\d/],
    ['HHmmss.SSSS', /\d\d\d\d\d\d\.\d+/],
    ['HHmmss,SSSS', /\d\d\d\d\d\d,\d+/],
    ['HHmmss', /\d\d\d\d\d\d/],
    ['HHmm', /\d\d\d\d/],
...
...
...

    }
}

// RFC 2822 regex: For details see https://tools.ietf.org/html/rfc2822#section-3.3
var basicRfcRegex = /^((?:Mon|Tue|Wed|Thu|Fri|Sat|Sun),?\s)?(\d?
\d\s(?:Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec)\s(?:\d\d)?\d\d\s)(\d\d:\d\d)(\:\d\d)?
(\s(?:UT|GMT|[ECMP][SD]T|[A-IK-Za-ik-z]|[+-]\d{4}))$/;

// date and time from ref 2822 format
function configFromRFC2822(config) {
    var string, match, dayFormat,
...
...
...
```

问题 2 / 7

TOC

发现可能的服务器路径泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8090/opus-front-sso/js/jquery.validate.min.js
实体：	jquery.validate.min.js (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修补程序
固定值：	为 Web 服务器或 Web 应用程序下载相关的安全补丁

差异：

推理： 响应包含服务器上文件的绝对路径和/或文件名。

测试请求和响应：

```
GET /opus-front-sso/js/jquery.validate.min.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/require
Cookie: JSESSIONID=D6A5925ADA251562D8C32F08668AA5EE
Connection: keep-alive
Host: 127.0.0.1:8090
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 28 Dec 2020 07:36:44 GMT
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Content-Length: 24379
X-Content-Type-Options: nosniff
Cache-Control: max-age=31556926
Date: Tue, 29 Dec 2020 02:44:19 GMT
Content-Type: application/javascript;charset=utf-8

/*! jQuery Validation Plugin - v1.19.1 - 6/15/2019
 * https://jqueryvalidation.org/
 * Copyright (c) 2019 Jörn Zaefferer; Licensed MIT */
!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):"object"==typeof
module&&module.exports?module.exports=a(require("jquery")):a(jQuery)}(function(a){a.extend(a.fn,
{validate:function(b){if(!this.length)return
void(b&&b.debug&&window.console&&console.warn("Nothing selected, can't validate, returning
nothing."));var c=a.data(this[0],"validator");return c?c:
(this.attr("novalidate","novalidate"),c=new
a.validator(b,this[0]),a.data(this[0],"validator",c),c.settings.onsubmit&&
(this.on("click.validate",":submit",function(b)
{c.submitButton=b.currentTarget,a(this).hasClass("cancel")&&(c.cancelSubmit=!0),void
0!==a(this).attr("formnovalidate")&&(c.cancelSubmit=!0)}),this.on("submit.validate",function(b)
{function d(){var d,e;return c.submitButton&&(c.settings.submitHandler||c.formSubmitted)&&(d=a("
<input
type='hidden'/>").attr("name",c.submitButton.name).val(a(c.submitButton).val()).appendTo(c.curren
tForm)),!(c.settings.submitHandler&&!c.settings.debug)||
(e=c.settings.submitHandler.call(c,c.currentForm,b),d&&d.remove(),void 0!==e&&e)}return
c.settings.debug&&b.preventDefault(),c.cancelSubmit?(c.cancelSubmit=!1,d()):c.form()?
c.pendingRequest?(c.formSubmitted=!0,!1):d():(c.focusInvalid(),!1)})),c)},valid:function(){var
b,c,d;return a(this[0]).is("form")?b=this.validate().form():(d=
[],b=!0,c=a(this[0].form).validate(),this.each(function(){b=c.element(this)&&b,b||
(d=d.concat(c.errorList))}),c.errorList=d),b},rules:function(b,c){var
d,e,f,g,h,i,j=this[0],k="undefined"!=typeof
this.attr("contenteditable")&&"false"!==this.attr("contenteditable");if(null!=j&&(!j.form&&k&&
(j.form=this.closest("form")[0],j.name=this.attr("name")),null!=j.form))
{if(b)switch(d=a.data(j.form,"validator").settings,e=d.rules,f=a.validator.staticRules(j),b)
{case"add":a.extend(f,a.validator.normalizeRule(c)),delete f.messages,e[j.name]=f,c.messages&&
(d.messages[j.name]=a.extend(d.messages[j.name],c.messages));break;case"remove":return c?(i=
{},a.each(c.split(/\s/),function(a,b){i[b]=f[b],delete f[b]}),i):(delete e[j.name],f)}return
g=a.validator.normalizeRules(a.extend({},a.validator.classRules(j),a.validator.attributeRules(j),
a.validator.dataRules(j),a.validator.staticRules(j)),j),g.required&&(h=g.req
...
...
...
name assigned",this),e&&(this.form=a(this).closest("form")
[0],this.name=d),this.form===b.currentForm&&(!(d in c||!b.objectLength(a(this).rules()))&&
(c[d]=!0,!0))})},clean:function(b){return a(b)[0]},errors:function(){var
b=this.settings.errorClass.split(" ").join(".");return
a(this.settings.errorElement+"."+b,this.errorContext)},resetInternals:function()
{this.successList=[],this.errorList=[],this.errorMap=
{},this.toShow=a([]),this.toHide=a([])},reset:function()
{this.resetInternals(),this.currentElements=a([])},prepareForm:function()
{this.reset(),this.toHide=this.errors().add(this.containers)},prepareElement:function(a)
{this.reset(),this.toHide=this.errorsFor(a)},elementValue:function(b){var
c,d,e=a(b),f=b.type,g="undefined"!=typeof
e.attr("contenteditable")&&"false"!==e.attr("contenteditable");return"radio"===f||"checkbox"===f?
this.findByName(b.name).filter(":checked").val():"number"===f&&"undefined"!=typeof b.validity?
b.validity.badInput?"NaN":e.val():(c=g?
e.text():e.val(),"file"===f?"C:\\fakepath\\"===c.substr(0,12)?c.substr(12):
(d=c.lastIndexOf("/"),d>=0?c.substr(d+1):(d=c.lastIndexOf("\\"),d>=0?
c.substr(d+1):c)):"string"==typeof c?c.replace(/\r/g,""):c)},check:function(b)
{b=this.validationTargetFor(this.clean(b));var c,d,e,f,g=a(b).rules(),h=a.map(g,function(a,b)
{return b}).length,i=!1,j=this.elementValue(b);"function"==typeof g.normalizer?
f=g.normalizer:"function"==typeof this.settings.normalizer&&(f=this.settings.normalizer),f&&
(j=f.call(b,j),delete g.normalizer);for(d in g){e=
{method:d,parameters:g[d]};try{if(c=a.validator.methods[d].call(this,j,b,e.parameters),"dependenc
y-mismatch"===c&&1===h){i=!0;continue}if(i=!1,"pending"===c)return
void(this.toHide=this.toHide.not(this.errorsFor(b)));if(!c)return
this.formatAndAdd(b,e),!1}catch(k){throw
this.settings.debug&&window.console&&console.log("Exception occurred when checking element
"+b.id+", check the '"+e.method+"' method.",k),k instanceof TypeError&&(k.message+=".
...
...
...
```

问题 3 / 7

TOC

发现可能的服务器路径泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/agcloud/framework/js-lib/element-2/element.js
实体：	element.js (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修补程序
固定值：	为 Web 服务器或 Web 应用程序下载相关的安全补丁

差异：

推理： 响应包含服务器上文件的绝对路径和/或文件名。

测试请求和响应：

```
GET /xmjg/agcloud/framework/js-lib/element-2/element.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 525328
Last-Modified: Tue, 22 Dec 2020 02:31:13 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:44:25 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-reval
...
...
...
){n.push.apply(n,e),++r===s&&i(n)}e.forEach(function(e){t(e,o)})}(n,i,u)})}function xo(e){return
```

```
function(t){return t&&t.message?(t.field=t.field||e.fullField,t):
{message:t,field:t.field||e.fullField}}}function Co(e,t){if(t)for(var i in
t)if(t.hasOwnProperty(i)){var n=t[i];"object"===(void 0===n?"undefined":mo()(n))&&"object"===mo()
(e[i])?e[i]=po()({},e[i],n):e[i]=n}return e}var ko=function(e,t,i,n,r,s)
{!e.required||i.hasOwnProperty(e.field)&&!yo(t,s||e.type)||n.push(bo(r.messages.required,e.fullFi
eld))};var So=function(e,t,i,n,r)
{(/^\s+$/.test(t)||""===t)&&n.push(bo(r.messages.whitespace,e.fullField))},Do={email:/^(([^<>()\
[\]\\.,;:\s@"]+(\.[^<>()\[\]\\.,;:\s@"]+)*)|(".+"))@((\[[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]
{1,3}])|(([a-zA-Z\-0-9]+\.)+[a-zA-Z]{2,}))$/,url:new RegExp("^(?!mailto:)(?:
(?:http|https|ftp)://|//)(?:\\S+(?::\\S*)?@)?(?:(?:(?:[1-9]\\d?|1\\d\\d|2[01]\\d|22[0-3])(?:\\.
(?:1?\\d{1,2}|2[0-4]\\d|25[0-5])){2}(?:\\.(?:[0-9]\\d?|1\\d\\d|2[0-4]\\d|25[0-4]))|(?:(?:[a-
z\\u00a1-\\uffff0-9]+-?)*[a-z\\u00a1-\\uffff0-9]+)(?:\\.(?:[a-z\\u00a1-\\uffff0-9]+-?)*[a-
z\\u00a1-\\uffff0-9]+)*(?:\\.(?:[a-z\\u00a1-\\uffff]{2,})))|localhost)(?::\\d{2,5})?(?:(/|\\?|#)
[^\\s]*)?$","i"),hex:/^#?([a-f0-9]{6}|[a-f0-9]{3})$/i},$o={integer:function(e){return
$o.number(e)&&parseInt(e,10)===e},float:function(e){return
$o.number(e)&&!$o.integer(e)},array:function(e){return Array.isArray(e)},regexp:function(e){if(e
instanceof RegExp)return!0;try{return!!new RegExp(e)}catch(e){return!1}},date:function(e)
{return"function"==typeof e.getTime&&"function"==typeof e.getMonth&&"function"==typeof
e.getYear},number:function(e){return!isNaN(e)&&"number"==typeof e},object:function(e)
{return"object"===(void 0===e?"undefined":mo()(e))&&!$o.array(e)},method:function(e)
{return"function"==typeof e},email:function(e){return"string"==typeof
e&&!!e.match(Do.email)&&e.length<255},url:function(e){return"string"==typeof
e&&!!e.match(Do.url)},hex:function(e){return"string"==typeof e&&!!e.match(Do.hex)}};var
Eo=function(e,t,i,n,r){if(e.required&&void 0===t)ko(e,t,i,n,r);else{var s=e.type;
...
...
...
upload-list.vue";var ml=fl.exports,vl=i(16),gl=i.n(vl);var bl=function(){var
e=this,t=e.$createElement;return(e._self._c||t)("div",{staticClass:"el-upload-dragger",class:
{"is-dragover":e.dragover},on:{drop:function(t){return
t.preventDefault(),e.onDrop(t)},dragover:function(t){return
t.preventDefault(),e.onDragover(t)},dragleave:function(t){t.preventDefault(),e.dragover=!1}}},
[e._t("default")],2)};bl._withStripped=!0;var yl=r({name:"ElUploadDrag",props:
{disabled:Boolean},inject:{uploader:{default:""}},data:function(){return{dragover:!1}},methods:
{onDragover:function(){this.disabled||(this.dragover=!0)},onDrop:function(e)
{if(!this.disabled&&this.uploader){var t=this.uploader.accept;this.dragover=!1,t?
this.$emit("file",[].slice.call(e.dataTransfer.files).filter(function(e){var
i=e.type,n=e.name,r=n.indexOf(".")>-1?"."+n.split(".").pop():"",s=i.replace(/\/.*$/,"");return
t.split(",").map(function(e){return e.trim()}).filter(function(e){return e}).some(function(e)
{return/\..+$/.test(e)?r===e:/\/\*$/.test(e)?
s===e.replace(/\/\*$/,""):!!/^[^\/]+\/[^\/]+$/.test(e)&&i===e})})):this.$emit("file",e.dataTransf
er.files)}}}},bl,[],!1,null,null,null);yl.options.__file="packages/upload/src/upload-
dragger.vue";var _l=r({inject:["uploader"],components:{UploadDragger:yl.exports},props:
{type:String,action:{type:String,required:!0},name:
{type:String,default:"file"},data:Object,headers:Object,withCredentials:Boolean,multiple:Boolean,
accept:String,onStart:Function,onProgress:Function,onSuccess:Function,onError:Function,beforeUplo
ad:Function,drag:Boolean,onPreview:{type:Function,default:function(){}},onRemove:
{type:Function,default:function()
{}},fileList:Array,autoUpload:Boolean,listType:String,httpRequest:
{type:Function,default:function(e){if("undefined"!=typeof XMLHttpRequest){var t=new
XMLHttpRequest,i=e.action;t.upload&&(t.upload.onprogress=function(t){t.total>0&&
(t.percent=t.loaded/t.total*100),e.onProgress(t)});var n=new FormData;e.data&&O
...
...
...
```

问题 4 / 7

TOC

发现可能的服务器路径泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/common/tool/cityselect/js/city_data.js
实体：	city_data.js (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修补程序
固定值：	为 Web 服务器或 Web 应用程序下载相关的安全补丁

差异：

推理： 响应包含服务器上文件的绝对路径和/或文件名。

测试请求和响应：

```
GET /xmjg/common/tool/cityselect/js/city_data.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 21338
Last-Modified: Mon, 21 Sep 2020 04:41:10 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:45:16 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

//执行 analysis-info!CreateCityData.action 方式生成最新城市数据
//生成的文件路径为 D:\city_data.js，请手动替换/common/tool/cityselect/js/city_data.js 中的内容
var __LocalDataCities={"list":{"110000":["北京","Beijing","BJ"],"120000":["天
津","Tianjin","TJ"],"130000":["河北","Hebei","HB"],"130100":["石家
庄","Shijiazhuang","SJZ"],"130181":["辛集市","Xinjishi","XJS"],"130200":["唐
山","Tangshan","TS"],"130300":["秦皇岛","Qinhuangdao","QHD"],"130400":["邯
郸","Handan","HD"],"130500":["邢台","Xingtai","XT"],"130600":["保定","Baoding","BD"],"130682":["定
州市","Dingzhoushi","DZS"],"130700":["张家口","Zhangjiakou","ZJK"],"130800":["承
德","Chengde","CD"],"130900":["沧州","Cangzhou","CZ"],"131000":["廊坊","Langfang","LF"],"131100":
["衡水","Hengshui","HS"],"131200":["雄安","Xionganxinqu","XAXQ"],"140000":["山
西","Shanxi","SX"],"140100":["太原","Taiyuan","TY"],"140200":["大同","Datong","DT"],"140300":["阳
泉","Yangquan","YQ"],"140400":["长治","Zhangzhi","CZ"],"140500":["晋城","Jincheng","JC"],"140600":
["朔州","Shuozhou","SZ"],"140700":["晋中","Jinzhong","JZ"],"140800":["运
城","Yuncheng","YC"],"140900":["忻州","Xinzhou","XZ"],"141000":["临汾","Linfen","LF"],"141100":["吕
梁","Lüliang","LL"],"150000":["内蒙古","Neimenggu","NMG"],"150100":["呼和浩
特","Huhehaote","HHHT"],"150200":["包头","Baotou","BT"],"150300":["乌海","Wuhai","WH"],"150400":
["赤峰","Chifeng","CF"],"150500":["通辽","Tongliao","TL"],"150600":["鄂尔多
斯","Eerduosi","EEDS"],"150700":["呼伦贝尔","Hulunbeier","HLBE"],"150800":["巴彦淖
尔","Bayannaoer","BYNE"],"150900":["乌兰察布","Wulanchabu","WLCB"],"152200":["兴
安","Xingan","XA"],"152500":["锡林郭勒","Xilinguole","XLGL"],"152900":["阿拉
善","Alashan","ALS"],"210000":["辽宁","Liaoning","LN"],"210100":["沈阳","Shenyang","SY"],"210200":
["大连","Dalian","DL"],"210300":["鞍山","Anshan","AS"],"210400":["抚顺","Fushun","FS"],"210500":
["本溪","Benxi","BX"],"210600":["丹东","Dandong","DD"],"210700":["锦州","Jinzhou","JZ"],"210800":
["营口","Yingkou","YK"],"210900":["阜新","Fuxin","FX"],"211000":["辽阳","Liaoyang","LY"],"211100":
["盘锦","Panjin","PJ"],"211200":["铁岭","Tieling","TL"],"211300":["朝阳","Chaoyang","CY"],"211400":
["葫芦岛","Huludao","HLD"],"220000":["吉林","Jilin","JL"],"220100":["长
春","Zhangchun","CC"],"220200":["吉林","Jilin","JL"],"220300":["四平","Siping","SP"],"220400":["辽
源","Liaoyuan","LY"],"220500":["通化","Tonghua","TH"],"220600":["白山","Baishan","BS"],"220700":
["松原","Songyuan","SY"],"220800":["白城","Baicheng","BC"],"222400":["延
边","Yanbian","YB"],"230000":["黑龙江","Heilongjiang","HLJ"],"230100":["哈尔
滨","Haerbin","HEB"],"230200":["齐齐哈尔","Qiqihaer","QQHE"],"230300":["鸡
西","Jixi","JX"],"230400":["鹤岗","Hegang","HG"],"230500":["双鸭山","Shuangyashan","SYS"],"230600":
["大庆","Daqing","DQ"],"230700":["伊春","Yichun","YC"],"230800":["佳木
斯","Jiamusi","JMS"],"230900":["七台河","Qitaihe","QTH"],"231000":["牡丹
江","Mudanjiang","MDJ"],"231100":["黑河","Heihe","HH"],"231200":["绥化","Suihua","SH"],"232700":
["大兴安岭","Daxinganling","DXAL"],"310000":["上海","Shanghai","SH"],"320000":["江
苏","Jiangsu","JS"],"320100":["南京","Nanjing","NJ"],"320200":["无锡","Wuxi","WX"],"320300":["徐
州","Xuzhou","XZ"],"320400":["常州","Changzhou","CZ"],"320500":["苏州","Suzhou","SZ"],"320600":["南
通","Nantong","NT"],"320700":["连云港","Lianyungang","LYG"],"320800":["淮
安","Huaian","HA"],"320900":["盐城","Yancheng","YC"],"321000":["扬州","Yangzhou","YZ"],"321100":
["镇江","Zhenjiang","ZJ"],"321200":["泰州","Taizhou","TZ"],"321300":["宿
迁","Xiuqian","SQ"],"330000":["浙江","Zhejiang","ZJ"],"330100":["杭州","Hangzhou","HZ"],"330200":
["宁波","Ningbo","NB"],"330300":["温州","Wenzhou","WZ"],"330400":["嘉兴","Jiaxing","JX"],"330500":
["湖州","Huzhou","HZ"],"330600":["绍兴","Shaoxing","SX"],"330700":["金华","Jinhua","JH"],"330800":
["衢州","Quzhou","QZ"],"330900":["舟山","Zhoushan","ZS"],"331000":["台州","Taizhou","TZ"],"331100":
["丽水","Lishui","LS"],"340000":["安徽","Anhui","AH"],"340100":["合肥","Hefei","HF"],"340200":["芜
湖","Wuhu","WH"],"340300":["蚌埠","Bangbu","BB"],"340400":["淮南","Huainan","HN"],"340500":["马鞍
山","Maanshan","MAS"],"340600":["淮北","Huaibei","HB"],"340700":["铜陵","Tongling","TL"],"340800":
["安庆","Anqing","AQ"],"341000":["黄山","Huangshan","HS"],"341100":["滁
州","Chuzhou","CZ"],"341200":["阜阳","Fuyang","FY"],"341300":["宿州","Xiuzhou","SZ"],"341400":["巢
湖市","Chaohushi","CHS"],"341500":["六安","Liuan","LA"],"341600":["亳州","Bozhou","BZ"],"341700":
["池州","Chizhou","CZ"],"341800":["宣城","Xuancheng","XC"],"350000":["福建","Fujian","FJ"],"3
...
...
...
```

问题 5 / 7

TOC

发现可能的服务器路径泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/element.js
实体：	element.js (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修补程序
固定值：	为 Web 服务器或 Web 应用程序下载相关的安全补丁

差异：

推理： 响应包含服务器上文件的绝对路径和/或文件名。

测试请求和响应：

```
GET /xmjg/xmjg/supervisionInspection/js/element.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-
00000002879
Cookie: JSESSIONID=BAD94CD62CFD05C63C4D2EF079DD5B06
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US
```

```
HTTP/1.1 200
Content-Length: 525328
Last-Modified: Tue, 22 Dec 2020 02:31:13 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:44:25 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
Cache-Control: no-c
...
...
...
){n.push.apply(n,e),++r===s&&i(n)}e.forEach(function(e){t(e,o)})}(n,i,u)})}function xo(e){return
function(t){return t&&t.message?(t.field=t.field||e.fullField,t):
{message:t,field:t.field||e.fullField}}}function Co(e,t){if(t)for(var i in
t)if(t.hasOwnProperty(i)){var n=t[i];"object"===(void 0===n?"undefined":mo()(n))&&"object"===mo()
(e[i])?e[i]=po()({},e[i],n):e[i]=n}return e}var ko=function(e,t,i,n,r,s)
{!e.required||i.hasOwnProperty(e.field)&&!yo(t,s||e.type)||n.push(bo(r.messages.required,e.fullFi
eld))};var So=function(e,t,i,n,r)
{(/^\s+$/.test(t)||""===t)&&n.push(bo(r.messages.whitespace,e.fullField))},Do={email:/^(([^<>()\
[\]\\.,;:\s@"]+(\.[^<>()\[\]\\.,;:\s@"]+)*)|(".+"))@((\[[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]
{1,3}])|(([a-zA-Z\-0-9]+\.)+[a-zA-Z]{2,}))$/,url:new RegExp("^(?!mailto:)(?:
(?:http|https|ftp)://|//)(?:\\S+(?::\\S*)?@)?(?:(?:(?:[1-9]\\d?|1\\d\\d|2[01]\\d|22[0-3])(?:\\.
(?:1?\\d{1,2}|2[0-4]\\d|25[0-5])){2}(?:\\.(?:[0-9]\\d?|1\\d\\d|2[0-4]\\d|25[0-4]))|(?:(?:[a-
z\\u00a1-\\uffff0-9]+-?)*[a-z\\u00a1-\\uffff0-9]+)(?:\\.(?:[a-z\\u00a1-\\uffff0-9]+-?)*[a-
z\\u00a1-\\uffff0-9]+)*(?:\\.(?:[a-z\\u00a1-\\uffff]{2,})))|localhost)(?::\\d{2,5})?(?:(/|\\?|#)
[^\\s]*)?$","i"),hex:/^#?([a-f0-9]{6}|[a-f0-9]{3})$/i},$o={integer:function(e){return
$o.number(e)&&parseInt(e,10)===e},float:function(e){return
$o.number(e)&&!$o.integer(e)},array:function(e){return Array.isArray(e)},regexp:function(e){if(e
instanceof RegExp)return!0;try{return!!new RegExp(e)}catch(e){return!1}},date:function(e)
{return"function"==typeof e.getTime&&"function"==typeof e.getMonth&&"function"==typeof
e.getYear},number:function(e){return!isNaN(e)&&"number"==typeof e},object:function(e)
{return"object"===(void 0===e?"undefined":mo()(e))&&!$o.array(e)},method:function(e)
{return"function"==typeof e},email:function(e){return"string"==typeof
e&&!!e.match(Do.email)&&e.length<255},url:function(e){return"string"==typeof
e&&!!e.match(Do.url)},hex:function(e){return"string"==typeof e&&!!e.match(Do.hex)}};var
Eo=function(e,t,i,n,r){if(e.required&&void 0===t)ko(e,t,i,n,r);else{var s=e.type;
...
...
...
upload-list.vue";var ml=fl.exports,vl=i(16),gl=i.n(vl);var bl=function(){var
e=this,t=e.$createElement;return(e._self._c||t)("div",{staticClass:"el-upload-dragger",class:
{"is-dragover":e.dragover},on:{drop:function(t){return
t.preventDefault(),e.onDrop(t)},dragover:function(t){return
t.preventDefault(),e.onDragover(t)},dragleave:function(t){t.preventDefault(),e.dragover=!1}}},
[e._t("default")],2)};bl._withStripped=!0;var yl=r({name:"ElUploadDrag",props:
{disabled:Boolean},inject:{uploader:{default:""}},data:function(){return{dragover:!1}},methods:
{onDragover:function(){this.disabled||(this.dragover=!0)},onDrop:function(e)
{if(!this.disabled&&this.uploader){var t=this.uploader.accept;this.dragover=!1,t?
this.$emit("file",[].slice.call(e.dataTransfer.files).filter(function(e){var
i=e.type,n=e.name,r=n.indexOf(".")>-1?"."+n.split(".").pop():"",s=i.replace(/\/.*$/,"");return
t.split(",").map(function(e){return e.trim()}).filter(function(e){return e}).some(function(e)
{return/\..+$/.test(e)?r===e:/\/\*$/.test(e)?
s===e.replace(/\/\*$/,""):!!/^[^\/]+\/[^\/]+$/.test(e)&&i===e})})):this.$emit("file",e.dataTransf
er.files)}}}},bl,[],!1,null,null,null);yl.options.__file="packages/upload/src/upload-
dragger.vue";var _l=r({inject:["uploader"],components:{UploadDragger:yl.exports},props:
{type:String,action:{type:String,required:!0},name:
{type:String,default:"file"},data:Object,headers:Object,withCredentials:Boolean,multiple:Boolean,
accept:String,onStart:Function,onProgress:Function,onSuccess:Function,onError:Function,beforeUplo
ad:Function,drag:Boolean,onPreview:{type:Function,default:function(){}},onRemove:
{type:Function,default:function()
{}},fileList:Array,autoUpload:Boolean,listType:String,httpRequest:
{type:Function,default:function(e){if("undefined"!=typeof XMLHttpRequest){var t=new
XMLHttpRequest,i=e.action;t.upload&&(t.upload.onprogress=function(t){t.total>0&&
(t.percent=t.loaded/t.total*100),e.onProgress(t)});var n=new FormData;e.data&&O
...
...
...
```

问题 6 / 7

TOC

发现可能的服务器路径泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrapValidator.js
实体：	bootstrapValidator.js (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修补程序
固定值：	为 Web 服务器或 Web 应用程序下载相关的安全补丁

差异：

推理： 响应包含服务器上文件的绝对路径和/或文件名。

测试请求和响应：

```
GET /xmjg/bootstrap/js/bootstrapValidator.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//xmjg-one-form!getYzbd.action?
name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&x
zqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 334075
Last-Modified: Mon, 21 Sep 2020 04:41:10 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:50:39 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

/*!
 * BootstrapValidator (http://bootstrapvalidator.com)
 * The best jQuery plugin to validate form fields. Designed to use with Bootstrap 3
 *
 * @version     v0.5.3, built on 2014-11-05 9:14:18 PM
 * @author      https://twitter.com/nghuuphuoc
 * @copyright   (c) 2013 - 2014 Nguyen Huu Phuoc
 * @license     Commercial: http://bootstrapvalidator.com/license/
 *          Non-commercial: http://creativecommons.org/licenses/by-nc-nd/3.0/
 */
if (typeof jQuery === 'undefined') {
    throw new Error('BootstrapValidator requires jQuery');
}

(function($) {
    var version = $.fn.jquery.split(' ')[0].split('.');
    if ((+version[0] < 2 && +version[1] < 9) || (+version[0] === 1 && +version[1] === 9 &&
+version[2] < 1)) {
        throw new Error('BootstrapValidator requires jQuery version 1.9.1 or higher');
    }
}(window.jQuery));

(function($) {
    var BootstrapValidator = function(form, options) {
        this.$form   = $(form);
        this.options = $.extend({}, $.fn.bootstrapValidator.DEFAULT_OPTIONS, options);

        this.$invalidFields = $([]);    // Array of invalid fields
        this.$submitButton  = null;     // The submit button which is clicked to submit form
        this.$hiddenButton  = null;

        // Validating status
        this.STATUS_NOT_VALIDATED = 'NOT_VALIDATED';
        this.STATUS_VALIDATING    = 'VALIDATING';
        this.STATUS_INVALID       = 'INVALID';
        this.STATUS_VALID         = 'VALID';

        // Determine the event that is fired when user change the field value
        // Most modern browsers supports input event except IE 7, 8.
        // IE 9 supports input event but the event is still not fired if I press the backspace
key.
        // Get IE version
        // https://gist.github.com/padolsey/527683/#comment-7595
        var ieVersion = (function() {
          var v = 3, div = document.createElement('div'), a = div.all || [];
          while (div.innerHTML = '<!--[if gt IE '+(++v)+']><br><![endif]-->', a[0]) {}
          return v > 4 ? v : !v;
        }());

        var el = document.createElement('div');
        this._changeEvent = (ieVersion === 9 || !('oninput' in el)) ? 'keyup' : 'input';

        // The flag to indicate that the form is ready to submit when a remote/callback validator
returns
        this._submitIfValid = null;

        // Field elements
        this._cacheFields = {};

        this._init();
    };

    BootstrapValidator.prototype = {
        constructor: BootstrapValidator,

        /**
         * Init form
         */
        _init: function() {
          var that    = this,
          options = {
          autoFocus:      this.$form.attr('data-bv-autofocus'),
          container:      this.$form.attr('data-bv-container'),
          events: {
          formInit:         this.$form.attr('data-bv-events-form-init'),
          formError:        this.$form.attr('data-bv-events-form-error'),
          formSuccess:      this.$form.attr('data-bv-events-form-success'),
          fieldAdded:       this.$form.attr('data-bv-events-field-add
...
...
...

          "(?:\\.(?:1?\\d{1,2}|2[0-4]\\d|25[0-5])){2}" +
          "(?:\\.(?:[1-9]\\d?|1\\d\\d|2[0-4]\\d|25[0-4]))" +
          "|" +
          // host name
          "(?:(?:[a-z\\u00a1-\\uffff0-9]+-?)*[a-z\\u00a1-\\uffff0-9]+)" +
          // domain name
          "(?:\\.(?:[a-z\\u00a1-\\uffff0-9]+-?)*[a-z\\u00a1-\\uffff0-9]+)*" +
          // TLD identifier
          "(?:\\.(?:[a-z\\u00a1-\\uffff]{2,}))" +
          // Allow intranet sites (no TLD) if `allowLocal` is true
          (allowLocal ? '?' : '') +
          ")" +
          // port number
...
...
...
```

问题 7 / 7

TOC

发现可能的服务器路径泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/agcloud/framework/ui-private/common/element-2/element.js
实体：	element.js (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修补程序
固定值：	为 Web 服务器或 Web 应用程序下载相关的安全补丁

差异：

推理： 响应包含服务器上文件的绝对路径和/或文件名。

测试请求和响应：

```
GET /xmjg/agcloud/framework/ui-private/common/element-2/element.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer:
http://127.0.0.1:8000/xmjg//supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?
averageTime=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-
29&provinceCode=660000
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 525328
Last-Modified: Tue, 22 Dec 2020 02:31:13 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tu
...
...
...
){n.push.apply(n,e),++r===s&&i(n)}e.forEach(function(e){t(e,o)})}(n,i,u)})}function xo(e){return
function(t){return t&&t.message?(t.field=t.field||e.fullField,t):
{message:t,field:t.field||e.fullField}}}function Co(e,t){if(t)for(var i in
t)if(t.hasOwnProperty(i)){var n=t[i];"object"===(void 0===n?"undefined":mo()(n))&&"object"===mo()
(e[i])?e[i]=po()({},e[i],n):e[i]=n}return e}var ko=function(e,t,i,n,r,s)
{!e.required||i.hasOwnProperty(e.field)&&!yo(t,s||e.type)||n.push(bo(r.messages.required,e.fullFi
eld))};var So=function(e,t,i,n,r)
{(/^\s+$/.test(t)||""===t)&&n.push(bo(r.messages.whitespace,e.fullField))},Do={email:/^(([^<>()\
[\]\\.,;:\s@"]+(\.[^<>()\[\]\\.,;:\s@"]+)*)|(".+"))@((\[[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]
{1,3}])|(([a-zA-Z\-0-9]+\.)+[a-zA-Z]{2,}))$/,url:new RegExp("^(?!mailto:)(?:
(?:http|https|ftp)://|//)(?:\\S+(?::\\S*)?@)?(?:(?:(?:[1-9]\\d?|1\\d\\d|2[01]\\d|22[0-3])(?:\\.
(?:1?\\d{1,2}|2[0-4]\\d|25[0-5])){2}(?:\\.(?:[0-9]\\d?|1\\d\\d|2[0-4]\\d|25[0-4]))|(?:(?:[a-
z\\u00a1-\\uffff0-9]+-?)*[a-z\\u00a1-\\uffff0-9]+)(?:\\.(?:[a-z\\u00a1-\\uffff0-9]+-?)*[a-
z\\u00a1-\\uffff0-9]+)*(?:\\.(?:[a-z\\u00a1-\\uffff]{2,})))|localhost)(?::\\d{2,5})?(?:(/|\\?|#)
[^\\s]*)?$","i"),hex:/^#?([a-f0-9]{6}|[a-f0-9]{3})$/i},$o={integer:function(e){return
$o.number(e)&&parseInt(e,10)===e},float:function(e){return
$o.number(e)&&!$o.integer(e)},array:function(e){return Array.isArray(e)},regexp:function(e){if(e
instanceof RegExp)return!0;try{return!!new RegExp(e)}catch(e){return!1}},date:function(e)
{return"function"==typeof e.getTime&&"function"==typeof e.getMonth&&"function"==typeof
```

```
e.getYear},number:function(e){return!isNaN(e)&&"number"==typeof e},object:function(e)
{return"object"===(void 0===e?"undefined":mo()(e))&&!$o.array(e)},method:function(e)
{return"function"==typeof e},email:function(e){return"string"==typeof
e&&!!e.match(Do.email)&&e.length<255},url:function(e){return"string"==typeof
e&&!!e.match(Do.url)},hex:function(e){return"string"==typeof e&&!!e.match(Do.hex)}};var
Eo=function(e,t,i,n,r){if(e.required&&void 0===t)ko(e,t,i,n,r);else{var s=e.type;
...
...
...
upload-list.vue";var ml=fl.exports,vl=i(16),gl=i.n(vl);var bl=function(){var
e=this,t=e.$createElement;return(e._self._c||t)("div",{staticClass:"el-upload-dragger",class:
{"is-dragover":e.dragover},on:{drop:function(t){return
t.preventDefault(),e.onDrop(t)},dragover:function(t){return
t.preventDefault(),e.onDragover(t)},dragleave:function(t){t.preventDefault(),e.dragover=!1}}},
[e._t("default")],2)};bl._withStripped=!0;var yl=r({name:"ElUploadDrag",props:
{disabled:Boolean},inject:{uploader:{default:""}},data:function(){return{dragover:!1}},methods:
{onDragover:function(){this.disabled||(this.dragover=!0)},onDrop:function(e)
{if(!this.disabled&&this.uploader){var t=this.uploader.accept;this.dragover=!1,t?
this.$emit("file",[].slice.call(e.dataTransfer.files).filter(function(e){var
i=e.type,n=e.name,r=n.indexOf(".")>-1?"."+n.split(".").pop():"",s=i.replace(/\/.*$/,"");return
t.split(",").map(function(e){return e.trim()}).filter(function(e){return e}).some(function(e)
{return/\..+$/.test(e)?r===e:/\/\*$/.test(e)?
s===e.replace(/\/\*$/,""):!!/^[^\/]+\/[^\/]+$/.test(e)&&i===e})})):this.$emit("file",e.dataTransf
er.files)}}}},bl,[],!1,null,null,null);yl.options.__file="packages/upload/src/upload-
dragger.vue";var _l=r({inject:["uploader"],components:{UploadDragger:yl.exports},props:
{type:String,action:{type:String,required:!0},name:
{type:String,default:"file"},data:Object,headers:Object,withCredentials:Boolean,multiple:Boolean,
accept:String,onStart:Function,onProgress:Function,onSuccess:Function,onError:Function,beforeUplo
ad:Function,drag:Boolean,onPreview:{type:Function,default:function(){}},onRemove:
{type:Function,default:function()
{}},fileList:Array,autoUpload:Boolean,listType:String,httpRequest:
{type:Function,default:function(e){if("undefined"!=typeof XMLHttpRequest){var t=new
XMLHttpRequest,i=e.action;t.upload&&(t.upload.onprogress=function(t){t.total>0&&
(t.percent=t.loaded/t.total*100),e.onProgress(t)});var n=new FormData;e.data&&O
...
...
...
```

参 发现内部 IP 泄露模式 1 TOC

问题 1 / 1 TOC

发现内部 IP 泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/xmjg-city-map-config!getMapurlByXzqhdm.action
实体：	xmjg-city-map-config!getMapurlByXzqhdm.action (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的内部 IP 地址

差异：

推理： AppScan 在响应中发现了看似为内部 IP 地址的内容。

测试请求和响应：

```
GET /xmjg/xmjg-city-map-config!getMapurlByXzqhdm.action?
xzqhdm=660100&accessEntry=%E5%9F%8E%E5%B8%82%E9%A6%96%E9%A1%B5 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8000/xmjg//city-page/getCsrk.action?
bigScreenFolder=&name=%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82&xzqhdm=660100&flag=1
&startDate=2020-01-01&endDate=2020-12-29
Cookie: JSESSIONID=525D8BA1AD386917420AFD6478A47671
Connection: keep-alive
Host: 127.0.0.1:8000
X-Requested-With: XMLHttpRequest
Accept: text/plain, */*; q=0.01
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 66
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Date: Tue, 29 Dec 2020 02:49:53 GMT
Content-Type: text/plain;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

http://10.4.4.16:8886/agcom/2dMap/interfaceMap.html?userName=admin
```

参 客户端（JavaScript）Cookie 引用 4 TOC

问题 1 / 4 TOC

客户端（JavaScript）Cookie 引用	
严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/common/tool/common-merge.js
实体：	/** (Page)
风险：	此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色
原因：	Cookie 是在客户端创建的
固定值：	除去客户端中的业务逻辑和安全逻辑

差异：

推理： AppScan 在 JavaScript 中找到对 cookie 的引用。

测试请求和响应：

```
GET /xmjg/common/tool/common-merge.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
```

```
Referer: http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
Cookie: JSESSIONID=BCBD8BB602314F1C74484B8880DE6958
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 28033
Last-Modified: Thu, 29 Oct 2020 15:39:15 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:10:06 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

/**
 * 外部js调用
 */
var commonWindow = {
    //打开页面
    toWindowForReturn: function (url, pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
//          pageObj.commonWindowAction.doWindowForReturn(encodeURI(url));
                 console.log(encodeURI(url))
          pageObj.commonWindowAction.doWindowForReturn(encodeURI(url));
        }
    },


    //打开页面  不支持返回
    toWindowNotReturn: function (url, pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
          pageObj.commonWindowAction.doWindowNotReturn(url);
        }
    },

    //返回上一页面
    returnParentWindow: function (pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
          pageObj.commonWindowAction.doReturnParentWindow();
        }
    },
    //跳转到对应页面(传入的url与之前的iframe地址一致的时候 退回到对应iframe,如果不存在 则调用
toWindowForReturn)
    jumpWindowForIframe: function (url, pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
          pageObj.commonWindowAction.doJumpWindowForIframe(url);
        }
    },
    //获取对应的页面  pageFlag (max-top-page: 最顶级页面;)
    getWindowObj: function (pageFlag) {
        if (!pageFlag) {
          pageFlag = "max-top-page";
        }
        var obj = window.self;
        var whileFlag = true;
        while (whileFlag) {

          if (obj.document.getElementById("page-level-flag-in")) {
          //最顶级页面
          if (obj.document.getElementById("page-level-flag-in").value == pageFlag) {
          return obj;
          }
          }
          if (whileFlag) {
          if (obj.window.parent != obj.window) {
          obj = obj.window.parent;
          } else {
          whileFlag = false;
          }
          }
        }
        return window.self;
    },
};

//==================================================================================================
=============================

var commonWindowAction = {
    doWindowForReturn: function (url) {
        var maxDataIndex = 0;
        var $lastIframe;
        $(".content-url-iframe").each(function () {
          var thisDataIndex = parseInt($(this).attr("data-index"));
          if (maxDataIndex < thisDataIndex) {
          maxDataIndex = thisDataIndex;
          }
          if (maxDataIndex == thisDataIndex) {
          $lastIframe = $(this);
          }
          commonWindowAction.doRemoveClass($(this), "curr-url-iframe");
        });
        if ($lastIframe) {
          var timestamp = (new Date()).valueOf();
          var key = "contentZframe-id-" + timestamp + "-" + (maxDataIndex + 1);
          $lastIframe.after("<iframe allowfullscreen  id=\"" + key + "\" width=\"100%\"
height=\"100%\" src=\"\" frameborder=\"0\" class=\"content-url-iframe  curr-url-iframe\" data-
index=\"" + (maxDataIndex + 1) + "\"></iframe>");
          $("#" + key).attr("src", url);
        }
        console.log(url)
        commonWindowAction.removeIframeOrHide(true);

    },
    doWindowNotReturn: function (url) {
        $(".content-url-iframe").each(function () {
                if($(this).hasClass("curr-url-iframe")){
                        if(url.indexOf("?")<=-1){
                                url+="?";
                        }else{
                                url+="&";
                        }
                        url+="notHaveReturnFlag=yes";
                        $(this).attr("src", url);
                        $(this).attr("id","contentZframe");
                        $(this).attr("data-index","0");
                }else{
          commonWindowAction.doRemoveClass($(this), "curr-url-iframe");
          }
        });
        commonWindowAction.removeIframeOrHide(false);
    },
    //执行返回上一页
    doReturnParentWindow: function () {
        var $lastIframe;
        var maxDataInde
...
...
...

          str += name + "=" + keyValueDir[name] + ";";
        }
        var exdate = new Date();
        exdate.setDate(exdate.getDate() + 30);
        document.cookie = str + "expires=" + exdate.toGMTString();
    },
    _getCookieArr: function () {
        var keyValues = document.cookie.split(";");
        var keyValueDir = {};
...
...
...
```

问题 2 / 4

TOC

客户端（JavaScript）Cookie 引用

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/vendors.bundle.js
实体：	/*! (Page)
风险：	此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色
原因：	Cookie 是在客户端创建的
固定值：	除去客户端中的业务逻辑和安全逻辑

差异：

推理： AppScan 在 JavaScript 中找到对 cookie 的引用。

测试请求和响应：

```
GET /opus-front-sso/framework/ui-themes/common/metronic/js/vendors.bundle.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/require
Cookie: JSESSIONID=4449CA63082A5569737A8C3BAFE8FEE6
Connection: keep-alive
Host: 127.0.0.1:8090
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 28 Dec 2020 07:36:44 GMT
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Content-Length: 3899883
X-Content-Type-Options: nosniff
Cache-Control: max-age=31556926
Date: Tue, 29 Dec 2020 02:10:02 GMT
Content-Type: application/javascript;charset=utf-8

/*!
 * jQuery JavaScript Library v3.2.1
 * https://jquery.com/
 *
 * Includes Sizzle.js
 * https://sizzlejs.com/
 *
 * Copyright JS Foundation and other contributors
 * Released under the MIT license
 * https://jquery.org/license
 *
 * Date: 2017-03-20T18:59Z
 */
( function( global, factory ) {

 "use strict";

 if ( typeof module === "object" && typeof module.exports === "object" ) {

         // For CommonJS and CommonJS-like environments where a proper `window`
         // is present, execute the factory and get jQuery.
         // For environments that do not have a `window` with a `document`
         // (such as Node.js), expose a factory as module.exports.
         // This accentuates the need for the creation of a real `window`.
         // e.g. var jQuery = require("jquery")(window);
         // See ticket #14549 for more info.
         module.exports = global.document ?
                 factory( global, true ) :
                 function( w ) {
                         if ( !w.document ) {
                                 throw new Error( "jQuery requires a window with a
document" );
                                }
                         return factory( w );
                 }       ;
 } else {
         factory( global );
        }

// Pass this if window is not defined yet
} )( typeof window !== "undefined" ? window : this, function( window, noGlobal ) {

// Edge <= 12 - 13+, Firefox <=18 - 45+, IE 10 - 11, Safari 5.1 - 9+, iOS 6 - 9.1
// throw exceptions when non-strict code (e.g., ASP.NET 4.5) accesses strict mode
// arguments.callee.caller (trac-13335). But as of jQuery 3.0 (2016), strict mode should be
common
// enough that all such attempts are guarded in a try block.
"use strict";

var arr = [];

var document = window.document;

var getProto = Object.getPrototypeOf;

var slice = arr.slice;

var concat = arr.concat;

var push = arr.push;

var indexOf = arr.indexOf;

var class2type = {};

var toString = class2type.toString;

var hasOwn = class2type.hasOwnProperty;

var fnToString = hasOwn.toString;

var ObjectFunctionString = fnToString.call( Object );

var support = {};



 function DOMEval( code, doc ) {
         doc = doc || document;

         var script = doc.createElement( "script" );

         script.text = code;
         doc.head.appendChild( script ).parentNode.removeChild( script );
        }
/* global Symbol */
// Defining this global in .eslintrc.json would create a danger of using the global
// unguarded in another place, it seems safer to define global only for this module



var
 version = "3.2.1",

 // Define a local copy of jQuery
 jQuery = function( selector, context ) {

         // The jQuery object is actually just the init constructor 'enhanced'
         // Need init if jQuery is called (just allow error to be thrown if not included)
         return new jQuery.fn.init( selector, context );
 },

 // Support: Android <=4.0 only
 // Make sure we trim BOM and NBSP
 rtrim = /^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,

 // Matches dashed string for camelizing
 rmsPrefix = /^-ms-/,
 rdashAlpha = /-([a-z])/g,

 // Used by jQuery.camelCase as callback to replace()
 fcamelCase = function( all, letter ) {
         return letter.toUpperCase();
 };

jQuery.fn = jQuery.prototype = {

 // The current version of jQuery being used
 jquery: version,

 constructor: jQuery,

 // The default length of a jQuery object is 0
 length: 0,

 toArray: function() {
         return slice.call( this );
 },

 // Get the Nth element in the matched element set OR
 // Get the whole matched element set as a clean array
 get: function( num ) {

         // Return all the elements in a clean array
         if ( num == null ) {
                 return slice.call( this );
                }

         // Return just the one element from the set
         return num < 0 ? this[ num + this.length ] : this[ num ];
 },

 // Take an array of elements and push it onto the stack
 // (returning the new matched element set)
 pushStack: function( elems ) {

         // Build a new jQuery matched element set
         var ret = jQuery.merge( this.constructor(), elems );

         // Add the old object onto the stack (as a reference)
         ret.prevObject = this;

         // Return the newly-formed element set
         return ret;
 },

 // Execute a callbac
...
...
...

                                         continue;
                                        }
                                 stringifiedAttributes += '=' + attributes[attributeName];
                                }
                         return (document       .cookie = key + '=' + value +
stringifiedAttributes);
                        }

                 // Read

...
...
...
```

问题 3 / 4

TOC

客户端（JavaScript）Cookie 引用

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/jquery.cookie.js
实体：	/** (Page)
风险：	此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色
原因：	Cookie 是在客户端创建的
固定值：	除去客户端中的业务逻辑和安全逻辑

差异：

推理： AppScan 在 JavaScript 中找到对 cookie 的引用。

测试请求和响应：

```
GET /opus-front-sso/framework/ui-themes/common/metronic/js/jquery.cookie.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/require
Cookie: JSESSIONID=4449CA63082A5569737A8C3BAFE8FEE6
Connection: keep-alive
Host: 127.0.0.1:8090
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Last-Modified: Mon, 28 Dec 2020 07:36:44 GMT
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Content-Length: 4467
X-Content-Type-Options: nosniff
Cache-Control: max-age=31556926
Date: Tue, 29 Dec 2020 02:10:02 GMT
Content-Type: application/javascript;charset=utf-8

/**
 * Cookie plugin
 *
 * Copyright (c) 2006 Klaus Hartl (stilbuero.de)
 * Dual licensed under the MIT and GPL licenses:
 * http://www.opensource.org/licenses/mit-license.php
 * http://www.gnu.org/licenses/gpl.html
 *
 */

/**
 * Create a cookie with the given name and value and other optional parameters.
 *
 * @example $.cookie('the_cookie', 'the_value');
 * @desc Set the value of a cookie.
 * @example $.cookie('the_cookie', 'the_value', { expires: 7, path: '/', domain: 'jquery.com',
secure: true });
 * @desc Create a cookie with all available options.
 * @example $.cookie('the_cookie', 'the_value');
 * @desc Create a session cookie.
 * @example $.cookie('the_cookie', null);
 * @desc Delete a cookie by passing null as value. Keep in mind that you have to use the same
path and domain
 *       used when the cookie was set.
 *
 * @param String name The name of the cookie.
 * @param String value The value of the cookie.
 * @param Object options An object literal containing key/value pairs to provide optional cookie
```

```
attributes.
 * @option Number|Date expires Either an integer specifying the expiration date from now on in
days or a Date object.
 *          If a negative value is specified (e.g. a date in the past), the cookie will be
deleted.
 *          If set to null or omitted, the cookie will be a session cookie and will not be
retained
 *          when the the browser exits.
 * @option String path The value of the path atribute of the cookie (default: path of page that
created the cookie).
 * @option String domain The value of the domain attribute of the cookie (default: domain of page
that created the cookie).
 * @option Boolean secure If true, the secure attribute of the cookie will be set and the cookie
transmission will
 *          require a secure protocol (like HTTPS).
 * @type undefined
 *
 * @name $.cookie
 * @cat Plugins/Cookie
 * @author Klaus Hartl/klaus.hartl@stilbuero.de
 */

/**
 * Get the value of a cookie with the given name.
 *
 * @example $.cookie('the_cookie');
 * @desc Get the value of a cookie.
 *
 * @param String name The name of the cookie.
 * @return The value of the cookie.
 * @type String
 *
 * @name $.cookie
 * @cat Plugins/Cookie
 * @author Klaus Hartl/klaus.hartl@stilbuero.de
 */
jQuery.cookie = function(name, value, options) {
    if (typeof value != 'undefined') { // name and value given, set cookie
        options = options || {};
        if (value === null) {
          value = '';
          options = $.extend({}, options); // clone object since it's unexpected behavior if the
expired property were changed
          options.expires = -1;
        }
        var expires = '';
        if (options.expires && (typeof options.expires == 'number' ||
options.expires.toUTCString)) {
          var date;
          if (typeof options.expires == 'number') {
          date = new Date();
          date.setTime(date.getTime() + (options.expires * 24 * 60 * 60 * 1000));
          } else {
          date = options.expires;
          }
          expires = '; expires=' + date.toUTCString(); // use expires attribute, max-age is not
supported by IE
        }
        // NOTE Needed to parenthesize options.path and options.domain
        // in the following expressions, otherwise they evaluate to undefined
        // in the packed version for some reason...
        var path = options.path ? '; path=' + (options.path) : '';
        var domain = options.domain ? '; domain=' + (options.domain) : '';
        var secure = options.secure ? '; secure' : '';
        document.cookie = [name, '=', encodeURIComponent(value), expires, path, domain,
secure].join('');
    } else { // only name given, get cookie
        var cookieValue = null;
        if (document.cookie && document.cookie != '') {
          var cookies = document.cookie.split(';');
          for (var i = 0; i < cookies.length; i++) {
          var cookie = jQuery.trim(cookies[i]);
          // Does this cookie string begin with the name we want?
          if (cookie.substring(0, name.length
...
...
...
```

问题 4 / 4

TOC

客户端（JavaScript）Cookie 引用

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8000/xmjg/common/tool/common-core.js
实体：	/** (Page)
风险：	此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色
原因：	Cookie 是在客户端创建的
固定值：	除去客户端中的业务逻辑和安全逻辑

差异：

推理： AppScan 在 JavaScript 中找到对 cookie 的引用。

测试请求和响应：

```
GET /xmjg/common/tool/common-core.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer:
http://127.0.0.1:8000/xmjg//supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?
provinceCode=660000&dataType=8&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-
29&bigScreenFolder=&dateEnd=2020-12-29
Cookie: JSESSIONID=BCBD8BB602314F1C74484B8880DE6958
Connection: keep-alive
Host: 127.0.0.1:8000
Accept: */*
Accept-Language: en-US


HTTP/1.1 200
Content-Length: 10844
Last-Modified: Mon, 21 Sep 2020 04:41:10 GMT
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Tue, 29 Dec 2020 02:10:46 GMT
Content-Type: application/javascript;charset=utf-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

/**
 *
 */


var Augur = Augur || {}
Augur.Xmjg = Augur.Xmjg || {}
Augur.Xmjg.CityDataCache = function () {
    this.mapDataCache = {};
    this.storeMapDataCache = function (name, data) {
        this.mapDataCache[name] = data;
    };
    this.getMapDataCache = function (name) {
        return this.mapDataCache[name];
    }
}
Augur.CookieHelper = {
    setCookie: function (cookieKey, cookieValue) {
        var cookieArr = {};
        cookieArr[cookieKey] = cookieValue;
        this._saveCookieArr(cookieArr);
    },
    getCookie: function (key) {
        var keyValues = document.cookie.split(";");
        var keyValueDir = [];
        for (var i = 0; i < keyValues.length; i++) {
          var keyIndex = keyValues[i].indexOf('=');
          var name = keyValues[i].substr(0, keyIndex).trim();
          if (key === name)
          return keyValues[i].substr(keyIndex + 1);
        }
        return "";
    },
    getCookieAsBoolean: function (key, defaultValue) {
        if (defaultValue == undefined)
          defaultValue = false;
        var result = this.getCookie(key);
        if (result == "" || result == null)
          return defaultValue;
        if (result == "false" || result == "0")
          return false;
        if (result == "true" || result == "1")
          return true;
        return result;
    },
    saveBackground: function (scene, param) {
        scene = scene || "background";
        var cookieArr = {};
        cookieArr[scene] = param;
        this._saveCookieArr(cookieArr);
    },
    getBackground: function (scene) {
        scene = scene || "background";
        return this.getCookie(scene);
    },
    _saveCookieArr: function (keyValueDir) {
        var str = "";
        for (var name in keyValueDir) {
          str += name + "=" + keyValueDir[name] + ";";
        }
        var exdate = new Date();
        exdate.setDate(exdate.getDate() + 30);
        document.cookie = str + "expires=" + exdate.toGMTString();
    },
    _getCookieArr: function () {
        var keyValues = document.cookie.split(";");
        var keyValueDir = {};
        for (var i = 0; i < keyValues.length; i++) {
          if (keyValues[i].length < 1)
          continue;
          var keyIndex = keyValues[i].indexOf('=');
          var name = keyValues[i].substr(0, keyIndex).trim();
          var value = keyValues[i].substr(keyIndex + 1).trim();
          keyValueDir[name] = value;
        }
        return keyValueDir;
    }
};
/**
 *  需要引用
 * <script type="text/javascript" src="js/libs/jquery-3.1.0.min.js"></script>
 */
Augur.AjaxGetter = {
    getHtmlSegment: function (url, successCallback, failCallback, params) {
        var isJsp = Augur.UrlHelper.isJspUrl(url);
        var dataTypeValue = isJsp ? "JSONP" : "text";
        url = Augur.UrlHelper.getFilterredUrl(url);

        $.ajax({
          type: 'GET',
          scriptCharset: 'utf-8',
          url: url,
          data: null,
          dataType: dataTypeValue,
          processData: false,
          contentType: false,
          sender: this,
          success: function (args1) {
          successCallback(args1, url, params);
          },
          error: function (XMLHttpRequest, textStatus, errorThrown) {
          console.log("getHtmlSegment loadPage error");
          if (failCallback)
          failCallback(XMLHttpRequest, textStatus, errorThrown, params);
          else
          this.sender.defaultFailCallback(url, XMLHttpRequest, textStatus, errorThrown);
          }
        });
    },
    getHtmlSegmentByPost: function (url, data, successCallback, failCallback, params) {
        var isJsp = Augur.UrlHelper.isJspUrl(url);
        var dataTypeValue = isJsp ? "JSONP" : "text";
        url = Augur.UrlHelper.getFilterredUrl(url);

        $.ajax({
          type: 'POST',
          url: url,
          data: data,
          processData: true,

...
...
...
```

参 应用程序错误 2 TOC

问题 1 / 2 TOC

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8090/opus-front-sso/oauth/authorize
实体：	redirect_uri (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

差异： **参数** `redirect_uri` 从以下位置进行控制： `http://127.0.0.1:8000/xmjg/login` 至： `;`

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

测试请求和响应：

```
GET /opus-front-sso/oauth/authorize?client_id=xmjg&redirect_uri=;&response_type=code&state=tba1ER
HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/form
Cookie: JSESSIONID=24E80C5845F452C87C1B10300BEF316D
Connection: Keep-Alive
Host: 127.0.0.1:8090
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 302
Location: http://127.0.0.1:8090/opus-front-sso/oauth/;?code=lWUDVg&state=tba1ER
X-XSS-Protection: 1; mode=block
Content-Length: 0
X-Content-Type-Options: nosniff
Cache-Control: no-store
Content-Language: en-US
Date: Tue, 29 Dec 2020 02:55:53 GMT
Content-Type: text/html;charset=utf-8



GET /opus-front-sso/oauth/;?code=lWUDVg&state=tba1ER HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/71.0.3578.98 Safari/537.36
Referer: http://127.0.0.1:8090/opus-front-sso/oauth/authorize?
client_id=xmjg&redirect_uri=;&response_type=code&state=tba1ER
Cookie: JSESSIONID=24E80C5845F452C87C1B10300BEF316D
Connection: Keep-Alive
Host: 127.0.0.1:8090
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 500
Connection: close
Content-Length: 393
Content-Language: en-US
Date: Tue, 29 Dec 2020 02:55:53 GMT
Content-Type: text/html;charset=UTF-8

<html><body><h1>Whitelabel Error Page</h1><p>This application has no explicit mapping for /error,
so you are seeing this as a fallback.</p><div id='created'>Tue Dec 29 10:55:54 CST 2020</div>
<div>There was an unexpected error (type=Internal Server Error, status=500).</div><div>The
request was rejected because the URL contained a potentially malicious String &quot;;&quot;</div>
</body></html>
```

问题 2 / 2

TOC

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://127.0.0.1:8090/opus-front-sso/oauth/authorize
实体：	client_id (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

差异： **参数** `client_id` 已从请求除去： `xmjg`

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

测试请求和响应：

```
GET /opus-front-sso/oauth/authorize?
redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=tba1ER HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://127.0.0.1:8090/opus-front-sso/authentication/form
Cookie: JSESSIONID=24E80C5845F452C87C1B10300BEF316D
Connection: Keep-Alive
Host: 127.0.0.1:8090
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 500
Content-Length: 757
Content-Language: en-US
X-Content-Type-Options: nosniff
Expires: 0
X-XSS-Protection: 1; mode=block
Connection: close
Date: Tue, 29 Dec 2020 02:55:45 GMT
Content-Type: text/html;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache, no-store, max-age=0, must-revalidate

<html><body><h1>Whitelabel Error Page</h1><p>This application has no explicit mapping for /error,
so you are seeing this as a fallback.</p><div id='created'>Tue Dec 29 10:55:45 CST 2020</div>
<div>There was an unexpected error (type=Internal Server Error, status=500).</div>
<div>PreparedStatementCallback; bad SQL grammar [select client_id, client_secret from
AGX_RS_CLOUD_SOFT where IS_ACTIVE = &#39;1&#39; AND IS_DELETED = &#39;0&#39; AND client_id = ?AND
IS_ADMIN = &#39;0&#39;]; nested exception is
com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: You have an error in your SQL syntax;
check the manual that corresponds to your MySQL server version for the right syntax to use near
&#39;IS_ADMIN = &#39;0&#39;&#39; at line 1</div></body></html>
```

修订建议

高 查看危险字符注入的可能解决方案 TOC

该任务修复的问题类型

- SQL 盲注
- SQL 注入
- 跨站点脚本编制
- 发现数据库错误模式

常规

SQL 盲注

有多种减轻威胁的技巧：
[1] 策略：库或框架
使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。
[2] 策略：参数化
如果可用，使用自动实施数据和代码之间的分离的结构化机制。这些机制也许能够自动提供相关引用、编码和验证，而不是依赖于开发者在生成输出的每一处提供此能力。
[3] 策略：环境固化
使用完成必要任务所需的最低特权来运行代码。
[4] 策略：输出编码
如果在有风险的情况下仍需要使用动态生成的查询字符串或命令，请对参数正确地加引号并将这些参数中的任何特殊字符转义。

[5] 策略：输入验证假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的白名单。拒绝任何没有严格遵守规范的输入，或者将其转换为遵守规范的内容。不要完全依赖于通过黑名单检测恶意或格式错误的输入。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入由于格式严重错误而应直接拒绝。

SQL 注入

有多种减轻威胁的技巧：
[1] 策略：库或框架
使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。
[2] 策略：参数化
如果可用，使用自动实施数据和代码之间的分离的结构化机制。这些机制也许能够提供自动提供相关引用、编码和验证，而不是依赖于开发者在生成输出的每个点提供此能力。

[3] 策略：环境固化

使用完成必要任务所需的最低特权来运行代码。
[4] 策略：输出编码
如果在有风险的情况下仍需要使用动态生成的查询字符串或命令，请对参数正确地加引号并将这些参数中的任何特殊字符转义。

[5] 策略：输入验证假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的白名单。拒绝任何没有严格遵守规范的输入，或者将其转换为遵守规范的内容。不要完全依赖于将恶意或格式错误的输入加入黑名单。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入由于格式严重错误而应直接拒绝。

跨站点脚本编制

有几种缓解技术：
[1] 策略：库或框架
使用经过审查的库或框架，这样的库或框架不允许出现这种漏洞或提供更容易避免这种漏洞的结构。
更容易生成正确编码的输出的库和框架的示例包括微软的反 XSS 库、OWASP ESAPI 编码模块和 Apache Wicket。
[2] 了解您的数据将用于的上下文及预期使用的编码。在不同组件之间传输数据时，或者生成可能同时包含多个编码的输出（如网页或多部分邮件消息）时，这一点特别重要。研究所有预期通信协议和数据表示形式，以确定所需的编码策略。
对于将输出到另一个网页的数据，特别是从外部输入接收到的数据，请对所有非字母数字字符使用相应的编码。
同一个输出文件的各个部分可能需要不同的编码，这会因输出是否处于以下各项中而不同：
[-] HTML 正文
[-] 元素属性（如 src="XYZ"）
[-] URI
[-] JavaScript 部分
[-] 级联样式表和样式属性
请注意，HTML 实体编码仅适用于 HTML 正文。
请参阅 XSS 防御速查表，
http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
了解有关所需编码和转义类型的更多详细信息。
[3] 策略：识别并减少攻击面
了解不可信输入可能进入您的软件的所有潜在区域：参数、cookie、从网络读取的任何内容、环境变量、反向 DNS 查找、查询结果、请求头、URL 组件、电子邮件、文件、文件名、数据库和向应用程序提供数据的任何外部系统。请记住，此类输入可能通过 API 调用间接获得。
[4] 策略：输出编码
对于生成的每一个网页，请使用并指定一个字符编码，如 ISO-8859-1 或 UTF-8。未指定编码时，Web 浏览器可能通过猜测网页实际使用了哪个编码，选择另一个编码。这可能导致 Web 浏览器对某些序列特殊对待，从而面向难以察觉的 XSS 攻击敞开客户机。请参阅 CWE-116 了解更多与编码/转义有关的缓解措施。
[5] 策略：识别并减少攻击面
为了帮助缓解针对用户会话 cookie 的 XSS 攻击，请将会话 cookie 设置为 HttpOnly。在支持 HttpOnly 功能的浏览器（如较新版本的 Internet Explorer 和 Firefox ）中，此属性可以防止使用 document.cookie 的恶意客户机端脚本访问用户的会话 cookie。这不是一个完善的解决方案，因为并不是所有的浏览器都支持 HttpOnly。更重要的是，XMLHTTPRequest 和其他功能强大的浏览器技术会向 HTTP 头（包括其中设置了 HttpOnly 标志的 Set-Cookie 头）提供读取权限。
[6] 策略：输入验证
假设所有输入都是恶意输入。使用“接受已知良好输入”输入验证策略：严格符合规范的可接受输入的白名单。拒绝不严格符合规范的所有输入，或者将其转换为严格符合规范的输入。请勿单独依靠列入黑名单的恶意输入或格式不正确的输入。不过，在检测潜在攻击或确定哪些输入格式不正确以至于应彻底拒绝方面，黑名单可能很有用。
执行输入验证时，请考虑所有潜在相关属性，包括长度、输入类型、可接受值的完整范围、缺少或多余的输入、语法、相关字段的一致性和业务规则的符合性。举一个业务规则逻辑的示例，“boat”在语法上可能有效，因为其仅包含字母数字字符，但是如果您期望输入的是颜色，如“red”或“blue”，则其就是无效的。
动态构建网页时，请使用基于请求中参数的预期值限制字符集的严格白名单。应验证并清理所有输入，不仅包括用户预计指定的参数，还包括请求中的所有数据（包括隐藏字段、cookie、头、URL 本身等）。导致持续 XSS 漏洞的常见错误是仅验证预计网站会重新显示的字段。应用程序服务器或应用程序反射请求中的其他数据很常见，开发团队很难预料到这一点。而且未来的开发人员也可能使用当前没有反射的字段。因此，建议验证 HTTP 请求的所有部分。
请注意，虽然输入验证可以提供一些深度防御，但是正确的输出编码、转义和引用才是防止 XSS 的最有效解决方案。输入验证可有效地限制输出中将显示的内容，却无法一直防止 XSS，特别是要求您支持可能包含任意字符的自由格式文本字段的情况。例如，在聊天应用程序中，心形表情符号 ("<3") 很可能会通过验证步骤，因为其经常使用。但是，该符号无法直接插入网页中，因为其包含需要转义或以其他方式处理的 "<" 字符。在这种情况下，删除 "<" 可能降低 XSS 风险，却会产生不正确的行为，因为不会记录表情符号。这似乎只是一个小小的不便之处，但是在希望表示不等式的数学论坛中会更加重要。

即使您在验证中犯了错（如忘记了验证 100 个输入字段的其中一个），正确的编码仍有可能保护您不受基于注入的攻击。只要不孤立进行，输入验证就仍是一种有用的手段，因为其可以显著减少攻击面，可让您检测一些攻击，并提供正确编码无法处理的其他安全优势。
确保您在应用程序内明确定义的界面中执行输入验证。这将有助于保护应用程序，即使重新使用组件或将组件移到别处也如此。

发现数据库错误模式

有多种减轻威胁的技巧：
[1] 策略：库或框架
使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。
[2] 策略：参数化
如果可用，使用自动实施数据和代码之间的分离的结构化机制。这些机制也许能够提供自动提供相关引用、编码和验证，而不是依赖于开发者在生成输出的每个点提供此能力。

[3] 策略：环境固化
使用完成必要任务所需的最低特权来运行代码。
[4] 策略：输出编码
如果在有风险的情况下仍需要使用动态生成的查询字符串或命令，请对参数正确地加引号并将这些参数中的任何特殊字符转义。

[5] 策略：输入验证假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的白名单。拒绝任何没有严格遵守规范的输入，或者将其转换为遵守规范的内容。不要完全依赖于将恶意或格式错误的输入加入黑名单。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入由于格式严重错误而应直接拒绝。

.Net

SQL 盲注

以下是保护 Web 应用程序免遭 SQL 注入攻击的两种可行方法：
[1] 使用存储过程，而不用动态构建的 SQL 查询字符串。 将参数传递给 SQL Server 存储过程的方式，可防止使用单引号和连字符。

以下是如何在 ASP.NET 中使用存储过程的简单示例：

```
' Visual Basic example
Dim DS As DataSet
Dim MyConnection As SqlConnection
Dim MyCommand As SqlDataAdapter

Dim SelectCommand As String = "select * from users where username = @username"
...
MyCommand.SelectCommand.Parameters.Add(New SqlParameter("@username", SqlDbType.NVarChar, 20))
MyCommand.SelectCommand.Parameters("@username").Value = UserNameField.Value


// C# example
String selectCmd = "select * from Authors where state = @username";
SqlConnection myConnection = new SqlConnection("server=...");
SqlDataAdapter myCommand = new SqlDataAdapter(selectCmd, myConnection);

myCommand.SelectCommand.Parameters.Add(new SqlParameter("@username", SqlDbType.NVarChar, 20));
myCommand.SelectCommand.Parameters["@username"].Value = UserNameField.Value;
```

[2] 您可以使用验证控件，将输入验证添加到“Web 表单”页面。 验证控件提供适用于所有常见类型的标准验证的易用机制 － 例如，测试验证日期是否有效，或验证值是否在范围内 － 以及进行定制编写验证的方法。此外，验证控件还使您能够完整定制向用户显示错误信息的方式。验证控件可搭配“Web 表单”页面的类文件中处理的任何控件使用，其中

包括 HTML 和 Web 服务器控件。
为了确保用户输入仅包含有效值，您可以使用以下其中一种验证控件：

a. “RangeValidator”：检查用户条目（值）是否在指定的上下界限之间。 您可以检查配对数字、字母字符和日期内的范围。

b. “RegularExpressionValidator”：检查条目是否与正则表达式定义的模式相匹配。 此类型的验证使您能够检查可预见的字符序列，如社会保险号码、电子邮件地址、电话号码、邮政编码等中的字符序列。

重要注意事项：验证控件不会阻止用户输入或更改页面处理流程；它们只会设置错误状态，并产生错误消息。程序员的职责是，在执行进一步的应用程序特定操作前，测试代码中控件的状态。
有两种方法可检查用户输入的有效性：
1. 测试常规错误状态：
在您的代码中，测试页面的 IsValid 属性。该属性会将页面上所有验证控件的 IsValid 属性值汇总（使用逻辑 AND）。如果将其中一个验证控件设置为无效，那么页面属性将会返回 false。
2. 测试个别控件的错误状态：
在页面的“验证器”集合中循环，该集合包含对所有验证控件的引用。然后，您就可以检查每个验证控件的 IsValid 属性。

SQL 注入

以下是保护 Web 应用程序免遭 SQL 注入攻击的两种可行方法：
[1] 使用存储过程，而不用动态构建的 SQL 查询字符串。 将参数传递给 SQL Server 存储过程的方式，可防止使用单引号和连字符。

以下是如何在 ASP.NET 中使用存储过程的简单示例：

```
' Visual Basic example
Dim DS As DataSet
Dim MyConnection As SqlConnection
Dim MyCommand As SqlDataAdapter

Dim SelectCommand As String = "select * from users where username = @username"
...
MyCommand.SelectCommand.Parameters.Add(New SqlParameter("@username", SqlDbType.NVarChar, 20))
MyCommand.SelectCommand.Parameters("@username").Value = UserNameField.Value


// C# example
String selectCmd = "select * from Authors where state = @username";
SqlConnection myConnection = new SqlConnection("server=...");
SqlDataAdapter myCommand = new SqlDataAdapter(selectCmd, myConnection);

myCommand.SelectCommand.Parameters.Add(new SqlParameter("@username", SqlDbType.NVarChar, 20));
myCommand.SelectCommand.Parameters["@username"].Value = UserNameField.Value;
```

[2] 您可以使用验证控件，将输入验证添加到“Web 表单”页面。 验证控件提供适用于所有常见类型的标准验证的易用机制 — 例如，测试验证日期是否有效，或验证值是否在范围内 — 以及进行定制编写验证的方法。此外，验证控件还使您能够完整定制向用户显示错误信息的方式。验证控件可搭配“Web 表单”页面的类文件中处理的任何控件使用，其中包括 HTML 和 Web 服务器控件。

为了确保用户输入仅包含有效值，您可以使用以下其中一种验证控件：

a. “RangeValidator”：检查用户条目（值）是否在指定的上下界限之间。 您可以检查配对数字、字母字符和日期内的范围。

b. “RegularExpressionValidator”：检查条目是否与正则表达式定义的模式相匹配。 此类型的验证使您能够检查可预见的字符序列，如社会保险号码、电子邮件地址、电话号码、邮政编码等中的字符序列。

重要注意事项：验证控件不会阻止用户输入或更改页面处理流程；它们只会设置错误状态，并产生错误消息。程序员的职责是，在执行进一步的应用程序特定操作前，测试代码中控件的状态。
有两种方法可检查用户输入的有效性：
1. 测试常规错误状态：
在您的代码中，测试页面的 IsValid 属性。该属性会将页面上所有验证控件的 IsValid 属性值汇总（使用逻辑 AND）。如果将其中一个验证控件设置为无效，那么页面属性将会返回 false。
2. 测试个别控件的错误状态：

在页面的“验证器”集合中循环，该集合包含对所有验证控件的引用。然后，您就可以检查每个验证控件的 IsValid 属性。

跨站点脚本编制

[1] 我们建议您将服务器升级到 .NET Framework 2.0（或更新版本），其中包含防止跨站点脚本编制攻击的固有安全检查。

[2] 您可以使用验证控件将输入验证添加到 Web 表单页面。验证控件可提供一种针对所有常见类型标准验证（例如，一个范围内的有效日期或有效值的测试）的易于使用的方式。验证控件还支持定制书面验证，允许您完全定制如何向用户显示错误信息。验证控件还可与 Web 表单页面类文件中处理的任何控件（包括 HTML 和 Web 服务器控件）配合使用。

为了确保用户输入仅包含有效值，您可以使用以下验证控件之一：

[1] "RangeValidator"：检查用户的输入（值）是否处于指定的上下限之间。您可以检查数字对、字母字符对和日期对限定的范围。

[2] "RegularExpressionValidator"：检查输入是否与正则表达式所定义的模式匹配。这类验证允许您检查可预测字符序列，如社会保险号、电子邮件地址、电话号码、邮政编码等等中的可预测字符序列。

可能帮助阻止跨站点脚本编制的正则表达式的示例：

- 将拒绝基本跨站点脚本编制变量的可能正则表达式可能是：^([^<]|\<[^a-zA-Z])*[<]?$
- 将拒绝所有上述字符的通用正则表达式可能是：^([^\<\>\"\'\%\;\)\(\&\+]*)$

重要事项：验证控件不会阻止用户输入或更改页面处理流；它们仅设置错误状态并产生错误消息。在执行进一步应用程序特定操作之前在代码中测试验证控件的状态是程序员的责任。

检查用户输入有效性的方法有两种：

1. 测试一般错误状态：

在您的代码中，测试页面的 IsValid 属性。此属性（使用逻辑 AND）汇总了页面上所有验证控件的 IsValid 属性值。如果其中一个验证控件设置为无效，则页面的属性将返回假值。

2. 测试个别控件的错误状态：

查看页面的验证程序集合，其中包含所有验证控件的引用。之后您可以检查各个验证控件的 IsValid 属性。

最后，我们建议使用微软反跨站点脚本编制库（v1.5 或更高版本）来编码不可信用户输入。

反跨站点脚本编制库公开了下列方法：

[1] HtmlEncode - 编码在 HTML 中使用的输入字符串

[2] HtmlAttributeEncode - 编码在 HTML 属性中使用的输入字符串

[3] JavaScriptEncode - 编码在 JavaScript 中使用的输入字符串

[4] UrlEncode - 编码在统一资源定位符 (URL) 中使用的输入字符串

[5] VisualBasicScriptEncode - 编码在 Visual Basic 脚本中使用的输入字符串

[6] XmlEncode - 编码在 XML 中使用的输入字符串

[7] XmlAttributeEncode - 编码在 XML 属性中使用的输入字符串

要正确使用微软反跨站点脚本编制库保护 ASP.NET Web 应用程序，您需要：

步骤 1：查看生成输出的 ASP.NET 代码

步骤 2：确定输出是否包括不可信输入参数

步骤 3：确定不可信输入被用作输出的上下文，并确定要使用的编码方法

步骤 4：编码输出

步骤 3 的示例：

注意：如果不可信输入将用于设置 HTML 属性，则应使用 Microsoft.Security.Application.HtmlAttributeEncode 方法编码不可信输入。

或者，如果不可信输入将在 JavaScript 上下文中使用，则应使用 Microsoft.Security.Application.JavaScriptEncode 对其进行编码。

```
  // Vulnerable code
  // Note that untrusted input is being treated as an HTML attribute
  Literal1.Text = "<hr noshade size=[untrusted input here]>";


  // Modified code
  Literal1.Text = "<hr noshade size="+Microsoft.Security.Application.AntiXss.HtmlAttributeEncode([untrusted
input here])+">";
```

步骤 4 的示例：

有关编码输出的一些重要事项：

[1] 输出应编码一次。

[2] 输出编码应尽可能接近输出的实际写入。例如，如果应用程序正在读取用户输入，处理该输入，然后以某种形式写出，则编码应发生在输出写入之前。

```
// Incorrect sequence
protected void Button1_Click(object sender, EventArgs e)
{
    // Read input
    String Input = TextBox1.Text;
    // Encode untrusted input
    Input = Microsoft.Security.Application.AntiXss.HtmlEncode(Input);
    // Process input
    ...
    // Write Output
    Response.Write("The input you gave was"+Input);
}


// Correct Sequence
protected void Button1_Click(object sender, EventArgs e)
{
    // Read input
    String Input = TextBox1.Text;
    // Process input
    ...
    // Encode untrusted input and write output
    Response.Write("The input you gave was"+
        Microsoft.Security.Application.AntiXss.HtmlEncode(Input));
}
```

发现数据库错误模式

以下是保护 Web 应用程序免遭 SQL 注入攻击的两种可行方法：
[1] 使用存储过程，而不用动态构建的 SQL 查询字符串。 将参数传递给 SQL Server 存储过程的方式，可防止使用单引号和连字符。

以下是如何在 ASP.NET 中使用存储过程的简单示例：

```
' Visual Basic example
Dim DS As DataSet
Dim MyConnection As SqlConnection
Dim MyCommand As SqlDataAdapter

Dim SelectCommand As String = "select * from users where username = @username"
...
MyCommand.SelectCommand.Parameters.Add(New SqlParameter("@username", SqlDbType.NVarChar, 20))
MyCommand.SelectCommand.Parameters("@username").Value = UserNameField.Value


// C# example
String selectCmd = "select * from Authors where state = @username";
SqlConnection myConnection = new SqlConnection("server=...");
SqlDataAdapter myCommand = new SqlDataAdapter(selectCmd, myConnection);

myCommand.SelectCommand.Parameters.Add(new SqlParameter("@username", SqlDbType.NVarChar, 20));
myCommand.SelectCommand.Parameters["@username"].Value = UserNameField.Value;
```

[2] 您可以使用验证控件，将输入验证添加到“Web 表单”页面。 验证控件提供适用于所有常见类型的标准验证的易用机制 — 例如，测试验证日期是否有效，或验证值是否在范围内 — 以及进行定制编写验证的方法。此外，验证控件还使您能够完整定制向用户显示错误信息的方式。验证控件可搭配“Web 表单”页面的类文件中处理的任何控件使用，其中包括 HTML 和 Web 服务器控件。
为了确保用户输入仅包含有效值，您可以使用以下其中一种验证控件：

a. “RangeValidator”：检查用户条目（值）是否在指定的上下界限之间。 您可以检查配对数字、字母字符和日期内的范围。
b. “RegularExpressionValidator”：检查条目是否与正则表达式定义的模式相匹配。 此类型的验证使您能够检查可预见的字符序列，如社会保险号码、电子邮件地址、电话号码、邮政编码等中的字符序列。

重要注意事项：验证控件不会阻止用户输入或更改页面处理流程；它们只会设置错误状态，并产生错误消息。程序员的职责是，在执行进一步的应用程序特定操作前，测试代码中控件的状态。

有两种方法可检查用户输入的有效性：

1. 测试常规错误状态：

在您的代码中，测试页面的 IsValid 属性。该属性会将页面上所有验证控件的 IsValid 属性值汇总（使用逻辑 AND）。如果将其中一个验证控件设置为无效，那么页面属性将会返回 false。

2. 测试个别控件的错误状态：

在页面的“验证器”集合中循环，该集合包含对所有验证控件的引用。然后，您就可以检查每个验证控件的 IsValid 属性。

J2EE

SQL 盲注

** 预编译语句：

以下是保护应用程序免遭 SQL 注入（即恶意篡改 SQL 参数）的三种可行方法。 使用以下方法，而非动态构建 SQL 语句：

[1] PreparedStatement，通过预编译并且存储在 PreparedStatement 对象池中。 PreparedStatement 定义 setter 方法，以注册与受支持的 JDBC SQL 数据类型兼容的输入参数。 例如，setString 应该用于 VARCHAR 或 LONGVARCHAR 类型的输入参数（请参阅 Java API，以获取进一步的详细信息）。 通过这种方法来设置输入参数，可防止攻击者通过注入错误字符（如单引号）来操纵 SQL 语句。

如何在 J2EE 中使用 PreparedStatement 的示例：

```
  // J2EE PreparedStatemenet Example
  // Get a connection to the database
  Connection myConnection;
  if (isDataSourceEnabled()) {
      // using the DataSource to get a managed connection
      Context ctx = new InitialContext();
      myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
  } else {
      try {
          // using the DriverManager to get a JDBC connection
          Class.forName(jdbcDriverClassPath);
          myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
      } catch (ClassNotFoundException e) {
          ...
      }
  }
  ...
  try {
      PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username =
?");
      myStatement.setString(1, userNameField);
      ResultSet rs = myStatement.executeQuery();
      ...
      rs.close();
  } catch (SQLException sqlException) {
      ...
  } finally {
      myStatement.close();
      myConnection.close();
  }
```

[2] CallableStatement，扩展 PreparedStatement 以执行数据库 SQL 存储过程。 该类继承 PreparedStatement 的输入 setter 方法（请参阅上面的 [1]）。

以下示例假定已创建该数据库存储过程：

CREATE PROCEDURE select_user (@username varchar(20))AS SELECT * FROM USERS WHERE USERNAME = @username;如何在 J2EE 中使用 CallableStatement 以执行以上存储过程的示例：

```
// J2EE PreparedStatemenet Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassPath);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareCall("{?= call select_user ?,?}");
    myStatement.setString(1, userNameField);
    myStatement.registerOutParameter(1, Types.VARCHAR);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[3] 实体 Bean，代表持久存储机制中的 EJB 业务对象。 实体 Bean 有两种类型：bean 管理和容器管理。 当使用 bean 管理的持久性时，开发者负责撰写访问数据库的 SQL 代码（请参阅以上的 [1] 和 [2] 部分）。 当使用容器管理的持久性时，EJB 容器会自动生成 SQL 代码。 因此，容器要负责防止恶意尝试篡改生成的 SQL 代码。

如何在 J2EE 中使用实体 Bean 的示例：

```
// J2EE EJB Example
try {
    // lookup the User home interface
    UserHome userHome = (UserHome)context.lookup(User.class);
    // find the User remote interface
    User = userHome.findByPrimaryKey(new UserKey(userNameField));
    ...
} catch (Exception e) {
    ...
}
```

推荐使用的 JAVA 工具
不适用

参考资料
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/PreparedStatement.html
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/CallableStatement.html

** 输入数据验证：虽然为方便用户而在客户端层上提供数据验证，但仍必须使用 Servlet 在服务器层上执行数据验证。 客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。

一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] cookie 值[8] HTTP 响应好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。
[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
        isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 Java 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。
验证数字字段（int 类型）的方式的示例：

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
        Integer.parseInt(value);
        isFieldValid = true;
        } catch (Exception e) {
        isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，开发者应将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...
```

应用程序应处理的主要 Java 数据类型：
- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证 userName 字段的长度是否在 8 至 20 个字符之间：

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
        validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
        validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] 字段范围
始终确保输入参数是在由功能需求定义的范围内。
以下示例验证输入 numberOfChoices 是否在 10 至 20 之间：

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
        // numberOfChoices is valid, continue processing request
        ...
```

```
            }
        }
    }
```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
        List list = Arrays.asList(options);
        if (list != null) {
        isValidValue = list.contains(value);
        }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] 字段模式
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]*$

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“Apache 正则表达式包”（请参阅以下“资源”）与 Java 1.3 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        RE r = new RE(expression);
        match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 引进了一种新的正则表达式包 (java.util.regex)。以下是使用新的 Java 1.4 正则表达式包的 Validator.matchPattern 修订版：

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] cookie 值使用 javax.servlet.http.Cookie 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。验证必需 cookie 值的示例：

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue()) {
        // valid cookie value, continue processing request
        ...
        }
        }
    }
}
```

[8] HTTP 响应
[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
        return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
        switch (value.charAt(i)) {
        case '<':
        result.append("&lt;");
        break;
```

```
          case '>':
          result.append("&gt;");
          break;
          case '"':
          result.append("&quot;");
          break;
          case '\'':
          result.append("&#39;");
          break;
          case '%':
          result.append("&#37;");
          break;
          case ';':
          result.append("&#59;");
          break;
          case '(':
          result.append("&#40;");
          break;
          case ')':
          result.append("&#41;");
          break;
          case '&':
          result.append("&amp;");
          break;
          case '+':
          result.append("&#43;");
          break;
          default:
          result.append(value.charAt(i));
          break;
          }
          return result;
      }
      ...
  }
  ...
  // Filter the HTTP response using Validator.filter
  PrintWriter out = response.getWriter();
  // set output response
  out.write(Validator.filter(response));
  out.close();
```

Java Servlet API 2.3 引进了“过滤器”，它支持拦截和转换 HTTP 请求或响应。
以下示例使用 Validator.filter 来用“Servlet 过滤器”清理响应：

```
  // Example to filter all sensitive characters in the HTTP response using a Java Filter.
  // This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
  public class SensitiveCharsFilter implements Filter {
      ...
      public void doFilter(ServletRequest request,
          ServletResponse response,
          FilterChain chain)
          throws IOException, ServletException {

          PrintWriter out = response.getWriter();
          ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
          chain.doFilter(request, wrapper);

          CharArrayWriter caw = new CharArrayWriter();
          caw.write(Validator.filter(wrapper.toString()));

          response.setContentType("text/html");
          response.setContentLength(caw.toString().length());
          out.write(caw.toString());
          out.close();
      }
      ...
      public class CharResponseWrapper extends HttpServletResponseWrapper {
          private CharArrayWriter output;

          public String toString() {
```

```
        return output.toString();
        }

        public CharResponseWrapper(HttpServletResponse response){
        super(response);
        output = new CharArrayWriter();
        }

        public PrintWriter getWriter(){
        return new PrintWriter(output);
        }
    }
}

}
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据时，确保使用 Cookie.setSecure（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。
保护“用户”cookie 的示例：

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。Jakarta Commons Validator 是一种强大的框架，用来实现所有以上数据验证需求。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，Struts 支持在使用 Struts“bean:write”标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“filter=false”标志来禁用该过滤。
Struts 定义以下基本输入验证器，但也可定义定制的验证器：
required：如果字段包含空格以外的任何字符，便告成功。
mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。
range：如果值在 min 和 max 属性给定的值的范围内（(value >= min) & (value <= max)），便告成功。
maxLength：如果字段长度小于或等于 max 属性，便告成功。
minLength：如果字段长度大于或等于 min 属性，便告成功。
byte、short、integer、long、float、double：如果可将值转换为对应的基本类型，便告成功。
date：如果值代表有效日期，便告成功。可能会提供日期模式。
creditCard：如果值可以是有效的信用卡号码，便告成功。
e-mail：如果值可以是有效的电子邮件地址，便告成功。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces 技术
“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和输入验证的 Java API (JSR 127)。
JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器： validate_doublerange：在组件上注册 DoubleRangeValidator
validate_length：在组件上注册 LengthValidator
validate_longrange：在组件上注册 LongRangeValidator
validate_required：在组件上注册 RequiredValidator
validate_stringrange：在组件上注册 StringRangeValidator
validator：在组件上注册定制的 Validator

JavaServer Faces API 定义以下 UIInput 和 UIOutput 处理器（标记）：
input_date：接受以 java.text.Date 实例格式化的 java.util.Date
output_date：显示以 java.text.Date 实例格式化的 java.util.Date
input_datetime：接受以 java.text.DateTime 实例格式化的 java.util.Date
output_datetime：显示以 java.text.DateTime 实例格式化的 java.util.Date
input_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）
output_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）
input_text：接受单行文本字符串。
output_text：显示单行文本字符串。
input_time：接受以 java.text.DateFormat 时间实例格式化的 java.util.Date
output_time：显示以 java.text.DateFormat 时间实例格式化的 java.util.Date
input_hidden：允许页面作者在页面中包括隐藏变量
input_secret：接受不含空格的单行文本，并在输入时，将其显示为一组星号
input_textarea：接受多行文本
output_errors：显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息
output_label：将嵌套的组件显示为指定输入字段的标签
output_message：显示本地化消息

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式包 －
http://jakarta.apache.org/regexp/
Jakarta 验证器 －
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 －
http://java.sun.com/j2ee/javaserverfaces/

** 错误处理：
许多 J2EE Web 应用程序体系结构都遵循"模型视图控制器（MVC）"模式。在该模式中，Servlet 扮演"控制器"的角色。Servlet 将应用程序处理委派给 EJB 会话 Bean（模型）之类的 JavaBean。然后，Servlet 再将请求转发给 JSP（视图），以呈现处理结果。Servlet 应检查所有的输入、输出、返回码、错误代码和已知的异常，以确保实际处理按预期进行。
数据验证可保护应用程序免遭恶意数据篡改，而有效的错误处理策略则是防止应用程序意外泄露内部错误消息（如异常堆栈跟踪）所不可或缺的。好的错误处理策略会处理以下项：
[1] 定义错误
[2] 报告错误
[3] 呈现错误
[4] 错误映射
[1] 定义错误
应避免在应用程序层（如 Servlet）中硬编码错误消息。 相反地，应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥，且该错误密钥映射到 HTML 表单字段或其他 Bean 属性的验证规则。例如，如果需要 "user_name"字段，其内容为字母数字，并且必须在数据库中是唯一的，那么就应定义以下错误密钥：

(a) ERROR_USERNAME_REQUIRED：该错误密钥用于显示消息，以通知用户需要 "user_name" 字段；
(b) ERROR_USERNAME_ALPHANUMERIC：该错误密钥用于显示消息，以通知用户 "user_name" 字段应该是字母数字；
(c) ERROR_USERNAME_DUPLICATE：该错误密钥用于显示消息，以通知用户 "user_name" 值在数据库中重复；
(d) ERROR_USERNAME_INVALID：该错误密钥用于显示一般消息，以通知用户 "user_name" 值无效；

好的做法是定义用于存储和报告应用程序错误的以下框架 Java 类：
- ErrorKeys：定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error：封装个别错误

```
// Example: Error encapsulates an error key.
```

```
        // Error is serializable to support code executing in multiple JVMs.
        public Class Error implements Serializable {

            // Constructor given a specified error key
            public Error(String key) {
            this(key, null);
            }

            // Constructor given a specified error key and array of placeholder objects
            public Error(String key, Object[] values) {
            this.key = key;
            this.values = values;
            }

            // Returns the error key
            public String getKey() {
            return this.key;
            }

            // Returns the placeholder values
            public Object[] getValues() {
            return this.values;
            }

            private String key = null;
            private Object[] values = null;
        }
```

- Errors：封装错误的集合

```
        // Example: Errors encapsulates the Error objects being reported to the presentation layer.
        // Errors are stored in a HashMap where the key is the bean property name and value is an
        // ArrayList of Error objects.
        public Class Errors implements Serializable {

            // Adds an Error object to the Collection of errors for the specified bean property.
            public void addError(String property, Error error) {
            ArrayList propertyErrors = (ArrayList)errors.get(property);
            if (propertyErrors == null) {
            propertyErrors = new ArrayList();
            errors.put(property, propertyErrors);
            }
            propertyErrors.put(error);
            }

            // Returns true if there are any errors
            public boolean hasErrors() {
            return (errors.size > 0);
            }

            // Returns the Errors for the specified property
            public ArrayList getErrors(String property) {
            return (ArrayList)errors.get(property);
            }

            private HashMap errors = new HashMap();
        }
```

以下是使用上述框架类来处理“user_name”字段验证错误的示例：

```
    // Example to process validation errors of the "user_name" field.
    Errors errors = new Errors();
    String userName = request.getParameter("user_name");
    // (a) Required validation rule
```

```
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] 报告错误
有两种方法可报告 web 层应用程序错误：
(a) Servlet 错误机制
(b) JSP 错误机制

[2-a] Servlet 错误机制
Servlet 可通过以下方式报告错误：
- 转发给输入 JSP（已将错误存储在请求属性中），或
- 使用 HTTP 错误代码参数来调用 response.sendError，或
- 抛出异常

好的做法是处理所有已知应用程序错误（如 [1] 部分所述），将这些错误存储在请求属性中，然后转发给输入 JSP。输入 JSP 应显示错误消息，并提示用户重新输入数据。以下示例阐明转发给输入 JSP（userInput.jsp）的方式：

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

如果 Servlet 无法转发给已知的 JSP 页面，那么第二个选项是使用 response.sendError 方法，将 HttpServletResponse.SC_INTERNAL_SERVER_ERROR（状态码 500）作为参数，来报告错误。请参阅 javax.servlet.http.HttpServletResponse 的 Javadoc，以获取有关各种 HTTP 状态码的更多详细信息。返回 HTTP 错误的示例：

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

作为最后的手段，Servlet 可以抛出异常，且该异常必须是以下其中一类的子类：
- RuntimeException
- ServletException
- IOException

[2-b] JSP 错误机制
JSP 页面通过定义 errorPage 伪指令来提供机制，以处理运行时异常，如以下示例所示：

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕获的 JSP 异常被转发给指定的 errorPage，并且原始异常设置在名称为 javax.servlet.jsp.jspException 的请求参数中。错误页面必须包括 isErrorPage 伪指令，如下所示：

```
<%@ page isErrorPage="true" %>
```

isErrorPage 伪指令导致“exception”变量初始化为所抛出的异常对象。
[3] 呈现错误
J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类，其中包括：

(a) 资源束
(b) 消息格式化

[3-a] 资源束
资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。
java.util.PropertyResourceBundle 将内容存储在外部属性文件中，对其进行使用或扩展都很常见，如以下示例所示：

```
################################################
# ErrorMessages.properties
################################################
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可定义多种资源，以支持不同的语言环境（因此名为资源束）。例如，可定义 ErrorMessages_fr.properties 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在，那么会使用缺省成员。在以上示例中，缺省资源是 ErrorMessages.properties。应用程序（JSP 或 Servlet）会根据用户的语言环境从适当的资源检索内容。
[3-b] 消息格式化
J2SE 标准类 java.util.MessageFormat 提供使用替换占位符来创建消息的常规方法。MessageFormat 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
```

```
    String userName = request.getParameter("user_name");
    Object[] args = new Object[1];
    args[0] = userName;
    String message = MessageFormat.format(pattern, args);
```

以下是使用 ResourceBundle 和 MessageFormat 来呈现错误消息的更加全面的示例：

```
    // Example to render an error message from a localized ErrorMessages resource (properties file)
    // Utility class to retrieve locale-specific error messages
    public Class ErrorMessageResource {

        // Returns the error message for the specified error key in the environment locale
        public String getErrorMessage(String errorKey) {
            return getErrorMessage(errorKey, defaultLocale);
        }

        // Returns the error message for the specified error key in the specified locale
        public String getErrorMessage(String errorKey, Locale locale) {
            return getErrorMessage(errorKey, null, locale);
        }

        // Returns a formatted error message for the specified error key in the specified locale
        public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
            // Get localized ErrorMessageResource
            ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
            // Get localized error message
            String errorMessage = errorMessageResource.getString(errorKey);
            if (args != null) {
            // Format the message using the specified placeholders args
            return MessageFormat.format(errorMessage, args);
            } else {
            return errorMessage;
            }
        }

        // default environment locale
        private Locale defaultLocale = Locale.getDefaultLocale();
    }
    ...
    // Get the user's locale
    Locale userLocale = request.getLocale();
    // Check if there were any validation errors
    Errors errors = (Errors)request.getAttribute("errors");
    if (errors != null && errors.hasErrors()) {
        // iterate through errors and output error messages corresponding to the "user_name" property
        ArrayList userNameErrors = errors.getErrors("user_name");
        ListIterator iterator = userNameErrors.iterator();
        while (iterator.hasNext()) {
            // Get the next error object
            Error error = (Error)iterator.next();
            String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
            output.write(errorMessage + "\r\n");
        }
    }
```

建议定义定制 JSP 标记（如 displayErrors），以迭代处理并呈现错误消息，如以上示例所示。
[4] 错误映射
通常情况下，“Servlet 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码或异常与 Web 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 Servlet 容器都会报告内部错误消息）。该映射配置在“Web 部署描述符（web.xml）”中，如以下示例所指定：

```
    <!-- Mapping of HTTP error codes and application exceptions to error pages -->
    <error-page>
      <exception-type>UserValidationException</exception-type>
```

```
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
...
</error-page>
...
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。验证规则配置在 XML 文件中，该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。Struts 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记，如以下示例所示：

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
    <table border="0" width="100%">
    <tr>
        <th align="right">
        <html:errors property="username"/>
        <bean:message key="prompt.username"/>
        </th>
        <td align="left">
        <html:text property="username" size="16"/>
        </td>
    </tr>
    <tr>
    <td align="right">
        <html:submit><bean:message key="button.submit"/></html:submit>
    </td>
    <td align="right">
        <html:reset><bean:message key="button.reset"/></html:reset>
    </td>
    </tr>
    </table>
    </html:form>
</body>
</html:html>
```

[2] JavaServer Faces 技术
“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。
使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式包 –
http://jakarta.apache.org/regexp/
Jakarta 验证器 –
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 –
http://java.sun.com/j2ee/javaserverfaces/

SQL 注入

** 预编译语句：
以下是保护应用程序免遭 SQL 注入（即恶意篡改 SQL 参数）的三种可行方法。 使用以下方法，而非动态构建 SQL 语句：
[1] PreparedStatement，通过预编译并且存储在 PreparedStatement 对象池中。 PreparedStatement 定义 setter 方法，以注册与受支持的 JDBC SQL 数据类型兼容的输入参数。 例如，setString 应该用于 VARCHAR 或 LONGVARCHAR 类型的输入参数（请参阅 Java API，以获取进一步的详细信息）。 通过这种方法来设置输入参数，可防止攻击者通过注入错误字符（如单引号）来操纵 SQL 语句。

如何在 J2EE 中使用 PreparedStatement 的示例：

```
  // J2EE PreparedStatemenet Example
  // Get a connection to the database
  Connection myConnection;
  if (isDataSourceEnabled()) {
      // using the DataSource to get a managed connection
      Context ctx = new InitialContext();
      myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
  } else {
      try {
          // using the DriverManager to get a JDBC connection
          Class.forName(jdbcDriverClassPath);
          myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
      } catch (ClassNotFoundException e) {
          ...
      }
  }
  ...
  try {
      PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username =
?");
      myStatement.setString(1, userNameField);
      ResultSet rs = myStatement.executeQuery();
      ...
      rs.close();
  } catch (SQLException sqlException) {
      ...
  } finally {
      myStatement.close();
      myConnection.close();
  }
```

[2] CallableStatement，扩展 PreparedStatement 以执行数据库 SQL 存储过程。 该类继承 PreparedStatement 的输入 setter 方法（请参阅上面的 [1]）。
以下示例假定已创建该数据库存储过程：
CREATE PROCEDURE select_user (@username varchar(20))AS SELECT * FROM USERS WHERE USERNAME = @username;如何在 J2EE 中使用 CallableStatement 以执行以上存储过程的示例：

```
  // J2EE PreparedStatemenet Example
  // Get a connection to the database
  Connection myConnection;
  if (isDataSourceEnabled()) {
      // using the DataSource to get a managed connection
      Context ctx = new InitialContext();
      myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
  } else {
      try {
          // using the DriverManager to get a JDBC connection
          Class.forName(jdbcDriverClassPath);
          myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
      } catch (ClassNotFoundException e) {
          ...
      }
  }
  ...
  try {
      PreparedStatement myStatement = myConnection.prepareCall("{?= call select_user ?,?}");
      myStatement.setString(1, userNameField);
```

```
    myStatement.registerOutParameter(1, Types.VARCHAR);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[3] 实体 Bean，代表持久存储机制中的 EJB 业务对象。 实体 Bean 有两种类型：bean 管理和容器管理。 当使用 bean 管理的持久性时，开发者负责撰写访问数据库的 SQL 代码（请参阅以上的 [1] 和 [2] 部分）。 当使用容器管理的持久性时，EJB 容器会自动生成 SQL 代码。 因此，容器要负责防止恶意尝试篡改生成的 SQL 代码。

如何在 J2EE 中使用实体 Bean 的示例：

```
// J2EE EJB Example
try {
    // lookup the User home interface
    UserHome userHome = (UserHome)context.lookup(User.class);
    // find the User remote interface
    User = userHome.findByPrimaryKey(new UserKey(userNameField));
    ...
} catch (Exception e) {
    ...
}
```

推荐使用的 JAVA 工具
不适用

参考资料
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/PreparedStatement.html
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/CallableStatement.html

** 输入数据验证：虽然为方便用户而在客户端层上提供数据验证，但仍必须使用 Servlet 在服务器层上执行数据验证。 客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。
一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] cookie 值[8] HTTP 响应好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。
[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
        isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
    }
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 Java 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。
验证数字字段（int 类型）的方式的示例：

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
        Integer.parseInt(value);
        isFieldValid = true;
        } catch (Exception e) {
        isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，开发者应将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...
```

应用程序应处理的主要 Java 数据类型：
- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证

userName 字段的长度是否在 8 至 20 个字符之间：

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
        validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
        validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] 字段范围
始终确保输入参数是在由功能需求定义的范围内。
以下示例验证输入 numberOfChoices 是否在 10 至 20 之间：

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
        // numberOfChoices is valid, continue processing request
        ...
        }
    }
}
```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
        List list = Arrays.asList(options);
        if (list != null) {
        isValidValue = list.contains(value);
        }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] 字段模式
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]*$

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“Apache 正则表达式包”（请参阅以下“资源”）与 Java 1.3 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        RE r = new RE(expression);
        match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 引进了一种新的正则表达式包 (java.util.regex)。以下是使用新的 Java 1.4 正则表达式包的 Validator.matchPattern 修订版：

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] cookie 值使用 javax.servlet.http.Cookie 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。验证必需 cookie 值的示例：

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue()) {
        // valid cookie value, continue processing request
        ...
        }
        }
    }
}
```

[8] HTTP 响应
[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
        return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
        switch (value.charAt(i)) {
        case '<':
        result.append("&lt;");
        break;
        case '>':
        result.append("&gt;");
        break;
        case '"':
        result.append("&quot;");
        break;
        case '\'':
        result.append("&#39;");
        break;
        case '%':
        result.append("&#37;");
        break;
        case ';':
        result.append("&#59;");
        break;
        case '(':
        result.append("&#40;");
        break;
        case ')':
        result.append("&#41;");
        break;
        case '&':
        result.append("&amp;");
        break;
        case '+':
        result.append("&#43;");
```

```
          break;
          default:
          result.append(value.charAt(i));
          break;
          }
          return result;
      }
      ...
  }
  ...
  // Filter the HTTP response using Validator.filter
  PrintWriter out = response.getWriter();
  // set output response
  out.write(Validator.filter(response));
  out.close();
```

Java Servlet API 2.3 引进了“过滤器”，它支持拦截和转换 HTTP 请求或响应。
以下示例使用 Validator.filter 来用“Servlet 过滤器”清理响应：

```
  // Example to filter all sensitive characters in the HTTP response using a Java Filter.
  // This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
  public class SensitiveCharsFilter implements Filter {
      ...
      public void doFilter(ServletRequest request,
          ServletResponse response,
          FilterChain chain)
          throws IOException, ServletException {

          PrintWriter out = response.getWriter();
          ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
          chain.doFilter(request, wrapper);

          CharArrayWriter caw = new CharArrayWriter();
          caw.write(Validator.filter(wrapper.toString()));

          response.setContentType("text/html");
          response.setContentLength(caw.toString().length());
          out.write(caw.toString());
          out.close();
      }
      ...
      public class CharResponseWrapper extends HttpServletResponseWrapper {
          private CharArrayWriter output;

          public String toString() {
          return output.toString();
          }

          public CharResponseWrapper(HttpServletResponse response){
          super(response);
          output = new CharArrayWriter();
          }

          public PrintWriter getWriter(){
          return new PrintWriter(output);
          }
      }
  }

  }
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据时，确保使用 Cookie.setSecure（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。
保护“用户”cookie 的示例：

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。Jakarta Commons Validator 是一种强大的框架，用来实现所有以上数据验证需求。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，Struts 支持在使用 Struts“bean:write”标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“filter=false”标志来禁用该过滤。
Struts 定义以下基本输入验证器，但也可定义定制的验证器：
required：如果字段包含空格以外的任何字符，便告成功。
mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。
range：如果值在 min 和 max 属性给定的值的范围内（(value >= min) & (value <= max)），便告成功。
maxLength：如果字段长度小于或等于 max 属性，便告成功。
minLength：如果字段长度大于或等于 min 属性，便告成功。
byte、short、integer、long、float、double：如果可将值转换为对应的基本类型，便告成功。
date：如果值代表有效日期，便告成功。可能会提供日期模式。
creditCard：如果值可以是有效的信用卡号码，便告成功。
e-mail：如果值可以是有效的电子邮件地址，便告成功。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces 技术
“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和输入验证的 Java API (JSR 127)。
JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器： validate_doublerange：在组件上注册 DoubleRangeValidator

validate_length：在组件上注册 LengthValidator
validate_longrange：在组件上注册 LongRangeValidator
validate_required：在组件上注册 RequiredValidator
validate_stringrange：在组件上注册 StringRangeValidator
validator：在组件上注册定制的 Validator

JavaServer Faces API 定义以下 UIInput 和 UIOutput 处理器（标记）：
input_date：接受以 java.text.Date 实例格式化的 java.util.Date
output_date：显示以 java.text.Date 实例格式化的 java.util.Date
input_datetime：接受以 java.text.DateTime 实例格式化的 java.util.Date
output_datetime：显示以 java.text.DateTime 实例格式化的 java.util.Date
input_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）
output_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）
input_text：接受单行文本字符串。
output_text：显示单行文本字符串。
input_time：接受以 java.text.DateFormat 时间实例格式化的 java.util.Date
output_time：显示以 java.text.DateFormat 时间实例格式化的 java.util.Date
input_hidden：允许页面作者在页面中包括隐藏变量
input_secret：接受不含空格的单行文本，并在输入时，将其显示为一组星号
input_textarea：接受多行文本
output_errors：显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息
output_label：将嵌套的组件显示为指定输入字段的标签
output_message：显示本地化消息

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式包 －
http://jakarta.apache.org/regexp/
Jakarta 验证器 －
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 －
http://java.sun.com/j2ee/javaserverfaces/

** 错误处理：
许多 J2EE Web 应用程序体系结构都遵循“模型视图控制器（MVC）”模式。在该模式中，Servlet 扮演“控制器”的角

色。Servlet 将应用程序处理委派给 EJB 会话 Bean（模型）之类的 JavaBean。然后，Servlet 再将请求转发给 JSP（视图），以呈现处理结果。Servlet 应检查所有的输入、输出、返回码、错误代码和已知的异常，以确保实际处理按预期进行。
数据验证可保护应用程序免遭恶意数据篡改，而有效的错误处理策略则是防止应用程序意外泄露内部错误消息（如异常堆栈跟踪）所不可或缺的。好的错误处理策略会处理以下项：
[1] 定义错误
[2] 报告错误
[3] 呈现错误
[4] 错误映射
[1] 定义错误
应避免在应用程序层（如 Servlet）中硬编码错误消息。 相反地，应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥，且该错误密钥映射到 HTML 表单字段或其他 Bean 属性的验证规则。例如，如果需要 "user_name"字段，其内容为字母数字，并且必须在数据库中是唯一的，那么就应定义以下错误密钥：

(a) ERROR_USERNAME_REQUIRED：该错误密钥用于显示消息，以通知用户需要 "user_name" 字段；
(b) ERROR_USERNAME_ALPHANUMERIC：该错误密钥用于显示消息，以通知用户 "user_name" 字段应该是字母数字；
(c) ERROR_USERNAME_DUPLICATE：该错误密钥用于显示消息，以通知用户 "user_name" 值在数据库中重复；
(d) ERROR_USERNAME_INVALID：该错误密钥用于显示一般消息，以通知用户 "user_name" 值无效；

好的做法是定义用于存储和报告应用程序错误的以下框架 Java 类：
- ErrorKeys：定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error：封装个别错误

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
    this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
    this.key = key;
    this.values = values;
    }

    // Returns the error key
    public String getKey() {
    return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
    return this.values;
    }

    private String key = null;
```

```
        private Object[] values = null;
    }
```

- Errors：封装错误的集合

```
    // Example: Errors encapsulates the Error objects being reported to the presentation layer.
    // Errors are stored in a HashMap where the key is the bean property name and value is an
    // ArrayList of Error objects.
    public Class Errors implements Serializable {

        // Adds an Error object to the Collection of errors for the specified bean property.
        public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
        propertyErrors = new ArrayList();
        errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
        }

        // Returns true if there are any errors
        public boolean hasErrors() {
        return (errors.size > 0);
        }

        // Returns the Errors for the specified property
        public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
        }

        private HashMap errors = new HashMap();
    }
```

以下是使用上述框架类来处理“user_name”字段验证错误的示例：

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] 报告错误
有两种方法可报告 web 层应用程序错误：
(a) Servlet 错误机制
(b) JSP 错误机制

[2-a] Servlet 错误机制
Servlet 可通过以下方式报告错误：
- 转发给输入 JSP（已将错误存储在请求属性中），或
- 使用 HTTP 错误代码参数来调用 response.sendError，或
- 抛出异常

好的做法是处理所有已知应用程序错误（如 [1] 部分所述），将这些错误存储在请求属性中，然后转发给输入 JSP。输入 JSP 应显示错误消息，并提示用户重新输入数据。以下示例阐明转发给输入 JSP（userInput.jsp）的方式：

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

如果 Servlet 无法转发给已知的 JSP 页面，那么第二个选项是使用 response.sendError 方法，将 HttpServletResponse.SC_INTERNAL_SERVER_ERROR（状态码 500）作为参数，来报告错误。请参阅 javax.servlet.http.HttpServletResponse 的 Javadoc，以获取有关各种 HTTP 状态码的更多详细信息。返回 HTTP 错误的示例：

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

作为最后的手段，Servlet 可以抛出异常，且该异常必须是以下其中一类的子类：
- RuntimeException
- ServletException
- IOException

[2-b] JSP 错误机制
JSP 页面通过定义 errorPage 伪指令来提供机制，以处理运行时异常，如以下示例所示：

```
    <%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕获的 JSP 异常被转发给指定的 errorPage，并且原始异常设置在名称为 javax.servlet.jsp.jspException 的请求参数中。错误页面必须包括 isErrorPage 伪指令，如下所示：

```
    <%@ page isErrorPage="true" %>
```

isErrorPage 伪指令导致“exception”变量初始化为所抛出的异常对象。
[3] 呈现错误
J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类，其中包括：

(a) 资源束
(b) 消息格式化

[3-a] 资源束
资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。
java.util.PropertyResourceBundle 将内容存储在外部属性文件中，对其进行使用或扩展都很常见，如以下示例所示：

```
################################################
# ErrorMessages.properties
################################################
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可定义多种资源，以支持不同的语言环境（因此名为资源束）。例如，可定义 ErrorMessages_fr.properties 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在，那么会使用缺省成员。在以上示例中，缺省资源是 ErrorMessages.properties。应用程序（JSP 或 Servlet）会根据用户的语言环境从适当的资源检索内容。
[3-b] 消息格式化
J2SE 标准类 java.util.MessageFormat 提供使用替换占位符来创建消息的常规方法。MessageFormat 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

以下是使用 ResourceBundle 和 MessageFormat 来呈现错误消息的更加全面的示例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
        // Format the message using the specified placeholders args
        return MessageFormat.format(errorMessage, args);
        } else {
        return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}
...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
```

建议定义定制 JSP 标记（如 displayErrors），以迭代处理并呈现错误消息，如以上示例所示。
[4] 错误映射
通常情况下，“Servlet 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码或异常与 Web 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 Servlet 容器都会报告内部错误消息）。该映射配置在“Web 部署描述符（web.xml）”中，如以下示例所指定：

```
<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
  <exception-type>UserValidationException</exception-type>
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
...
</error-page>
...
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。验证规则配置在 XML 文件中，该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。Struts 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记，如以下示例所示：

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
    <table border="0" width="100%">
    <tr>
        <th align="right">
        <html:errors property="username"/>
        <bean:message key="prompt.username"/>
        </th>
        <td align="left">
        <html:text property="username" size="16"/>
        </td>
    </tr>
    <tr>
    <td align="right">
        <html:submit><bean:message key="button.submit"/></html:submit>
    </td>
    <td align="right">
        <html:reset><bean:message key="button.reset"/></html:reset>
    </td>
    </tr>
    </table>
    </html:form>
</body>
</html:html>
```

[2] JavaServer Faces 技术

“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。
使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式包 －
http://jakarta.apache.org/regexp/
Jakarta 验证器 －
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 －
http://java.sun.com/j2ee/javaserverfaces/

跨站点脚本编制

**输入数据验证：
虽然为了用户便利可以在“客户机”层数据上提供数据验证，但是验证必须使用 Servlet 在服务器层上执行。客户机端验证本身不安全，因为很容易就能绕过这些验证，例如通过禁用 Javascript。
良好设计通常要求 Web 应用程序框架提供服务器端实用程序例程来验证下列各项：
[1] 必填字段
[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是字符串）
[3] 字段长度
[4] 字段范围
[5] 字段选项
[6] 字段模式
[7] Cookie 值
[8] HTTP 响应
良好实践是在“验证程序”实用程序类中作为静态方法实施上述例程。以下部分介绍一个示例验证程序类。
[1] 必填字段
始终确保字段不为空且其长度大于零，不包括前导空格和尾随空格。
如何验证必填字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
        isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] 字段数据类型
在 Web 应用程序中，输入参数的类型不佳。例如，所有 HTTP 请求参数或 cookie 值都是字符串类型。开发人员负责验证输入是否是正确数据类型。使用 Java 原始封装类检查字段值是否可以安全地转换为所需原始数据类型。
如何验证数字字段（类型 int）的示例：

```
    // Java example to validate that a field is an int number
    public Class Validator {
        ...
        public static boolean validateInt(String value) {
            boolean isFieldValid = false;
            try {
            Integer.parseInt(value);
            isFieldValid = true;
            } catch (Exception e) {
            isFieldValid = false;
            }
            return isFieldValid;
        }
        ...
    }
    ...
    // check if the HTTP request parameter is of type int
    String fieldValue = request.getParameter("fieldName");
    if (Validator.validateInt(fieldValue)) {
        // fieldValue is valid, continue processing request
        ...
    }
```

良好实践是将所有 HTTP 请求参数转换为其各自的数据类型。例如，开发人员应在请求属性中存储请求参数的“integerValue”，并如以下示例所示使用它：

```
    // Example to convert the HTTP request parameter to a primitive wrapper data type
    // and store this value in a request attribute for further processing
    String fieldValue = request.getParameter("fieldName");
    if (Validator.validateInt(fieldValue)) {
        // convert fieldValue to an Integer
        Integer integerValue = Integer.getInteger(fieldValue);
        // store integerValue in a request attribute
        request.setAttribute("fieldName", integerValue);
    }
    ...
    // Use the request attribute for further processing
    Integer integerValue = (Integer)request.getAttribute("fieldName");
    ...
```

应用程序应处理的主要 Java 数据类型：

- 字节
- 短
- 整数
- 长
- 浮动
- 双字节
- 日期

[3] 字段长度
始终确保输入参数（HTTP 请求参数或 cookie 值）受最小长度和/或最大长度限制。
验证 userName 字段长度是否在 8 到 20 个字符之间的示例：

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
        validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
        validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] 字段范围
始终确保输入参数在功能要求定义的范围之内。
验证输入 numberOfChoices 是否在 10 到 20 之间的示例：

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
        // numberOfChoices is valid, continue processing request
        ...
        }
    }
}
```

[5] 字段选项
通常，Web 应用程序会向用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但是未能执行服务器端验证，以确保所选值是允许选项之一。请记住，恶意用户可以轻松修改任何选项值。始终根据功能要求定义的允许选项验证所选用户值。
根据允许选项列表验证用户选择的示例：

```
    // Example to validate user selection against a list of options
    public Class Validator {
        ...
        public static boolean validateOption(Object[] options, Object value) {
            boolean isValidValue = false;
            try {
            List list = Arrays.asList(options);
            if (list != null) {
            isValidValue = list.contains(value);
            }
            } catch (Exception e) {
            }
            return isValidValue;
        }
        ...
    }
    ...
    // Allowed options
    String[] options = {"option1", "option2", "option3");
    // Verify that the user selection is one of the allowed options
    String userSelection = request.getParameter("userSelection");
    if (Validator.validateOption(options, userSelection)) {
        // valid user selection, continue processing request
        ...
    }
```

[6] 字段模式
始终检查用户输入是否匹配功能要求定义的模式。例如，如果 userName 字段仅应允许字母数字字符，不区分大小写，则使用以下正则表达式：
^[a-zA-Z0-9]*$
Java 1.3 或更低版本不包括任何正则表达式程序包。建议将 Apache 正则表达式程序包（参阅下面的资源）与 Java 1.3 一起使用，解决这种缺乏支持问题。执行正则表达式验证的示例：

```
    // Example to validate that a given value matches a specified pattern
    // using the Apache regular expression package
    import org.apache.regexp.RE;
    import org.apache.regexp.RESyntaxException;
    public Class Validator {
        ...
        public static boolean matchPattern(String value, String expression) {
            boolean match = false;
            if (validateRequired(expression)) {
            RE r = new RE(expression);
            match = r.match(value);
            }
            return match;
        }
        ...
    }
    ...
    // Verify that the userName request parameter is alphanumeric
    String userName = request.getParameter("userName");
    if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
        // userName is valid, continue processing request
        ...
    }
```

Java 1.4 引入了一个新的正则表达式程序包 (java.util.regex)。下面是使用新的 Java 1.4 正则表达式程序包的 Validator.matchPattern 修改版本：

```
    // Example to validate that a given value matches a specified pattern
    // using the Java 1.4 regular expression package
    import java.util.regex.Pattern;
    import java.util.regexe.Matcher;
    public Class Validator {
        ...
        public static boolean matchPattern(String value, String expression) {
            boolean match = false;
            if (validateRequired(expression)) {
            match = Pattern.matches(expression, value);
            }
            return match;
        }
        ...
    }
```

[7] Cookie 值
使用 javax.servlet.http.Cookie 对象验证 cookie 值。将（上述）相同的验证规则应用于 cookie 值，具体取决于应用程序要求（验证必需值、验证长度等）。
验证必需 cookie 值的示例：

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue()) {
        // valid cookie value, continue processing request
        ...
        }
        }
    }
}
```

[8] HTTP 响应
[8-1] 过滤用户输入
为了保护应用程序不受跨站点脚本编制攻击，请将敏感字符转换为其相应的字符实体，清理 HTML。以下这些是 HTML 敏感字符：
< > " ' % ;) (& +
通过将敏感字符转换为其相应的字符实体从而过滤指定字符串的示例：

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
        return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
        switch (value.charAt(i)) {
        case '<':
        result.append("&lt;");
        break;
        case '>':
        result.append("&gt;");
        break;
        case '"':
        result.append("&quot;");
        break;
        case '\'':
        result.append("&#39;");
        break;
        case '%':
        result.append("&#37;");
        break;
        case ';':
        result.append("&#59;");
        break;
```

```
          case '(':
          result.append("&#40;");
          break;
          case ')':
          result.append("&#41;");
          break;
          case '&':
          result.append("&amp;");
          break;
          case '+':
          result.append("&#43;");
          break;
          default:
          result.append(value.charAt(i));
          break;
          }
          return result;
      }
      ...
  }
  ...
  // Filter the HTTP response using Validator.filter
  PrintWriter out = response.getWriter();
  // set output response
  out.write(Validator.filter(response));
  out.close();
```

Java Servlet API 2.3 引入了过滤器，支持 HTTP 请求或响应的截取和转换。
使用 Servlet 过滤器清理使用 Validator.filter 的响应的示例：

```
  // Example to filter all sensitive characters in the HTTP response using a Java Filter.
  // This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
  public class SensitiveCharsFilter implements Filter {
      ...
      public void doFilter(ServletRequest request,
          ServletResponse response,
          FilterChain chain)
          throws IOException, ServletException {

          PrintWriter out = response.getWriter();
          ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
          chain.doFilter(request, wrapper);

          CharArrayWriter caw = new CharArrayWriter();
          caw.write(Validator.filter(wrapper.toString()));

          response.setContentType("text/html");
          response.setContentLength(caw.toString().length());
          out.write(caw.toString());
          out.close();
      }
      ...
      public class CharResponseWrapper extends HttpServletResponseWrapper {
          private CharArrayWriter output;

          public String toString() {
          return output.toString();
          }

          public CharResponseWrapper(HttpServletResponse response){
          super(response);
          output = new CharArrayWriter();
          }

          public PrintWriter getWriter(){
          return new PrintWriter(output);
          }
      }
  }

  }
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据时，确保在 HTTP 响应中设置 cookie 的安全标志，使用 Cookie.setSecure(boolean flag) 指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。
保护“用户”cookie 的示例：

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

建议的 Java 工具
适用于服务器端验证的两个主要 Java 框架：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）
Jakarta Commons Validator 是一种功能强大的框架，可实施所有上述数据验证要求。在定义表单字段输入验证规则的 XML 文件中配置这些规则。缺省情况下，针对使用 Struts‘bean:write’标记写入的所有数据，Struts 支持 [8] HTTP 响应中的危险字符输出过滤。这种过滤功能可通过设置‘filter=false’标志禁用。
Struts 可定义以下基本输入验证程序，但也可能定义定制验证程序：
required：如果字段包含空格之外的任何字符，则成功。
mask：如果值与掩码属性给定的正则表达式匹配，则成功。
range：如果值在 min 属性和 max 属性给定的值（（值 >= min）和（值 <= max））的范围之内，则成功。
maxLength：如果字段长度小于或等于 max 属性，则成功。
minLength：如果字段长度大于或等于 min 属性，则成功。
byte、short、integer、long、float、double：如果值可以转换为相应的原始数据，则成功。
date：如果值显示一个有效日期，则成功。可以提供日期模式。
creditCard：如果值可能是有效的信用卡号，则成功。
e-mail：如果值可能是有效的电子邮件地址，则成功。
使用 Struts 验证程序验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces 技术
JavaServer Faces 技术是一组 Java API (JSR 127)，可显示 UI 组件、管理 UI 组件的状态、处理事件并验证输入。
JavaServer Faces API 可实施以下基本验证程序，但也可定义定制验证程序：
validate_doublerange：在组件上注册 DoubleRangeValidator。
validate_length：在组件上注册 LengthValidator。
validate_longrange：在组件上注册 LongRangeValidator。
validate_required：在组件上注册 RequiredValidator。
validate_stringrange：在组件上注册 StringRangeValidator。
validator：在组件上注册定制验证程序。
JavaServer Faces API 可定义以下 UIInput 和 UIOutput Renderer（标记）：
input_date：接受 java.text.Date 实例格式化的 java.util.Date。
output_date：显示 java.text.Date 实例格式化的 java.util.Date。
input_datetime：接受 java.text.DateTime 实例格式化的 java.util.Date。
output_datetime：显示 java.text.DateTime 实例格式化的 java.util.Date。
input_number：显示 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或原始）。
output_number：显示 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或原始）。
input_text：接受一行文本字符串。
output_text：显示一行文本字符串。
input_time：接受 java.text.DateFormat 时间实例格式化的 java.util.Date。
output_time：显示 java.text.DateFormat 时间实例格式化的 java.util.Date。
input_hidden：允许页面作者在页面中包含隐藏变量。
input_secret：接受一行没有空格的文本，文本输入时显示为一组星号。
input_textarea：接受多行文本。
output_errors：显示整个页面的错误消息，或者显示与指定客户机标识相关的错误消息。
output_label：将嵌套组件显示为指定输入字段的标签。
output_message：显示本地化消息。
使用 JavaServer Faces 技术验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式程序包 -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 -
http://java.sun.com/j2ee/javaserverfaces/
**处理时出错：
许多 J2EE Web 应用程序架构遵循模型-视图-控制器 (MVC) 模式。在此模式中，Servlet 充当控制器。Servlet 将应用

程序处理委派给 JavaBean，如 EJB Session Bean（模型）。然后 Servlet 将请求转发到 JSP（视图）呈现处理结果。Servlet 应检查所有输入、输出、返回代码、错误代码和已知异常，以确保预期处理实际发生。

虽然数据验证会防止应用程序发生恶意数据篡改，但还是需要有健全的错误处理策略来防止应用程序意外披露内部错误消息，如异常堆栈跟踪。良好的错误处理策略可解决以下各项事宜：

[1] 定义错误
[2] 报告错误
[3] 呈现错误
[4] 错误映射
[1] 定义错误

应避免应用层中的硬编码错误消息（如 Servlet）。应用程序应使用映射到已知应用程序失败的错误密钥。良好实践是定义映射到 HTML 表单字段或其他 bean 属性的验证规则的错误密钥。例如，如果“user_name”字段是必填的字母数字字段，且必须在数据库中具有唯一性，则应定义以下错误密钥：

(a) ERROR_USERNAME_REQUIRED：此错误密钥用于显示一条通知用户“user_name”字段是必填字段的消息；
(b) ERROR_USERNAME_ALPHANUMERIC：此错误密钥用于显示一条通知用户“user_name”字段应是字母数字字段的消息；
(c) ERROR_USERNAME_DUPLICATE：此错误密钥用于显示一条通知用户“user_name”值在数据库中是重复值的消息；
(d) ERROR_USERNAME_INVALID：此错误密钥用于显示一条通知用户“user_name”值无效的通用消息；

良好实践是定义用于存储和报告应用程序错误的以下框架 Java 类：

- ErrorKeys：定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error：封装单个错误

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
    this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
    this.key = key;
    this.values = values;
    }

    // Returns the error key
    public String getKey() {
    return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
    return this.values;
    }

    private String key = null;
    private Object[] values = null;
}
```

- Errors：封装错误集合

```
// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public Class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
    public void addError(String property, Error error) {
    ArrayList propertyErrors = (ArrayList)errors.get(property);
    if (propertyErrors == null) {
    propertyErrors = new ArrayList();
    errors.put(property, propertyErrors);
    }
    propertyErrors.put(error);
    }

    // Returns true if there are any errors
    public boolean hasErrors() {
    return (errors.size > 0);
    }

    // Returns the Errors for the specified property
    public ArrayList getErrors(String property) {
    return (ArrayList)errors.get(property);
    }

    private HashMap errors = new HashMap();
}
```

下面是一个使用上述框架类处理“user_name”字段的验证错误的示例：

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] 报告错误
有两种报告 Web 层应用程序错误的方法：
(a) Servlet 错误机制

(b) JSP 错误机制
[2-a] Servlet 错误机制
Servlet 可能通过以下方式报告错误：
- 转发到输入 JSP（已在请求属性中存储错误），或
- 使用一个 HTTP 错误代码参数调用 response.sendError，或
- 抛出异常
良好实践是处理所有已知应用程序错误（如部分 [1] 中所述），将这些错误存储在请求属性中，然后转发到输入 JSP。输入 JSP 应显示错误消息，并提示用户重新输入数据。以下示例说明了如何转发到输入 JSP (userInput.jsp)：

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

如果 Servlet 无法转发到已知 JSP 页面，则第二个选项是使用 response.sendError 方法报告错误，该方法使用 HttpServletResponse.SC_INTERNAL_SERVER_ERROR（状态代码 500）作为参数。请参阅 javax.servlet.http.HttpServletResponse 的 javadoc，了解有关不同 HTTP 状态代码的更多详细信息。
返回 HTTP 错误的示例：

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

作为最后手段，Servlet 可以抛出异常，该异常必须是以下其中一个类的子类：
- RuntimeException
- ServletException
- IOException
[2-b] JSP 错误机制
JSP 页面提供一种通过定义 errorPage 指令处理运行时异常的机制，如以下示例所示：

```
    <%@ page errorPage="/errors/userValidation.jsp" %>
```

将未捕获 JSP 异常转发到指定 errorPage，并在称为 javax.servlet.jsp.jspException 的请求参数中设置原始异常。错误页面必须包括 isErrorPage 指令：

```
    <%@ page isErrorPage="true" %>
```

isErrorPage 指令导致“exception”变量初始化为要抛出的异常对象。
[3] 呈现错误
J2SE 国际化 API 可提供用于外部化应用程序资源和格式化消息的实用程序类，包括：
(a) 资源包
(b) 消息格式化
[3-a] 资源包
资源包通过将本地化数据与使用这些数据的源代码分开来支持国际化。每个资源包都存储一个特定语言环境的密钥/值对的映射。
使用或扩展在外部属性文件中存储内容的 java.util.PropertyResourceBundle 很常见，如以下示例所示：

```
################################################
# ErrorMessages.properties
################################################
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可以定义多个资源来支持不同的语言环境（因此命名资源包）。例如，可以定义 ErrorMessages_fr.properties 来支持资源包家族的法语成员。如果所请求语言环境的资源成员不存在，则使用缺省成员。在上述示例中，缺省资源是 ErrorMessages.properties。应用程序（JSP 或 Servlet）可根据用户的语言环境从相应资源中检索内容。

[3-b] 消息格式化

J2SE 标准类 java.util.MessageFormat 可提供一种使用替换占位符创建消息的通用方法。MessageFormat 对象中包含一个带嵌入式格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

下面是一个使用 ResourceBundle 和 MessageFormat 呈现错误消息的更全面的示例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
        // Format the message using the specified placeholders args
        return MessageFormat.format(errorMessage, args);
        } else {
        return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}
...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
```

```
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
```

建议定义一个定制 JSP 标记（如 displayErrors），重复并呈现错误消息，如上述示例所示。
[4] 错误映射
通常，Servlet 容器将返回一个对应响应状态代码或异常的缺省错误页面。可以使用定制错误页面指定状态代码或异常与 Web 资源之间的映射。良好实践是开发不披露内部错误或状态的静态错误页面（缺省情况下，大多数 Servlet 容器都将报告内部错误消息）。此映射在 Web 部署描述符 (web.xml) 中配置，如以下示例所示：

```
<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
  <exception-type>UserValidationException</exception-type>
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
...
</error-page>
...
```

建议的 Java 工具
适用于服务器端验证的两个主要 Java 框架：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）
Jakarta Commons Validator 是一种 Java 框架，可如上所述定义错误处理机制。在可为表单字段和相应验证错误密钥定义输入验证规则的 XML 文件中配置验证规则。Struts 提供国际化支持，以使用资源包和消息格式化构建本地化应用程序。
使用 Struts 验证程序验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

Struts JSP 标记库定义可有条件地显示一组累积错误消息的“errors”标记，如以下示例所示：

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
    <table border="0" width="100%">
    <tr>
        <th align="right">
        <html:errors property="username"/>
        <bean:message key="prompt.username"/>
        </th>
        <td align="left">
        <html:text property="username" size="16"/>
        </td>
    </tr>
    <tr>
    <td align="right">
        <html:submit><bean:message key="button.submit"/></html:submit>
    </td>
    <td align="right">
        <html:reset><bean:message key="button.reset"/></html:reset>
    </td>
    </tr>
    </table>
    </html:form>
</body>
</html:html>
```

[2] JavaServer Faces 技术
JavaServer Faces 技术是一组 Java API (JSR 127)，可显示 UI 组件、管理 UI 组件的状态、处理事件、验证输入并支持国际化。
JavaServer Faces API 可定义“output_errors”UIOutput Renderer，显示整个页面的错误消息，或者显示与指定客户机标识相关的错误消息。
使用 JavaServer Faces 技术验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式程序包 -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 -
http://java.sun.com/j2ee/javaserverfaces/

发现数据库错误模式

** 预编译语句：
以下是保护应用程序免遭 SQL 注入（即恶意篡改 SQL 参数）的三种可行方法。 使用以下方法，而非动态构建 SQL 语句：
[1] PreparedStatement，通过预编译并且存储在 PreparedStatement 对象池中。 PreparedStatement 定义 setter 方法，以注册与受支持的 JDBC SQL 数据类型兼容的输入参数。 例如，setString 应该用于 VARCHAR 或 LONGVARCHAR 类型的输入参数（请参阅 Java API，以获取进一步的详细信息）。 通过这种方法来设置输入参数，可防止攻击者通过注入错误字符（如单引号）来操纵 SQL 语句。

如何在 J2EE 中使用 PreparedStatement 的示例：

```
  // J2EE PreparedStatemenet Example
  // Get a connection to the database
  Connection myConnection;
  if (isDataSourceEnabled()) {
      // using the DataSource to get a managed connection
      Context ctx = new InitialContext();
      myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
  } else {
      try {
          // using the DriverManager to get a JDBC connection
          Class.forName(jdbcDriverClassPath);
          myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
      } catch (ClassNotFoundException e) {
          ...
      }
  }
  ...
  try {
      PreparedStatement myStatement = myConnection.prepareStatement("select * from users where username =
?");
      myStatement.setString(1, userNameField);
      ResultSet rs = myStatement.executeQuery();
      ...
      rs.close();
  } catch (SQLException sqlException) {
      ...
  } finally {
      myStatement.close();
      myConnection.close();
  }
```

[2] CallableStatement，扩展 PreparedStatement 以执行数据库 SQL 存储过程。 该类继承 PreparedStatement 的输入 setter 方法（请参阅上面的 [1]）。
以下示例假定已创建该数据库存储过程：
CREATE PROCEDURE select_user (@username varchar(20))AS SELECT * FROM USERS WHERE USERNAME = @username;如何在 J2EE 中使用 CallableStatement 以执行以上存储过程的示例：

```
// J2EE PreparedStatemenet Example
// Get a connection to the database
Connection myConnection;
if (isDataSourceEnabled()) {
    // using the DataSource to get a managed connection
    Context ctx = new InitialContext();
    myConnection = ((DataSource)ctx.lookup(datasourceName)).getConnection(dbUserName, dbPassword);
} else {
    try {
        // using the DriverManager to get a JDBC connection
        Class.forName(jdbcDriverClassPath);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareCall("{?= call select_user ?,?}");
    myStatement.setString(1, userNameField);
    myStatement.registerOutParameter(1, Types.VARCHAR);
    ResultSet rs = myStatement.executeQuery();
    ...
    rs.close();
} catch (SQLException sqlException) {
    ...
} finally {
    myStatement.close();
    myConnection.close();
}
```

[3] 实体 Bean，代表持久存储机制中的 EJB 业务对象。 实体 Bean 有两种类型：bean 管理和容器管理。 当使用 bean 管理的持久性时，开发者负责撰写访问数据库的 SQL 代码（请参阅以上的 [1] 和 [2] 部分）。 当使用容器管理的持久性时，EJB 容器会自动生成 SQL 代码。 因此，容器要负责防止恶意尝试篡改生成的 SQL 代码。

如何在 J2EE 中使用实体 Bean 的示例：

```
// J2EE EJB Example
try {
    // lookup the User home interface
    UserHome userHome = (UserHome)context.lookup(User.class);
    // find the User remote interface
    User = userHome.findByPrimaryKey(new UserKey(userNameField));
    ...
} catch (Exception e) {
    ...
}
```

推荐使用的 JAVA 工具
不适用

参考资料
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/PreparedStatement.html
http://java.sun.com/j2se/1.4.1/docs/api/java/sql/CallableStatement.html

** 输入数据验证：

虽然为方便用户而在客户端层上提供数据验证，但仍必须使用 Servlet 在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。

一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] cookie 值[8] HTTP 响应好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。

[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
        isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 Java 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。

验证数字字段（int 类型）的方式的示例：

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
        Integer.parseInt(value);
        isFieldValid = true;
        } catch (Exception e) {
        isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，开发者应将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
```

```
        // store integerValue in a request attribute
        request.setAttribute("fieldName", integerValue);
    }
    ...
    // Use the request attribute for further processing
    Integer integerValue = (Integer)request.getAttribute("fieldName");
    ...
```

应用程序应处理的主要 Java 数据类型：
- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证 userName 字段的长度是否在 8 至 20 个字符之间：

```
    // Example to validate the field length
    public Class Validator {
        ...
        public static boolean validateLength(String value, int minLength, int maxLength) {
            String validatedValue = value;
            if (!validateRequired(value)) {
            validatedValue = "";
            }
            return (validatedValue.length() >= minLength &&
            validatedValue.length() <= maxLength);
        }
        ...
    }
    ...
    String userName = request.getParameter("userName");
    if (Validator.validateRequired(userName)) {
        if (Validator.validateLength(userName, 8, 20)) {
            // userName is valid, continue further processing
            ...
        }
    }
```

[4] 字段范围
始终确保输入参数是在由功能需求定义的范围内。
以下示例验证输入 numberOfChoices 是否在 10 至 20 之间：

```
    // Example to validate the field range
    public Class Validator {
        ...
        public static boolean validateRange(int value, int min, int max) {
            return (value >= min && value <= max);
        }
        ...
    }
    ...
    String fieldValue = request.getParameter("numberOfChoices");
    if (Validator.validateRequired(fieldValue)) {
        if (Validator.validateInt(fieldValue)) {
            int numberOfChoices = Integer.parseInt(fieldValue);
            if (Validator.validateRange(numberOfChoices, 10, 20)) {
            // numberOfChoices is valid, continue processing request
            ...
        }
    }
}
```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
        List list = Arrays.asList(options);
        if (list != null) {
        isValidValue = list.contains(value);
        }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] 字段模式
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]*$

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“Apache 正则表达式包”（请参阅以下“资源”）与 Java 1.3 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        RE r = new RE(expression);
        match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 引进了一种新的正则表达式包 (java.util.regex)。以下是使用新的 Java 1.4 正则表达式包的 Validator.matchPattern 修订版：

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] cookie 值使用 javax.servlet.http.Cookie 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。验证必需 cookie 值的示例：

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue()) {
        // valid cookie value, continue processing request
        ...
        }
        }
    }
}
```

[8] HTTP 响应
[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
        return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
        switch (value.charAt(i)) {
        case '<':
        result.append("&lt;");
        break;
```

```
          case '>':
          result.append("&gt;");
          break;
          case '"':
          result.append("&quot;");
          break;
          case '\'':
          result.append("&#39;");
          break;
          case '%':
          result.append("&#37;");
          break;
          case ';':
          result.append("&#59;");
          break;
          case '(':
          result.append("&#40;");
          break;
          case ')':
          result.append("&#41;");
          break;
          case '&':
          result.append("&amp;");
          break;
          case '+':
          result.append("&#43;");
          break;
          default:
          result.append(value.charAt(i));
          break;
          }
          return result;
      }
      ...
  }
  ...
  // Filter the HTTP response using Validator.filter
  PrintWriter out = response.getWriter();
  // set output response
  out.write(Validator.filter(response));
  out.close();
```

Java Servlet API 2.3 引进了“过滤器”，它支持拦截和转换 HTTP 请求或响应。
以下示例使用 Validator.filter 来用“Servlet 过滤器”清理响应：

```
  // Example to filter all sensitive characters in the HTTP response using a Java Filter.
  // This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
  public class SensitiveCharsFilter implements Filter {
      ...
      public void doFilter(ServletRequest request,
          ServletResponse response,
          FilterChain chain)
          throws IOException, ServletException {

          PrintWriter out = response.getWriter();
          ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
          chain.doFilter(request, wrapper);

          CharArrayWriter caw = new CharArrayWriter();
          caw.write(Validator.filter(wrapper.toString()));

          response.setContentType("text/html");
          response.setContentLength(caw.toString().length());
          out.write(caw.toString());
          out.close();
      }
      ...
      public class CharResponseWrapper extends HttpServletResponseWrapper {
          private CharArrayWriter output;

          public String toString() {
```

```
        return output.toString();
        }

        public CharResponseWrapper(HttpServletResponse response){
        super(response);
        output = new CharArrayWriter();
        }

        public PrintWriter getWriter(){
        return new PrintWriter(output);
        }
    }
}

}
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据时，确保使用 Cookie.setSecure（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。
保护“用户”cookie 的示例：

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。Jakarta Commons Validator 是一种强大的框架，用来实现所有以上数据验证需求。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，Struts 支持在使用 Struts“bean:write”标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“filter=false”标志来禁用该过滤。
Struts 定义以下基本输入验证器，但也可定义定制的验证器：
required：如果字段包含空格以外的任何字符，便告成功。
mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。
range：如果值在 min 和 max 属性给定的值的范围内（(value >= min) & (value <= max)），便告成功。
maxLength：如果字段长度小于或等于 max 属性，便告成功。
minLength：如果字段长度大于或等于 min 属性，便告成功。
byte、short、integer、long、float、double：如果可将值转换为对应的基本类型，便告成功。
date：如果值代表有效日期，便告成功。可能会提供日期模式。
creditCard：如果值可以是有效的信用卡号码，便告成功。
e-mail：如果值可以是有效的电子邮件地址，便告成功。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces 技术
“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和输入验证的 Java API (JSR 127)。
JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器： validate_doublerange：在组件上注册 DoubleRangeValidator
validate_length：在组件上注册 LengthValidator
validate_longrange：在组件上注册 LongRangeValidator
validate_required：在组件上注册 RequiredValidator
validate_stringrange：在组件上注册 StringRangeValidator
validator：在组件上注册定制的 Validator

JavaServer Faces API 定义以下 UIInput 和 UIOutput 处理器（标记）：
input_date：接受以 java.text.Date 实例格式化的 java.util.Date
output_date：显示以 java.text.Date 实例格式化的 java.util.Date
input_datetime：接受以 java.text.DateTime 实例格式化的 java.util.Date
output_datetime：显示以 java.text.DateTime 实例格式化的 java.util.Date
input_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）
output_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）
input_text：接受单行文本字符串。
output_text：显示单行文本字符串。
input_time：接受以 java.text.DateFormat 时间实例格式化的 java.util.Date
output_time：显示以 java.text.DateFormat 时间实例格式化的 java.util.Date
input_hidden：允许页面作者在页面中包括隐藏变量
input_secret：接受不含空格的单行文本，并在输入时，将其显示为一组星号
input_textarea：接受多行文本
output_errors：显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息
output_label：将嵌套的组件显示为指定输入字段的标签
output_message：显示本地化消息

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式包 —
http://jakarta.apache.org/regexp/
Jakarta 验证器 —
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 —
http://java.sun.com/j2ee/javaserverfaces/

** 错误处理：
许多 J2EE Web 应用程序体系结构都遵循“模型视图控制器（MVC）”模式。在该模式中，Servlet 扮演“控制器”的角色。Servlet 将应用程序处理委派给 EJB 会话 Bean（模型）之类的 JavaBean。然后，Servlet 再将请求转发给 JSP（视图），以呈现处理结果。Servlet 应检查所有的输入、输出、返回码、错误代码和已知的异常，以确保实际处理按预期进行。
数据验证可保护应用程序免遭恶意数据篡改，而有效的错误处理策略则是防止应用程序意外泄露内部错误消息（如异常堆栈跟踪）所不可或缺的。好的错误处理策略会处理以下项：
[1] 定义错误
[2] 报告错误
[3] 呈现错误
[4] 错误映射
[1] 定义错误
应避免在应用程序层（如 Servlet）中硬编码错误消息。 相反地，应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥，且该错误密钥映射到 HTML 表单字段或其他 Bean 属性的验证规则。例如，如果需要 "user_name"字段，其内容为字母数字，并且必须在数据库中是唯一的，那么就应定义以下错误密钥：

(a) ERROR_USERNAME_REQUIRED：该错误密钥用于显示消息，以通知用户需要 "user_name" 字段；
(b) ERROR_USERNAME_ALPHANUMERIC：该错误密钥用于显示消息，以通知用户 "user_name" 字段应该是字母数字；
(c) ERROR_USERNAME_DUPLICATE：该错误密钥用于显示消息，以通知用户 "user_name" 值在数据库中重复；
(d) ERROR_USERNAME_INVALID：该错误密钥用于显示一般消息，以通知用户 "user_name" 值无效；

好的做法是定义用于存储和报告应用程序错误的以下框架 Java 类：
- ErrorKeys：定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error：封装个别错误

```
// Example: Error encapsulates an error key.
```

```
    // Error is serializable to support code executing in multiple JVMs.
    public Class Error implements Serializable {

        // Constructor given a specified error key
        public Error(String key) {
        this(key, null);
        }

        // Constructor given a specified error key and array of placeholder objects
        public Error(String key, Object[] values) {
        this.key = key;
        this.values = values;
        }

        // Returns the error key
        public String getKey() {
        return this.key;
        }

        // Returns the placeholder values
        public Object[] getValues() {
        return this.values;
        }

        private String key = null;
        private Object[] values = null;
    }
```

- Errors：封装错误的集合

```
    // Example: Errors encapsulates the Error objects being reported to the presentation layer.
    // Errors are stored in a HashMap where the key is the bean property name and value is an
    // ArrayList of Error objects.
    public Class Errors implements Serializable {

        // Adds an Error object to the Collection of errors for the specified bean property.
        public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
        propertyErrors = new ArrayList();
        errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
        }

        // Returns true if there are any errors
        public boolean hasErrors() {
        return (errors.size > 0);
        }

        // Returns the Errors for the specified property
        public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
        }

        private HashMap errors = new HashMap();
    }
```

以下是使用上述框架类来处理“user_name”字段验证错误的示例：

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
```

```
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] 报告错误
有两种方法可报告 web 层应用程序错误：
(a) Servlet 错误机制
(b) JSP 错误机制

[2-a] Servlet 错误机制
Servlet 可通过以下方式报告错误：
- 转发给输入 JSP（已将错误存储在请求属性中），或
- 使用 HTTP 错误代码参数来调用 response.sendError，或
- 抛出异常

好的做法是处理所有已知应用程序错误（如 [1] 部分所述），将这些错误存储在请求属性中，然后转发给输入 JSP。输入 JSP 应显示错误消息，并提示用户重新输入数据。以下示例阐明转发给输入 JSP（userInput.jsp）的方式：

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

如果 Servlet 无法转发给已知的 JSP 页面，那么第二个选项是使用 response.sendError 方法，将 HttpServletResponse.SC_INTERNAL_SERVER_ERROR（状态码 500）作为参数，来报告错误。请参阅 javax.servlet.http.HttpServletResponse 的 Javadoc，以获取有关各种 HTTP 状态码的更多详细信息。返回 HTTP 错误的示例：

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

作为最后的手段，Servlet 可以抛出异常，且该异常必须是以下其中一类的子类：
- RuntimeException
- ServletException
- IOException

[2-b] JSP 错误机制
JSP 页面通过定义 errorPage 伪指令来提供机制，以处理运行时异常，如以下示例所示：

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕获的 JSP 异常被转发给指定的 errorPage，并且原始异常设置在名称为 javax.servlet.jsp.jspException 的请求参数中。错误页面必须包括 isErrorPage 伪指令，如下所示：

```
<%@ page isErrorPage="true" %>
```

isErrorPage 伪指令导致“exception”变量初始化为所抛出的异常对象。
[3] 呈现错误
J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类，其中包括：

(a) 资源束
(b) 消息格式化

[3-a] 资源束
资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。
java.util.PropertyResourceBundle 将内容存储在外部属性文件中，对其进行使用或扩展都很常见，如以下示例所示：

```
################################################
# ErrorMessages.properties
################################################
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可定义多种资源，以支持不同的语言环境（因此名为资源束）。例如，可定义 ErrorMessages_fr.properties 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在，那么会使用缺省成员。在以上示例中，缺省资源是 ErrorMessages.properties。应用程序（JSP 或 Servlet）会根据用户的语言环境从适当的资源检索内容。
[3-b] 消息格式化
J2SE 标准类 java.util.MessageFormat 提供使用替换占位符来创建消息的常规方法。MessageFormat 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
```

```
    String userName = request.getParameter("user_name");
    Object[] args = new Object[1];
    args[0] = userName;
    String message = MessageFormat.format(pattern, args);
```

以下是使用 ResourceBundle 和 MessageFormat 来呈现错误消息的更加全面的示例：

```
    // Example to render an error message from a localized ErrorMessages resource (properties file)
    // Utility class to retrieve locale-specific error messages
    public Class ErrorMessageResource {

        // Returns the error message for the specified error key in the environment locale
        public String getErrorMessage(String errorKey) {
            return getErrorMessage(errorKey, defaultLocale);
        }

        // Returns the error message for the specified error key in the specified locale
        public String getErrorMessage(String errorKey, Locale locale) {
            return getErrorMessage(errorKey, null, locale);
        }

        // Returns a formatted error message for the specified error key in the specified locale
        public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
            // Get localized ErrorMessageResource
            ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
            // Get localized error message
            String errorMessage = errorMessageResource.getString(errorKey);
            if (args != null) {
            // Format the message using the specified placeholders args
            return MessageFormat.format(errorMessage, args);
            } else {
            return errorMessage;
            }
        }

        // default environment locale
        private Locale defaultLocale = Locale.getDefaultLocale();
    }
    ...
    // Get the user's locale
    Locale userLocale = request.getLocale();
    // Check if there were any validation errors
    Errors errors = (Errors)request.getAttribute("errors");
    if (errors != null && errors.hasErrors()) {
        // iterate through errors and output error messages corresponding to the "user_name" property
        ArrayList userNameErrors = errors.getErrors("user_name");
        ListIterator iterator = userNameErrors.iterator();
        while (iterator.hasNext()) {
            // Get the next error object
            Error error = (Error)iterator.next();
            String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
            output.write(errorMessage + "\r\n");
        }
    }
```

建议定义定制 JSP 标记（如 displayErrors），以迭代处理并呈现错误消息，如以上示例所示。
[4] 错误映射
通常情况下，“Servlet 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码或异常与 Web 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 Servlet 容器都会报告内部错误消息）。该映射配置在“Web 部署描述符（web.xml）”中，如以下示例所指定：

```
    <!-- Mapping of HTTP error codes and application exceptions to error pages -->
    <error-page>
      <exception-type>UserValidationException</exception-type>
```

```
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
...
</error-page>
...
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。验证规则配置在 XML 文件中，该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。Struts 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记，如以下示例所示：

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
    <table border="0" width="100%">
    <tr>
        <th align="right">
        <html:errors property="username"/>
        <bean:message key="prompt.username"/>
        </th>
        <td align="left">
        <html:text property="username" size="16"/>
        </td>
    </tr>
    <tr>
    <td align="right">
        <html:submit><bean:message key="button.submit"/></html:submit>
    </td>
    <td align="right">
        <html:reset><bean:message key="button.reset"/></html:reset>
    </td>
    </tr>
    </table>
    </html:form>
</body>
</html:html>
```

[2] JavaServer Faces 技术
“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。
使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式包 —
http://jakarta.apache.org/regexp/
Jakarta 验证器 —
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 —
http://java.sun.com/j2ee/javaserverfaces/

PHP

SQL 盲注

** 过滤用户输入

将任何数据传给 SQL 查询之前，应始终先使用筛选技术来适当过滤。 这无论如何强调都不为过。 过滤用户输入可让许多注入缺陷在到达数据库之前便得到更正。

** 对用户输入加引号

不论任何数据类型，只要数据库允许，使用单引号括住所有用户数据，始终是好的观念。 MySQL 允许此格式化技术。

** 转义数据值

如果使用 MySQL 4.3.0 或更新的版本，您应该用 mysql_real_escape_string() 来转义所有字符串。 如果使用旧版的 MySQL，便应该使用 mysql_escape_string() 函数。 如果未使用 MySQL，您可以选择使用特定数据库的特定换码功能。 如果不知道换码功能，您可以选择使用较一般的换码功能，例如，addslashes()。

如果使用 PEAR DB 数据库抽象层，您可以使用 DB::quote() 方法或使用 ? 之类的查询占位符，它会自动转义替换占位符的值。

参考资料
http://ca3.php.net/mysql_real_escape_string
http://ca.php.net/mysql_escape_string
http://ca.php.net/addslashes
http://pear.php.net/package-info.php?package=DB

** 输入数据验证：虽然为方便用户而在客户端层上提供数据验证，但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。
一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] cookie 值[8] HTTP 响应好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。
[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。[4] 字段范围
始终确保输入参数是在由功能需求定义的范围内。
[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。[6] 字段模式
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分

大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]+$

[7] cookie 值
适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。
[8] HTTP 响应[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

PHP 包含一些自动化清理实用程序函数，如 htmlentities()：

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

此外，为了避免“跨站点脚本编制”的 UTF-7 变体，您应该显式定义响应的 Content-Type 头，例如：

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 cookie 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 cookie。
为了保护 cookie，您可以使用以下代码示例：

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

此外，我们建议您使用 HttpOnly 标志。当 HttpOnly 标志设置为 TRUE 时，将只能通过 HTTP 协议来访问 cookie。这意味着无法用脚本语言（如 JavaScript）来访问 cookie。该设置可有效地帮助减少通过 XSS 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。
在 PHP 5.2.0 中添加了 HttpOnly 标志。
引用[1] 使用 HTTP 专用 cookie 来减轻“跨站点脚本编制”的影响：
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP 安全协会：
http://phpsec.org/
[3] PHP 和 Web 应用程序安全博客 (Chris Shiflett)：
http://shiflett.org/

SQL 注入

** 过滤用户输入

将任何数据传给 SQL 查询之前，应始终先使用筛选技术来适当过滤。 这无论如何强调都不为过。 过滤用户输入可让许多注入缺陷在到达数据库之前便得到更正。

** 对用户输入加引号

不论任何数据类型，只要数据库允许，便用单引号括住所有用户数据，始终是好的观念。 MySQL 允许此格式化技术。

** 转义数据值

如果使用 MySQL 4.3.0 或更新的版本，您应该用 mysql_real_escape_string() 来转义所有字符串。 如果使用旧版的 MySQL，便应该使用 mysql_escape_string() 函数。 如果未使用 MySQL，您可以选择使用特定数据库的特定换码功能。 如果不知道换码功能，您可以选择使用较一般的换码功能，例如，addslashes()。

如果使用 PEAR DB 数据库抽象层，您可以使用 DB::quote() 方法或使用 ? 之类的查询占位符，它会自动转义替换占位符的值。

参考资料
http://ca3.php.net/mysql_real_escape_string
http://ca.php.net/mysql_escape_string
http://ca.php.net/addslashes
http://pear.php.net/package-info.php?package=DB

** 输入数据验证：虽然为方便用户而在客户端层上提供数据验证，但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。
一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] cookie 值[8] HTTP 响应好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。
[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。[4] 字段范围
始终确保输入参数是在由功能需求定义的范围内。
[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。[6] 字段模式
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]+$

[7] cookie 值

适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。
[8] HTTP 响应[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

PHP 包含一些自动化清理实用程序函数，如 htmlentities()：

```
$input = htmlentities($input, ENT_QUOTES, UTF-8);
```

此外，为了避免“跨站点脚本编制”的 UTF-7 变体，您应该显式定义响应的 Content-Type 头，例如：

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 cookie 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 cookie。
为了保护 cookie，您可以使用以下代码示例：

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

此外，我们建议您使用 HttpOnly 标志。当 HttpOnly 标志设置为 TRUE 时，将只能通过 HTTP 协议来访问 cookie。这意味着无法用脚本语言（如 JavaScript）来访问 cookie。该设置可有效地帮助减少通过 XSS 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。
在 PHP 5.2.0 中添加了 HttpOnly 标志。
引用[1] 使用 HTTP 专用 cookie 来减轻“跨站点脚本编制”的影响：
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP 安全协会：
http://phpsec.org/
[3] PHP 和 Web 应用程序安全博客 (Chris Shiflett)：
http://shiflett.org/

跨站点脚本编制

**输入数据验证：
虽然为了用户便利可以在客户机层上提供数据验证，但是数据验证必须始终在服务器层上执行。客户机端验证本身不安全，因为很容易就能绕过这些验证，例如通过禁用 Javascript。

良好设计通常要求 Web 应用程序框架提供服务器端实用程序例程来验证下列各项：
[1] 必填字段
[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是字符串）
[3] 字段长度
[4] 字段范围
[5] 字段选项
[6] 字段模式
[7] Cookie 值
[8] HTTP 响应
良好实践是执行一个或多个可验证各个应用程序参数的函数。以下部分介绍一些示例检查。
[1] 必填字段
始终确保字段不为空且其长度大于零，排除前导空格和尾随空格。
如何验证必填字段的示例：

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] 字段数据类型
在 Web 应用程序中，输入参数的类型不佳。例如，所有 HTTP 请求参数或 cookie 值都是字符串类型。开发人员负责验证输入是否是正确数据类型。
[3] 字段长度
始终确保输入参数（HTTP 请求参数或 cookie 值）受最小长度和/或最大长度限制。
[4] 字段范围
始终确保输入参数在功能要求定义的范围之内。
[5] 字段选项
通常，Web 应用程序会向用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但是未能执行服务器端验证，以确保所选值是允许选项之一。请记住，恶意用户可以轻松修改任何选项值。始终根据功能要求定义的允许选项验证所选用户值。
[6] 字段模式
始终检查用户输入是否匹配功能要求定义的模式。例如，如果 userName 字段仅应允许字母数字字符，不区分大小写，则使用以下正则表达式：
^[a-zA-Z0-9]+$
[7] Cookie 值
将（上述）相同的验证规则应用于 cookie 值，具体取决于应用程序要求，例如，验证必需值、验证长度等。
[8] HTTP 响应
[8-1] 过滤用户输入
为了保护应用程序不受跨站点脚本编制攻击，开发人员应将敏感字符转换为其相应的字符实体，清理 HTML。以下这些是 HTML 敏感字符：
< > " ' % ;) (& +
PHP 包括一些自动清理实用程序函数，如 htmlentities()：

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

此外，为了避免跨站点脚本编制的 UTF-7 变量，您应明确定义响应的内容类型头，例如：

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据并通过 SSL 传输该 cookie 时，请确保先在 HTTP 响应中设置 cookie 的安全标志。这将指导浏览器仅通过 SSL 连接使用该 cookie。
您可以使用以下代码示例保护 cookie：

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

此外，我们建议您使用 HttpOnly 标志。HttpOnly 标志设置为 TRUE 时，cookie 将仅可通过 HTTP 协议进行访问。这意味着将无法通过脚本编制语言（如 JavaScript）访问 cookie。此设置可有效地减少通过 XSS 攻击进行的身份盗用（虽然并不是所有浏览器都支持此设置）。
在 PHP 5.2.0 中添加了 HttpOnly 标志。
引用
[1] 使用仅 HTTP Cookie 缓解跨站点脚本编制：
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP 安全联盟：
http://phpsec.org/
[3] PHP 和 Web 应用程序安全博客 (Chris Shiflett)：
http://shiflett.org/

发现数据库错误模式

** 过滤用户输入

将任何数据传给 SQL 查询之前，应始终先使用筛选技术来适当过滤。 这无论如何强调都不为过。 过滤用户输入可让许多注入缺陷在到达数据库之前便得到更正。

** 对用户输入加引号

不论任何数据类型，只要数据库允许，便用单引号括住所有用户数据，始终是好的观念。 MySQL 允许此格式化技术。

** 转义数据值

如果使用 MySQL 4.3.0 或更新的版本，您应该用 mysql_real_escape_string() 来转义所有字符串。 如果使用旧版的 MySQL，便应该使用 mysql_escape_string() 函数。 如果未使用 MySQL，您可以选择使用特定数据库的特定换码功能。 如果不知道换码功能，您可以选择使用较一般的换码功能，例如，addslashes()。

如果使用 PEAR DB 数据库抽象层，您可以使用 DB::quote() 方法或使用 ? 之类的查询占位符，它会自动转义替换占位符的值。

参考资料
http://ca3.php.net/mysql_real_escape_string
http://ca.php.net/mysql_escape_string

http://ca.php.net/addslashes
http://pear.php.net/package-info.php?package=DB

** 输入数据验证：虽然为方便用户而在客户端层上提供数据验证，但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。
一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：[1] 必需字段[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）[3] 字段长度[4] 字段范围[5] 字段选项[6] 字段模式[7] cookie 值[8] HTTP 响应好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。
[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。[4] 字段范围
始终确保输入参数是在由功能需求定义的范围内。
[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。[6] 字段模式
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]+$

[7] cookie 值
适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。
[8] HTTP 响应[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

PHP 包含一些自动化清理实用程序函数，如 htmlentities()：

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

此外，为了避免“跨站点脚本编制”的 UTF-7 变体，您应该显式定义响应的 Content-Type 头，例如：

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 cookie 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 cookie。
为了保护 cookie，您可以使用以下代码示例：

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

此外，我们建议您使用 HttpOnly 标志。当 HttpOnly 标志设置为 TRUE 时，将只能通过 HTTP 协议来访问 cookie。这意味着无法用脚本语言（如 JavaScript）来访问 cookie。该设置可有效地帮助减少通过 XSS 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。
在 PHP 5.2.0 中添加了 HttpOnly 标志。
引用[1] 使用 HTTP 专用 cookie 来减轻“跨站点脚本编制”的影响：
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP 安全协会：
http://phpsec.org/
[3] PHP 和 Web 应用程序安全博客 (Chris Shiflett)：
http://shiflett.org/

高 禁用基于参数值指向外部站点的重定向

TOC

该任务修复的问题类型

- 通过 URL 重定向钓鱼

常规

有多种减轻威胁的技巧：
[1] 策略：库或框架
使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。
可用于更轻松生成正确编码的输出的库和框架示例包括 Microsoft 的 Anti-XSS 库、OWASP ESAPI 编码模块和 Apache Wicket。
[2] 了解将在其中使用数据的上下文，以及预期的编码。在不同组件之间传输数据时，或在生成可同时包含多个编码的输出（如 Web 页面或多部分邮件消息）时，这尤为重要。研究所有预期的通信协议和数据表示法以确定所需的编码策略。对于将输出到另一个 Web 页面的任何数据（尤其是从外部输入接收到的任何数据），请对所有非字母数字字符使用恰当的编码。
相同输出文档的某些部分可能需要不同的编码，具体取决于输出是在以下哪一项中：

[-] HTML 主体
[-] 元素属性（如 src="XYZ"）
[-] URI
[-] JavaScript 段
[-] 级联样式表和样式属性
请注意，“HTML 实体编码”仅适用于 HTML 主体。
请咨询 XSS Prevention Cheat Sheet
http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
以获取有关所需编码和转义类型的更多详细信息。
[3] 策略：识别和减少攻击出现的机会
了解您的软件中可能出现不可信输入的所有潜在区域：参数或自变量、cookie、从网络读取的任何内容、环境变量、反向 DNS 查找、查询结果、请求头、URL 组成部分、电子邮件、文件、文件名、数据库以及向应用程序提供数据的任何外部系统。请记住，此类输入可通过 API 调用间接获取。
[4] 策略：输出编码
对于生成的每个 Web 页面，请使用并指定 ISO-8859-1 或 UTF-8 之类的字符编码。如果未指定编码，Web 浏览器可能通过猜测 Web 页面实际使用的编码来选择不同的编码。这可能导致 Web 浏览器将特定序列视为特殊序列，从而使客户机暴露在不易察觉的 XSS 攻击之下。请参阅 CWE-116 以获取与编码/转义相关的更多减轻威胁的方法。
[5] 策略：识别和减少攻击出现的机会
要帮助减轻针对用户会话 cookie 的 XSS 攻击带来的威胁，请将会话 cookie 设置为 HttpOnly。在支持 HttpOnly 功能的浏览器（如 Internet Explorer 和 Firefox 的较新版本）中，此属性可防止使用 document.cookie 的恶意客户机端脚本访问用户的会话 cookie。这不是完整的解决方案，因为 HttpOnly 并不受所有浏览器支持。更重要的是，XMLHTTPRequest 和其他功能强大的浏览器技术提供了对 HTTP 头的读访问权，包括在其中设置 HttpOnly 标志的 Set-Cookie 头。
[6] 策略：输入验证
假定所有输入都是恶意的。使用“接受已知善意”输入验证策略：严格遵守规范的可接受输入的白名单。拒绝任何没有严格遵守规范的输入，或者将其转换为遵守规范的内容。不要完全依赖于针对恶意或格式错误的输入的黑名单。但是，黑名单可帮助检测潜在攻击，或者确定哪些输入由于格式严重错误而应直接拒绝。执行输入验证时，请考虑所有潜在相关的属性，包括长度、输入类型、可接受的值的完整范围、缺少或多余的输入、语法、在相关字段之间是否一致以及是否遵守了业务规则。作为业务规则逻辑的示例，“boat”可能在语法上有效（因为它仅包含字母数字字符），但如果预期为颜色（如“red”或“blue”），那么它就无效。动态构造 Web 页面时，请使用严格的白名单以根据请求中参数的预期值来限制字符集。所有输入都应进行验证和清理，不仅限于用户应指定的参数，而是涉及请求中的所有数据，包括隐藏字段、cookie、头、URL 本身，等等。导致 XSS 脆弱性持续存在的一个常见错误是仅验证预期会由站点重新显示的字段。常见的情况是，在请求中出现由应用程序服务器或应用程序反射的数据，而开发团队却未能预料到此情况。另外，将来的开发者可能会使用当前未反映的字段。因此，建议验证 HTTP 请求的所有部分。请注意，适当的输出编码、转义和引用是防止 XSS 的最有效解决方案，虽然输入验证可能会提供一定的深度防御。这是因为，它会有效限制将在输出中出现的内容。输入验证并不总是能够防止 XSS，尤其是在您需要支持可包含任意字符的自由格式文本字段的情况下。例如，在聊天应用程序中，心型表情图标（“<3”）可能会通过验证步骤，因为它的使用频率很高。但是，不能将其直接插入到 Web 页面中，因为它包含“<”字符，该字符需要转义或以其他方式进行处理。在此情况下，消除“<”可能会降低 XSS 的风险，但是这会产生不正确的行为，因为这样就不会记录表情图标。
这可能看起来只是略有不便，但在需要表示不等式的数学论坛中，这种情况就更为重要。即使在验证中出错（例如，在 100 个输入字段中忘记一个字段），相应的编码仍有可能针对基于注入的攻击为您提供防护。只要输入验证不是孤立完成的，便仍是有用的技巧，因为它可以大大减少攻击出现的机会，使您能够检测某些攻击，并提供正确编码所无法解决的其他安全性优势。请确保在应用程序内定义良好的界面中执行输入验证。即使某个组件进行了复用或移动到其他位置，这也将有助于保护应用程序。

中 将您的服务器配置为仅允许所需 HTTP 方法 TOC

该任务修复的问题类型

- 使用 HTTP 动词篡改的认证旁路

常规

如果使用基于 HTTP 方法的访问控制，配置 web 服务器以仅允许所需 HTTP 方法。
确保配置的确限制未列出的方法：
在 Apache .htaccess 文件中：避免使用有问题的“LIMIT”伪指令。使用“LimitExcept”伪指令。
在 JAVA EE 中，避免在访问控制策略中使用 <http-method> 元素。
在 ASP.NET 授权中，在允许所需动词的白名单之后，使用 <deny verbs="*" users="*" />。

中 验证“Referer”头的值，并对每个提交的表单使用 one-time-nonce TOC

该任务修复的问题类型

- 跨站点请求伪造

常规

有多种减轻威胁的技巧：
[1] 策略：库或框架
使用不允许此弱点出现的经过审核的库或框架，或提供更容易避免此弱点的构造。
例如，使用能防御 CSRF 的软件包，例如 OWASP CSRFGuard -
http://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet
另一个示例为“ESAPI 会话管理”控件，其中包括针对 CSRF 的组件 -
http://www.owasp.org/index.php/ESAPI

[2] 确保应用程序中没有跨站点脚本编制问题 (CWE-79)，因为通过使用攻击者控制的脚本可绕过大部分 CSRF 防御。
[3] 为每个表单生成唯一的现时标志，将现时标志放到表单中，并在接收表单时验证现时标志。请确保现时标志是不可预测的 (CWE-330) -
http://www.cgisecurity.com/articles/csrf-faq.shtml
请注意，通过使用 XSS (CWE-79) 可绕过这一点。
[4] 识别特别危险的操作。在用户执行危险操作时，发送单独的确认请求以确保是用户自己希望执行该操作。请注意，通过使用 XSS (CWE-79) 可绕过这一点。
[5] 使用“两次提交的 cookie”方法，如 Felten 和 Zeller 所述：
在用户访问站点时，该站点应生成伪随机值，并将其设置为用户机器上的 cookie。站点应要求每次表单提交都包括该值作为表单和 cookie 值。向站点发送 POST 请求时，只有表单和 cookie 值相同时才应将该请求视为有效。
由于同源策略，攻击者无法读取或修改 cookie 中存储的值。要以用户的身份成功提交表单，攻击者必须正确猜出伪随机值。如果伪随机值的保密性很强，这将是极端困难的。此技巧需要 JavaScript，因此对于禁用了 JavaScript 的浏览器可能无效 -
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.147.1445
请注意，使用 XSS (CWE-79) 有可能绕过这一点，或者在使用支持攻击者从 HTTP 请求中读取原始头的 Web 技术时也有可能绕过这一点。
[6] 请勿对触发状态更改的任何请求使用 GET 方法。
[7] 检查 HTTP Referer 头以查看请求是否源自预期的页面。这可能会破坏合法功能，因为用户或代理可能已出于隐私原因而禁止发送 Referer。请注意，通过使用 XSS (CWE-79) 可绕过这一点。
攻击者可能使用 XSS 来生成欺骗性的 Referer，或从允许使用其 Referer 的页面生成恶意请求。

低 除去 HTML 注释中的敏感信息 TOC

该任务修复的问题类型

- HTML 注释敏感信息泄露

常规

[1] 请勿在 HTML 注释中遗留任何重要信息（如文件名或文件路径）。
[2] 从生产站点注释中除去以前（或未来）站点链接的跟踪信息。
[3] 避免在 HTML 注释中放置敏感信息。
[4] 确保 HTML 注释不包括源代码片段。
[5] 确保程序员没有遗留重要信息。

低 除去 Web 站点中的电子邮件地址 TOC

该任务修复的问题类型

- 发现电子邮件地址模式

常规

从 Web 站点中除去任何电子邮件地址，以便其不会被恶意用户利用。

低 除去 Web 站点中的内部 IP 地址 TOC

该任务修复的问题类型

- 发现内部 IP 泄露模式

常规

内部 IP 通常显现在 Web 应用程序/服务器所生成的错误消息中，或显现在 HTML/JavaScript 注释中。
[1] 关闭 Web 应用程序/服务器中有问题的详细错误消息。
[2] 确保已安装相关的补丁。
[3] 确保内部 IP 信息未留在 HTML/JavaScript 注释中。

低 除去 web-server 中的源代码文件并应用任何相关补丁 TOC

该任务修复的问题类型

- 发现 Web 应用程序源代码泄露模式

常规

许多方式可以诱使 Web 应用程序显示其源代码。
要确保应用程序不允许 Web 用户访问源代码，请执行下列操作：
[1] 检查已安装与源代码泄露相关的所有系统补丁。
[2] 检查未将应用程序源代码留在 HTML 注释中。
[3] 检查已从生产环境中除去所有源代码文件。

低 除去客户端中的业务逻辑和安全逻辑 TOC

该任务修复的问题类型

- 客户端（JavaScript）Cookie 引用

常规

[1] 避免在客户端放置业务/安全逻辑。
[2] 查找并除去客户端不安全的 JavaScript 代码，该代码可能会对站点造成安全威胁。

低 将“autocomplete”属性正确设置为“off” TOC

该任务修复的问题类型

- 自动填写未对密码字段禁用的 HTML 属性

常规

如果“input”元素的“password”字段中缺失“autocomplete”属性，请进行添加并将其设置为“off“。

如果“autocomplete”属性设置为“on”，请将其更改为“off”。
例如：易受攻击站点：

```
<form action="AppScan.html" method="get">
    Username: <input type="text" name="firstname" /><br />
    Password: <input type="password" name="lastname" />
    <input type="submit" value="Submit" />
<form>
```

非易受攻击站点：

```
<form action="AppScan.html" method="get">
    Username: <input type="text" name="firstname" /><br />
    Password: <input type="password" name="lastname" autocomplete="off"/>
    <input type="submit" value="Submit" />
<form>
```

低 将服务器配置为使用安全策略的“Content-Security-Policy”头

TOC

该任务修复的问题类型

- “Content-Security-Policy”头缺失或不安全

常规

将服务器配置为发送“Content-Security-Policy”头。
关于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
关于 IIS，请参阅：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
关于 nginx，请参阅：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

低 将服务器配置为使用值为 DENY 或 SAMEORIGIN 的“X-Frame-Options”头

TOC

该任务修复的问题类型

- 跨帧脚本编制防御缺失或不安全

常规

使用 X-Frame-Options 可防止（或限制）页面嵌入 iFrame 中。对于较旧版本的浏览器，请在每个页面中包含一个不应成帧的“框架破坏程序”脚本。

低 拒绝恶意请求并防止直接执行 JavaScript 响应 TOC

该任务修复的问题类型

- JavaScript 劫持

常规

原始咨询如下：

“第一代 Web 应用程序不容易遭受“JavaScript 劫持”，因为它们的数据通常作为 HTML 文档的一部分来传输，而不是作为纯 JavaScript 来传输。对攻击者无秘密可防的应用程序，反而能够免受“JavaScript 劫持”攻击。
如果 Web 应用程序有可供利用的跨站点脚本编制漏洞，便难免受到“JavaScript 劫持”之类窃取数据的攻击，因为跨站点脚本编制可让攻击者运行 JavaScript，并且造成其源于应用程序的域的假象。 反过来并不成立：如果 Web 应用程序未包含任何跨站点脚本编制漏洞，它不一定能免于“JavaScript 劫持”。
对于处理机密数据的 Web 2.0 应用程序而言，有两个基本方法可以防御“JavaScript 劫持”： - 拒绝恶意的请求 - 防止直接执行 JavaScript 响应 防御“JavaScript 劫持”的最佳方式是确实采取这两个防御手段。
拒绝恶意的请求 从服务器的角度来看，“JavaScript 劫持”攻击看似意在跨站点伪造请求，防御跨站点伪造请求也就防御了“JavaScript 劫持”攻击。
为了便于检测出恶意请求，每个请求都应该包括一个攻击者难以猜中的参数。 其中一个方法是将会话 Cookie 作为一个参数添加到请求。 当服务器接收到这类请求时，它可以检查确认会话 Cookie 是否与请求参数的值匹配。 恶意代码无法访问会话 cookie（cookie 也遵循“同源策略”），因此，攻击者难以设计出可以绕过这项测试的请求。 不同的秘密也可用来代替会话 cookie。 只要秘密难以猜中，且出现在合法应用程序能够访问，但无法从其他域访问的环境中，就可以防止攻击者发出有效请求。
有些框架只在客户端运行。 换句话来说，它们完全是用 JavaScript 来撰写，完全不知道服务器的运作。 这暗示它们并不知道会话 cookie 的名称。 即使不知道会话 cookie 的名称，它们也能够将所有 cookie 添加到对服务器的每个请求中，以参与基于 cookie 的防御。 下列 JavaScript 片段概述这个“盲目客户端”策略： var httpRequest = new XMLHttpRequest(); ... var cookies="cookies="+escape(document.cookie); http_request.open('POST', url, true); httpRequest.send(cookies); 服务器也可以检查 HTTP Referer 头，以确保请求是来自合法的应用程序，不是来自恶意应用程序。 从历史上来看，Referer 头并不可靠，因此，建议不要将其用作任何安全机制的基础。
服务器可以只响应 HTTP POST 请求，不响应 HTTP GET 请求，从而防御“JavaScript 劫持”。 这是一个防御性的技术，因为 <script> 标记始终使用 GET 来装入外部来源的 JavaScript。 这个防御也很容易出错。 Sun 及其他地方的 Web 应用程序专家都鼓励使用 GET 以提高性能。 即使是内部使用 POST 请求的框架（例如 GWT）也记录了支持 GET 请求的必要步骤，但并未提及任何潜在的安全后果。 这项 HTTP 方法选项与安全性之间的连接遗漏，表示程序员可能有时会将这一功能的缺失误认为是疏漏之处，而不能正确认识到这是安全预防措施，于是修改应用程序来响应 GET 请求。
防止直接执行响应 为了使恶意站点无法执行含有 JavaScript 的响应，合法的客户端应用程序可以运用下列事实：对于收到的数据，它可以先修改，再执行，恶意应用程序只能使用 <script> 标记来加以执行。 当服务器将对象串行化时，它应该包含前缀（也可能包含后缀），以使得无法使用 <script> 标记来执行 JavaScript 。 合法的客户端应用程序可以在运行 JavaScript 之前，除去这个额外的数据。 该方法有许多可能的实现方式。 我们概述两种方式。
首先，服务器可以将下列语句加到每个消息的开头作为前缀： while(1);

除非客户端除去这个前缀，否则，在对消息求值时，JavaScript 解释器会陷入无限循环。 Google 就利用这项技术来修订 Grossman 所识别的漏洞。 客户机搜索并移除如下前缀：

```
var object;
var req = new XMLHttpRequest();
req.open("GET", "/object.json",true);
req.onreadystatechange = function () {
req.onreadystatechange = function () { if (req.readyState == 4) { var txt = req.responseText; if (txt.substr(0,9) ==
"while(1);") { txt = txt.substring(10); } object = eval("(" + txt + ")"); req = null; } };var txt = req.responseText;
if (txt.substr(0,9) == "while(1);") {
txt = txt.substring(10);
}
object = eval("(" + txt + ")");
req = null;
}
};
req.send(null);
```

其次，服务器可以在发送给 eval() 之前必须除去的 JavaScript 前后加上注释字符。下列 JSON 对象已括在块注释中：

```
/*
[{"fname":"Brian", "lname":"Chess", "phone":"6502135600",
"purchases":60000.00, "email":"brian@fortifysoftware.com" }
]
*/
```

客户机可以搜索并移除如下所示的注释字符：

```
var object;
var req = new XMLHttpRequest();
req.open("GET", "/object.json",true);
req.onreadystatechange = function () {
req.onreadystatechange = function () { if (req.readyState == 4) { var txt = req.responseText; if (txt.substr(0,9) ==
"while(1);") { txt = txt.substring(10); } object = eval("(" + txt + ")"); req = null; } };var txt = req.responseText;
if (txt.substr(0,2) == "/*") {
txt = txt.substring(2, txt.length - 2);
}
object = eval("(" + txt + ")");
req = null;
}
};
req.send(null);
```

通过 <script> 标记检索敏感 JavaScript 的恶意站点将无法访问此标记中包含的数据。"

低 请勿接受在查询字符串中发送的主体参数 TOC

该任务修复的问题类型

- 查询中接受的主体参数

常规

重新对应用程序编程以禁用对查询中列出的 POST 参数的处理

低 为 Web 服务器或 Web 应用程序下载相关的安全补丁 TOC

该任务修复的问题类型

- 发现可能的服务器路径泄露模式

常规

有几种缓解技术：
[1] 如果漏洞存在于应用程序内，请修复服务器代码，以使得任何输出中都不包含文件位置。
[2] 否则，如果应用程序位于第三方产品中，请根据 Web 服务器或 Web 应用程序上使用的第三方产品下载相关的安全补丁。

低 验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常 TOC

该任务修复的问题类型

- 应用程序错误

常规

[1] 检查入局请求，以了解所有预期的参数和值是否存在。 当参数缺失时，发出适当的错误消息，或使用缺省值。
[2] 应用程序应验证其输入是否由有效字符组成（解码后）。 例如，应拒绝包含空字节（编码为 %00）、单引号、引号等的输入值。
[3] 确保值符合预期范围和类型。 如果应用程序预期特定参数具有特定集合中的值，那么该应用程序应确保其接收的值确实属于该集合。 例如，如果应用程序预期值在 10..99 范围内，那么就该确保该值确实是数字，且在 10..99 范围内。
[4] 验证数据是否属于提供给客户端的集合。
[5] 请勿在生产环境中输出调试错误消息和异常。

.Net

要在 ASP.NET 中禁用调试，请编辑 web.config 文件，使其包含以下属性：

```
<compilation
   debug="false"
/>
```

要获取更多信息，请参阅“HOW TO: Disable Debugging for ASP.NET Applications”，位置如下：
http://support.microsoft.com/default.aspx?scid=kb;en-us;815157

您可以使用验证控件，将输入验证添加到“Web 表单”页面。验证控件提供适用于所有常见类型的标准验证的易用机制（例如，测试验证日期是否有效，或验证值是否在范围内），以及进行定制编写验证的方法。此外，验证控件还使您能够完整定制向用户显示错误信息的方式。验证控件可搭配“Web 表单”页面的类文件中处理的任何控件使用，其中包括 HTML 和 Web 服务器控件。
要确保所有的必需参数都存在于请求中，请使用 "RequiredFieldValidator" 验证控件。该控件确保用户不会跳过 web 表单中的任何条目。

要确保用户输入仅包含有效值，您可以使用以下验证控件中的一种：
[1] “RangeValidator”：检查用户条目（值）是否在指定的上下界限之间。您可以检查配对数字、字母字符和日期内的范围。
[2] “RegularExpressionValidator”：检查条目是否与正则表达式定义的模式相匹配。此类型的验证使您能够检查可预见的字符序列，如社会保险号码、电子邮件地址、电话号码、邮政编码等中的字符序列。
重要注意事项：验证控件不会阻止用户输入或更改页面处理流程；它们只会设置错误状态，并产生错误消息。程序员的职责是，在执行进一步的应用程序特定操作前，测试代码中控件的状态。
有两种方法可检查用户输入的有效性：
1. 测试常规错误状态： 在您的代码中，测试页面的 IsValid 属性。该属性会将页面上所有验证控件的 IsValid 属性值汇总（使用逻辑 AND）。如果将其中一个验证控件设置为无效，那么页面属性将会返回 false。
2. 测试个别控件的错误状态：
在页面的“验证器”集合中循环，该集合包含对所有验证控件的引用。然后，您就可以检查每个验证控件的 IsValid 属性。

J2EE

** 输入数据验证：** 输入数据验证：虽然为方便用户而在客户端层上提供数据验证，但仍必须使用 Servlet 在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。
一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：
[1] 必需字段
[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）
[3] 字段长度
[4] 字段范围
[5] 字段选项
[6] 字段模式
[7] cookie 值
[8] HTTP 响应好的做法是将以上例程作为“验证器”实用程序类中的静态方法实现。以下部分描述验证器类的一个示例。
[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
        isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。使用 Java 基本包装程序类，来检查是否可将字段值安全地转换为所需的基本数据类型。
验证数字字段（int 类型）的方式的示例：

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
        Integer.parseInt(value);
        isFieldValid = true;
        } catch (Exception e) {
```

```
        isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

好的做法是将所有 HTTP 请求参数转换为其各自的数据类型。例如，将请求参数的“integerValue”存储在请求属性中，并按以下示例所示来使用：

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...
```

应用程序应处理的主要 Java 数据类型：
- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。以下示例验证 userName 字段的长度是否在 8 至 20 个字符之间：

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
        validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
        validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] 字段范围
始终确保输入参数是在由功能需求定义的范围内。
以下示例验证输入 numberOfChoices 是否在 10 至 20 之间：

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
        // numberOfChoices is valid, continue processing request
        ...
        }
    }
}
```

[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需求定义的受允许的选项来验证选定的用户值。以下示例验证用户针对允许的选项列表进行的选择：

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
        List list = Arrays.asList(options);
        if (list != null) {
        isValidValue = list.contains(value);
        }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] 字段模式
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]*$

Java 1.3 或更早的版本不包含任何正则表达式包。建议将“Apache 正则表达式包”（请参阅以下“资源”）与 Java 1.3 一起使用，以解决该缺乏支持的问题。执行正则表达式验证的示例：

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        RE r = new RE(expression);
        match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 引进了一种新的正则表达式包 (java.util.regex)。以下是使用新的 Java 1.4 正则表达式包的 Validator.matchPattern 修订版：

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] cookie 值使用 javax.servlet.http.Cookie 对象来验证 cookie 值。适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。验证必需 cookie 值的示例：

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue()) {
        // valid cookie value, continue processing request
        ...
        }
        }
    }
}
```

[8] HTTP 响应
[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，请通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

以下示例通过将敏感字符转换为其对应的字符实体来过滤指定字符串：

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
        return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
        switch (value.charAt(i)) {
        case '<':
        result.append("&lt;");
        break;
        case '>':
        result.append("&gt;");
        break;
        case '"':
        result.append("&quot;");
        break;
        case '\'':
        result.append("&#39;");
        break;
        case '%':
        result.append("&#37;");
        break;
        case ';':
        result.append("&#59;");
        break;
        case '(':
        result.append("&#40;");
        break;
        case ')':
        result.append("&#41;");
        break;
        case '&':
        result.append("&amp;");
        break;
        case '+':
        result.append("&#43;");
        break;
        default:
        result.append(value.charAt(i));
        break;
        }
        return result;
    }
    ...
}
...
// Filter the HTTP response using Validator.filter
PrintWriter out = response.getWriter();
// set output response
out.write(Validator.filter(response));
out.close();
```

Java Servlet API 2.3 引进了“过滤器”，它支持拦截和转换 HTTP 请求或响应。

以下示例使用 Validator.filter 来用“Servlet 过滤器”清理响应：

```
  // Example to filter all sensitive characters in the HTTP response using a Java Filter.
  // This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
  public class SensitiveCharsFilter implements Filter {
      ...
      public void doFilter(ServletRequest request,
          ServletResponse response,
          FilterChain chain)
          throws IOException, ServletException {

          PrintWriter out = response.getWriter();
          ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
          chain.doFilter(request, wrapper);

          CharArrayWriter caw = new CharArrayWriter();
          caw.write(Validator.filter(wrapper.toString()));

          response.setContentType("text/html");
          response.setContentLength(caw.toString().length());
          out.write(caw.toString());
          out.close();
      }
      ...
      public class CharResponseWrapper extends HttpServletResponseWrapper {
          private CharArrayWriter output;

          public String toString() {
          return output.toString();
          }

          public CharResponseWrapper(HttpServletResponse response){
          super(response);
          output = new CharArrayWriter();
          }

          public PrintWriter getWriter(){
          return new PrintWriter(output);
          }
      }
  }

  }
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据时，确保使用 Cookie.setSecure（布尔标志）在 HTTP 响应中设置 cookie 的安全标志，以指导浏览器使用安全协议（如 HTTPS 或 SSL）发送 cookie。
保护“用户”cookie 的示例：

```
  // Example to secure a cookie, i.e. instruct the browser to
  // send the cookie using a secure protocol
  Cookie cookie = new Cookie("user", "sensitive");
  cookie.setSecure(true);
  response.addCookie(cookie);
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。Jakarta Commons Validator 是一种强大的框架，用来实现所有以上数据验证需求。这些规则配置在定义表单字段的输入验证规则的 XML 文件中。在缺省情况下，Struts 支持在使用 Struts“bean:write”标记撰写的所有数据上，过滤 [8] HTTP 响应中输出的危险字符。可通过设置“filter=false”标志来禁用该过滤。
Struts 定义以下基本输入验证器，但也可定义定制的验证器：
required：如果字段包含空格以外的任何字符，便告成功。

mask：如果值与掩码属性给定的正则表达式相匹配，便告成功。
range：如果值在 min 和 max 属性给定的值的范围内（(value >= min) & (value <= max)），便告成功。
maxLength：如果字段长度小于或等于 max 属性，便告成功。
minLength：如果字段长度大于或等于 min 属性，便告成功。
byte、short、integer、long、float、double：如果可将值转换为对应的基本类型，便告成功。
date：如果值代表有效日期，便告成功。可能会提供日期模式。
creditCard：如果值可以是有效的信用卡号码，便告成功。
e-mail：如果值可以是有效的电子邮件地址，便告成功。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces 技术
“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件和输入验证的 Java API (JSR 127)。
JavaServer Faces API 实现以下基本验证器，但可定义定制的验证器： validate_doublerange：在组件上注册 DoubleRangeValidator
validate_length：在组件上注册 LengthValidator
validate_longrange：在组件上注册 LongRangeValidator
validate_required：在组件上注册 RequiredValidator
validate_stringrange：在组件上注册 StringRangeValidator
validator：在组件上注册定制的 Validator

JavaServer Faces API 定义以下 UIInput 和 UIOutput 处理器（标记）：
input_date：接受以 java.text.Date 实例格式化的 java.util.Date
output_date：显示以 java.text.Date 实例格式化的 java.util.Date
input_datetime：接受以 java.text.DateTime 实例格式化的 java.util.Date
output_datetime：显示以 java.text.DateTime 实例格式化的 java.util.Date
input_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）
output_number：显示以 java.text.NumberFormat 格式化的数字数据类型（java.lang.Number 或基本类型）
input_text：接受单行文本字符串。
output_text：显示单行文本字符串。
input_time：接受以 java.text.DateFormat 时间实例格式化的 java.util.Date
output_time：显示以 java.text.DateFormat 时间实例格式化的 java.util.Date

input_hidden：允许页面作者在页面中包括隐藏变量
input_secret：接受不含空格的单行文本，并在输入时，将其显示为一组星号
input_textarea：接受多行文本
output_errors：显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息
output_label：将嵌套的组件显示为指定输入字段的标签
output_message：显示本地化消息

使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式包 －
http://jakarta.apache.org/regexp/
Jakarta 验证器 －
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 －
http://java.sun.com/j2ee/javaserverfaces/
** 错误处理：
许多 J2EE Web 应用程序体系结构都遵循“模型视图控制器（MVC）”模式。在该模式中，Servlet 扮演“控制器”的角色。Servlet 将应用程序处理委派给 EJB 会话 Bean（模型）之类的 JavaBean。然后，Servlet 再将请求转发给 JSP（视图），以呈现处理结果。Servlet 应检查所有的输入、输出、返回码、错误代码和已知的异常，以确保实际处理按预期进行。
数据验证可保护应用程序免遭恶意数据篡改，而有效的错误处理策略则是防止应用程序意外泄露内部错误消息（如异常堆栈跟踪）所不可或缺的。好的错误处理策略会处理以下项：
[1] 定义错误
[2] 报告错误
[3] 呈现错误
[4] 错误映射
[1] 定义错误
应避免在应用程序层（如 Servlet）中硬编码错误消息。 相反地，应用程序应该使用映射到已知应用程序故障的错误密钥。好的做法是定义错误密钥，且该错误密钥映射到 HTML 表单字段或其他 Bean 属性的验证规则。例如，如果需要 "user_name"字段，其内容为字母数字，并且必须在数据库中是唯一的，那么就应定义以下错误密钥：

(a) ERROR_USERNAME_REQUIRED：该错误密钥用于显示消息，以通知用户需要 "user_name" 字段；
(b) ERROR_USERNAME_ALPHANUMERIC：该错误密钥用于显示消息，以通知用户 "user_name" 字段应该是字母数字；
(c) ERROR_USERNAME_DUPLICATE：该错误密钥用于显示消息，以通知用户 "user_name" 值在数据库中重复；

(d) ERROR_USERNAME_INVALID：该错误密钥用于显示一般消息，以通知用户 "user_name" 值无效；

好的做法是定义用于存储和报告应用程序错误的以下框架 Java 类：
- ErrorKeys：定义所有错误密钥

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error：封装个别错误

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
    this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
    this.key = key;
    this.values = values;
    }

    // Returns the error key
    public String getKey() {
    return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
    return this.values;
    }

    private String key = null;
    private Object[] values = null;
}
```

- Errors：封装错误的集合

```
// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public Class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
    public void addError(String property, Error error) {
    ArrayList propertyErrors = (ArrayList)errors.get(property);
    if (propertyErrors == null) {
    propertyErrors = new ArrayList();
```

```
        errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
        }

        // Returns true if there are any errors
        public boolean hasErrors() {
        return (errors.size > 0);
        }

        // Returns the Errors for the specified property
        public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
        }

        private HashMap errors = new HashMap();
    }
```

以下是使用上述框架类来处理“user_name”字段验证错误的示例：

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] 报告错误
有两种方法可报告 web 层应用程序错误：
(a) Servlet 错误机制
(b) JSP 错误机制

[2-a] Servlet 错误机制
Servlet 可通过以下方式报告错误：
- 转发给输入 JSP（已将错误存储在请求属性中），或
- 使用 HTTP 错误代码参数来调用 response.sendError，或
- 抛出异常

好的做法是处理所有已知应用程序错误（如 [1] 部分所述），将这些错误存储在请求属性中，然后转发给输入 JSP。输入 JSP 应显示错误消息，并提示用户重新输入数据。以下示例阐明转发给输入 JSP（userInput.jsp）的方式：

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

如果 Servlet 无法转发给已知的 JSP 页面，那么第二个选项是使用 response.sendError 方法，将 HttpServletResponse.SC_INTERNAL_SERVER_ERROR（状态码 500）作为参数，来报告错误。请参阅 javax.servlet.http.HttpServletResponse 的 Javadoc，以获取有关各种 HTTP 状态码的更多详细信息。返回 HTTP 错误的示例：

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

作为最后的手段，Servlet 可以抛出异常，且该异常必须是以下其中一类的子类：
- RuntimeException
- ServletException
- IOException

[2-b] JSP 错误机制
JSP 页面通过定义 errorPage 伪指令来提供机制，以处理运行时异常，如以下示例所示：

```
    <%@ page errorPage="/errors/userValidation.jsp" %>
```

未捕获的 JSP 异常被转发给指定的 errorPage，并且原始异常设置在名称为 javax.servlet.jsp.jspException 的请求参数中。错误页面必须包括 isErrorPage 伪指令，如下所示：

```
    <%@ page isErrorPage="true" %>
```

isErrorPage 伪指令导致“exception”变量初始化为所抛出的异常对象。
[3] 呈现错误
J2SE Internationalization API 提供使应用程序资源外部化以及将消息格式化的实用程序类，其中包括：

(a) 资源束
(b) 消息格式化

[3-a] 资源束
    资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。资源束通过将本地化数据从使用该数据的源代码中分离来支持国际化。每一资源束都会为特定的语言环境存储键/值对的映射。
java.util.PropertyResourceBundle 将内容存储在外部属性文件中，对其进行使用或扩展都很常见，如以下示例所示：

```
################################################
# ErrorMessages.properties
################################################
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

可定义多种资源，以支持不同的语言环境（因此名为资源束）。例如，可定义 ErrorMessages_fr.properties 以支持该束系列的法语成员。如果请求的语言环境的资源成员不存在，那么会使用缺省成员。在以上示例中，缺省资源是 ErrorMessages.properties。应用程序（JSP 或 Servlet）会根据用户的语言环境从适当的资源检索内容。

[3-b] 消息格式化

J2SE 标准类 java.util.MessageFormat 提供使用替换占位符来创建消息的常规方法。MessageFormat 对象包含嵌入了格式说明符的模式字符串，如下所示：

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

以下是使用 ResourceBundle 和 MessageFormat 来呈现错误消息的更加全面的示例：

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
        // Format the message using the specified placeholders args
        return MessageFormat.format(errorMessage, args);
        } else {
        return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}
...
// Get the user's locale
Locale userLocale = request.getLocale();
```

```
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
```

建议定义定制 JSP 标记（如 displayErrors），以迭代处理并呈现错误消息，如以上示例所示。
[4] 错误映射
通常情况下，“Servlet 容器”会返回与响应状态码或异常相对应的缺省错误页面。可以使用定制错误页面来指定状态码或异常与 Web 资源之间的映射。好的做法是开发不会泄露内部错误状态的静态错误页面（缺省情况下，大部分 Servlet 容器都会报告内部错误消息）。该映射配置在“Web 部署描述符（web.xml）”中，如以下示例所指定：

```
<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
  <exception-type>UserValidationException</exception-type>
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
...
</error-page>
...
```

推荐使用的 JAVA 工具用于服务器端验证的两个主要 Java 框架是：
[1] Jakarta Commons Validator（与 Struts 1.1 集成）Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。Jakarta Commons Validator 是 Java 框架，定义如上所述的错误处理机制。验证规则配置在 XML 文件中，该文件定义了表单字段的输入验证规则以及对应的验证错误密钥。Struts 提供国际化支持以使用资源束和消息格式化来构建本地化应用程序。
使用“Struts 验证器”来验证 loginForm 的 userName 字段的示例：

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
```

```
            <arg0 key="login.userName.displayname"/>
            <var>
            <var-name>mask</var-name>
            <var-value>^[a-zA-Z0-9]*$</var-value>
            </var>
            </field>
            ...
            </form>
            ...
        </formset>
    </form-validation>
```

Struts JSP 标记库定义了有条件地显示一组累计错误消息的“errors”标记，如以下示例所示：

```
    <%@ page language="java" %>
    <%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
    <%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
    <html:html>
    <head>
    <body>
        <html:form action="/logon.do">
        <table border="0" width="100%">
        <tr>
            <th align="right">
            <html:errors property="username"/>
            <bean:message key="prompt.username"/>
            </th>
            <td align="left">
            <html:text property="username" size="16"/>
            </td>
        </tr>
        <tr>
        <td align="right">
            <html:submit><bean:message key="button.submit"/></html:submit>
        </td>
        <td align="right">
            <html:reset><bean:message key="button.reset"/></html:reset>
        </td>
        </tr>
        </table>
        </html:form>
    </body>
    </html:html>
```

[2] JavaServer Faces 技术
“JavaServer Faces 技术”是一组代表 UI 组件、管理组件状态、处理事件、验证输入和支持国际化的 Java API（JSR 127）。

JavaServer Faces API 定义“output_errors”UIOutput 处理器，该处理器显示整个页面的错误消息，或与指定的客户端标识相关联的错误消息。
使用 JavaServer Faces 来验证 loginForm 的 userName 字段的示例：

```
    <%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
    <%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
    ...
    <jsp:useBean id="UserBean"
        class="myApplication.UserBean" scope="session" />
    <f:use_faces>
      <h:form formName="loginForm" >
        <h:input_text id="userName" size="20" modelReference="UserBean.userName">
            <f:validate_required/>
            <f:validate_length minimum="8" maximum="20"/>
        </h:input_text>
        <!-- display errors if present -->
        <h:output_errors id="loginErrors" clientId="userName"/>
        <h:command_button id="submit" label="Submit" commandName="submit" /><p>
      </h:form>
    </f:use_faces>
```

引用
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java 正则表达式包 —
http://jakarta.apache.org/regexp/
Jakarta 验证器 —
http://jakarta.apache.org/commons/validator/
JavaServer Faces 技术 —
http://java.sun.com/j2ee/javaserverfaces/

PHP

** 输入数据验证：** 输入数据验证：虽然为方便用户而在客户端层上提供数据验证，但仍必须始终在服务器层上执行数据验证。客户端验证本身就不安全，因为这些验证可轻易绕过，例如，通过禁用 Javascript。
一份好的设计通常需要 Web 应用程序框架，以提供服务器端实用程序例程，从而验证以下内容：
[1] 必需字段
[2] 字段数据类型（缺省情况下，所有 HTTP 请求参数都是“字符串”）
[3] 字段长度
[4] 字段范围
[5] 字段选项
[6] 字段模式
[7] cookie 值
[8] HTTP 响应好的做法是实现一个或多个验证每个应用程序参数的函数。以下部分描述一些检查的示例。
[1] 必需字段“始终”检查字段不为空，并且其长度要大于零，不包括行距和后面的空格。如何验证必需字段的示例：

```
    // PHP example to validate required fields
    function validateRequired($input) {
        ...
        $pass = false;
        if (strlen(trim($input))>0){
            $pass = true;
        }
        return $pass;
        ...
    }
    ...
    if (validateRequired($fieldName)) {
        // fieldName is valid, continue processing request
        ...
    }
```

[2] 输入的 Web 应用程序中的字段数据类型和输入参数欠佳。例如，所有 HTTP 请求参数或 cookie 值的类型都是“字符串”。开发者负责验证输入的数据类型是否正确。[3] 字段长度“始终”确保输入参数（HTTP 请求参数或 cookie 值）有最小长度和/或最大长度的限制。[4] 字段范围
始终确保输入参数是在由功能需求定义的范围内。
[5] 字段选项 Web 应用程序通常会为用户显示一组可供选择的选项（例如，使用 SELECT HTML 标记），但不能执行服务器端验证以确保选定的值是其中一个允许的选项。请记住，恶意用户能够轻易修改任何选项值。始终针对由功能需

求定义的受允许的选项来验证选定的用户值。[6] 字段模式
始终检查用户输入与由功能需求定义的模式是否匹配。例如，如果 userName 字段应仅允许字母数字字符，且不区分大小写，那么请使用以下正则表达式：^[a-zA-Z0-9]+$

[7] cookie 值
适用于 cookie 值的相同的验证规则（如上所述）取决于应用程序需求（如验证必需值、验证长度等）。
[8] HTTP 响应[8-1] 过滤用户输入要保护应用程序免遭跨站点脚本编制的攻击，开发者应通过将敏感字符转换为其对应的字符实体来清理 HTML。这些是 HTML 敏感字符：< > " ' % ;) (& +

PHP 包含一些自动化清理实用程序函数，如 htmlentities()：

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

此外，为了避免“跨站点脚本编制”的 UTF-7 变体，您应该显式定义响应的 Content-Type 头，例如：

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] 保护 cookie
在 cookie 中存储敏感数据且通过 SSL 来传输时，请确保先在 HTTP 响应中设置 cookie 的安全标志。这将会指示浏览器仅通过 SSL 连接来使用该 cookie。
为了保护 cookie，您可以使用以下代码示例：

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

此外，我们建议您使用 HttpOnly 标志。当 HttpOnly 标志设置为 TRUE 时，将只能通过 HTTP 协议来访问 cookie。这意味着无法用脚本语言（如 JavaScript）来访问 cookie。该设置可有效地帮助减少通过 XSS 攻击盗用身份的情况（虽然并非所有浏览器都支持该设置）。
在 PHP 5.2.0 中添加了 HttpOnly 标志。
引用[1] 使用 HTTP 专用 cookie 来减轻“跨站点脚本编制”的影响：
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP 安全协会：
http://phpsec.org/
[3] PHP 和 Web 应用程序安全博客 (Chris Shiflett)：
http://shiflett.org/

咨询

SQL 盲注

TOC

测试类型：

应用程序级别测试

威胁分类：

SQL 注入

原因：

未对用户输入正确执行危险字符清理

安全性风险：

可能会查看、修改或删除数据库条目和表

受影响产品：

CWE:

89

X-Force：

8783

引用：

“Web Application Disassembly with ODBC Error Messages”（作者：David Litchfield）
“Using Binary Search with SQL Injection”（作者：Sverre H. Huseby）

技术描述：

该软件使用受外部影响的输入来构造 SQL 命令的全部或一部分，但是它未能对可能在 SQL 命令发送到数据库时修改该命令的元素进行无害化处理。如果在用户可控制的输入中没有对 SQL 语法充分地除去或加上引号，那么生成的 SQL 查询可能会导致将这些输入解释为 SQL 而不是普通用户数据。这可用于修改查询逻辑以绕过安全性检查，或者插入其他用于修改后端数据库的语句，可能包括执行系统命令。
例如，假设有一个带有登录表单的 HTML 页面，该页面最终使用用户输入对数据库运行以下 SQL 查询：

```
SELECT * FROM accounts WHERE username='$user' AND password='$pass'
```

这两个变量（$user 和 $pass）包含了用户在登录表单中输入的用户凭证。如果用户输入“jsmith”作为用户名，并输入“Demo1234”作为密码，那么 SQL 查询将如下所示：

```
SELECT * FROM accounts WHERE username='jsmith' AND password='Demo1234'
```

但如果用户输入“'”（单引号）作为用户名，输入“'”（单引号）作为密码，那么 SQL 查询将如下所示：

```
SELECT * FROM accounts WHERE username=''' AND password='''
```

当然，这是格式错误的 SQL 查询，并将调用错误消息，而 HTTP 响应中可能会返回此错误消息。通过此类错误，攻击者会知道 SQL 注入已成功，这样攻击者就会尝试进一步的攻击媒介。SQL 盲注类似于 SQL 注入。不同之处在于，要利用该攻击，攻击者无需寻找响应中的 SQL 错误。因此，AppScan 用于识别该攻击的方法也不同。AppScan 会查找易受 SQL 注入（通过多个请求来操纵应用程序的逻辑，而不是尝试调用 SQL 错误）影响的脚本。

该技巧需要发送特定请求，其中易受攻击的参数（嵌入在 SQL 查询中的参数）进行了相应修改，以便响应中会指示是否在 SQL 查询上下文中使用数据。该修改涉及将 AND 布尔表达式与原始字符串一起使用，使其一时求值为 True，一时求值为 False。在一种情况下，净结果应该与原始结果相同（登录成功），而在另一种情况下，结果应该完全不同（登录失败）。在某些少见的情况下，求值为 True 的 OR 表达式也可能很有用。如果原始数据是数字，可以使用更简单的花招。假设原始数据为 123。此数据可以在一个请求中替换为 0+123，而在另一个请求中替换为 456+123。第一个请求的结果应该与原始结果相同，第二个请求的结果应该不同（因为得出的数字是 579）。在某些情况中，我们仍需要上面所说明的攻击版本（使用 AND 和 OR），但并不转义字符串上下文。

SQL 盲注背后的概念是，即使不直接从数据库接收数据（以错误消息或泄漏的信息的形式），也可能从数据库中抽取数据（每次一个比特），或以恶意方式修改查询。其原理在于，应用程序的行为（返回与原始响应相同或不同的响应）可以提供有关所求值的（已修改）查询的单比特信息，也就是说，攻击者有可能设计出一个 SQL 布尔表达式，其求值（单比特）通过应用程序行为（与原始行为相同/不同）来造成破坏。

SQL 注入

TOC

测试类型：

应用程序级别测试

威胁分类：

SQL 注入

原因：

未对用户输入正确执行危险字符清理

安全性风险：

可能会查看、修改或删除数据库条目和表

受影响产品：

CWE:

89

X-Force：

8783

引用：

“Web Application Disassembly with ODBC Error Messages”（作者：David Litchfield）

技术描述：

该软件使用受外部影响的输入构造整个 SQL 命令或 SQL 命令的一部分，但是会错误的无害化某些特殊元素，这些元素可在所需 SQL命令发送到数据库时对其进行修改。如果在用户可控制的输入中没有对 SQL 语法充分地除去或加上引号，那么生成的 SQL 查询可能会导致将这些输入解释为 SQL 而不是普通用户数据。这可用于修改查询逻辑以绕过安全性检查，或者插入其他用于修改后端数据库的语句，也可能包括执行系统命令。
例如，假设有一个带有登录表单的 HTML 页面，该页面最终使用用户输入对数据库运行以下 SQL 查询：

```
SELECT * FROM accounts WHERE username='$user' AND password='$pass'
```

这两个变量（$user 和 $pass）包含了用户在登录表单中输入的用户凭证。因此，如果用户输入“jsmith”作为用户名，输入“Demo1234”作为密码，那么 SQL 查询将如下所示：

```
SELECT * FROM accounts WHERE username='jsmith' AND password='Demo1234'
```

但如果用户输入“”（单引号）作为用户名，输入“”（单引号）作为密码，那么 SQL 查询将如下所示：

```
SELECT * FROM accounts WHERE username=''' AND password='''
```

当然，这是格式错误的 SQL 查询，并将调用错误消息，而 HTTP 响应中可能会返回此错误消息。通过此类错误，攻击者会知道 SQL 注入已成功，这样攻击者就会尝试进一步的攻击媒介。利用的样本：
以下 C# 代码会动态构造并执行 SQL 代码来搜索与指定名称匹配的项。该查询将所显示的项限制为其所有者与当前已认证用户的用户名相匹配的项。

```
...
string userName = ctx.getAuthenticatedUserName();
string query = "SELECT * FROM items WHERE owner = "'"
                              + userName + "' AND itemname = '"
                              + ItemName.Text + "'";
sda = new SqlDataAdapter(query, conn);
DataTable dt = new DataTable();
sda.Fill(dt);
...
```

此代码打算执行的查询如下所示：

```
SELECT * FROM items WHERE owner =  AND itemname = ;
```

不过，由于该查询是通过将常量基本查询字符串和用户输入字符串进行并置来自动构造而成，因此仅当 itemName 不包含单引号字符时，查询才会正常工作。如果用户名为 wiley 的攻击者针对 itemName 输入字符串“name' OR 'a'='a”，那么查询将变为以下内容：

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name' OR 'a'='a';
```

添加 OR 'a'='a' 条件导致 where 子句始终求值为 true，因此该查询在逻辑上将变为等价于以下更简单的查询：

```
SELECT * FROM items;
```

跨站点脚本编制

TOC

测试类型：

应用程序级别测试

威胁分类：

跨站点脚本编制

原因：

未对用户输入正确执行危险字符清理

安全性风险：

受影响产品：

CWE:

79

X-Force：

6784

引用：

CERT Advisory CA-2000-02
微软如何在 ASP.NET 中防止跨站点脚本编制
微软如何在 ASP.NET 中防止注入攻击
微软如何在 ASP.NET 中使用正则表达式限制输入

技术描述：

AppScan 检测到应用程序在将用户可控输入放入作为网页的输出中之前未正确中和该用户可控输入。
这可能被用于跨站点脚本编制攻击中。
在以下情况下会出现跨站点脚本编制 (XSS) 漏洞：
[1] Web 应用程序中输入不可信数据，通常来自 Web 请求。
[2] Web 应用程序动态生成一个包含这些不可信数据的网页。
[3] 在页面生成期间，应用程序没有阻止数据包含 Web 浏览器可执行的内容，如 JavaScript、HTML 标记、HTML 属性、鼠标事件、Flash、ActiveX。
[4] 受害者通过 Web 浏览器访问生成的网页，该网页包含使用不可信数据注入的恶意脚本。
[5] 因为脚本来自 Web 服务器发送的网页，所以受害者的 Web 浏览器会在 Web 服务器的域环境中执行该恶意脚本。
[6] 这实际上违反了 Web 浏览器同源策略的意图，同源策略声明一个域中的脚本不能在另一个域中访问资源或运行代码。
注入恶意脚本后，攻击者便可以进行各种恶意活动了。攻击者可以将私人信息（如可能包含会话信息的 cookie）从受害机器发送给攻击者。攻击者可以用受害者的身份向网站发送恶意请求，如果受害者拥有管理该网站的管理员权限，则这可能对网站特别危险。
钓鱼攻击可用于模仿可信网站并哄骗受害者输入密码，从而允许攻击者在该网站上盗用受害者的帐户。最后，该脚本可以攻击 Web 浏览器本身的漏洞，从而可能接管受害者的机器（有时被称为“路过式入侵”）。
XSS 有三种主要类型：
类型 1：反射型 XSS（也称为“非持久性”）
服务器直接从 HTTP 请求读取数据并在 HTTP 响应中将其反射回去。攻击者导致受害者向易受攻击的 Web 应用程序提供危险内容时，会发生反射型 XSS 攻击，这些危险内容之后会反射回给受害者并由 Web 浏览器执行。提供恶意内容的最常见途径是将恶意内容作为参数包含在公开发布的 URL 中，或者直接通过电子邮件发送给受害者。以这种方式构建的 URL 构成了许多网络钓鱼方案的核心，攻击者借此说服受害者访问易受攻击站点的 URL。在该站点将攻击者的内容反射回给受害者后，受害者的浏览器会执行这些内容。
类型 2：存储型 XSS（也称为“持久性”）
应用程序在数据库、消息论坛、访问者日志或其他可信数据存储中存储危险数据。稍后，应用程序会重新读取这些危险数据并将其包含在动态内容中。从攻击者的角度来说，注入恶意内容的最佳位置位于面向许多用户或攻击者特别感兴趣的用户显示的区域。攻击者感兴趣的用户通常拥有应用程序的提升特权，或者能与易受攻击者攻击的敏感数据互动。如果这些用户之一执行了恶意内容，则攻击者就可能能够以该用户的身份执行特权操作，或者获得访问属于该用户的敏感数据的权限。例如，攻击者可能将 XSS 注入管理员查看日志时可能没有正确处理的日志消息中。
类型 0：基于 DOM 的 XSS
在基于 DOM 的 XSS 中，由客户机执行页面中的 XSS 注入；而在其他类型 XSS 中，则由服务器执行注入。基于 DOM 的 XSS 通常涉及发送给客户机的受服务器控制的可信脚本，如在用户提交表单之前对表单执行完整性检查的 Javascript。如果服务器提供的脚本处理用户提供的数据，然后再将这些数据注入回网页（如使用动态 HTML）中，则可能会发生基于 DOM 的 XSS 攻击。
下面的示例显示了一个在响应中返回了一个参数值的脚本。
该参数值通过使用 GET 请求发送给该脚本，然后在响应中嵌入在 HTML 中返回。

```
[REQUEST]
GET /index.aspx?name=JSmith HTTP/1.1
```

```
[RESPONSE]
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 27

<HTML>
Hello JSmith
</HTML>
```

攻击者可能利用类似这样的攻击：

```
[ATTACK REQUEST]
GET /index.aspx?name=>"'><script>alert('PWND')</script> HTTP/1.1
```

```
[ATTACK RESPONSE]
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 83

<HTML>
Hello >"'><script>alert('PWND')</script>
</HTML>
```

在这种情况下，JavaScript 代码将由浏览器执行（在此处 **>"'>** 部分不相关）。

通过 URL 重定向网络钓鱼

TOC

测试类型：

应用程序级别测试

威胁分类：

URL 重定向滥用

原因：

Web 应用程序执行指向外部站点的重定向

安全性风险：

可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品：

CWE:

601

X-Force：

52830

引用：

FTC Consumer Alert -“How Not to Get Hooked by a 'Phishing' Scam”

技术描述：

网络钓鱼是一种社会工程技巧，其中攻击者伪装成受害者可能会与其进行业务往来的合法实体，以便提示用户透露某些机密信息（往往是认证凭证），而攻击者以后可以利用这些信息。网络钓鱼在本质上是一种信息收集形式，或者说是对信息的“渔猎”。
某个 HTTP 参数被发现保存有 URL 值，并导致 Web 应用程序将请求重定向至指定的 URL。攻击者可以将 URL 值改成指向恶意站点，从而顺利启用网络钓鱼欺骗并窃得用户凭证。
事实上，已修改的链接中的服务器名称与原始站点的服务器名称相同，这可为攻击者的网络钓鱼尝试提供更可靠的外观，从而帮助了攻击者。

跨站点请求伪造

TOC

测试类型：

应用程序级别测试

威胁分类：

跨站点请求伪造

原因：

应用程序使用的认证方法不充分

安全性风险：

可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务

受影响产品：

CWE:

352

X-Force：

6784

引用：

跨站点伪造请求 Wiki 页面
“JavaScript 劫持”，作者：Fortify

技术描述：

即使是格式正确、有效且一致的请求也可能已在用户不知情的情况下发送。因此，Web 应用程序应检查所有请求以发现其不合法的迹象。此测试的结果指示所扫描的应用程序没有执行此操作。此脆弱性的严重性取决于受影响应用程序的功能。例如，对搜索页面的 CSRF 攻击的严重性低于对转账或概要文件更新页面的 CSRF 攻击。如果某个 Web 服务器设计为接收客户机的请求时无任何机制来验证该请求是否确实是客户机发送的，那么攻击者就有可能诱导客户机向该 Web 服务器误发请求，而该请求将视为真实请求。这可通过 URL、图像装入、XMLHttpRequest 等来完成，并可导致数据暴露或意外的代码执行。如果用户当前已登录到受害者站点，请求将自动使用用户的凭证（包括会话 cookie、IP 地址和其他浏览器认证方法）。通过使用此方法，攻击者可伪造受害者的身份，并以其身份提交操作。

使用 HTTP 动词篡改的认证旁路

TOC

测试类型：

应用程序级别测试

威胁分类：

认证不充分

原因：

Web 应用程序编程或配置不安全

安全性风险：

- 可能会升级用户特权并通过 Web 应用程序获取管理许可权
- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

CWE:

287

引用：

通过 HTTP 动词篡改绕过 VBAAC
Http 动词篡改 - 绕过 Web 认证和授权

技术描述：

很多 web 服务器都允许使用 HTTP 方法（也称为动词）来配置访问控制，从而支持使用一种或多种方法进行访问。问题在于这些配置实现中的很多都允许访问未在访问控制规则中列出的方法，从而导致访问控制违规。利用的样本如下：
BOGUS /some_protected_resource.html HTTP/1.1
host: www.vulnerable_site.com

“Content-Security-Policy”头缺失或不安全

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
-

受影响产品：

CWE:

200

引用：

有用 HTTP 头列表
内容安全策略简介
MDN Web 文档 - 内容安全策略

技术描述：

“内容安全策略”标头旨在修改浏览器呈现页面的方式，从而防止各种跨站点注入，包括跨站点脚本。以不妨碍网站正常运行的方式正确设置标头值非常重要。例如，如果将标头设置为阻止执行内联 JavaScript，则网站不得在其页面中使用内联 JavaScript。
为了防止跨站点脚本、跨框架脚本和点击劫持，使用适当的值设置以下策略非常重要：
'default-src' 和 'frame-ancestors'策略、*或*所有 'script-src'、'object-src' 和 'frame-ancestors’ 策略。
对于 'default-src'、'script-src' 和 'object-src'，应避免使用不安全的值，例如 '*'、'data:'、'unsafe-inline' 或 'unsafe-eval'。
对于 'frame-ancestors'，应避免使用不安全的值，例如 '*' 或 'data:'。
有关更多信息，请参阅以下链接。

JavaScript 劫持

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

应用程序使用的认证方法不充分

安全性风险：

可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

CWE:

352

X-Force：

52661

引用：

“JavaScript Hijacking”作者：FortifySoftware

技术描述：

原始咨询如下：

“Web 浏览器施行“同源策略”来保护用户免受恶意 Web 站点的侵害。
“同源策略”要求：JavaScript 若要访问 Web 页面内容，JavaScript 和 Web 页面必须源于相同域。 如果没有“同源策略”，恶意 Web 站点所提供的 JavaScript 便可以通过客户端的凭证来装入其他 Web 站点的敏感信息，挑选这些信息，再返回给攻击者。

当 Web 应用程序利用 JavaScript 来传递机密信息时，“JavaScript 劫持”可让攻击者绕过“同源策略”。 “同源策略”的漏洞是它允许在任何其他 Web站点的环境中，包含并执行任何 Web 站点的 JavaScript。 虽然恶意站点无法直接在客户端检查从易受攻击的站点装入的任何数据，但它通过设置一个环境来观察 JavaScript 的执行状况及其可能产生的任何相关副作用，便能对该漏洞加以利用。 由于许多 Web 2.0 应用程序都利用 JavaScript 作为数据传输机制，它们通常都易受攻击，而传统的 Web 应用程序反而不易受攻击。

“JavaScript 对象表示法 (JSON)”是使用 JavaScript 传递信息的最流行格式。 JSON RFC 将 JSON 语法定义为 JavaScript 对象字面值语法的子集。 JSON 基于两类数据结构：数组和对象。 任何能够将消息解释为一或多个有效 JavaScript 语句的数据传输格式，都很容易遭受“JavaScript 劫持”。 JSON 使得“JavaScript 劫持”更加容易，因为 JSON 数组本身就是有效的 JavaScript 语句。 由于数组是用来传达列表的自然形式，因此，在应用程序需要传递多值的任何场合中，通常都会使用数组。 换言之，JSON 数组正好容易直接遭受“JavaScript 劫持”。 只有在包装于本身就是有效 JavaScript 语句的其他 JavaScript 构造中时，JSON 对象才容易受攻击。”由于 JavaScript 劫持攻击的特性，要求为执行 JavaScript 页面设置环境，只有纯 JavaScript（或 JSON）页面容易受 JavaScript 劫持。
换言之，只有可以执行的页面容易被 JavaScript 劫持攻击。
另一方面，如果 JavaScript 部分嵌入到 HTML 页面或任何其他非 JavaScript 文本中，那么此页面不会遭受该技术的攻击。

查询中接受的主体参数

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
- 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息

受影响产品：

CWE:

200

引用：

超文本传输协议 (HTTP/1.1) 语义和内容：
GET
POST

技术描述：

GET 请求设计的目的在于查询服务器，而 POST 请求用于提交数据。但是，除了技术目的之外，攻击查询参数比攻击主体参数更容易，因为向原始站点发送链接或在博客或注释中发布链接更容易，而且得到的结果比另一种方法更好，为了攻击带有主体参数的请求，攻击者需要创建其中包含表单的页面，当受害者访问表单时就会提交表单。
说服受害者访问他不了解的页面比让受害者访问原始站点要难很多。因此，不建议支持可到达查询字符串的主体参数。

发现 Web 应用程序源代码泄露模式

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

- 未安装第三方产品的最新补丁或最新修订程序
- 在生产环境中留下临时文件
- 程序员在 Web 页面上留下调试信息

安全性风险：

可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息

受影响产品：

CWE:

540

X-Force：

52479

技术描述：

AppScan 检测到含有应用程序源代码片段的响应。Web 用户不应具有访问应用程序源代码的能力，因为它可能含有敏感的应用程序信息及后端逻辑。
虽然这类泄漏不一定代表安全的违规，但它为攻击者提供了有用的指导，以进行进一步利用。
泄漏敏感信息可能带来不同级别的风险，应该尽可能加以限制。

发现数据库错误模式

TOC

测试类型：

应用程序级别测试

威胁分类：

SQL 注入

原因：

未对用户输入正确执行危险字符清理

安全性风险：

可能会查看、修改或删除数据库条目和表

受影响产品：

CWE:

209

X-Force：

52577

引用：

“Web Application Disassembly with ODBC Error Messages”（作者：David Litchfield）

技术描述：

AppScan 在测试响应中发现数据库错误，该错误可能已被“SQL 注入”以外的攻击所触发。
虽然不确定，但这个错误可能表示应用程序有“SQL 注入”漏洞。
若是如此，请仔细阅读下列“SQL 注入”咨询。该软件使用受外部影响的输入构造整个 SQL 命令或 SQL 命令的一部分，但是会错误的无害化某些特殊元素，这些元素可在所需 SQL命令发送到数据库时对其进行修改。如果在用户可控制的输入中没有对 SQL 语法充分地除去或加上引号，那么生成的 SQL 查询可能会导致将这些输入解释为 SQL 而不是普通用户数据。这可用于修改查询逻辑以绕过安全性检查，或者插入其他用于修改后端数据库的语句，也可能包括执行系统命令。
例如，假设有一个带有登录表单的 HTML 页面，该页面最终使用用户输入对数据库运行以下 SQL 查询：

```
SELECT * FROM accounts WHERE username='$user' AND password='$pass'
```

这两个变量（$user 和 $pass）包含了用户在登录表单中输入的用户凭证。因此，如果用户输入“jsmith”作为用户名，输入“Demo1234”作为密码，那么 SQL 查询将如下所示：

```
SELECT * FROM accounts WHERE username='jsmith' AND password='Demo1234'
```

但如果用户输入“'”（单引号）作为用户名，输入“'”（单引号）作为密码，那么 SQL 查询将如下所示：

```
SELECT * FROM accounts WHERE username=''' AND password='''
```

当然，这是格式错误的 SQL 查询，并将调用错误消息，而 HTTP 响应中可能会返回此错误消息。通过此类错误，攻击者会知道 SQL 注入已成功，这样攻击者就会尝试进一步的攻击媒介。利用的样本：
以下 C# 代码会动态构造并执行 SQL 代码来搜索与指定名称匹配的项。该查询将所显示的项限制为其所有者与当前已认证用户的用户名相匹配的项。

```
...
string userName = ctx.getAuthenticatedUserName();
string query = "SELECT * FROM items WHERE owner = "'"
                              + userName + "' AND itemname = '"
                              + ItemName.Text + "'";
sda = new SqlDataAdapter(query, conn);
DataTable dt = new DataTable();
sda.Fill(dt);
...
```

此代码打算执行的查询如下所示：

```
SELECT * FROM items WHERE owner =  AND itemname = ;
```

不过，由于该查询是通过将常量基本查询字符串和用户输入字符串进行并置来自动构造而成，因此仅当 itemName 不包含单引号字符时，查询才会正常工作。如果用户名为 wiley 的攻击者针对 itemName 输入字符串“name' OR 'a'='a”，那么查询将变为以下内容：

```
SELECT * FROM items WHERE owner = 'wiley' AND itemname = 'name' OR 'a'='a';
```

添加 OR 'a'='a' 条件导致 where 子句始终求值为 true，因此该查询在逻辑上将变为等价于以下更简单的查询：

```
SELECT * FROM items;
```

跨帧脚本编制防御缺失或不安全

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

- 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
-

受影响产品：

CWE:

693

引用：

跨帧脚本编制
Clickjacking

技术描述：

跨帧脚本编制是一种攻击技术，攻击者利用这种技术在其恶意网站上的 iFrame 中加载易受攻击的应用程序。
然后，攻击者可以发起 Clickjacking 攻击，这可能导致网络钓鱼、跨网站请求伪造、敏感信息泄露等。
为实现最佳保护，建议将报头值设置为 DENY 或 SAMEORIGIN。

示例攻击：
在恶意网站中，可以嵌入易受攻击的网页：
<frame src="http://vulnerable.com/login.html">

自动填写未对密码字段禁用的 HTML 属性

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

可能会绕开 Web 应用程序的认证机制

受影响产品：

CWE:

522

X-Force：

85989

技术描述：

“autocomplete”属性已在 HTML5 标准中进行规范。W3C 的站点声明该属性有两种状态：“on”和“off”，完全忽略时等同于设置为“on”。
该页面易受攻击，因为“input”元素的“password”字段中的“autocomplete”属性没有设置为“off”。
这可能会使未授权用户（具有授权客户机的本地访问权）能够自动填写用户名和密码字段，并因此登录站点。

HTML 注释敏感信息泄露

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

程序员在 Web 页面上留下调试信息

安全性风险：

可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

CWE:

615

X-Force：

52601

引用：

WASC 威胁分类：信息泄露

技术描述：

很多 Web 应用程序程序员使用 HTML 注释，以在需要时帮助调试应用程序。尽管添加常规注释有助于调试应用程序，但一些程序员往往会遗留重要数据（例如：与 Web 应用程序相关的文件名、旧的链接或原非供用户浏览的链接、旧的代码片段等）。

发现电子邮件地址模式

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

CWE:

359

X-Force：

52584

引用：

Spambot 的定义（维基百科）

技术描述：

Spambot 搜寻因特网站点，开始查找电子邮件地址来构建发送自发电子邮件（垃圾邮件）的邮件列表。
AppScan 检测到含有一或多个电子邮件地址的响应，可供利用以发送垃圾邮件。
而且，找到的电子邮件地址也可能是专用电子邮件地址，对于一般大众应是不可访问的。

发现可能的服务器路径泄露模式

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

未安装第三方产品的最新补丁或最新修补程序

安全性风险：

可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息

受影响产品：

CWE:

200

X-Force：

52839

技术描述：

AppScan 检测到包含文件绝对路径的响应（例如，Windows 中的 c:\dir\file，或 Unix 中的 /dir/file）。

攻击者可能能够利用这一信息访问服务器机器目录结构上的敏感信息，进而对站点发起进一步攻击。

发现内部 IP 泄露模式

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Web 应用程序编程或配置不安全

安全性风险：

可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置

受影响产品：

CWE:

200

X-Force：

52657

技术描述：

AppScan 检测到包含内部 IP 地址的响应。
内部 IP 定义为以下 IP 范围内的 IP：
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

内部 IP 公开对于攻击者非常有价值，因为它揭示了内部网络的 IP 联网模式。获知内部网络的 IP 联网模式可能会帮助攻击者计划针对内部网络的进一步攻击。

客户端（JavaScript）Cookie 引用

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

Cookie 是在客户端创建的

安全性风险：

此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色

受影响产品：

CWE:

602

X-Force：

52514

引用：

WASC 威胁分类：信息泄露

技术描述：

cookie 是一则信息，通常由 Web 服务器创建并存储在 Web 浏览器中。
web 应用程序主要（但不只是）使用 cookie 包含的信息来识别用户并维护用户的状态。
AppScan 检测到客户端上的 JavaScript 代码用于操控（创建或修改）站点的 cookie。
攻击者有可能查看此代码、了解其逻辑并根据所了解的知识将其用于组成其自己的 cookie，或修改现有 cookie。
攻击者可能导致的损坏取决于应用程序使用其 cookie 的方式或应用程序存储在这些 cookie 中的信息内容。
此外，cookie 操控还可能导致会话劫持或特权升级。
由 cookie 毒害导致的其他漏洞包含 SQL 注入和跨站点脚本编制。

应用程序错误

TOC

测试类型：

应用程序级别测试

威胁分类：

信息泄露

原因：

- 未对入局参数值执行适当的边界检查
- 未执行验证以确保用户输入与预期的数据类型匹配

安全性风险：

可能会收集敏感的调试信息

受影响产品：

CWE:

550

X-Force：

52502

引用：

使用单引号入侵站点的示例，可参阅“How I hacked PacketStorm (by Rain Forest Puppy), RFP's site”
“Web Application Disassembly with ODBC Error Messages”（作者：David Litchfield）
CERT 咨询（CA-1997-25）：清理 CGI 脚本中用户提供的数据

技术描述：

如果攻击者通过伪造包含非应用程序预期的参数或参数值的请求，来探测应用程序（如以下示例所示），那么应用程序

可能会进入易受攻击的未定义状态。 攻击者可以从应用程序对该请求的响应中获取有用的信息，且可利用该信息，以找出应用程序的弱点。

例如，如果参数字段是单引号括起来的字符串（如在 ASP 脚本或 SQL 查询中），那么注入的单引号将会提前终止字符串流，从而更改脚本的正常流程/语法。

错误消息中泄露重要信息的另一个原因，是脚本编制引擎、Web 服务器或数据库配置错误。

以下是一些不同的变体：

[1] 除去参数

[2] 除去参数值

[3] 将参数值设置为空值

[4] 将参数值设置为数字溢出（+/- 99999999）

[5] 将参数值设置为危险字符，如 ' " \' \") ;

[6] 将某字符串附加到数字参数值

[7] 在参数名称后追加“.”（点）或“[]”（尖括号）

应用程序数据

已访问的 URL 218

TOC

URL
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
http://127.0.0.1:8000/xmjg/login
http://127.0.0.1:8090/opus-front-sso/oauth/authorize?client_id=xmjg&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=tba1ER
http://127.0.0.1:8090/opus-front-sso/authentication/require
http://127.0.0.1:8090/opus-front-sso/js/jquery-3.4.1.min.js
http://127.0.0.1:8090/opus-front-sso/js/layui.all.js
http://127.0.0.1:8090/opus-front-sso/js/jquery.validate.min.js
http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/scripts.bundle.js
http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/jquery.cookie.js
http://127.0.0.1:8090/opus-front-sso/js/login.js
http://127.0.0.1:8090/opus-front-sso/js/md5.js
http://127.0.0.1:8090/opus-front-sso/js/sm3/sm3.js
http://127.0.0.1:8090/opus-front-sso/js/base64.js
http://127.0.0.1:8090/opus-front-sso/js/sm4.js
http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/jquery.mousewheel.min.js
http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/vendors.bundle.js
http://127.0.0.1:8090/opus-front-sso/authentication/form
http://127.0.0.1:8000/xmjg/agcloud/framework/js-lib/jquery-v1/jquery.min.js
http://127.0.0.1:8000/xmjg/login?code=Hu24Qr&state=tba1ER
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
http://127.0.0.1:8000/xmjg/agcloud/framework/js-lib/vue-v2/vue.js
http://127.0.0.1:8000/xmjg/common/tool/common-merge.js
http://127.0.0.1:8000/xmjg/agcloud/framework/js-lib/element-2/element.js
http://127.0.0.1:8000/xmjg/agcloud/framework/js-lib/agcloud-lib/js/common.js
http://127.0.0.1:8000/xmjg/agcloud/framework/ui-schemes/dark-blue/js/index.js
http://127.0.0.1:8000/xmjg/agcloud/login/js/sm3-sm4-md5-base64-merge.js
http://127.0.0.1:8000/xmjg/xmjg/xmjg-project-info!getScreen.action
http://127.0.0.1:8000/xmjg/index/getSystemName
http://127.0.0.1:8000/xmjg/opus/front/om/users/currOpusLoginUser?time=1609207807040
http://127.0.0.1:8000/xmjg/opus/front/om/users?loginName=admin&time=1609207807212

http://127.0.0.1:8000/xmjg/opus/front/om/users/user/10000/allMenus?isTree=true&netName=前端网络入口&tmnId=1&topOrgId=A&userId=10000&time=1609207807212

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js

http://127.0.0.1:8000/xmjg/common/tool/date/js/bootstrap.min.js

http://127.0.0.1:8000/xmjg/common/tool/date/js/bootstrap-datepicker.min.js

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/dg-jdkh-main.js

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/numberAnimate.js

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/echarts.min.js

http://127.0.0.1:8000/xmjg/common/tool/cityselect/js/city_data.js

http://127.0.0.1:8000/xmjg/common/tool/cityselect/js/areadata.js

http://127.0.0.1:8000/xmjg/common/tool/cityselect/js/auto_area.js

http://127.0.0.1:8000/xmjg/region/vue.min.js

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/element.js

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/indexMap.js

http://127.0.0.1:8000/xmjg/analysis-info!getPilotCity.action

http://127.0.0.1:8000/xmjg/mapShowConfig.do

http://127.0.0.1:8000/xmjg/xmjg-project-info/getProvinceAuthority

http://127.0.0.1:8000/xmjg/supervisionInspection/getProvinceTopFive.do?province=660000&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/supervisionInspection/getYsTotalOfMultidimensional.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29&spysDy0=

http://127.0.0.1:8000/xmjg/analysis-info!getHaveProjectCitys.action

http://127.0.0.1:8000/xmjg/supervisionInspection/getMapCountryAndProvinceXms.do?xzqhdm=660000&tjfs=xmsl&cityType=province&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/supervisionInspection/getYslAndXzblxms.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action

http://127.0.0.1:8000/xmjg/supervisionInspection/getMergeData.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/xmjg-project-info!getMapConfigData.action?bigScreenFolder=

http://127.0.0.1:8000/xmjg/xmjg/xndc/map/mapJson/abbrMapJson/province/66.json

http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=8&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29

http://127.0.0.1:8000/xmjg/common/tool/common-core.js

http://127.0.0.1:8000/xmjg/common/tool/projectManager.js

http://127.0.0.1:8000/xmjg/common/tool/common.js

http://127.0.0.1:8000/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js

http://127.0.0.1:8000/xmjg/xmjg/xndc/js/common-charts.js

http://127.0.0.1:8000/xmjg/common/tool/date/js/dateQuery.js

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/analysis-ranking-stage.js

http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=

http://127.0.0.1:8000/xmjg/xmjg/xndc/js/jquery-2.1.0.min.js

http://127.0.0.1:8000/xmjg/xmjg/xndc/js/echarts.min.js

http://127.0.0.1:8000/xmjg/resources/js/common/validate.js http://127.0.0.1:8000/xmjg/resources/js/common/public.js

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/city-project-stage-list.js

http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=&xmmc=&cityxzqh=660700&orderBy=&orderDir=&pageNo=2

http://127.0.0.1:8000/xmjg/supervisionInspection/getProvinceTopFive.do?province=&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/supervisionInspection/getProvinceTopFive.do?province=getTopFiveCity&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/resources/js/jquery/jquery.js

http://127.0.0.1:8000/xmjg/resources/easyui/easycore.js

http://127.0.0.1:8000/xmjg/resources/js/dghy/index.js

http://127.0.0.1:8000/xmjg/dghyindex/js/index-dghy-main.js

http://127.0.0.1:8000/xmjg/dghyindex/js/dghy-public.js

http://127.0.0.1:8000/xmjg/resources/easyui/locale/easyui-lang-zh_CN.js

http://127.0.0.1:8000/xmjg/resources/easyui/jquery.easyui.min.js

http://127.0.0.1:8000/xmjg/resources/easyui/jquery.min.js

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.6466467024008973

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action?bigScreenFolder=&name=一师阿拉尔市&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/region/vue.js

http://127.0.0.1:8000/xmjg/xmjg/xndc/js/bootstrap.min.js

http://127.0.0.1:8000/xmjg/xmjg/xndc/js/bootstrap-datepicker.min.js

http://127.0.0.1:8000/xmjg/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js

http://127.0.0.1:8000/xmjg/xmjg/csrk/js/echarts.min.js

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/city-page.js

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-table.js

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-table-zh-CN.js

http://127.0.0.1:8000/xmjg/city-page/getCountyMapData.do?xzqhdm=660100&tjfs=xmsl&startDate=&endDate=

http://127.0.0.1:8000/xmjg/bsc/dic/code/lgetItemsByTypeCode.do?typeCode=TJ_DATE_CONFIG&flag=false

http://127.0.0.1:8000/xmjg/city-page/getJdxms.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/city-page/getQqxtCount.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/supervisionInspection/getJdbjs.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/city-page/getProjectCount.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/supervisionInspection/getAllPjysByTjjssj.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29

http://127.0.0.1:8000/xmjg/city-page/getSPPJSLCS.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
http://127.0.0.1:8000/xmjg/city-page/getDataListOfSplcbm.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
http://127.0.0.1:8000/xmjg/city-page/getGjdspblqk.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
http://127.0.0.1:8000/xmjg/city-page/getCountyMapData.do?xzqhdm=660100&tjfs=xmsl&startDate=2020-01-01&endDate=2020-12-29
http://127.0.0.1:8000/xmjg/xmjg/xndc/map/mapJson/city/660100.json
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.212760996225412
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.051773143618017325
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660100&dataType=12&name=一师阿拉尔市&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splcmc=&splclx=&sfType=
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=5&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splcmc=&splclx=
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do
http://127.0.0.1:8000/xmjg/xmjg-city-map-config!getMapurlByXzqhdm.action?xzqhdm=660100&accessEntry=城市首页
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do?city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29&provinceCode=
http://127.0.0.1:8000/xmjg/xmjg/js/jquery.min.js
http://127.0.0.1:8000/xmjg/xmjg/xndc/js/dg-md-xndc-main.js
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByXzqhdm2.action?xzqhdm=660100
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSxlx.action?xzqhdm=660100
http://127.0.0.1:8000/xmjg/xmjg-project-info!getLct.action?xzqhdm=660100&cityName=一师阿拉尔市
http://127.0.0.1:8000/xmjg/city/getMDAllSpjd.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-31
http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do
http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-31
http://127.0.0.1:8000/xmjg/xmjg-one-window!getYgck.action?name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
http://127.0.0.1:8000/xmjg/xmjg/xndc/js/DateUtils.js
http://127.0.0.1:8000/xmjg/xmjg/ygck/js/ygck.js
http://127.0.0.1:8000/xmjg/xmjg-one-window!getXmjgEditor.action?xzqhdm=660100
http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action?name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29
http://127.0.0.1:8000/xmjg/bootstrap/js/jquery.min.js
http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap.js
http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-common.js
http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-datetimepicker.js
http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrapValidator.js
http://127.0.0.1:8000/xmjg/bootstrap/js/toastr.js
http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-editable.js
http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-table-editable.js

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-treeview.js
http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-combotree.js
http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-select.js
http://127.0.0.1:8000/xmjg/bootstrap/js/jquery.eeyellow.Timeline.js
http://127.0.0.1:8000/xmjg/resources/js/common/tool.js
http://127.0.0.1:8000/xmjg/adsfw/sysfile/public/attachment-operation.js
http://127.0.0.1:8000/xmjg/adswf/engine/public/public.js
http://127.0.0.1:8000/xmjg/handsontable-master/dist/handsontable.full.js
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByXzqhdm.action?xzqhdm=660100
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSpjdByxmlx.action?xzqhdm=660100&splclx=1&splcbbh=1&splcmc=政府投资房屋建筑类项目&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783
http://127.0.0.1:8000/xmjg/xmjg-project-info!getGeLeiXingXiangMuCanShuByXzqhdm.action?xzqhdm=660100&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783&splcbbh=1&splclx=1&startDate=&endDate=
http://127.0.0.1:8000/xmjg/xmjg-gzgl-oneform-tabname!getTabName.action?xzqhdm=660100&xmlxbh=1&spjdbh=1
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByParamsMap.action?xzqhdm=660100&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783
http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=d4ba4952-9be6-4a10-9431-7a099bf5e783&spjdbh=1&bgbh=1&splcbbh=1
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html?file= /xmjg/file/yzbd/yishialaer/pdf/7fa992eb-5923-419b-9cbc-612db98522ba※一阶段办事指南.pdf
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/build/pdf.js
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.js
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/build/pdf.worker.js
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSpjdByxmlx.action?xzqhdm=660100&splclx=2&splcbbh=1&splcmc=政府投资城市基础设施工程类项目&splcbm=5e6d7d7b-be47-4092-b8d9-c873cd74a8ae
http://127.0.0.1:8000/xmjg/xmjg-project-info!getGeLeiXingXiangMuCanShuByXzqhdm.action?xzqhdm=660100&splcbm=5e6d7d7b-be47-4092-b8d9-c873cd74a8ae&splcbbh=1&splclx=2&startDate=&endDate=
http://127.0.0.1:8000/xmjg/xmjg-gzgl-oneform-tabname!getTabName.action?xzqhdm=660100&xmlxbh=2&spjdbh=1
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByParamsMap.action?xzqhdm=660100&splcbm=5e6d7d7b-be47-4092-b8d9-c873cd74a8ae
http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=5e6d7d7b-be47-4092-b8d9-c873cd74a8ae&spjdbh=1&bgbh=1&splcbbh=1
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSpjdByxmlx.action?xzqhdm=660100&splclx=3&splcbbh=1&splcmc=一般社会投资项目（不含带方案出让用地项目和小型社会投资项目）&splcbm=d21d7468-ca0c-478c-b700-e086340478e0
http://127.0.0.1:8000/xmjg/xmjg-project-info!getGeLeiXingXiangMuCanShuByXzqhdm.action?xzqhdm=660100&splcbm=d21d7468-ca0c-478c-b700-e086340478e0&splcbbh=1&splclx=3&startDate=&endDate=
http://127.0.0.1:8000/xmjg/xmjg-gzgl-oneform-tabname!getTabName.action?xzqhdm=660100&xmlxbh=3&spjdbh=1
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByParamsMap.action?xzqhdm=660100&splcbm=d21d7468-ca0c-478c-b700-e086340478e0
http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=d21d7468-ca0c-478c-b700-e086340478e0&spjdbh=1&bgbh=1&splcbbh=1
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSpjdByxmlx.action?xzqhdm=660100&splclx=4&splcbbh=1&splcmc=社会投资小型工程项目&splcbm=0cce535b-bc83-4a61-be72-3d151e1a16e1
http://127.0.0.1:8000/xmjg/xmjg-project-info!getGeLeiXingXiangMuCanShuByXzqhdm.action?xzqhdm=660100&splcbm=0cce535b-bc83-4a61-be72-3d151e1a16e1&splcbbh=1&splclx=4&startDate=&endDate=
http://127.0.0.1:8000/xmjg/xmjg-gzgl-oneform-tabname!getTabName.action?xzqhdm=660100&xmlxbh=4&spjdbh=1
http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=0cce535b-bc83-4a61-be72-3d151e1a16e1&spjdbh=1&bgbh=1&splcbbh=1
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByParamsMap.action?xzqhdm=660100&splcbm=0cce535b-bc8

3-4a61-be72-3d151e1a16e1
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSpjdByxmlx.action?xzqhdm=660100&splclx=5&splcbbh=1&splcmc=含带方案出让用地的社会投资项目&splcbm=92c57c71-4a4a-4768-8888-97efcae9d5c4
http://127.0.0.1:8000/xmjg/xmjg-project-info!getGeLeiXingXiangMuCanShuByXzqhdm.action?xzqhdm=660100&splcbm=92c57c71-4a4a-4768-8888-97efcae9d5c4&splcbbh=1&splclx=5&startDate=&endDate=
http://127.0.0.1:8000/xmjg/xmjg-gzgl-oneform-tabname!getTabName.action?xzqhdm=660100&xmlxbh=5&spjdbh=1
http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByParamsMap.action?xzqhdm=660100&splcbm=92c57c71-4a4a-4768-8888-97efcae9d5c4
http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=92c57c71-4a4a-4768-8888-97efcae9d5c4&spjdbh=1&bgbh=1&splcbbh=1
http://127.0.0.1:8000/xmjg/xmjg-gzgl-oneform-tabname!getTabName.action?xzqhdm=660100&xmlxbh=5&spjdbh=2
http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=92c57c71-4a4a-4768-8888-97efcae9d5c4&spjdbh=2&bgbh=1&splcbbh=1
http://127.0.0.1:8000/xmjg/xmjg-gzgl-oneform-tabname!getTabName.action?xzqhdm=660100&xmlxbh=5&spjdbh=3
http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=92c57c71-4a4a-4768-8888-97efcae9d5c4&spjdbh=3&bgbh=1&splcbbh=1
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do?provinceCode=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29
http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/analysis-ranking-overdue.js
http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/common-charts.js
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getAnalysisCityOverdueRankingData.do
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?averageTime=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&provinceCode=660000
http://127.0.0.1:8000/xmjg/xmjg/sjjc/js/tool/common.js
http://127.0.0.1:8000/xmjg/agcloud/framework/ui-private/common/element-2/element.js
http://127.0.0.1:8000/xmjg/supervisionInspection/getPjysByTjjssj.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29&spysDy0=0
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?dataType=1&fromOrgPage=2&tjkssj=2020-01-01&tjjssj=2020-12-29&showKssj=2020-01-01&showJssj=2020-12-29&backBtnFlag=0&dateEnd=2020-12-29&name=三师图木舒克市&sfzb=1&xzqhdm=660300&bjl=88
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?dataType=15&fromOrgPage=2&tjkssj=2020-01-01&tjjssj=2020-12-29&showKssj=2020-01-01&showJssj=2020-12-29&backBtnFlag=0&dateEnd=2020-12-29&name=新疆生产建设兵团&sfzb=1&xzqhdm=660000&spjd=1&blqk=1&bjl=794&stageType=1
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660300&qtTypeVal=0&dataType=15&name=三师图木舒克市&stageType=1&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=&bjl=40&blqk=3&spjd=1
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do
http://127.0.0.1:8090/opus-front-sso/authentication/form
http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/locale/locale.properties
http://127.0.0.1:8090/opus-front-sso/authentication/require?error=true
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660300&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=15&stageType=1&sfbyxz=&sfjgqqxt=&name=三师图木舒克市&spjd=1&blqk=3&splcbm=&sfyq=&bjl=40&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=12

34&xmmc=1234&jsddxzqh=660300&orderBy=&orderDir=&pageNo=25
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html
http://127.0.0.1:8000/xmjg/login
http://127.0.0.1:8090/opus-front-sso/oauth/authorize?client_id=xmjg&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=pybX0O
http://127.0.0.1:8000/xmjg/login?code=O8hA5h&state=pybX0O
http://127.0.0.1:8000/xmjg/opus/front/om/users/currOpusLoginUser?time=1609209683314
http://127.0.0.1:8000/xmjg/xmjg/xmjg-project-info!getScreen.action
http://127.0.0.1:8000/xmjg/index/getSystemName
http://127.0.0.1:8000/xmjg/opus/front/om/users?loginName=admin&time=1609209684703
http://127.0.0.1:8000/xmjg/opus/front/om/users/user/10000/allMenus?isTree=true&netName=前端网络入口&tmnId=1&topOrgId=A&userId=10000&time=1609209684701
http://127.0.0.1:8000/xmjg/analysis-info!getPilotCity.action
http://127.0.0.1:8000/xmjg/mapShowConfig.do
http://127.0.0.1:8000/xmjg/xmjg-project-info/getProvinceAuthority
http://127.0.0.1:8000/xmjg/supervisionInspection/getMergeData.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29
http://127.0.0.1:8000/xmjg/supervisionInspection/getProvinceTopFive.do?province=660000&startDate=2020-01-01&endDate=2020-12-29
http://127.0.0.1:8000/xmjg/supervisionInspection/getYsTotalOfMultidimensional.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29&spysDy0=
http://127.0.0.1:8000/xmjg/analysis-info!getHaveProjectCitys.action
http://127.0.0.1:8000/xmjg/supervisionInspection/getYslAndXzblxms.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29
http://127.0.0.1:8000/xmjg/supervisionInspection/getMapCountryAndProvinceXms.do?xzqhdm=660000&tjfs=xmsl&cityType=province&startDate=2020-01-01&endDate=2020-12-29
http://127.0.0.1:8000/xmjg/xmjg-project-info!getMapConfigData.action?bigScreenFolder=
http://127.0.0.1:8000/xmjg/xmjg/xndc/map/mapJson/abbrMapJson/province/66.json

参数 311

TOC

名称	值	URL	类型
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspection/getYslAndXzblxms.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29	简单链接
->"totals"[4]->"sjyxbs"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

-> "totals"[2] -> "id"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
-> "totals"[4] -> "fjmc"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
-> "totals"[2] -> "strId"	70	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
-> "totals"[1] -> "splclx"	2	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
cityName	一师阿拉尔市	http://127.0.0.1:8000/xmjg/xmjg-project-info!getLct.action?xzqhdm=660100&cityName=一师阿拉尔市	简单链接
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/city-page/getQqxtCount.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/supervisionInspection/getPjysByTjjssj.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29&spysDy0=0	隐藏
splc	政府投资房屋建筑类项目 政府投资城市基础设施工程类项	http://127.0.0.1:8000/xmjg/xmjg-project-info!getSpjdByxmlx.action?xzqhdm=660100&splclx=1&splcbbh=1&splcmc=政府投资房屋建筑类项	简单链接

mc	目 一般社会投资项目（不含带方案出让用地项目和小型社会投资项目） 社会投资小型工程项目 含带方案出让用地的社会投资项目	目&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783	
spjd		http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	隐藏
tjjssj	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=8&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29	文本
bigScreenFolder		http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=8&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29	隐藏
jsddxzqh	660300	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660300&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=15&stageType=1&sfbyxz=&sfjgqqxt=&name=三师图木舒克市&spjd=1&blqk=3&splcbm=&sfyq=&bjl=40&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&jsddxzqh=660300&orderBy=&orderDir=&pageNo=25	选择
stageType	0 1	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=	隐藏
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspection/getMergeData.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29	简单链接
splcmc		http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do	主体
flag	1	http://127.0.0.1:8000/xmjg/city-page/getCsrk.action?bigScreenFolder=&name=一师阿拉尔市&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29	简单链接
xzqhdm	660100	http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-31	隐藏
->"endD	2020-12-31	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

ate"			
backBtnFlag	0	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?dataType=1&fromOrgPage=2&tjkssj=2020-01-01&tjjssj=2020-12-29&showKssj=2020-01-01&showJssj=2020-12-29&backBtnFlag=0&dateEnd=2020-12-29&name=三师图木舒克市&sfzb=1&xzqhdm=660300&bjl=88	简单链接
->"totals"[1]->"splcbbh"	1	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
provinceCode	660000	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do	隐藏
->"totals"[4]->"title"	\u542b\u5e26\u65b9\u6848\u51fa\u8ba9\u7528\u5730\u7684\u793e\u4f1a\u6295\u8d44\u9879\u76ee	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
dataType	8 5	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=8&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29	隐藏
->"totals"[4]->"id"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
->"totals"[3]->"sjwxy	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

y"			
tjfs	xmsl	http://127.0.0.1:8000/xmjg/supervisionInspection/getMapCountryAndProvinceXms.do?xzqhdm=660000&tjfs=xmsl&cityType=province&startDate=2020-01-01&endDate=2020-12-29	简单链接
name	%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82	http://127.0.0.1:8000/xmjg/xmjg-one-window!getYgck.action?name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspection/getYsTotalOfMultidimensional.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29&spysDy0=	简单链接
->"totals"[4]->"splclx"	5	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspection/getMapCountryAndProvinceXms.do?xzqhdm=660000&tjfs=xmsl&cityType=province&startDate=2020-01-01&endDate=2020-12-29	简单链接
pageNum	25	http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	文本
splclx		http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=	隐藏
provinceCode		http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do?city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29&provinceCode=	隐藏
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action?name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
resetPasswordI	0	http://127.0.0.1:8090/opus-front-sso/authentication/form	隐藏

d			
-> "totals"[3] -> "splcmc"	\u793e\u4f1a\u6295\u8d44\u5c0f\u578b\u5de5\u7a0b\u9879\u76ee	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
-> "totals"[0] -> "splclx"	1	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
name	一师阿拉尔市	http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-31	隐藏
-> "totals"[4] -> "splcbbh"	1	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
response_type	code	http://127.0.0.1:8090/opus-front-sso/oauth/authorize?client_id=xmjg&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=tba1ER	简单链接
spjdbh	1 2 3	http://127.0.0.1:8000/xmjg/xmjg-gzgl-oneform-tabname!getTabName.action?xzqhdm=660100&xmlxbh=1&spjdbh=1	简单链接
splcbbh	1	http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=d4ba4952-9be6-4a10-9431-7a099bf5e783&spjdbh=1&bgbh=1&splcbbh=1	简单链接
name	%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82	http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action?name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
pr	660000	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionI	隐藏

ovinceCode		nspectionDrillPage.do?provinceCode=660000&dataType=8&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29	
userId	10000	http://127.0.0.1:8000/xmjg/opus/front/om/users/user/10000/allMenus?isTree=true&netName=前端网络入口&tmnId=1&topOrgId=A&userId=10000&time=1609207807212	简单链接
topOrgId	A	http://127.0.0.1:8000/xmjg/opus/front/om/users/user/10000/allMenus?isTree=true&netName=前端网络入口&tmnId=1&topOrgId=A&userId=10000&time=1609207807212	简单链接
->"totals"[4]->"strId"	71	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
provinceCode		http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	隐藏
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29	简单链接
xmdm	1234	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	文本
endDate	2020-12-31	http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-31	隐藏
->"totals"[1]->"sjyxbs"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

-> "totals"[1] -> "splcmc"	\u653f\u5e9c\u6295\u8d44\u57ce\u5e02\u57fa\u7840\u8bbe\u65bd\u5de5\u7a0b\u7c7b...)	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
bigScreenFolder		http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do?provinceCode=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29	隐藏
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/city-page/getGjdspblqk.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
page.orderBy	${page.orderBy}	http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	隐藏
-> "totals"[3] -> "sjyxbs"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
-> "totals"[2] -> "sjwxyy"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
splcbm	d4ba4952-9be6-4a10-9431-7a099bf5e783 5e6d7d7b-be47-4092-b8d9-c873cd74a8ae d21d7468-ca0c-478c-b700-e086	http://127.0.0.1:8000/xmjg/xmjg-project-info!getSpjdByxmlx.action?xzqhdm=660100&splclx=1&splcbbh=1&splcmc=政府投资房屋建筑类项目&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783	隐藏

	340478e0 0cce535b-bc83-4a61-be72-3d151e1a16e1 92c57c71-4a4a-4768-8888-97efcae9d5c4		
splcbbh	1	http://127.0.0.1:8000/xmjg/xmjg-project-info!getSpjdByxmlx.action?xzqhdm=660100&splclx=1&splcbbh=1&splcmc=政府投资房屋建筑类项目&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783	简单链接
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/city-page/getProjectCount.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
xzqhdms		http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	简单链接
sfType		http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do	隐藏
endDate	2020-12-31	http://127.0.0.1:8000/xmjg/city/getMDAllSpjd.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-31	简单链接
redirect_uri	http://127.0.0.1:8000/xmjg/login	http://127.0.0.1:8090/opus-front-sso/oauth/authorize?client_id=xmjg&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=tba1ER	简单链接
orderByName	orderByZBDESC	http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	隐藏
functionName	监督检测-全国首页	http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	主体
->"totals"[3]->"fjmc"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

qtTypeVal	0	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660300&qtTypeVal=0&dataType=15&name=三师图木舒克市&stageType=1&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=&bjl=40&blqk=3&spjd=1	简单链接
->"totals"[4]->"splcsm"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
dataType	8 5 6 7	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do	隐藏
xmmc		http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	隐藏
currentCityName		http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	隐藏
->"totals"[2]->"xzqhdm"	660100	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
city	%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82	http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do?city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29&provinceCode=	简单链接
time	1609207807040 1609209683314	http://127.0.0.1:8000/xmjg/opus/front/om/users/currOpusLoginUser?time=1609207807040	简单链接
->"tot	0cce535b-bc83-4a61-be72-3d151e1a16e1	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

als"[3] -> "splcbm"			
-> "totals"[0] -> "fjlx"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/xmjg-one-window!getYgck.action?name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
sfType		http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	隐藏
xmdm	1234	http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	文本
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/city-page/getSPPJSLCS.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
bgbh	1	http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=d4ba4952-9be6-4a10-9431-7a099bf5e783&spjdbh=1&bgbh=1&splcbbh=1	简单链接
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByParamsMap.action?xzqhdm=660100&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783	隐藏
-> "totals"[2] -> "splcbbh"	1	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

xzqhdm	660000	http://127.0.0.1:8000/xmjg/supervisionInspection/getYslAndXzblxms.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29	简单链接
orderByFlag	0 1 2	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do	主体
splcbm	d4ba4952-9be6-4a10-9431-7a099bf5e783 5e6d7d7b-be47-4092-b8d9-c873cd74a8ae d21d7468-ca0c-478c-b700-e086340478e0 0cce535b-bc83-4a61-be72-3d151e1a16e1 92c57c71-4a4a-4768-8888-97efcae9d5c4	http://127.0.0.1:8000/xmjg/xmjg-project-info!getGeLeiXingXiangMuCanShuByXzqhdm.action?xzqhdm=660100&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783&splcbbh=1&splclx=1&startDate=&endDate=	隐藏
sfjgqqxt		http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	隐藏
bigScreenFolder		http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=	隐藏
splclx	1 2 3 4 5	http://127.0.0.1:8000/xmjg/xmjg-project-info!getGeLeiXingXiangMuCanShuByXzqhdm.action?xzqhdm=660100&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783&splcbbh=1&splclx=1&startDate=&endDate=	隐藏
blqk	1 3	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	隐藏
->"totals"[3]->"fjid"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
->"tot	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

als"[4] -> "sjwxyy"			
bigScreenFolder		http://127.0.0.1:8000/xmjg/xmjg-project-info!getMapConfigData.action?bigScreenFolder=	简单链接
xzqhdm	660100	http://127.0.0.1:8000/xmjg/city-page/getCsrk.action?bigScreenFolder=&name=一师阿拉尔市&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29	隐藏
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspection/getPjysByTjjssj.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29&spysDy0=0	隐藏
-> "totals"[0] -> "title"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
-> "totals"[3] -> "fjlx"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
jsddxzqh		http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	简单链接
-> "totals"[1] -> "sjwxy	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

y"			
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-project-info!getLct.action?xzqhdm=660100&cityName=一师阿拉尔市	隐藏
xzqhdm	660100	http://127.0.0.1:8000/xmjg/city-page/getQqxtCount.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
->"totals"[1]->"title"	\u653f\u5e9c\u6295\u8d44\u57ce\u5e02\u57fa\u7840\u8bbe\u65bd\u5de5\u7a0b\u7c7b\u9879\u76ee	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
cityType	province	http://127.0.0.1:8000/xmjg/supervisionInspection/getMapCountryAndProvinceXms.do?xzqhdm=660000&tjfs=xmsl&cityType=province&startDate=2020-01-01&endDate=2020-12-29	简单链接
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/supervisionInspection/getJdbjs.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
splclx		http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=5&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splcmc=&splclx=	隐藏
->"totals"[4]->"splcsxsj"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
->"totals"[4]->"fjlx"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
spjdbh	1 2 3	http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=d4ba4952-9be6-4a10-9431-7a099bf5e783&spjdbh=1&bgbh=1&splcbbh=1	简单链接
->"tot	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

als"[1] -> "id"			
tjjssj	2020-12-29	http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	隐藏
tjTypeVal	1	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do	主体
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/city-page/getJdxms.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
spysDy0		http://127.0.0.1:8000/xmjg/supervisionInspection/getYsTotalOfMultidimensional.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29&spysDy0=	简单链接
tjkssj	2020-01-01	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getAnalysisCityOverdueRankingData.do	文本
-> "totals"[2] -> "fjid"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
splcbm		http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	隐藏
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/city-page/getDataListOfSplcbm.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
orderByName	sfyq+DESC sfyq DESC	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	隐藏
page	1 2	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dat	文本

No	25	eEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	
splclx		http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	隐藏
->"totals"[0]->"splcsxsj"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspection/getProvinceTopFive.do?province=660000&startDate=2020-01-01&endDate=2020-12-29	简单链接
xmdm		http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	隐藏
proPassword	0f69100a8b0e588685d4048f7a0c066d7be2ee2d79c6e39fbb2b5643da00aa7e	http://127.0.0.1:8090/opus-front-sso/authentication/form	隐藏
->"totals"[1]->"splcsxsj"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
file	/xmjg/file/yzbd/yishialaer/pdf/7fa992eb-5923-419b-9cbc-612db98522ba※一阶段办事指南.pdf	http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html?file= /xmjg/file/yzbd/yishialaer/pdf/7fa992eb-5923-419b-9cbc-612db98522ba※一阶段办事指南.pdf	简单链接
star	2020-01-01	http://127.0.0.1:8000/xmjg/supervisionInspection/getYslAndXzblxms.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29	简单链接

tDate			
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29	简单链接
whether_cehua		http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	隐藏
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByXzqhdm2.action?xzqhdm=660100	隐藏
state	tba1ER pybX0O	http://127.0.0.1:8090/opus-front-sso/oauth/authorize?client_id=xmjg&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=tba1ER	简单链接
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/city-page/getDataListOfSplcbm.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
->"totals"[2]->"splcbm"	d21d7468-ca0c-478c-b700-e086340478e0	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=d4ba4952-9be6-4a10-9431-7a099bf5e783&spjdbh=1&bgbh=1&splcbbh=1	隐藏
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-one-window!getXmjgEditor.action?xzqhdm=660100	隐藏
qtTypeVal	0 1 3	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do	主体
->"totals"[3]	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

->"id"			
->"totals"[2]->"sjyxbs"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
->"totals"[3]->"splcsxsj"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
xmlxbh	1 2 3 4 5	http://127.0.0.1:8000/xmjg/xmjg-gzgl-oneform-tabname!getTabName.action?xzqhdm=660100&xmlxbh=1&spjdbh=1	简单链接
splcmc		http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=5&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splcmc=&splclx=	简单链接
error	true	http://127.0.0.1:8090/opus-front-sso/authentication/require?error=true	简单链接
->"totals"[1]->"fjmc"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
splcmc		http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660100&dataType=12&name=一师阿拉尔市&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splcmc=&splclx=&sfType=	简单链接
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/city-page/getCountyMapData.do?xzqhdm=660100&tjfs=xmsl&startDate=&endDate=	简单链接
xz	660000	http://127.0.0.1:8000/xmjg/supervisionInspection/getMapCountryAnd	简单

qhdm		ProvinceXms.do?xzqhdm=660000&tjfs=xmsl&cityType=province&startDate=2020-01-01&endDate=2020-12-29	链接
splclx		http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do	隐藏
client_id	xmjg	http://127.0.0.1:8090/opus-front-sso/oauth/authorize?client_id=xmjg&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=tba1ER	简单链接
xzqhdm	660000	http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	隐藏
tjjssj	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do?provinceCode=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29	文本
xzqhdm	660100	http://127.0.0.1:8000/xmjg/city-page/getDataListOfSplcbm.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
xzqhdm	660100	http://127.0.0.1:8000/xmjg/city-page/getCountyMapData.do?xzqhdm=660100&tjfs=xmsl&startDate=&endDate=	隐藏
state	tba1ER pybX0O	http://127.0.0.1:8000/xmjg/login?code=Hu24Qr&state=tba1ER	简单链接
-> "totals"[1] -> "fjlx"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
orgId	KuE1eO8LWLplc8ODTQt8Ag==	http://127.0.0.1:8090/opus-front-sso/authentication/form	隐藏
cityxzqh	660700	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	选择
xzqhdm	660100	http://127.0.0.1:8000/xmjg/city-page/getGjdspblqk.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
dataType	8 12 1 15	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=	隐藏
-> "t	\u653f\u5e9c\u6295\u8d44\u623f\u5c4b\u5efa\u7b51\u7c7b\u987	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

otals"[0]->"splcmc"	9\u76ee		
code	Hu24QrO8hA5h	http://127.0.0.1:8000/xmjg/login?code=Hu24Qr&state=tba1ER	简单链接
xzqhdm	660100	http://127.0.0.1:8000/xmjg/city-page/getJdxms.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
stageType	0	http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	隐藏
xzqhdm	660000	http://127.0.0.1:8000/xmjg/supervisionInspection/getMergeData.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29	简单链接
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-project-info!getGeLeiXingXiangMuCanShuByXzqhdm.action?xzqhdm=660100&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783&splcbbh=1&splclx=1&startDate=&endDate=	隐藏
dataDesc	受理项目数项目列表	http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	简单链接
spysDy0	0	http://127.0.0.1:8000/xmjg/supervisionInspection/getPjysByTjjssj.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29&spysDy0=0	简单链接
orderByName	sfyq+DESC	http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	隐藏
tjkssj	2020-01-01	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=	隐藏
->"totals"[3]->"title"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

sfyq		http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	隐藏
orderByFlag	1	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getAnalysisCityOverdueRankingData.do	主体
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.6466467024008973	主体
->"totals"[2]->"fjmc"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
averageTime	0	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?averageTime=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&provinceCode=660000	简单链接
xmmc	1234	http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	文本
tjjssj	2020-12-29	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=	隐藏
isTree	true	http://127.0.0.1:8000/xmjg/opus/front/om/users/user/10000/allMenus?isTree=true&netName=前端网络入口&tmnId=1&topOrgId=A&userId=10000&time=1609207807212	简单链接
->"totals"[2]->"fjlx"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
splcbbh	1	http://127.0.0.1:8000/xmjg/xmjg-project-info!getGeLeiXingXiangMuCanShuByXzqhdm.action?xzqhdm=660100&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783&splcbbh=1&splclx=1&startDate=&endDate=	简单链接

dateEnd	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do?provinceCode=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29	隐藏
xzqhdm	660000	http://127.0.0.1:8000/xmjg/supervisionInspection/getPjysByTjjssj.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29&spysDy0=0	隐藏
->"totals"[1]->"fjid"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-one-window!getYgck.action?name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/city/getMDAllSpjd.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-31	简单链接
->"totals"[0]->"splcbbh"	1	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
xzqhdm	660100	http://127.0.0.1:8000/xmjg/supervisionInspection/getJdbjs.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
splclx		http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	隐藏
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action?name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
name	一师阿拉尔市 三师图木舒克市 新疆生产建设兵团	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=	隐藏
startDat	2020-01-01	http://127.0.0.1:8000/xmjg/city-page/getJdxms.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接

e			
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-project-info!getSpjdByxmlx.action?xzqhdm=660100&splclx=1&splcbbh=1&splcmc=政府投资房屋建筑类项目&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783	隐藏
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspection/getAllPjysByTjjssj.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspection/getJdbjs.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
->"totals"[1]->"strId"	69	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
xzqhdm	660100	http://127.0.0.1:8000/xmjg/supervisionInspection/getAllPjysByTjjssj.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
tjkssj	2020-01-01	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do?provinceCode=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29	文本
xmmc	1234	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	文本
xzqhdm	660100	http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do?city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29&provinceCode=	隐藏
tjkssj	2020-01-01	http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	隐藏
functionUrl	http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879	http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	主体
flag	1	http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&x	简单链接

		mdm=1234&xmmc=1234&orderByName=sfyq+DESC	
sfzb	1	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?dataType=1&fromOrgPage=2&tjkssj=2020-01-01&tjjssj=2020-12-29&showKssj=2020-01-01&showJssj=2020-12-29&backBtnFlag=0&dateEnd=2020-12-29&name=三师图木舒克市&sfzb=1&xzqhdm=660300&bjl=88	简单链接
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/supervisionInspection/getProvinceTopFive.do?province=660000&startDate=2020-01-01&endDate=2020-12-29	简单链接
dateEnd	2020-12-29	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=	隐藏
tjkssj	2020-01-01	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do	文本
->"totals"[0]->"splcbm"	d4ba4952-9be6-4a10-9431-7a099bf5e783	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
xzqhdm	660100	http://127.0.0.1:8000/xmjg/city-page/getSPPJSLCS.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
xzqhdm	660000	http://127.0.0.1:8000/xmjg/supervisionInspection/getYsTotalOfMultidimensional.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29&spysDy0=	简单链接
startDate		http://127.0.0.1:8000/xmjg/xmjg-project-info!getGeLeiXingXiangMuCanShuByXzqhdm.action?xzqhdm=660100&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783&splcbbh=1&splclx=1&startDate=&endDate=	隐藏
flag	1	http://127.0.0.1:8000/xmjg/analysis-info!getHaveProjectCitys.action	主体
tjkssj	2020-01-01	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=8&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29	文本
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/city-page/getSPPJSLCS.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
orderByF		http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&x	简单链接

lag		mdm=1234&xmmc=1234&orderByName=sfyq+DESC	
menuId	opu-rs-menu-00000002879	http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879	简单链接
bjl	2102 88 794 40	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	隐藏
tjfs	xmsl	http://127.0.0.1:8000/xmjg/city-page/getCountyMapData.do?xzqhdm=660100&tjfs=xmsl&startDate=&endDate=	简单链接
xzqhdm	660000 660100	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.6466467024008973	隐藏
->"totals"[1]->"xzqhdm"	660100	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
showJssj	2020-12-29	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?dataType=1&fromOrgPage=2&tjkssj=2020-01-01&tjjssj=2020-12-29&showKssj=2020-01-01&showJssj=2020-12-29&backBtnFlag=0&dateEnd=2020-12-29&name=三师图木舒克市&sfzb=1&xzqhdm=660300&bjl=88	简单链接
sjXzqhdm	660000	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29	简单链接
showKssj	2020-01-01	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?dataType=1&fromOrgPage=2&tjkssj=2020-01-01&tjjssj=2020-12-29&showKssj=2020-01-01&showJssj=2020-12-29&backBtnFlag=0&dateEnd=2020-12-29&name=三师图木舒克市&sfzb=1&xzqhdm=660300&bjl=88	简单链接
tmnId	1	http://127.0.0.1:8000/xmjg/opus/front/om/users/user/10000/allMenus?isTree=true&netName=前端网络入口&tmnId=1&topOrgId=A&userId=10000&time=1609207807212	简单链接
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do?city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29&provinceCode=	简单链接
sfbyxz		http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splc	隐藏

		lx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	
dataType	8	http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	隐藏
->"totals"[3]->"splcsm"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
sfType		http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	隐藏
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do?city=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29&provinceCode=	简单链接
page.orderDir	${page.orderDir}	http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	隐藏
->"totals"[3]->"splclx"	4	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
province	660000 getTopFiveCity	http://127.0.0.1:8000/xmjg/supervisionInspection/getProvinceTopFive.do?province=660000&startDate=2020-01-01&endDate=2020-12-29	简单链接
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-31	隐藏
end	2020-12-29	http://127.0.0.1:8000/xmjg/city-page/getCountyMapData.do?xzqhdm=660100&tjfs=xmsl&startDate=&endDate=	简单链接

Date			
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/city-page/getGjdspblqk.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
time	1609207807212 1609209684703	http://127.0.0.1:8000/xmjg/opus/front/om/users?loginName=admin&time=1609207807212	简单链接
xmlxbh	d4ba4952-9be6-4a10-9431-7a099bf5e783 5e6d7d7b-be47-4092-b8d9-c873cd74a8ae d21d7468-ca0c-478c-b700-e086340478e0 0cce535b-bc83-4a61-be72-3d151e1a16e1 92c57c71-4a4a-4768-8888-97efcae9d5c4	http://127.0.0.1:8000/xmjg/xmjg-gzgl-upload!getFileName.action?xzqhdm=660100&xmlxbh=d4ba4952-9be6-4a10-9431-7a099bf5e783&spjdbh=1&bgbh=1&splcbbh=1	简单链接
->"totals"[0]->"xzqhdm"	660100	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
->"totals"[4]->"splcbm"	92c57c71-4a4a-4768-8888-97efcae9d5c4	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
->"totals"[4]->"xzqhdm"	660100	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
->"st	2020-01-01	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

artDate"			
->"totals"[3]->"xzqhdm"	660100	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
dateEnd	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=8&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29	隐藏
tjjssj	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getAnalysisCityOverdueRankingData.do	文本
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-project-info!getSxlx.action?xzqhdm=660100	隐藏
loginName	admin	http://127.0.0.1:8000/xmjg/opus/front/om/users?loginName=admin&time=1609207807212	简单链接
provinceCode		http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	隐藏
->"totals"[4]->"fjid"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
->"totals"[0]->"id	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

"			
-> "totals"[2] -> "splcsxsj"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
xzqhdm	660100	http://127.0.0.1:8000/xmjg/city/getMDAllSpjd.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-31	隐藏
-> "totals"[1] -> "splcsm"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/city-page/getCsrk.action?bigScreenFolder=&name=一师阿拉尔市&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29	简单链接
-> "totals"[0] -> "fjmc"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
password	d52905779872d27732690e458472f8dbfd01ecfd60c676041f8430f7527c81f2	http://127.0.0.1:8090/opus-front-sso/authentication/form	隐藏
typeCode	TJ_DATE_CONFIG	http://127.0.0.1:8000/xmjg/bsc/dic/code/lgetItemsByTypeCode.do?typeCode=TJ_DATE_CONFIG&flag=false	简单链接
t	0.6466467024008973 0.212760996225412 0.051773143618017325	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.6466467024008973	简单链接
en	2020-12-29	http://127.0.0.1:8000/xmjg/xmjg-one-window!getYgck.action?name=	隐藏

dDate		%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	
->"totals"[3]->"strId"	72	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
deviceType	kSmztErKOGJRIn+36B2OfA== pc	http://127.0.0.1:8090/opus-front-sso/authentication/form	隐藏
time	1609207807212 1609209684701	http://127.0.0.1:8000/xmjg/opus/front/om/users/user/10000/allMenus?isTree=true&netName=前端网络入口&tmnId=1&topOrgId=A&userId=10000&time=1609207807212	简单链接
xzqhdm	660000 660100 660300	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?xzqhdm=660000&dataType=8&name=&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splclx=	隐藏
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-city-map-config!getMapurlByXzqhdm.action?xzqhdm=660100&accessEntry=城市首页	隐藏
splcbm		http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	隐藏
->"totals"[2]->"splcsm"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
provinceCode	660000	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do?provinceCode=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29	隐藏
endD	2020-12-29	http://127.0.0.1:8000/xmjg/city-page/getCsrk.action?bigScreenFolder=&name=一师阿拉尔市&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29	简单链接

ate			
provinceCode	660000	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getAnalysisCityOverdueRankingData.do	隐藏
splclx	1 2 3 4 5	http://127.0.0.1:8000/xmjg/xmjg-project-info!getSpjdByxmlx.action?xzqhdm=660100&splclx=1&splcbbh=1&splcmc=政府投资房屋建筑类项目&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783	隐藏
endDate		http://127.0.0.1:8000/xmjg/xmjg-project-info!getGeLeiXingXiangMuCanShuByXzqhdm.action?xzqhdm=660100&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783&splcbbh=1&splclx=1&startDate=&endDate=	隐藏
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByXzqhdm.action?xzqhdm=660100	隐藏
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/xmjg-statis-show!getProjectCategoryCountDl.action?t=0.6466467024008973	主体
fromOrgPage	2	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?dataType=1&fromOrgPage=2&tjkssj=2020-01-01&tjjssj=2020-12-29&showKssj=2020-01-01&showJssj=2020-12-29&backBtnFlag=0&dateEnd=2020-12-29&name=三师图木舒克市&sfzb=1&xzqhdm=660300&bjl=88	简单链接
orderDir		http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	隐藏
djzt		http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	隐藏
tjjssj	2020-12-29	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillData.do	文本
xzqhdm	660100	http://127.0.0.1:8000/xmjg/city-page/getProjectCount.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
star	2020-01-01	http://127.0.0.1:8000/xmjg/supervisionInspection/getYsTotalOfMultidimensional.do?xzqhdm=660000&startDate=2020-01-01&endDate=20	简单链接

tDate		20-12-29&spysDy0=	
->"totals"[3]->"splcbbh"	1	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
spjd	1	http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	隐藏
accessEntry	城市首页	http://127.0.0.1:8000/xmjg/xmjg-city-map-config!getMapurlByXzqhdm.action?xzqhdm=660100&accessEntry=城市首页	简单链接
netName	前端网络入口	http://127.0.0.1:8000/xmjg/opus/front/om/users/user/10000/allMenus?isTree=true&netName=前端网络入口&tmnId=1&topOrgId=A&userId=10000&time=1609207807212	简单链接
orderBy		http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	隐藏
->"totals"[0]->"sjyxbs"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
sfyq		http://127.0.0.1:8000/xmjg/excel-export!exportProjectNumber.action?xzqhdms=&orderByFlag=&dataType=8&stageType=0&dataDesc=受理项目数项目列表&tjkssj=2020-01-01&tjjssj=2020-12-29&xzqhdm=660000&flag=1&sfyq=&splclx=&sfType=&provinceCode=&jsddxzqh=&xmdm=1234&xmmc=1234&orderByName=sfyq+DESC	隐藏
usernam	DneqHwQJ+KcpguDo0UVQiw==	http://127.0.0.1:8090/opus-front-sso/authentication/form	隐藏

e			
endDate	2020-12-29	http://127.0.0.1:8000/xmjg/city-page/getQqxtCount.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
->"totals"[0]->"sjwxyy"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action?name=%25E4%25B8%2580%25E5%25B8%2588%25E9%2598%25BF%25E6%258B%2589%25E5%25B0%2594%25E5%25B8%2582&xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	隐藏
->"totals"[0]->"splcsm"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
splcbm	d4ba4952-9be6-4a10-9431-7a099bf5e783 5e6d7d7b-be47-4092-b8d9-c873cd74a8ae d21d7468-ca0c-478c-b700-e086340478e0 0cce535b-bc83-4a61-be72-3d151e1a16e1 92c57c71-4a4a-4768-8888-97efcae9d5c4	http://127.0.0.1:8000/xmjg/xmjg-project-info!getSplcByParamsMap.action?xzqhdm=660100&splcbm=d4ba4952-9be6-4a10-9431-7a099bf5e783	隐藏
->"totals"[4]->"splcmc"	\u542b\u5e26\u65b9\u6848\u51fa\u8ba9\u7528\u5730\u7684\u793e\u4f1a\u6295\u8d44...)	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
->"tot	3	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

als"[2] -> "splclx"			
name	一师阿拉尔市	http://127.0.0.1:8000/xmjg/city-page/getCsrk.action?bigScreenFolder=&name=一师阿拉尔市&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29	隐藏
-> "totals"[2] -> "title"	\u4e00\u822c\u793e\u4f1a\u6295\u8d44\u9879\u76ee\uff08\u4e0d\u542b\u5e26\u65b9\u6848\u51fa\u8ba9\u7528\u5730\u9879\u76ee\u548c\u5c0f\u578b\u793e\u4f1a\u6295\u8d44\u9879\u76ee\uff09	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
stageType	0	http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=8&stageType=0&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29	隐藏
whetherBinglian		http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do?name=一师阿拉尔市&currentCityName=&xzqhdm=660100&splclx=&djzt=&spjd=&whetherBinglian=&whether_cehua=&xmmc=&xmdm=&splcbm=&startDate=2020-01-01&endDate=2020-12-31&orderByName=orderByZBDESC&page.orderBy=%24{page.orderBy}&page.orderDir=%24{page.orderDir}&pageNum=25	隐藏
-> "totals"[1] -> "splcbm"	5e6d7d7b-be47-4092-b8d9-c873cd74a8ae	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/city-page/getProjectCount.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接
-> "totals"[0] -> "fjid"	null	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON

bigScreenFolder		http://127.0.0.1:8000/xmjg/city-page/getCsrk.action?bigScreenFolder=&name=一师阿拉尔市&xzqhdm=660100&flag=1&startDate=2020-01-01&endDate=2020-12-29	隐藏
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/supervisionInspection/getMergeData.do?xzqhdm=660000&startDate=2020-01-01&endDate=2020-12-29	简单链接
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/supervisionInspection/getMapCountryAndProvinceXms.do?xzqhdm=660000&tjfs=xmsl&cityType=province&startDate=2020-01-01&endDate=2020-12-29	简单链接
->"totals"[0]->"strId"	68	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
->"totals"[2]->"splcmc"	\u4e00\u822c\u793e\u4f1a\u6295\u8d44\u9879\u76ee\uff08\u4e0d\u542b\u5e26\u65b9...)	http://127.0.0.1:8000/xmjg/city/getTotalByMdList.do	JSON
flag	false	http://127.0.0.1:8000/xmjg/bsc/dic/code/lgetItemsByTypeCode.do?typeCode=TJ_DATE_CONFIG&flag=false	简单链接
xzqhdm	660100	http://127.0.0.1:8000/xmjg/xmjg-gzgl-oneform-tabname!getTabName.action?xzqhdm=660100&xmlxbh=1&spjdbh=1	隐藏
startDate	2020-01-01	http://127.0.0.1:8000/xmjg/supervisionInspection/getAllPjysByTjjssj.do?xzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	简单链接

失败的请求 14

TOC

URL	原因
http://127.0.0.1:8000/xmjg/monitorEarlyWarning/earlyWarningRecord/noticeToConfirm.do	响应状态“404” — 找不到
http://127.0.0.1:8000/xmjg/monitorEarlyWarning/earlyWarningRecord/allToConfirm.do	响应状态“404” — 找不到
http://127.0.0.1:8000/xmjg/dghyindex/echarts/build/dist/echarts.js	响应状态“404” — 找不到
http://127.0.0.1:8000/xmjg/dghyindex/echarts/build/dist/echarts.min3.8.5.js	响应状态“404” — 找不到
http://127.0.0.1:8000/xmjg/ie-css3.htc	响应状态“404” — 找不到
http://127.0.0.1:8000/xmjg/projectInfo/xmjg-project-info!projectInfo.action?id=	响应状态“404” — 找不到
http://127.0.0.1:8090/opus-front-sso/authentication/form	
http://127.0.0.1:8090/opus-front-sso/oauth/authorize?client_id=xmjg&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=pybX0O	
http://127.0.0.1:8000/xmjg/monitorEarlyWarning/earlyWarningRecord/noticeToConfirm.do	响应状态“404” — 找不到
http://127.0.0.1:8000/xmjg/login?code=O8hA5h&state=pybX0O	
http://127.0.0.1:8000/xmjg/login	
http://127.0.0.1:8090/opus-front-sso/oauth/authorize?client_id=xmjg&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=q3VTkk	
http://127.0.0.1:8000/xmjg/login?code=E3KLh9&state=q3VTkk	
http://127.0.0.1:8000/xmjg/error?code=O8hA5h&state=pybX0O	

已过滤的 URL 140

TOC

URL	原因
http://127.0.0.1:8090/opus-front-sso/images/guohui.png	文件扩展名
http://127.0.0.1:8090/opus-front-sso/css/global.css	文件扩展名
http://127.0.0.1:8090/opus-front-sso/css/login_new.css	文件扩展名
http://127.0.0.1:8090/opus-front-sso/css/layui.css	文件扩展名
http://127.0.0.1:8090/opus-front-sso/images/login_logo.png	文件扩展名
http://127.0.0.1:8090/opus-front-sso/oauth/authorize?client_id=xmjg&redirect_uri=http://127.0.0.1:8000/xmjg/login&response_type=code&state=tba1ER	类似 DOM
http://127.0.0.1:8000/xmjg/agcloud/framework/ui-schemes/dark-blue/images/system_guohui.png	文件扩展名
http://127.0.0.1:8000/xmjg/agcloud/framework/js-lib/element-2/element.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/file/工程建设项目审批管理系统操作手册.doc	文件扩

	展名
http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/img/loading.gif	文件扩展名
http://127.0.0.1:8000/xmjg/agcloud/framework/ui-schemes/dark-blue/css/images/system_name.png	文件扩展名
http://127.0.0.1:8000/xmjg/agcloud/framework/ui-schemes/dark-blue/css/images/system_guohui.png	文件扩展名
http://127.0.0.1:8000/xmjg/common/tool/date/css/bootstrap.min.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/css/element.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/css/dg-jdkh-main-rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/common/tool/date/css/bootstrap-datepicker3.standalone.css	文件扩展名
http://127.0.0.1:8000/xmjg/common/tool/cityselect/css/city_select.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/css/common_new_rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/img/fiveStarReplace.png	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/css/analysis-index-rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/css/analysis-statistics-rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/common/tool/date/css/dateQuery.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/css/common_new.css	文件扩展名
http://127.0.0.1:8000/xmjg/resources/css/dghyindex/css/global-rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/xndc/css/data-list.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/css/common_new.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/css/common_new_rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/resources/css/dghyindex/css/frame.css	文件扩展名
http://127.0.0.1:8000/xmjg/resources/css/dghyindex/css/global.css	文件扩展名
http://127.0.0.1:8000/xmjg/resources/css/dghyindex/css/index.css	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/loding.gif	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/nlmyy.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/cky.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/zzy.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/drrs.png	文件扩

	展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/jzy.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/pfhlsy.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/jtyschhyzy.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/zshcyy.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/rjxx.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/jry.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/fdcy.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/zlhswfwy.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/kxyjhjsfwy.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/slhjhggssgly.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/jmfwxlhqtfwy.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/jy.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/wshshgz.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/whtyhyly.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/ggglshbzhshzz.png	文件扩展名
http://127.0.0.1:8000/xmjg/dghyindex/img/xmjg/gjzz.png	文件扩展名
http://127.0.0.1:8000/dghyindex/img/h2_bg.png	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/css/bootstrap.min.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/xndc/css/bootstrap-datepicker3.standalone.css	文件扩展名
http://127.0.0.1:8000/xmjg/bootstrap/css/bootstrap-table.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/csrk/img/page_up.png	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/csrk/img/page_down.png	文件扩展名
http://10.4.4.16:8886/agcom/2dMap/interfaceMap.html?userName=admin	未测试的 Web Server
http://127.0.0.1:8000/xmjg/xmjg/xndc/css/index-rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/xndc/css/jieduan3-rem.css	文件扩

	展名
http://127.0.0.1:8000/xmjg/xmjg/xndc/css/searchArea-rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/xndc/css/global-rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/resources/easyui/themes/icon.css	文件扩展名
http://127.0.0.1:8000/xmjg/resources/easyui/themes/default/easyui.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/xndc/css/dg-xndc-main-rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmzh/project/img/picture1.png	文件扩展名
http://127.0.0.1:8000/xmjg/xmzh/project/img/picture2.png	文件扩展名
http://127.0.0.1:8000/xmjg/xmzh/project/img/picture3.png	文件扩展名
http://127.0.0.1:8000/xmjg/xmzh/project/img/picture4.png	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/ygck/css/common.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/ygck/css/common-rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/bootstrap/css/bootstrap.css	文件扩展名
http://127.0.0.1:8000/xmjg/bootstrap/css/bootstrap.min.css	文件扩展名
http://127.0.0.1:8000/xmjg/bootstrap/css/bootstrap-datetimepicker.css	文件扩展名
http://127.0.0.1:8000/xmjg/bootstrap/css/bootstrap-datetimepicker.min.css	文件扩展名
http://127.0.0.1:8000/xmjg/bootstrap/css/bootstrapValidator.css	文件扩展名
http://127.0.0.1:8000/xmjg/bootstrap/css/toastr.css	文件扩展名
http://127.0.0.1:8000/xmjg/bootstrap/css/bootstrap-editable.css	文件扩展名
http://127.0.0.1:8000/xmjg/bootstrap/css/bootstrap-treeview.css	文件扩展名
http://127.0.0.1:8000/xmjg/bootstrap/css/bootstrap-select.css	文件扩展名
http://127.0.0.1:8000/xmjg/bootstrap/css/jquery.eeyellow.Timeline.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/css/page-rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/csrk/css/common-rem.css	文件扩展名
http://127.0.0.1:8000/xmjg/handsontable-master/dist/handsontable.full.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/css/analysis-index.css	文件扩

	展名
http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/css/analysis-statistics.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg/css/element.ui-v2.10.1.css	文件扩展名
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	类似 DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	类似 DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	类似 DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=&xmmc=&cityxzqh=660700&orderBy=&orderDir=&pageNo=1	类似 DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	类似 DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	类似 DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=&xmmc=&cityxzqh=660700&orderBy=&orderDir=&pageNo=5	类似 DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	类似 DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=&xmmc=&cityxzqh=&orderBy=&orderDir=&pageNo=2	类似 DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的 DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=&xmmc=&cityxzqh=&orderBy=&orderDir=&pageNo=82	类似 DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的 DOM
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action?sjXzqhdm=660100&startDate=2020-01-01&endDate=2020-12-29	类似 DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的 DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的 DOM
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html?file= /xmjg/file/yzbd/yishialaer/pdf/656ca598-7968-43c4-a43f-ac2d0e741a83※一阶段办事指南.pdf	类似 DOM
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html?file= /xmjg/file/yzbd/yishialaer/pdf/e03f4af9-3948-4e9a-91e0-88eb4afd4cd2※一阶段办事指南.pdf	类似 DOM
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html?file= /xmjg/file/yzbd/yishialaer/pdf/bc7fd088-6596-44b5-a89a-158bfd67471c※一阶段办事指南.pdf	类似 DOM
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html?file= /xmjg/file/yzbd/yishialaer/pdf/0b1e7ea	类似

d-7158-4eb1-9468-6a9cc01001d0※一阶段办事指南.pdf	DOM
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html?file= /xmjg/file/yzbd/yishialaer/pdf/d2c60892-20c4-4cf5-aaae-66f493bc483b※一阶段办事指南.pdf	类似DOM
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html?file= /xmjg/file/yzbd/yishialaer/pdf/562ba43b-53a6-4e3e-8018-2570b02a279a※竣工验收办事指南.pdf	类似DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?dataType=1&fromOrgPage=2&tjkssj=2020-01-01&tjjssj=2020-12-29&showKssj=2020-01-01&showJssj=2020-12-29&backBtnFlag=0&dateEnd=2020-12-29&name=六师五家渠市&sfzb=1&xzqhdm=660600&bjl=28	类似DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?dataType=1&fromOrgPage=2&tjkssj=2020-01-01&tjjssj=2020-12-29&showKssj=2020-01-01&showJssj=2020-12-29&backBtnFlag=0&dateEnd=2020-12-29&name=二师铁门关市&sfzb=1&xzqhdm=660200&bjl=37	类似DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?dataType=1&fromOrgPage=2&tjkssj=2020-01-01&tjjssj=2020-12-29&showKssj=2020-01-01&showJssj=2020-12-29&backBtnFlag=0&dateEnd=2020-12-29&name=五师双河市&sfzb=1&xzqhdm=660500&bjl=38	类似DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?dataType=1&fromOrgPage=2&tjkssj=2020-01-01&tjjssj=2020-12-29&showKssj=2020-01-01&showJssj=2020-12-29&backBtnFlag=0&dateEnd=2020-12-29&name=九师&sfzb=1&xzqhdm=660900&bjl=43	类似DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的DOM
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=6&stageType=1&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splcmc=&splclx=	类似DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的DOM
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=7&stageType=1&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splcmc=&splclx=	类似DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?dataType=15&fromOrgPage=2&tjkssj=2020-01-	类似

01&tjjssj=2020-12-29&showKssj=2020-01-01&showJssj=2020-12-29&backBtnFlag=0&dateEnd=2020-12-29&name=新疆生产建设兵团&sfzb=1&xzqhdm=660000&spjd=2&blqk=1&bjl=242&stageType=2	DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的DOM
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=6&stageType=2&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splcmc=&splclx=	类似DOM
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	可能类似的DOM
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do?provinceCode=660000&dataType=7&stageType=2&tjkssj=2020-01-01&tjjssj=2020-12-29&bigScreenFolder=&dateEnd=2020-12-29&splcmc=&splclx=	类似DOM
http://127.0.0.1:8000/xmjg/projectInfo/_hover.png	文件扩展名
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=661300&orderBy=&orderDir=&pageNo=25	类似DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=8&stageType=0&sfbyxz=&sfjgqqxt=&name=&spjd=&blqk=&splcbm=&sfyq=&bjl=2102&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=660700&orderBy=&orderDir=&pageNo=25	类似DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660100&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=12&stageType=0&sfbyxz=&sfjgqqxt=&name=一师阿拉尔市&spjd=&blqk=&splcbm=&sfyq=&bjl=400&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&jsddxzqh=660100&orderBy=&orderDir=&pageNo=25	类似DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660300&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=1&stageType=&sfbyxz=&sfjgqqxt=&name=三师图木舒克市&spjd=&blqk=&splcbm=&sfyq=&bjl=88&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&jsddxzqh=660300&orderBy=&orderDir=&pageNo=25	类似DOM
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do?bigScreenFolder=&xzqhdm=660000&tjkssj=2020-01-01&tjjssj=2020-12-29&dateEnd=2020-12-29&provinceCode=&dataType=15&stageType=1&sfbyxz=&sfjgqqxt=&name=新疆生产建设兵团&spjd=1&blqk=1&splcbm=&sfyq=&bjl=721&splclx=&sfType=&orderByName=sfyq+DESC&xmdm=1234&xmmc=1234&cityxzqh=661300&orderBy=&orderDir=&pageNo=25	类似DOM
http://127.0.0.1:8090/opus-front-sso/authentication/require	类似主体
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	类似主体
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do?menuId=opu-rs-menu-00000002879	类似主体
http://127.0.0.1:8000/xmjg/xmjg-project-info!saveFunctionLog.action	类似主体

注释 243

TOC

URL	注释
http://127.0.0.1:8090/opus-front-sso/authentication/require	<!DOCTYPE html>

http://127.0.0.1:8090/opus-front-sso/authentication/require	系统登录界面
http://127.0.0.1:8090/opus-front-sso/authentication/require	<div class="m-login__logo"> <span class="pro-logo-name"> 工程建设项目审批管理平台</span> </div>
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	@Author: ZL
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	@Date: 2019/5/14
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	@Last Modified by: ZL
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	@Last Modified time: $ $
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	<title>国家工程建设项目审批监管信息系统</title>
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	<th:block th:insert="adsfw/taglibs :: taglibs"/>
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	<link rel="stylesheet" href="../../../../../static/agcloud/framework/icon-lib/agcloud-fonts/iconfont.css" th:href="@{/agcloud/framework/icon-lib/agcloud-fonts/iconfont.css}"> <link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-private/common/plugins/agcloud-fonts/iconfont.css" th:href="@{/agcloud/framework/ui-private/common/plugins/agcloud-fonts/iconfont.css}">
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	<link rel="stylesheet" href="../../../../../static/agcloud/framework/ui-schemes/dark-blue/css/index-rem.css" th:href="@{/agcloud/framework/ui-schemes/dark-blue/css/index-rem.css}">
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	BEGIN:头部
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	<div class="subsystem-logo"></div>
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	<img :src="item.bigImgPath" alt="">
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	<img :src="itemHide.bigImgPath" alt="">
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	<img v-if="userSex==0" src="../../../../../static/agcloud/framework/ui-schemes/dark-blue/images/user.png" th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/user.png}"> <img v-else src="../../../../../static/agcloud/framework/ui-schemes/dark-blue/images/user.png" th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/user.png}"> </div>
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	<img src="../../../../../static/agcloud/framework/ui-schemes/dark-blue/images/lock.png" th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/lock.png}" alt="">
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	<img src="../../../../../static/agcloud/framework/ui-schemes/dark-blue/images/exit.png" th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/exit.png}" alt="">
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	<img src="../../../../../static/agcloud/framework/ui-schemes/dark-blue/images/help.png" th:src="@{/agcloud/framework/ui-schemes/dark-blue/images/help.png}" alt="">
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	END:头部
http://127.0.0.1:8000/xmjg/opu	iframe 主体内容 START

s/front/blue/index.html	
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	用于解决那些页面和数据一起回来的 页面需加 loading的情况
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	iframe 主体内容 END
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	修改密码弹窗 start
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	修改密码弹窗 end
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	服务器监控日志弹窗 start
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	服务器监控日志弹窗 end
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	<script src="/framework-ui/src/main/resources/static/agcloud/login/js/md5.js" th:src="@{/agcloud/login/js/md5.js}"></script> <script src="/framework-ui/src/main/resources/static/agcloud/login/js/base64.js" th:src="@{/agcloud/login/js/base64.js}"></script> <script src="/framework-ui/src/main/resources/static/agcloud/login/js/sm4.js" th:src="@{/agcloud/login/js/sm4.js}"></script>
http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	END:js文件
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	<link th:href="@{/xmjg/xndc/css/dg-jdkh-main.css}" href="${ctx}/xmjg/xndc/css/dg-jdkh-main.css" rel="stylesheet" type="text/css"/>
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	<link rel="stylesheet" href="/framework-ui/src/main/resources/static/agcloud/framework/ui-private/common/element-2/element.css" th:href="@{/agcloud/framework/ui-private/common/element-2/element.css}">
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	jquery
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	<script th:src="@{/xmjg/js/jquery.min.js}" type="text/javascript" charset="utf-8"></script>
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	<script th:src="@{/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js}" src="${ctx}/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js" type="text/javascript"></script>
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	<script th:src="@{/common/tool/date/js/dateQuery.js}" type="text/javascript" charset="utf-8"></script>
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	城市选择插件 开始
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	城市选择插件 结束
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	左边
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	<span style="margin-left: 24%">省排名</span> <span style="margin-left: 5%"> 城市排名</span>
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-mai	<div class="index-card-tit-province cursor" >省排名</div> <div class="index-card-tit-city cursor" > 城市排名

n.do	</div>
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	<div class="index-card-tit" >本月新增项目数前五名(个)</div>
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	中间
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	<a class="active" href="javascript:">项目数(个)</a> <a href="javascript:"> 审批程序（个）</a> <a href="javascript:"> 审批时间（天）</a> <a href="javascript:"> 审批成本</a> <a href="javascript:"> 审批质量控制指标</a>
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	<div class="index-card-tit" id="indexMap-tit">国家工程建设项目分布</div>
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	新疆选择弹框
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	<button class="btn btn-info dropdown-toggle" data-toggle="dropdown" aria-expanded="false" style="background-color: #2B8CEC;border: 0px;border-radius: .20rem;font-size: 0.14rem;">请选择类型<span class="caret"></span></button>
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	<div class="islands-ico" title="钓鱼岛"></div>
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	新疆生产建设兵团 乌鲁木齐 上的五角星
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	右边
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	<div class="index-card-tit stage-tit">平均用时(天)</div>
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	跨度用时
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	最长用时
http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do	固定弹窗
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do	项目名称
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do	<c:set var="ctx" value="${pageContext.request.contextPath}"/>
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do	风格样式
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do	<c:set var="css" value="${SYS_CONFIG_CSS}" scope="application"/>
http://127.0.0.1:8000/xmjg/sup	<script th:src="@{/xmjg/xndc/js/jquery.min.js}"

ervisionInspectionDrill/getSupervisionInspectionDrillPage.do	src="/xmjg/xmjg/xndc/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do	图表柱状图展示操作
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do	时间查询控件 开始
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do	时间查询控件 结束
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do	<div class="rank-date-d">(<span id="sDate"></span>—<span id="endDate"></span>)</div>
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do	<script th:src="@{/xmjg/xndc/js/jquery.min.js}" src="${ctx}/xmjg/xndc/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do	<script th:src="@{/xmjg/xndc/js/analysis/analysis-project-stage-list.js}" src="${ctx}/xmjg/xndc/js/analysis/analysis-project-stage-list.js" type="text/javascript" charset="utf-8"></script>
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do	大屏的
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do	<input type="button" class="rank-btn2" name="" id="spyssfx_export" value="导出"/>
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do	<p type="button" id='spyssfx_export' class="unselectstyle" style="position:absolute;right:0px;top:0px; cursor:pointer;width:40px;height:22px;margin-right:0px;">导出</p>
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do	<td width="4%" align="right">省份：</td> <td width="5%"> <select id="province" class="change_to_label w250 inputCss" name="jsddxzqh" editable="false" style="width: 2rem;"> <option value=""> 请选择</option> </select> </td > <td width="4%" align="right"> 城市：</td> <td width="10%"> <select id="city" class="change_to_label w250 inputCss" name="jsddxzqh" editable="false" style="width: 2rem;"> <option value=""> 请选择</option> </select> </td >
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do	<th:block th:if="${dataType eq '1'}">
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do	<th:block th:if="${dataType nq '3'} " > <t d th:text="${results.JDZYS}">${results.JDZYS}</td> </th:block>
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do	-------------- 公共分页子页面 ---------------
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do	<input type="text" name="page.pageSize" id="pageSize" value="${page.pageSize}" size="3"/>
http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do	<td><input type="button" value=" >> " onclick="newsearch()"/></td>
http://127.0.0.1:8000/xmjg/xmj	<script type="text/javascript"

g-statis-show!getSkipPage.action	th:src="@{/resources/components/raphael_jquery/js/raphael.js}" src="${ctx}/resources/components/raphael_jquery/js/raphael.js"></script>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<script type="text/javascript" th:src="@{/dghyindex/echarts/doc/example/www2/js/echarts-all.js}" src="${ctx}/dghyindex/echarts/doc/example/www2/js/echarts-all.js"></script>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<script type="text/javascript" src="js/ajaxfileupload.js"></script>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;"> <img th:src="@{/dghyindex/img/loding.gif}" src="../../img/loding.gif" /> </div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	main
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	main_left
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;width:66%;height:100%;margin-left:5px;" >
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="seachfilter" > <div style="height:27px;"> <input type="button" class="btnSearchCss" style="width:78px;float:right;" value="综合查询" onclick="zhQuery();" /> <input id="showBtn" type="button" class="btnSearchCss" style="width:78px;float:right;" value="简单查询" onclick="showMore();" /> <input id="hideBtn" type="button" class="btnSearchCss" style="width:78px;float:right;display:none;" value="收起" onclick="hideMore();" /> </div> <div class="moreInfo" style="padding:0px 0px 5px 40px;display:none;"> <span>　项目类型：</span> <span> <select id="xmlx" class="easyui-combobox" name="xmlx" style="width:160px;"> <option value="">　请选择</option> <option value="A00001" >　审批</option> <option value="A00002" >　核准</option> <option value="A00003" >　备案</option> </select> </span> <span style="margin-left:20px;">　总投资(万元):</span> <span><input id="startNum" style="width:130px;"/></span> <span style="font-size:16px;">~</span> <span><input id="endNum" style="width:130px;"/></span> <span style="margin-left:10px;"> <button class="searchbutton" onclick="query()" >　确 定 </button> </span> <span style="margin-left:10px;"> <button class="searchbutton" onclick="cancleQuery()" >　取 消 </button> </span> </div> </div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.acti	<%&#45;&#45; <div class="smzq" style="border: 1px solid #d3e3f3;height: 180px;width:100%;">

on	
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<h2><span>项目生命周期</span></h2>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;margin-left:1%;width:100%;">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash; 工程规划许可 &ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="label" style="float:left;height:100px;margin-top:25px;width:20%;" onclick="clickSmzq('1','立项用地规划许可阶段')"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;margin-top:53px;width:1%;margin-left:1%;"><img th:src="@{/dghyindex/img/arrow.png}" src="${ctx}/dghyindex/img/arrow.png" /></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash; 工程建设许可 &ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="label2" style="float:left;height:100px;margin-top:25px;width:20%;margin-left:2%;" onclick="clickSmzq('2','工程建设许可')"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash; 施工许可 &ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="label3" style="float:left;height:100px;margin-top:25px;width:20%;margin-left:2%;" onclick="clickSmzq('3','施工许可')"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash; 竣工验收 &ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="label4" style="float:left;height:100px;margin-top:25px;width:20%;margin-left:2%;" onclick="clickSmzq('4','竣工验收')"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	</div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div class="smzq" style="border: 1px solid #d3e3f3;height: 220px;margin-top: 10px;width:100%;margin-bottom:20px;">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<h2><span>建设项目类型</span></h2>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="margin-top:10px;width:100%;"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;margin-top:0px;width:100%;" align="center">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash; 财政性投融资工程建设项目(房屋建筑类)&ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;width:21%;height:166px;text-align:center;">

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="margin-top:0px;width:100%;height:1px;"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<img id="zzyimg" th:src="@{/dghyindex/img/xmjg/czjz.png}" src="${ctx}/dghyindex/img/xmjg/czjz.png" style="cursor:pointer;" onclick="clickXmfl('1')"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	onmouseover="setImgSrc(this,'over')" onmouseout="setImgSrc(this,'out')" />
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="czjz"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash; 财政性投融资工程建设项目(线性工程类)&ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;/*margin-left:1%;*/width:10%;height:166px;text-align:center;">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<img id="drrsimg" th:src="@{/dghyindex/img/xmjg/czxx.png}" src="${ctx}/dghyindex/img/xmjg/czxx.png" style="cursor:pointer;" onclick="clickXmfl('2')"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="czxx"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash; 小型社会投资项目 &ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;/*margin-left:1%;*/width:22%;height:166px;text-align:center;">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<img id="nlmyyimg" th:src="@{/dghyindex/img/xmjg/shba.png}" src="${ctx}/dghyindex/img/xmjg/shba.png" style="cursor:pointer;" onclick="clickXmfl('3')"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="xxsh"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash; 一般社会投资项目(公开出让用地) &ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;/*margin-left:2%;*/width:10%;height:166px;text-align:center;">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<img id="ckyimg" th:src="@{/dghyindex/img/xmjg/shhz.png}" src="${ctx}/dghyindex/img/xmjg/shhz.png" style="cursor:pointer;" onclick="clickXmfl('4')"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="ybsh"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash; 带方案出让用地的社会投资项。&ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;/*margin-left:2%;*/width:22%;height:166px;text-align:center;">
http://127.0.0.1:8000/xmjg/xmj	<img id="ckyimg" th:src="@{/dghyindex/img/xmjg/shhz.png}"

g-statis-show!getSkipPage.action	src="${ctx}/dghyindex/img/xmjg/shhz.png" style="cursor:pointer;" onclick="clickXmfl('5')"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="dfsh"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash; 其他 &ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;/*margin-left:2%;width:16%;*/height:166px;text-align:center;">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<img id="ckyimg" th:src="@{/dghyindex/img/xmjg/shhz.png}" src="${ctx}/dghyindex/img/xmjg/shhz.png" style="cursor:pointer;" onclick="clickXmfl('6')"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="qtlx"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div class="smzq" style="border: 1px solid #d3e3f3;height: 225px;margin-bottom:20px;margin-top: 10px;width:100%;">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<h2><span>项目所属区域</span></h2><div style="margin-top: -28px;margin-left:95%;"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="main" style="height:109%;width:108%;margin-left: -40px;margin-top: -10px;" ></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	</div> &#45;&#45;%>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	农、林、牧、渔业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	采矿业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	制造业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	电力、热力、燃气及水生产和供应业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	建筑业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	批发和零售业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	交通运输、仓储和邮政业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	住宿和餐饮业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.acti	信息传输、软件和信息技术服务业

on	
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	金融业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	房地产业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	租赁和商务服务业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	科学研究和技术服务业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	水利、环境和公共设施管理业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	居民服务、修理和其他服务业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	教育
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	卫生和社会工作
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	文化、体育和娱乐业
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	公共管理、社会保障和社会组织
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	国际组织
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	main_left End
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<%&#45;&#45; <div class="main_right"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	style="width:27%;float: right;min-width：700px;margin-top: -35px;margin-right:1%;">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash;content_tab&ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div class="content_tab"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash;content_box End&ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div class="con_box">

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div class="con_box_02" style="width:115%">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<h2 style="height: 32px;line-height: 33px;">地图展示</h2>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div id="mainMap" style="height:500px;border:1px solid #ccc;padding:0px 5px 5px 5px;"></div>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<h2 style="height: 32px;line-height: 33px;">快捷入口</h2>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;margin-top:10%;margin-left:2%;margin-bottom: 10%">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;width:100%;">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;width:32%;" align="center">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash; <img style="cursor:pointer;" onclick="clickSSZD()" id="sszdimg"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	src="${ctx}/xmzh/project/img/sszd.png" onmouseover="oversszd()"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	onmouseout="outsszd()" /> <br />&ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<img style="cursor:pointer;" onclick="clickPmtj()" id="pmtjimg"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	th:src="@{/xmzh/project/img/tjpm.png}" src="${ctx}/xmzh/project/img/tjpm.png" onmouseover="overcyy()"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	align="center" onmouseout="outcyy()" /> <br />
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	&lt;!&ndash; <div style="float:left;margin-left:0px;width:32%;" align="center">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<img style="cursor:pointer;" onclick="clickZBLS()" id="zblsimg"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	src="${ctx}/xmzh/project/img/zbls.png" onmouseover="overzbls()"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	align="center" onmouseout="outzbls()" /> <br />
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;margin-left:0px;width:30%;" align="center">
http://127.0.0.1:8000/xmjg/xmj	<img style="cursor:pointer;" onclick="clickCYL()" id="cylimg"

g-statis-show!getSkipPage.action	
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	src="${ctx}/xmzh/project/img/cyl.png" onmouseover="overcyl()"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	align="center" onmouseout="outcyl()" /> <br />
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;width:32%;margin-left:0px;margin-top:20px;"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	align="center">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<img style="cursor:pointer;" onclick="clickTZTJ()" id="tztjimg"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	src="${ctx}/xmzh/project/img/tztj.png" onmouseover="overtztj()"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	onmouseout="outtztj()" />
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;margin-left:0px;width:30%;margin-top:20px;"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<img style="cursor:pointer;" onclick="clickCYY()" id="cyyimg"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	src="${ctx}/xmzh/project/img/cyy.png" onmouseover="overcyy()"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	<div style="float:left;margin-left:3px;width:30%;margin-top:20px;" align="center">
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	src="${ctx}/xmzh/project/img/tjpm.png" onmouseover="overcyy()"
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	</div>&ndash;&gt;
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	</div>&#45;&#45;%>
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	main End
http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action	ECharts单文件引入
http://127.0.0.1:8000/xmjg/city-page/getCsrk.action	<link rel="stylesheet" type="text/css" th:href="@{/xmjg/csrk/css/xmjg-csrk-main-new-rem.css}" href="${ctx}/xmjg/csrk/css/xmjg-csrk-main-new-rem.css"/>
http://127.0.0.1:8000/xmjg/city-page/getCsrk.action	<link rel="stylesheet" type="text/css" th:href="@{/xmjg/css/{screen}/common_new.css(screen=${session.screen})}"/>

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action	<script th:src="@{/xmjg/csrk/js/jquery.min.js}" src="${ctx}/xmjg/csrk/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>
http://127.0.0.1:8000/xmjg/city-page/getCsrk.action	<script th:src="@{/xmjg/csrk/js/city-csrk-main-new.js}" src="${ctx}/xmjg/csrk/js/city-csrk-main-new.js" type="text/javascript" charset="utf-8"></script>
http://127.0.0.1:8000/xmjg/city-page/getCsrk.action	<h3>总数(个)</h3><p id="yrkxms_zs_p" style='cursor:pointer;' onclick="transToQueryAndShow('1','${xzqhdm}',",",",",",",",")"><span>个</span></p>
http://127.0.0.1:8000/xmjg/city-page/getCsrk.action	<h3>本月新增(个)</h3><p id="yrkxms_byxz_p" style="cursor:pointer;" onclick="transToQueryAndShow('1','${xzqhdm}',",'1',",")"><span>个</span></p>
http://127.0.0.1:8000/xmjg/city-page/getCsrk.action	<h3>总数(个)</h3><p id="jgqqxtxms_zx_p" style="cursor:pointer;" onclick="transToQueryAndShow('1','${xzqhdm}',",",",'1')" ><span>个</span></p>
http://127.0.0.1:8000/xmjg/city-page/getCsrk.action	<li> <div class="item-ul-bg"> <p id="QQXT_XZBJL" style="cursor:pointer;" > <span>个</span></p> <h3 >办件总量(件)</h3> </div > </li >
http://127.0.0.1:8000/xmjg/city-page/getCsrk.action	<a id="city-select-btn" style="display:none" href="javascript:doSelectCitys('city-select-btn');" data-select-city-input-id="city_select_input">师市切换</a>
http://127.0.0.1:8000/xmjg/city-page/getCsrk.action	<th>补正</th> <th>挂起</th>
http://127.0.0.1:8000/xmjg/city-page/getCsrk.action	<td>-</td> <td>-</td>
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	引入样式
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	<script src="/xmjg/resources/easyui/jquery.min.js" type="text/javascript"></script>
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	暂时没有调用的地方，是否删除
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	判断点击了左侧哪个项目统计分类
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	当前选择的城市
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	投资类型 饼图
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	审批阶段 4个环形图
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	<a id="zt2" href="javascript:;" onclick="showProInfo_img('zt2','已办结',",'3');namechange('已办结');">已办结<span class="number_1" id="count_yb"></span></a>
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	<a id="zt4" href="javascript:;" onclick="showProInfo_img('zt4','办结逾期',",'6');namechange('办结逾期');">办结逾期<span class="number_1" id="count_csybList"></span></a>
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	style="height:270px;"
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	******
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	<div class="xmspjd_time" style="width: auto;height: 24px;float: right;margin: 10px 20px ;border: 0px" id="timeSearchDiv"> <input class="form-control selectData" type="text" name="" id="dateStart" value="2019-01-01" readonly="readonly" /> <span>-</span>

	<input class='form-control' type="text" name="" id="dateEnd" readonly="readonly" /> <input type="button" class="oneSystemSearch" name="" id="timeSearch" value="查询" /> <input type="button" class="oneSystemReset" name="" id="timeReset" value="重置" /> </div>
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	chageClass(this.id);
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	柱状图区
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	<div class="table-right">
http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do	历史附件
http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do	tab End
http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do	<th style="text-align:center" width="10%">建设项目类型</th>
http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do	<th style="text-align:center" width="6%">在办数 <span onclick="orderByTitle('orderByZB',this)" id="orderImgZB" class="order-img pt-arrow"></span></th> <th style="text-align:center" width="6%">办结数 <span onclick="orderByTitle('orderImgBJ',this)" id="orderImgBJ" class="order-img pt-arrow"></span></th> <th style="text-align:center" width="6%">逾期数 <span onclick="orderByTitle('orderImgYQ',this)" id="orderImgYQ" class="order-img pt-arrow"></span></th> <th style="text-align:center" width="8%">并行事项数 <span onclick="orderByTitle('orderImgBX',this)" id="orderImgBX" class="order-img pt-arrow"></span></th> <th style="text-align:center" width="6%">退件数 <span onclick="orderByTitle('orderImgTJ',this)" id="orderImgTJ" class="order-img pt-arrow"></span></th>
http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do	sg_content END
http://127.0.0.1:8000/xmjg/xmjg-one-window!getYgck.action	<div class="time-row">发表日期：2018-10-16 </div>
http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action	<script src="/xmjg/xmjg/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>
http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action	<script src="/xmjg/xmjg/js/jquery.easyui.min.js" type="text/javascript" charset="utf-8"></script>
http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action	<script src="/xmjg/resources/js/jquery/form/jquery.form.js" type="text/javascript"></script>
http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action	<a id="backid" style="" href="javascript:">返　回</a>
http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action	<div class="file-list" style=""> 审批流程版本号：<select style="height: 30px;width: 80px;" id="splcbbh" onchange="changeSplcbbh()"></select> </div >
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html	Copyright 2012 Mozilla Foundation Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

	http://www.apache.org/licenses/LICENSE-2.0 Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License. Adobe CMap resources are covered by their own copyright but the same license: Copyright 1990-2015 Adobe Systems Incorporated. See https://github.com/adobe-type-tools/cmap-resources
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html	This snippet is used in production (included from viewer.html)
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html	sidebarContainer
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html	findbar
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html	secondaryToolbar
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html	mainContainer
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html	overlayContainer
http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.html	outerContainer
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do	<div style="font-size: 40px;margin-left: 39.7%;letter-spacing: 3px;" class="index-card-tit center-tit">各城市项目逾期率排名</div> <div style="font-size: 28px;margin-left: 41.8%;color:#fff">(<span id="startDay">2</span>—<span id="endDay"></span>)</div>
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do	<div class="index-card-tit center-tit rank-title1">各城市项目逾期率排名</div>
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do	<div class="rank-date-d1">(<span id="startDay"></span>—<span id="endDay"></span>)</div>
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do	<a class="rank-btn" id="goBackBtn" ><i></i>返回</a>
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do	计算规则一
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do	剔除异常数据
http://127.0.0.1:8000/xmjg/sup	计算规则二

ervisionInspectionDrill/getSupervisionInspectionDrillPage.do	
http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do	计算规则三

JavaScript 305

TOC

URL / 代码

http://127.0.0.1:8090/opus-front-sso/js/jquery.validate.min.js

```
/*! jQuery Validation Plugin - v1.19.1 - 6/15/2019
 * https://jqueryvalidation.org/
 * Copyright (c) 2019 Jörn Zaefferer; Licensed MIT */
!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):"object"==typeof
module&&module.exports?module.exports=a(require("jquery")):a(jQuery)}(function(a){a.extend(a.fn,
{validate:function(b){if(!this.length)return void(b&&b.debug&&window.console&&console.warn("Nothing selected,
can't validate, returning nothing."));var c=a.data(this[0],"validator");return c?c:
(this.attr("novalidate","novalidate"),c=new
a.validator(b,this[0]),a.data(this[0],"validator",c),c.settings.onsubmit&&
(this.on("click.validate",":submit",function(b){c.submitButton=b.currentTarget,a(this).hasClass("cancel")&&
(c.cancelSubmit=!0),void 0!==a(this).attr("formnovalidate")&&
(c.cancelSubmit=!0)}),this.on("submit.validate",function(b){function d(){var d,e;return c.submitButton&&
(c.settings.submitHandler||c.formSubmitted)&&(d=a("<input
type='hidden'/>").attr("name",c.submitButton.name).val(a(c.submitButton).val()).appendTo(c.currentForm)),!
(c.settings.submitHandler&&!c.settings.debug)||
(e=c.settings.submitHandler.call(c,c.currentForm,b),d&&d.remove(),void 0!==e&&e)}return
c.settings.debug&&b.preventDefault(),c.cancelSubmit?(c.cancelSubmit=!1,d()):c.form()?c.pendingRequest?
(c.formSubmitted=!0,!1):d():(c.focusInvalid(),!1)})),c)},valid:function(){var b,c,d;return
a(this[0]).is("form")?b=this.validate().form():(d=[],b=!0,c=a(this[0].form).validate(),this.each(function()
{b=c.element(this)&&b,b||(d=d.concat(c.errorList))}),c.errorList=d),b},rules:function(b,c){var
d,e,f,g,h,i,j=this[0],k="undefined"!=typeof
this.attr("contenteditable")&&"false"!==this.attr("contenteditable");if(null!=j&&(!j.form&&k&&
(j.form=this.closest("form")[0],j.name=this.attr("name")),null!=j.form))
{if(b)switch(d=a.data(j.form,"validator").settings,e=d.rules,f=a.validator.staticRules(j),b)
{case"add":a.extend(f,a.validator.normalizeRule(c)),delete f.messages,e[j.name]=f,c.messages&&
(d.messages[j.name]=a.extend(d.messages[j.name],c.messages));break;case"remove":return c?(i=
{},a.each(c.split(/\s/),function(a,b){i[b]=f[b],delete f[b]}),i):(delete e[j.name],f)}return
g=a.validator.normalizeRules(a.extend({},a.validator.classRules(j),a.validator.attributeRules(j),a.validator.
dataRules(j),a.validator.staticRules(j)),j),g.required&&(h=g.required,delete
g.required,g=a.extend({required:h},g)),g.remote&&(h=g.remote,delete g.remote,g=a.extend(g,
{remote:h})),g}}}),a.extend(a.expr.pseudos||a.expr[":"],{blank:function(b)
{return!a.trim(""+a(b).val())},filled:function(b){var c=a(b).val();return
null!==c&&!!a.trim(""+c)},unchecked:function(b){return!a(b).prop("checked")}}),a.validator=function(b,c)
{this.settings=a.extend(!0,
{},a.validator.defaults,b),this.currentForm=c,this.init()},a.validator.format=function(b,c){return
1===arguments.length?function(){var c=a.makeArray(arguments);return
c.unshift(b),a.validator.format.apply(this,c)}:void 0===c?b:(arguments.length>2&&c.constructor!==Array&&
(c=a.makeArray(arguments).slice(1)),c.constructor!==Array&&(c=[c]),a.each(c,function(a,c){b=b.replace(new
RegExp("\\{"+a+"\\}","g"),function(){return c})}),b)},a.extend(a.validator,{defaults:{messages:{},groups:
{},rules:
{},errorClass:"error",pendingClass:"pending",validClass:"valid",errorElement:"label",focusCleanup:!1,focusInv
alid:!0,errorContainer:a([]),errorLabelContainer:a([]),onsubmit:!0,ignore:":hidden",ignoreTitle:!1,onfocusin:
function(a){this.lastActive=a,this.settings.focusCleanup&&
(this.settings.unhighlight&&this.settings.unhighlight.call(this,a,this.settings.errorClass,this.settings.vali
dClass),this.hideThese(this.errorsFor(a)))},onfocusout:function(a){this.checkable(a)||!(a.name in
this.submitted)&&this.optional(a)||this.element(a)},onkeyup:function(b,c){var d=
[16,17,18,20,35,36,37,38,39,40,45,144,225];9===c.which&&""===this.elementValue(b)||a.inArray(c.keyCode,d)!==-
1||(b.name in this.submitted||b.name in this.invalid)&&this.element(b)},onclick:function(a){a.name in
this.submitted?this.element(a):a.parentNode.name in
this.submitted&&this.element(a.parentNode)},highlight:function(b,c,d){"radio"===b.type?
this.findByName(b.name).addClass(c).removeClass(d):a(b).addClass(c).removeClass(d)},unhighlight:function(b,c,
d){"radio"===b.type?
this.findByName(b.name).removeClass(c).addClass(d):a(b).removeClass(c).addClass(d)}},setDefaults:function(b)
{a.extend(a.validator.defaults,b)},messages:{required:"This field is required.",remote:"Please fix this
field.",email:"Please enter a valid email address.",url:"Please enter a valid URL.",date:"Please enter a
```

```
valid date.",dateISO:"Please enter a valid date (ISO).",number:"Please enter a valid number.",digits:"Please
enter only digits.",equalTo:"Please enter the same value again.",maxlength:a.validator.format("Please enter
no more than {0} characters."),minlength:a.validator.format("Please enter at least {0}
characters."),rangelength:a.validator.format("Please enter a value between {0} and {1} characters
long."),r...
```

http://127.0.0.1:8090/opus-front-sso/js/jquery-3.4.1.min.js

```
/*! jQuery v3.4.1 | (c) JS Foundation and other contributors | jquery.org/license */
!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?
module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a
document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(C,e){"use strict";var t=
[],E=C.document,r=Object.getPrototypeOf,s=t.slice,g=t.concat,u=t.push,i=t.indexOf,n=
{},o=n.toString,v=n.hasOwnProperty,a=v.toString,l=a.call(Object),y={},m=function(e){return"function"==typeof
e&&"number"!=typeof e.nodeType},x=function(e){return null!=e&&e===e.window},c=
{type:!0,src:!0,nonce:!0,noModule:!0};function b(e,t,n){var r,i,o=
(n=n||E).createElement("script");if(o.text=e,t)for(r in c)
(i=t[r]||t.getAttribute&&t.getAttribute(r))&&o.setAttribute(r,i);n.head.appendChild(o).parentNode.removeChild
(o)}function w(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?n[o.call(e)]||"object":typeof
e}var f="3.4.1",k=function(e,t){return new k.fn.init(e,t)},p=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g;function
d(e){var t=!!e&&"length"in e&&e.length,n=w(e);return!m(e)&&!x(e)&&("array"===n||0===t||"number"==typeof
t&&0<t&&t-1 in e)}k.fn=k.prototype={jquery:f,constructor:k,length:0,toArray:function(){return
s.call(this)},get:function(e){return null==e?s.call(this):e<0?
this[e+this.length]:this[e]},pushStack:function(e){var t=k.merge(this.constructor(),e);return
t.prevObject=this,t},each:function(e){return k.each(this,e)},map:function(n){return
this.pushStack(k.map(this,function(e,t){return n.call(e,t,e)}))},slice:function(){return
this.pushStack(s.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return this.eq(-
1)},eq:function(e){var t=this.length,n=+e+(e<0?t:0);return this.pushStack(0<=n&&n<t?[this[n]]:
[])},end:function(){return
this.prevObject||this.constructor()},push:u,sort:t.sort,splice:t.splice},k.extend=k.fn.extend=function(){var
e,t,n,r,i,o,a=arguments[0]||{},s=1,u=arguments.length,l=!1;for("boolean"==typeof a&&(l=a,a=arguments[s]||
{},s++),"object"==typeof a||m(a)||(a={}),s===u&&(a=this,s--);s<u;s++)if(null!=(e=arguments[s]))for(t in
e)r=e[t],"__proto__"!==t&&a!==r&&(l&&r&&(k.isPlainObject(r)||(i=Array.isArray(r)))?
(n=a[t],o=i&&!Array.isArray(n)?[]:i||k.isPlainObject(n)?n:{},i=!1,a[t]=k.extend(l,o,r)):void 0!==r&&
(a[t]=r));return a},k.extend({expando:"jQuery"+
(f+Math.random()).replace(/\D/g,""),isReady:!0,error:function(e){throw new Error(e)},noop:function()
{},isPlainObject:function(e){var t,n;return!(!e||"[object Object]"!==o.call(e))&&(!
(t=r(e))||"function"==typeof(n=v.call(t,"constructor")&&t.constructor)&&a.call(n)===l)},isEmptyObject:functio
n(e){var t;for(t in e)return!1;return!0},globalEval:function(e,t){b(e,{nonce:t&&t.nonce})},each:function(e,t)
{var n,r=0;if(d(e)){for(n=e.length;r<n;r++)if(!1===t.call(e[r],r,e[r]))break}else for(r in
e)if(!1===t.call(e[r],r,e[r]))break;return e},trim:function(e){return null==e?"":
(e+"").replace(p,"")},makeArray:function(e,t){var n=t||[];return null!=e&&(d(Object(e))?
k.merge(n,"string"==typeof e?[e]:e):u.call(n,e)),n},inArray:function(e,t,n){return null==t?-
1:i.call(t,e,n)},merge:function(e,t){for(var n=+t.length,r=0,i=e.length;r<n;r++)e[i++]=t[r];return
e.length=i,e},grep:function(e,t,n){for(var r=
[],i=0,o=e.length,a=!n;i<o;i++)!t(e[i],i)!==a&&r.push(e[i]);return r},map:function(e,t,n){var r,i,o=0,a=
[];if(d(e))for(r=e.length;o<r;o++)null!=(i=t(e[o],o,n))&&a.push(i);else for(o in e)null!=
(i=t(e[o],o,n))&&a.push(i);return g.apply([],a)},guid:1,support:y}),"function"==typeof Symbol&&
(k.fn[Symbol.iterator]=t[Symbol.iterator]),k.each("Boolean Number String Function Array Date RegExp Object
Error Symbol".split(" "),function(e,t){n["[object "+t+"]"]=t.toLowerCase()});var h=function(n){var
e,d,b,o,i,h,f,g,w,u,l,T,C,a,E,v,s,c,y,k="sizzle"+1*new
Date,m=n.document,S=0,r=0,p=ue(),x=ue(),N=ue(),A=ue(),D=function(e,t){return e===t&&(l=!0),0},j=
{}.hasOwnProperty,t=[],q=t.pop,L=t.push,H=t.push,O=t.slice,P=function(e,t){for(var
n=0,r=e.length;n<r;n++)if(e[n]===t)return n;return-
1},R="checked|selected|async|autofocus|autoplay|controls|defer|disabled|hidden|ismap|loop|multiple|open|reado
nly|required|scoped",M="[\\x20\\t\\r\\n\\f]",I="(?:\\\\.|[\\w-]|[^\0-\\xa0])+",W="\\["+M+"*("+I+")(?:"+M+"*
([*^$|!~]?=)"+M+"*(?:'((?:\\\\.|[^\\\\'])*)'|\"((?:\\\\.|[^\\\\\"])*)\"|("+I+"))|)"+M+"*\\]",$=":("+I+")(?:\\
((('((?:\\\\.|[^\\\\'])*)'|\"((?:\\\\.|[^\\\\\"])*)\")|((?:\\\\.|[^\\\\()[\\]]|"+W+")*)|.*)\\)|)",F=new
RegExp(M+"+","g"),B=new RegExp("^"+M+"+|((?:^|[^\\\\])(?:\\\\.)*)"+M+"+$","g"),_=new
RegExp("^"+M+"*,"+M+"*"),z=new RegExp("^"+M+"*([>+~]|"+M+")"+M+"*"),U=new RegExp(M+"|>"),X=new
RegExp($),V=new RegExp("^"+I+"$"),G={ID:new RegExp("^#("+I+")"),CLASS:new RegExp("^\\.("+I+")"),TAG:new
RegExp("^("+I+"|[*])"),ATTR:new RegExp("^"+W),PSEUDO:new RegExp("^"+$),CHILD:new RegExp("^:
(only|first|last|nth|nth-last)-(child|of-type)(?:\\("+M+"*(even|odd|(([+-]|)(\\d*)n|)"+M+"*(?:([+-]|)"+M+"*
(\\d+...
```

http://127.0.0.1:8090/opus-front-sso/authentication/require

```
        var ctx = '/opus-front-sso/';        var verifyCodeIsOpen = '${verifyCodeIsOpen}';        //设置高亮
```

```
(对象,位置)        function setCaret(textbox,start){          try{          if(textbox.createTextRange){
var r=textbox.createTextRange();          r.moveStart('character',start);          r.select();          }else
if(textbox.setSelectionRange){          textbox.setSelectionRange(0,textbox.value.length);
textbox.focus();          }          }catch(e){}        }        function getPic(){
$('#verifyCodeImg').attr("src", ctx + 'code/image?time1='+ new Date().getTime());        }        function
checkPwd() {          var layer ;          layui.use('layer', function(){          layer = layui.layer;
});          var reg = new RegExp(/^[0-9]+.?[0-9]*$/);//工作密码是否是数字串          var pwd =
$('#password_text').val().trim();          if  (pwd.length < 8 || reg.test(pwd)){          layer.msg('密码过于
简单，请登录后进行修改！', {time: 2000, icon:6});          }        }
```

http://127.0.0.1:8090/opus-front-sso/authentication/require

```
setCaret(this,0)
```

http://127.0.0.1:8090/opus-front-sso/js/layui.all.js

```
/** layui-v2.5.5 MIT License By https://www.layui.com */
 ;!function(e){"use strict";var t=document,o={modules:{},status:{},timeout:10,event:{}},n=function()
{this.v="2.5.5"},r=function(){var e=t.currentScript?t.currentScript.src:function(){for(var
e,o=t.scripts,n=o.length-1,r=n;r>0;r--)if("interactive"===o[r].readyState){e=o[r].src;break}return
e||o[n].src}();return e.substring(0,e.lastIndexOf("/")+1)}(),i=function(t)
{e.console&&console.error&&console.error("Layui hint: "+t)},a="undefined"!=typeof opera&&"[object
Opera]"===opera.toString(),u=
{layer:"modules/layer",laydate:"modules/laydate",laypage:"modules/laypage",laytpl:"modules/laytpl",layim:"mod
ules/layim",layedit:"modules/layedit",form:"modules/form",upload:"modules/upload",transfer:"modules/transfer"
,tree:"modules/tree",table:"modules/table",element:"modules/element",rate:"modules/rate",colorpicker:"modules
/colorpicker",slider:"modules/slider",carousel:"modules/carousel",flow:"modules/flow",util:"modules/util",cod
e:"modules/code",jquery:"modules/jquery",mobile:"modules/mobile","layui.all":"../layui.all"};n.prototype.cach
e=o,n.prototype.define=function(e,t){var n=this,r="function"==typeof e,i=function(){var e=function(e,t)
{layui[e]=t,o.status[e]=!0};return"function"==typeof t&&t(function(n,r){e(n,r),o.callback[n]=function()
{t(e)}}),this};return r&&(t=e,e=[]),!layui["layui.all"]&&layui["layui.mobile"]?i.call(n):
(n.use(e,i),n)},n.prototype.use=function(e,n,l){function s(e,t){var n="PLaySTATION
3"===navigator.platform?/^complete$/:/^(complete|loaded)$/;
("load"===e.type||n.test((e.currentTarget||e.srcElement).readyState))&&
(o.modules[f]=t,d.removeChild(v),function r(){return++m>1e3*o.timeout/4?i(f+" is not a valid
module"):void(o.status[f]?c():setTimeout(r,4))}())}function c(){l.push(layui[f]),e.length>1?
y.use(e.slice(1),n,l):"function"==typeof n&&n.apply(layui,l)}var y=this,p=o.dir=o.dir?
o.dir:r,d=t.getElementsByTagName("head")[0];e="string"==typeof e?[e]:e,window.jQuery&&jQuery.fn.on&&
(y.each(e,function(t,o){"jquery"===o&&e.splice(t,1)}),layui.jquery=layui.$=jQuery);var f=e[0],m=0;if(l=l||
[],o.host=o.host||(p.match(/\/\/([\s\S]+?)\//)||["//"+location.host+"/"])
[0],0===e.length||layui["layui.all"]&&u[f]||!layui["layui.all"]&&layui["layui.mobile"]&&u[f])return
c(),y;if(o.modules[f])!function g(){return++m>1e3*o.timeout/4?i(f+" is not a valid
module"):void("string"==typeof o.modules[f]&&o.status[f]?c():setTimeout(g,4))}();else{var
v=t.createElement("script"),h=(u[f]?p+"lay/":/^\{\/\}/.test(y.modules[f])?"":o.base||"")+
(y.modules[f]||f)+".js";h=h.replace(/^\{\/\}/,""),v.async=!0,v.charset="utf-8",v.src=h+function(){var
e=o.version===!0?o.v||(new Date).getTime():o.version||"";return e?"?v="+e:""}
(),d.appendChild(v),!v.attachEvent||v.attachEvent.toString&&v.attachEvent.toString().indexOf("[native code")
<0||a?v.addEventListener("load",function(e){s(e,h)},!1):v.attachEvent("onreadystatechange",function(e)
{s(e,h)}),o.modules[f]=h}return y},n.prototype.getStyle=function(t,o){var n=t.currentStyle?
t.currentStyle:e.getComputedStyle(t,null);return n[n.getPropertyValue?"getPropertyValue":"getAttribute"]
(o)},n.prototype.link=function(e,n,r){var a=this,u=t.createElement("link"),l=t.getElementsByTagName("head")
[0];"string"==typeof n&&(r=n);var s=(r||e).replace(/\.|\//g,""),c=u.id="layuicss-"+s,y=0;return
u.rel="stylesheet",u.href=e+(o.debug?"?v="+(new
Date).getTime():""),u.media="all",t.getElementById(c)||l.appendChild(u),"function"!=typeof n?a:(function p()
{return++y>1e3*o.timeout/100?i(e+" timeout"):void(1989===parseInt(a.getStyle(t.getElementById(c),"width"))?
function(){n()}():setTimeout(p,100))}(),a)},o.callback={},n.prototype.factory=function(e)
{if(layui[e])return"function"==typeof o.callback[e]?o.callback[e]:null},n.prototype.addcss=function(e,t,n)
{return layui.link(o.dir+"css/"+e,t,n)},n.prototype.img=function(e,t,o){var n=new Image;return
n.src=e,n.complete?t(n):(n.onload=function(){n.onload=null,"function"==typeof
t&&t(n)},void(n.onerror=function(e){n.onerror=null,"function"==typeof
o&&o(e)}))},n.prototype.config=function(e){e=e||{};for(var t in e)o[t]=e[t];return
this},n.prototype.modules=function(){var e={};for(var t in u)e[t]=u[t];return e}
(),n.prototype.extend=function(e){var t=this;e=e||{};for(var o in e)t[o]||t.modules[o]?i("模块名 "+o+" 已被占
用"):t.modules[o]=e[o];return t},n.prototype.router=function(e){var t=this,e=e||location.hash,o={path:
[],search:{},hash:(e.match(/[^#](#.*$)/)||[])[1]||""};return/^#\//.test(e)?
(e=e.replace(/^#\//,""),o.href="/"+e,e=e.replace(/([^#])(#.*$)/,"$1").split("/")||[],t.each(e,function(e,t)
{/^\w+=/.test(t)?function(){t=t.split("="),o.search[t[0]]=t[1]}
():o.path.push(t)}),o):o},n.prototype.data=function(t,o,n)
```

```
{if(t=t||"layui",n=n||localStorage,e.JSON&&e.JSON.parse){if(null===o)return delete n[t];o="object"==typeof o?
o:{key:o};try{var r=JSON.parse(n[t])}catch(i){var r={}}return"value"in o&&(r[o.key]=o.value),o.remove&&delete
r[o.key],n[t]=JSON.stringify(r),o.key?r[o.key]:r}},n.prototype.sessionData=function(e,t){return
this.data(e,t...
```

http://127.0.0.1:8090/opus-front-sso/js/md5.js

```
/*
 * A JavaScript implementation of the RSA Data Security, Inc. MD5 Message
 * Digest Algorithm, as defined in RFC 1321.
 * Version 2.2 Copyright (C) Paul Johnston 1999 - 2009
 * Other contributors: Greg Holt, Andrew Kepert, Ydnar, Lostinet
 * Distributed under the BSD License
 * See http://pajhome.org.uk/crypt/md5 for more info.
 */

/*
 * Configurable variables. You may need to tweak these to be compatible with
 * the server-side, but the defaults work in most cases.
 */
var hexcase = 0;   /* hex output format. 0 - lowercase; 1 - uppercase        */
var b64pad  = "";  /* base-64 pad character. "=" for strict RFC compliance   */

/*
 * These are the functions you'll usually want to call
 * They take string arguments and return either hex or base-64 encoded strings
 */
function hex_md5(s)    { return rstr2hex(rstr_md5(str2rstr_utf8(s))); }
function b64_md5(s)    { return rstr2b64(rstr_md5(str2rstr_utf8(s))); }
function any_md5(s, e) { return rstr2any(rstr_md5(str2rstr_utf8(s)), e); }
function hex_hmac_md5(k, d)
  { return rstr2hex(rstr_hmac_md5(str2rstr_utf8(k), str2rstr_utf8(d))); }
function b64_hmac_md5(k, d)
  { return rstr2b64(rstr_hmac_md5(str2rstr_utf8(k), str2rstr_utf8(d))); }
function any_hmac_md5(k, d, e)
  { return rstr2any(rstr_hmac_md5(str2rstr_utf8(k), str2rstr_utf8(d)), e); }

/*
 * Perform a simple self-test to see if the VM is working
 */
function md5_vm_test()
{
  return hex_md5("abc").toLowerCase() == "900150983cd24fb0d6963f7d28e17f72";
}

/*
 * Calculate the MD5 of a raw string
 */
function rstr_md5(s)
{
  return binl2rstr(binl_md5(rstr2binl(s), s.length * 8));
}

/*
 * Calculate the HMAC-MD5, of a key and some data (raw strings)
 */
function rstr_hmac_md5(key, data)
{
  var bkey = rstr2binl(key);
  if(bkey.length > 16) bkey = binl_md5(bkey, key.length * 8);

  var ipad = Array(16), opad = Array(16);
  for(var i = 0; i < 16; i++)
  {
    ipad[i] = bkey[i] ^ 0x36363636;
    opad[i] = bkey[i] ^ 0x5C5C5C5C;
  }

  var hash = binl_md5(ipad.concat(rstr2binl(data)), 512 + data.length * 8);
  return binl2rstr(binl_md5(opad.concat(hash), 512 + 128));
}

/*
```

```
 * Convert a raw string to a hex string
 */
function rstr2hex(input)
{
  try { hexcase } catch(e) { hexcase=0; }
  var hex_tab = hexcase ? "0123456789ABCDEF" : "0123456789abcdef";
  var output = "";
  var x;
  for(var i = 0; i < input.length; i++)
  {
    x = input.charCodeAt(i);
    output += hex_tab.charAt((x >>> 4) & 0x0F)
          +  hex_tab.charAt( x        & 0x0F);
  }
  return output;
}

/*
 * Convert a raw string to a base-64 string
 */
function rstr2b64(input)
{
  try { b64pad } catch(e) { b64pad=''; }
  var tab = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";
  var output = "";
  var len = input.length;
  for(var i = 0; i < len; i += 3)
  {
    var triplet = (input.charCodeAt(i) << 16)
          | (i + 1 < len ? input.charCodeAt(i+1) << 8 : 0)
          | (i + 2 < len ? input.charCodeAt(i+2)      : 0);
    for(var j = 0; j < 4; j++)
    {
      if(i * 8 + j * 6 > input.length * 8) output += b64pad;
      else output += tab.charAt((triplet >>> 6*(3-j)) & 0x3F);
    }
  }
  return output;
}

/*
 * Convert a raw string to an arbitrary string encoding
 */
function rstr2any(input, encoding)
{
  var divisor = encoding.length;
  var i, j, q, x, quotient;

  /* Convert to an array of 16-bit big-endian values, forming the dividend */
  var dividend = Array(Math.ceil(input.length / 2));
  for(i = 0; i < dividend.length; i++)
  {
    dividend[i] = (input.charCodeAt(i * 2) << 8) | input.charCodeAt(i * 2 + 1);
  }

  /*
   * Repeatedly perform a long division. The binary array forms the dividend,
   * the length of the encoding is the divisor. Once computed, the quotient
   * forms the dividend for the next step. All remainders are stored for later
   * use.
   */
  var full_length = Math.ceil(input.length * 8 /
          (Math.log(encoding.length) / Math.log(2)));
  var remainders = Array(full_length);
  for(j = 0; j < full_length; j++)
  {
    quotient = Array();
    x = 0;
    for(i = 0; i < dividend.length; i++)
    {
      x = (x << 16) + dividend[i];
      q = Math.floor(x / divisor);
      x -= q * divisor;
      if(quotient.length > 0 || q > 0)
        quotient[quotient.length] = q;
    }
    remainders[j] = x;
    dividend = quotient;
  }

  /* Convert the remainders to the output string */
  var output = "";
  for(i = remainders.length - 1; i >= 0; i--)
    output += encoding.charAt(remainders[i]);

  return output;
}

/*
 * Encode a string as utf-8.
 * For efficiency, this assumes the input is valid utf-16.
 */
function str2rstr_utf8(input)
{
  var output = "";
  var i = -1;
  var x, y;

  while(++i < input.length)
  {
    /* Decode utf-16 surrogate pairs */
    x = input.charCodeAt(i);
    y = i + 1 < input.le...
```

http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/jquery.cookie.js

```
/**
 * Cookie plugin
 *
 * Copyright (c) 2006 Klaus Hartl (stilbuero.de)
 * Dual licensed under the MIT and GPL licenses:
 * http://www.opensource.org/licenses/mit-license.php
 * http://www.gnu.org/licenses/gpl.html
 *
 */

/**
 * Create a cookie with the given name and value and other optional parameters.
 *
 * @example $.cookie('the_cookie', 'the_value');
 * @desc Set the value of a cookie.
 * @example $.cookie('the_cookie', 'the_value', { expires: 7, path: '/', domain: 'jquery.com', secure: true
});
 * @desc Create a cookie with all available options.
 * @example $.cookie('the_cookie', 'the_value');
 * @desc Create a session cookie.
 * @example $.cookie('the_cookie', null);
 * @desc Delete a cookie by passing null as value. Keep in mind that you have to use the same path and domain
 *       used when the cookie was set.
 *
 * @param String name The name of the cookie.
 * @param String value The value of the cookie.
 * @param Object options An object literal containing key/value pairs to provide optional cookie attributes.
 * @option Number|Date expires Either an integer specifying the expiration date from now on in days or a Date
object.
 *          If a negative value is specified (e.g. a date in the past), the cookie will be deleted.
 *          If set to null or omitted, the cookie will be a session cookie and will not be retained
 *          when the the browser exits.
 * @option String path The value of the path atribute of the cookie (default: path of page that created the
cookie).
 * @option String domain The value of the domain attribute of the cookie (default: domain of page that
created the cookie).
 * @option Boolean secure If true, the secure attribute of the cookie will be set and the cookie transmission
will
 *          require a secure protocol (like HTTPS).
 * @type undefined
 *
 * @name $.cookie
 * @cat Plugins/Cookie
 * @author Klaus Hartl/klaus.hartl@stilbuero.de
 */
```

```
/**
 * Get the value of a cookie with the given name.
 *
 * @example $.cookie('the_cookie');
 * @desc Get the value of a cookie.
 *
 * @param String name The name of the cookie.
 * @return The value of the cookie.
 * @type String
 *
 * @name $.cookie
 * @cat Plugins/Cookie
 * @author Klaus Hartl/klaus.hartl@stilbuero.de
 */
jQuery.cookie = function(name, value, options) {
    if (typeof value != 'undefined') { // name and value given, set cookie
        options = options || {};
        if (value === null) {
          value = '';
          options = $.extend({}, options); // clone object since it's unexpected behavior if the expired
property were changed
          options.expires = -1;
        }
        var expires = '';
        if (options.expires && (typeof options.expires == 'number' || options.expires.toUTCString)) {
          var date;
          if (typeof options.expires == 'number') {
          date = new Date();
          date.setTime(date.getTime() + (options.expires * 24 * 60 * 60 * 1000));
          } else {
          date = options.expires;
          }
          expires = '; expires=' + date.toUTCString(); // use expires attribute, max-age is not supported by
IE
        }
        // NOTE Needed to parenthesize options.path and options.domain
        // in the following expressions, otherwise they evaluate to undefined
        // in the packed version for some reason...
        var path = options.path ? '; path=' + (options.path) : '';
        var domain = options.domain ? '; domain=' + (options.domain) : '';
        var secure = options.secure ? '; secure' : '';
        document.cookie = [name, '=', encodeURIComponent(value), expires, path, domain, secure].join('');
    } else { // only name given, get cookie
        var cookieValue = null;
        if (document.cookie && document.cookie != '') {
          var cookies = document.cookie.split(';');
          for (var i = 0; i < cookies.length; i++) {
          var cookie = jQuery.trim(cookies[i]);
          // Does this cookie string begin with the name we want?
          if (cookie.substring(0, name.length + 1) == (name + '=')) {
          cookieValue = decodeURIComponent(cookie.substring(name.length + 1));
          break;
          }
          }
        }
        return cookieValue;
    }
};
```

http://127.0.0.1:8090/opus-front-sso/js/login.js

```
var rules = {};
var messages = {};
if (verifyCodeIsOpen == 'true') {
    rules = {
        username_text: {
          required: true,
          minlength: 2
        },
        password_text: {
          required: true,
          minlength: 3
        },
        imageCode: {
          required: true,
        }
    };

    messages = {
        username_text: {
          required: "请输入用户名",
          minlength: "用户名不能小于3个字符"
        },
        password_text: {
          required: "请输入密码",
          minlength: "密码不能小于3个字符"
        },
        imageCode: {
          required: "请输入验证码",
        }
    };
} else {
    rules = {
        username_text: {
          required: true,
          minlength: 2
        },
        password_text: {
          required: true,
          minlength: 3
        }
    };

    messages = {
        username_text: {
          required: "请输入用户名",
          minlength: "用户名不能小于3个字符"
        },
        password_text: {
          required: "请输入密码",
          minlength: "密码不能小于3个字符"
        }
    };
}

var _base64 = null;
var sm4 = null;
$(function(){
 //       判断是否启用验证码，启用则输入框纵向排列
 if($(".verify-code").length > 0){
     $(".login_wel").addClass('login_wel_new');
     $(".login-content").addClass('login-content-new');
     $(".login01").addClass('login01-new');
     $(".login-input-group ").addClass("verify-code-Ul");
     $(".login-btn").addClass('login-btn-new ');
        }
 $(".login-content").show();

    var orgId = 'A';
    // var orgId ='b5b092b5-dcad-4524-9631-a73d78e55591';

    _base64 = new Base64();
    sm4 = new SM4Util();
    var spring_error = $("#spring_error").html();

    if (spring_error != undefined) {
        if (spring_error.indexOf("初始化密码") != -1) {

          var form = $("#editPassword");
          var loginName = $.cookie("username");
          if (loginName == "") {
          loginName = $("#username_text").val();
          }
          layer.open({
          type: 1,
          title: '重置初始化密码',
          area: ['490px', '350px'],
          shadeClose: true, //点击遮罩关闭
          content: form,
          btn: ['保存', '取消'],
          btn2: function() {
          layer.closeAll();
          },
          yes: function() {
          if (!form.valid()) {
          return;
          } else {
          $.ajax({
          type: "post",
          url: ctx + 'authentication/user/password',
          data: {
          'loginName': sm4.encryptData_ECB(loginName),
          'oldPassword': sm3(hex_md5($("input[name='oldPassword']").val())),
          'proPassword': sm3(sm4.encryptData_ECB($("input[name='oldPassword']").val())),
          'newPassword': sm3(sm4.encryptData_ECB($("input[name='newPassword']").val()))
          },
          success: function(data) {
          if (data.success) {
          $("#password_text").val($("input[name='newPassword']").val());
          $("#password").val($("input[name='newPassword']").val());
          if (verifyCodeIsOpen) {
          $("#resetPasswordId").val("1");
          }
          $.cookie("username", $("#username_text").val(), { expires: 7 });
          $("#orgId").val(sm4.encryptData_ECB(orgId));
          $("#username").val(sm4.encryptData_ECB($("#username_text").val()));
          $("#password").val(sm3(hex_md5($("#password_text").val())));
          $("#proPassword").val(sm3(sm4.encryptData_ECB($("#password_text").val())));
          $('#deviceType').val(sm4.encryptData_ECB($("#deviceType").val()));
          $('#login_form').submit();
          layer.closeAll();
          } else {
          showErrorMsg(data.message);
          }
          }
          });
          }
          }
          });

          jQuery.validator.addMethod("checkOldPassword", function(value, element) {
          var oldPassword = $("input[name='oldPassword']").val();
          if (value == oldPassword) {
          return false;
          }
          return true;
          }, "<font color='ff0000' style='margin-left: 10%'>新密码和原密码不能相同</font>");

          jQuery.validator.addMethod("checkPasswor...
```

http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/jquery.mousewheel.min.js

```
/*!
 * jQuery Mousewheel 3.1.13
 *
 * Copyright 2015 jQuery Foundation and other contributors
 * Released under the MIT license.
 * http://jquery.org/license
 */
!
function(a) {
 "function" == typeof define && define.amd ? define(["jquery"], a) : "object" == typeof exports ?
module.exports = a : a(jQuery)
}(function(a) {
 function b(b) {
        var g = b || window.event,
                h = i.call(arguments, 1),
                j = 0,
                l = 0,
                m = 0,
                n = 0,
                o = 0,
                p = 0;
```

```
         if (b = a.event.fix(g), b.type = "mousewheel", "detail" in g && (m = -1 * g.detail),
"wheelDelta" in g && (m = g.wheelDelta), "wheelDeltaY" in g && (m = g.wheelDeltaY), "wheelDeltaX" in g && (l
= -1 * g.wheelDeltaX), "axis" in g && g.axis === g.HORIZONTAL_AXIS && (l = -1 * m, m = 0), j = 0 === m ? l :
m, "deltaY" in g && (m = -1 * g.deltaY, j = m), "deltaX" in g && (l = g.deltaX, 0 === m && (j = -1 * l)), 0
!== m || 0 !== l) {
                 if (1 === g.deltaMode) {
                         var q = a.data(this, "mousewheel-line-height");
                         j *= q, m *= q, l *= q
                 } else if (2 === g.deltaMode) {
                         var r = a.data(this, "mousewheel-page-height");
                         j *= r, m *= r, l *= r
                        }
                 if (n = Math.max(Math.abs(m), Math.abs(l)), (!f || f > n) && (f = n, d(g, n) && (f /=
40)), d(g, n) && (j /= 40, l /= 40, m /= 40), j = Math[j >= 1 ? "floor" : "ceil"](j / f), l = Math[l >= 1 ?
"floor" : "ceil"](l / f), m = Math[m >= 1 ? "floor" : "ceil"](m / f), k.settings.normalizeOffset &&
this.getBoundingClientRect) {
                         var s = this.getBoundingClientRect();
                         o = b.clientX - s.left, p = b.clientY - s.top
                        }
                 return b.deltaX = l, b.deltaY = m, b.deltaFactor = f, b.offsetX = o, b.offsetY = p,
b.deltaMode = 0, h.unshift(b, j, l, m), e && clearTimeout(e), e = setTimeout(c, 200), (a.event.dispatch ||
a.event.handle).apply(this, h)
                }
        }
 function c() {
         f = null
        }
 function d(a, b) {
         return k.settings.adjustOldDeltas && "mousewheel" === a.type && b % 120 === 0
        }
 var e, f, g = ["wheel", "mousewheel", "DOMMouseScroll", "MozMousePixelScroll"],
         h = "onwheel" in document || document.documentMode >= 9 ? ["wheel"] : ["mousewheel",
"DomMouseScroll", "MozMousePixelScroll"],
         i = Array.prototype.slice;
 if (a.event.fixHooks) for (var j = g.length; j;) a.event.fixHooks[g[--j]] = a.event.mouseHooks;
 var k = a.event.special.mousewheel = {
         version: "3.1.12",
         setup: function() {
                 if (this.addEventListener) for (var c = h.length; c;) this.addEventListener(h[--c],
b, !1);
                 else this.onmousewheel = b;
                 a.data(this, "mousewheel-line-height", k.getLineHeight(this)), a.data(this,
"mousewheel-page-height", k.getPageHeight(this))
         }       ,
         teardown: function() {
                 if (this.removeEventListener) for (var c = h.length; c;) this.removeEventListener(h[-
-c], b, !1);
                 else this.onmousewheel = null;
                 a.removeData(this, "mousewheel-line-height"), a.removeData(this, "mousewheel-page-
height")
         }       ,
         getLineHeight: function(b) {
                 var c = a(b),
                         d = c["offsetParent" in a.fn ? "offsetParent" : "parent"]();
                 return d.length || (d = a("body")), parseInt(d.css("fontSize"), 10) ||
parseInt(c.css("fontSize"), 10) || 16
         }       ,
         getPageHeight: function(b) {
                 return a(b).height()
         }       ,
         settings: {
                 adjustOldDeltas: !0,
                 normalizeOffset: !0
                }
 };
 a.fn.extend({
         mousewheel: function(a) {
                 return a ? this.bind("mousewheel", a) : this.trigger("mousewheel")
         }       ,
         unmousewheel: function(a) {
                 return this.unbind("mousewheel", a)
                }
 })
});
```

http://127.0.0.1:8090/opus-front-sso/js/sm3/sm3.js

```
'use strict';

// 左补0到指定长度
function leftPad(str, totalLength) {
  var len = str.length;
  return Array(totalLength > len ? totalLength - len + 1 : 0).join(0) + str;
}

// 二进制转化为十六进制
function binary2hex(binary) {
  var binaryLength = 8;
  var hex = '';
  for (var i = 0; i < binary.length / binaryLength; i += 1) {
    hex += leftPad(parseInt(binary.substr(i * binaryLength, binaryLength), 2).toString(16), 2);
  }
  return hex;
}

// 十六进制转化为二进制
function hex2binary(hex) {
  var hexLength = 2;
  var binary = '';
  for (var i = 0; i < hex.length / hexLength; i += 1) {
    binary += leftPad(parseInt(hex.substr(i * hexLength, hexLength), 16).toString(2), 8);
  }
  return binary;
}

// 普通字符串转化为二进制
function str2binary(str){
  var result = [];
  var list = str.split("");
  for(var i=0;i<list.length;i++){
    if(i != 0){
      result.push("");
    }
    var item = list[i];
    // var binaryStr = item.charCodeAt().toString(2);
    var binaryStr = leftPad(item.charCodeAt().toString(2), 8);
    result.push(binaryStr);
  }
  return result.join("");
}

// 循环左移
function rol(str, n) {
  return str.substring(n % str.length) + str.substr(0, n % str.length);
}

// 二进制运算
function binaryCal(x, y, method) {
  var a = x || '';
  var b = y || '';
  var result = [];
  var prevResult = void 0;
  // for (let i = 0; i < a.length; i += 1) { // 小端
  for (var i = a.length - 1; i >= 0; i -= 1) {
    // 大端
    prevResult = method(a[i], b[i], prevResult);
    result[i] = prevResult[0];
  }
  // console.log(`x     :${x}\ny     :${y}\nresult:${result.join('')}\n`);
  return result.join('');
}

// 二进制异或运算
function xor(x, y) {
  return binaryCal(x, y, function (a, b) {
    return [a === b ? '0' : '1'];
  });
}

// 二进制与运算
function and(x, y) {
  return binaryCal(x, y, function (a, b) {
    return [a === '1' && b === '1' ? '1' : '0'];
  });
}

// 二进制或运算
function or(x, y) {
  return binaryCal(x, y, function (a, b) {
    return [a === '1' || b === '1' ? '1' : '0'];
  }); // a === '0' && b === '0' ? '0' : '1'
}

// 二进制与运算
function add(x, y) {
  var result = binaryCal(x, y, function (a, b, prevResult) {
    var carry = prevResult ? prevResult[1] : '0' || '0';
    if (a !== b) return [carry === '0' ? '1' : '0', carry]; // a,b不等时,carry不变，结果与carry相反
    // a,b相等时，结果等于原carry，新carry等于a
    return [carry, a];
  });
  // console.log('x: ' + x + '\ny: ' + y + '\n=  ' + result + '\n');
  return result;
}

// 二进制非运算
function not(x) {
  return binaryCal(x, undefined, function (a) {
    return [a === '1' ? '0' : '1'];
  });
}

function calMulti(method) {
  return function () {
    for (var _len = arguments.length, arr = Array(_len), _key = 0; _key < _len; _key++) {
      arr[_key] = arguments[_key];
    }

    return arr.reduce(function (prev, curr) {
      return method(prev, curr);
    });
  };
}

// function xorMulti(...arr) {
//   return arr.reduce((prev, curr) => xor(prev, curr));
// }

// 压缩函数中的置换函数 P1(X) = X xor (X <<< 9) xor (X <<< 17)
function P0(X) {
  return calMulti(xor)(X, rol(X, 9), rol(X, 17));
}

// 消息扩展中的置换函数 P1(X) = X xor (X <<< 15) xor (X <<< 23)
function P1(X) {
  return calMulti(xor)(X, rol(X, 15), rol(X, 23));
}

// 布尔函数，随j的变化取不同的表达式
function FF(X, Y, Z, j) {
  return j >= 0 && j <= 15 ? calMulti(xor)(X, Y, Z) : calMulti(or)(and(X, Y), and(X, Z), and(Y, Z));
}

// 布尔函数，随j的变化取不同的表达式
function GG(X, Y, Z, j) {
  return j >= 0 && j <= 15 ? calMulti(xor)(X, Y, Z) : or(and(X, Y), and(not(X), Z));
}

// 常量，随j的变化取不同的值
function T(j) {
  return j >= 0 && j <= 15 ? hex2binary('79cc4519') : hex2binary('7a879d8a');
}

// 压缩函数
function CF(V, Bi) {
  // 消息扩展
  var wordLength = 32;
  var W = [];
  var M = []; // W'
  // 将消息分组B划分为16个字W0， W1，…… ，W15 （字为长度为32的比特串）
  for (var i = 0; i < 16; i += 1) {
    W.push(Bi.substr(i * wordLength, wordLength));
  }

  // W[j] <- P1(W[j-16] xor W[j-9] xor (W[j-3] <<< 15)) xor (W[j-13] <<< 7) xor W[j-6]
  for (var j = 16; j < 68; j += 1) {
    W.push(calMulti(xor)(P1(calMulti(xor)(W[j - 16], W[j - 9], rol(W[j - 3], 15))), rol(W[j - 13], 7), W[j -
6]));
  }

  // W'[j] = W[j] xor W[j+4]
  for (var _j = 0; _j < 64; _j += 1) {
    M.push(xor(W[_j], W[_j + 4]));
  }

  // 压缩
  var wordRegister = []; // 字寄存器
  for (var _j2 = 0; _j2 < 8; _j2 += 1) {
    wordRegister.push(V.substr(_j2 * wordLength, wordLength));
  }

  var A = wordRegister[0];
  var B = wordRegister[1];
  var C = wordRegister[2];
  var D = wordRegister[3];
  var E = wordRegister[4];
  var F = wordRegister[5];
  var G = wordRegister[6];
  var H = wordRegister[7];

  // 中间变量
  var SS1 = void 0;
  var SS2 = void 0;
  var TT1 = void 0;
  var TT2 = void 0;
  for (var _j3 = 0; _j3 < 64; _j3 += 1) {
    SS1 = rol(calMulti(add)(rol(A, 12), E, rol(T(_j3), _j3)), 7);
    SS2 = xor(SS1, rol(A, 12));

    TT1 = calMulti(add)(FF(A, B, C, _j3), D, SS2, M[_j3]);
    TT2 = calMulti(add)(GG(E, ...
```

http://127.0.0.1:8090/opus-front-sso/js/sm4.js

```
/**
 * base64js
 */
/**
 * base64js
 * base64js.toByteArray(d.input)
 * base64js.fromByteArray(c);
 * @author c.z.s
 * @email 1048829253@qq.com
 * @company
 * @date 2018-07
 *
 */
(function(r){if(typeof exports==="object"&&typeof module!=="undefined"){module.exports=r()}else{if(typeof
define===
    "function"&&define.amd){define([],r)}else{var e;if(typeof window!=="undefined"){e=window}else{if(typeof
global
    !=="undefined"){e=global}else{if(typeof self!=="undefined"){e=self}else{e=this}}}e.base64js=r()}}})
(function(){
  var r,e,t;return function r(e,t,n){function o(i,a){if(!t[i]){if(!e[i]){var u=typeof
require=="function"&&require;if(!a&&u){
    return u(i,!0)}if(f){return f(i,!0)}var d=new Error("Cannot find module '"+i+"'");throw
d.code="MODULE_NOT_FOUND",d}
    var c=t[i]={exports:{}};e[i][0].call(c.exports,function(r){var t=e[i][1][r];return o(t?
t:r)},c,c.exports,r,e,t,n)}return t[i].exports}
    var f=typeof require=="function"&&require;for(var i=0;i<n.length;i++){o(n[i])}return o}({"/":
[function(r,e,t){t.byteLength=c;
      t.toByteArray=v;t.fromByteArray=s;var n=[];var o=[];var f=typeof Uint8Array!=="undefined"?
Uint8Array:Array;
      var i="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";for(var
a=0,u=i.length;a<u;++a){n[a]=i[a];
        o[i.charCodeAt(a)]=a}o["-".charCodeAt(0)]=62;o["_".charCodeAt(0)]=63;function d(r){var
e=r.length;if(e%4>0){
        throw new Error("Invalid string. Length must be a multiple of 4")}return r[e-2]==="="?2:r[e-1]==="="?
1:0}
      function c(r){return r.length*3/4-d(r)}function v(r){var e,t,n,i,a;var u=r.length;i=d(r);a=new f(u*3/4-
i);t=i>0?u-4:u;
        var c=0;for(e=0;e<t;e+=4){n=o[r.charCodeAt(e)]<<18|o[r.charCodeAt(e+1)]<<12|o[r.charCodeAt(e+2)]
<<6|o[r.charCodeAt(e+3)];
          a[c++]=n>>16&255;a[c++]=n>>8&255;a[c++]=n&255}if(i===2){n=o[r.charCodeAt(e)]
<<2|o[r.charCodeAt(e+1)]>>4;a[c++]=n&255}
        else{if(i===1){n=o[r.charCodeAt(e)]<<10|o[r.charCodeAt(e+1)]
<<4|o[r.charCodeAt(e+2)]>>2;a[c++]=n>>8&255;a[c++]=n&255}}return a}
      function l(r){return n[r>>18&63]+n[r>>12&63]+n[r>>6&63]+n[r&63]}function h(r,e,t){var n;var o=
[];for(var f=e;f<t;f+=3){
        n=(r[f]<<16)+(r[f+1]<<8)+r[f+2];o.push(l(n))}return o.join("")}function s(r){var e;var t=r.length;var
o=t%3;var f="";var i=[];
        var a=16383;for(var u=0,d=t-o;u<d;u+=a){i.push(h(r,u,u+a>d?d:u+a))}if(o===1){e=r[t-
1];f+=n[e>>2];f+=n[e<<4&63];f+="=="}else{if(o===2){
          e=(r[t-2]<<8)+r[t-1];f+=n[e>>10];f+=n[e>>4&63];f+=n[e<<2&63];f+="="}}i.push(f);return i.join("")}},
{}]},{},[])("/")});


/**
 * 国密SM4加密算法
 * @author c.z.s
 * @email 1048829253@qq.com
 * @company GDT-ZWZX-DEV-PT
 * @date 2018-07
 */
function SM4_Context() {
  this.mode=1;
  this.isPadding = true;
  this.sk = new Array(32);
}

function SM4() {
  this.SM4_ENCRYPT=1;
  this.SM4_DECRYPT = 0;

  var SboxTable = [0xd6,0x90,0xe9,0xfe,0xcc,0xe1,0x3d,0xb7,0x16,0xb6,0x14,0xc2,0x28,0xfb,0x2c,0x05,
    0x2b,0x67,0x9a,0x76,0x2a,0xbe,0x04,0xc3,0xaa,0x44,0x13,0x26,0x49,0x86,0x06,0x99,
    0x9c,0x42,0x50,0xf4,0x91,0xef,0x98,0x7a,0x33,0x54,0x0b,0x43,0xed,0xcf,0xac,0x62,
    0xe4,0xb3,0x1c,0xa9,0xc9,0x08,0xe8,0x95,0x80,0xdf,0x94,0xfa,0x75,0x8f,0x3f,0xa6,
    0x47,0x07,0xa7,0xfc,0xf3,0x73,0x17,0xba,0x83,0x59,0x3c,0x19,0xe6,0x85,0x4f,0xa8,
    0x68,0x6b,0x81,0xb2,0x71,0x64,0xda,0x8b,0xf8,0xeb,0x0f,0x4b,0x70,0x56,0x9d,0x35,
    0x1e,0x24,0x0e,0x5e,0x63,0x58,0xd1,0xa2,0x25,0x22,0x7c,0x3b,0x01,0x21,0x78,0x87,
    0xd4,0x00,0x46,0x57,0x9f,0xd3,0x27,0x52,0x4c,0x36,0x02,0xe7,0xa0,0xc4,0xc8,0x9e,
    0xea,0xbf,0x8a,0xd2,0x40,0xc7,0x38,0xb5,0xa3,0xf7,0xf2,0xce,0xf9,0x61,0x15,0xa1,
    0xe0,0xae,0x5d,0xa4,0x9b,0x34,0x1a,0x55,0xad,0x93,0x32,0x30,0xf5,0x8c,0xb1,0xe3,
    0x1d,0xf6,0xe2,0x2e,0x82,0x66,0xca,0x60,0xc0,0x29,0x23,0xab,0x0d,0x53,0x4e,0x6f,
    0xd5,0xdb,0x37,0x45,0xde,0xfd,0x8e,0x2f,0x03,0xff,0x6a,0x72,0x6d,0x6c,0x5b,0x51,
    0x8d,0x1b,0xaf,0x92,0xbb,0xdd,0xbc,0x7f,0x11,0xd9,0x5c,0x41,0x1f,0x10,0x5a,0xd8,
    0x0a,0xc1,0x31,0x88,0xa5,0xcd,0x7b,0xbd,0x2d,0x74,0xd0,0x12,0xb8,0xe5,0xb4,0xb0,
    0x89,0x69,0x97,0x4a,0x0c,0x96,0x77,0x7e,0x65,0xb9,0xf1,0x09,0xc5,0x6e,0xc6,0x84,
    0x18,0xf0,0x7d,0xec,0x3a,0xdc,0x4d,0x20,0x79,0xee,0x5f,0x3e,0xd7,0xcb,0x39,0x48];

  var FK = [ 0xa3b1bac6, 0x56aa3350, 0x677d9197, 0xb27022dc ];

  var CK = [ 0x00070e15,0x1c232a31,0x383f464d,0x545b6269,
    0x70777e85,0x8c939aa1,0xa8afb6bd,0xc4cbd2d9,
    0xe0e7eef5,0xfc030a11,0x181f262d,0x343b4249,
    0x50575e65,0x6c737a81,0x888f969d,0xa4abb2b9,
    0xc0c7ced5,0xdce3eaf1,0xf8ff060d,0x141b2229,
    0x30373e45,0x4c535a61,0x686f767d,0x848b9299,
    0xa0a7aeb5,0xbcc3cad1,0xd8dfe6ed,0xf4fb0209,
    0x10171e25,0x2c333a41,0x484f565d,0x646b7279 ];

  this.GET_ULONG_BE=function(b,i) {
    return (b[i] & 0xff) << 24 | ((b[i + 1] & 0xff) << 16) | ((b[i + 2] & 0xff) << 8) | (b[i + 3] & 0xff) &
0xffffffff;
  }

  this.PUT_ULONG_BE=function( n, b, i){
    var t1=(0xFF & (n >> 24));
    ...
```

http://127.0.0.1:8090/opus-front-sso/js/base64.js

```
function Base64() {

    // private property
    _keyStr = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";

    // public method for encoding
    this.encode = function (input) {
        var output = "";
        var chr1, chr2, chr3, enc1, enc2, enc3, enc4;
        var i = 0;
        input = _utf8_encode(input);
        while (i < input.length) {
          chr1 = input.charCodeAt(i++);
          chr2 = input.charCodeAt(i++);
          chr3 = input.charCodeAt(i++);
          enc1 = chr1 >> 2;
          enc2 = ((chr1 & 3) << 4) | (chr2 >> 4);
          enc3 = ((chr2 & 15) << 2) | (chr3 >> 6);
          enc4 = chr3 & 63;
          if (isNaN(chr2)) {
          enc3 = enc4 = 64;
          } else if (isNaN(chr3)) {
          enc4 = 64;
          }
          output = output +
          _keyStr.charAt(enc1) + _keyStr.charAt(enc2) +
          _keyStr.charAt(enc3) + _keyStr.charAt(enc4);
        }
        return output;
    }

    // public method for decoding
    this.decode = function (input) {
        var output = "";
        var chr1, chr2, chr3;
        var enc1, enc2, enc3, enc4;
        var i = 0;
        input = input.replace(/[^A-Za-z0-9\+\/\=]/g, "");
        while (i < input.length) {
          enc1 = _keyStr.indexOf(input.charAt(i++));
          enc2 = _keyStr.indexOf(input.charAt(i++));
          enc3 = _keyStr.indexOf(input.charAt(i++));
          enc4 = _keyStr.indexOf(input.charAt(i++));
          chr1 = (enc1 << 2) | (enc2 >> 4);
          chr2 = ((enc2 & 15) << 4) | (enc3 >> 2);
          chr3 = ((enc3 & 3) << 6) | enc4;
          output = output + String.fromCharCode(chr1);
          if (enc3 != 64) {
          output = output + String.fromCharCode(chr2);
          }
          if (enc4 != 64) {
          output = output + String.fromCharCode(chr3);
          }
        }
        output = _utf8_decode(output);
        return output;
    }

    // private method for UTF-8 encoding
    _utf8_encode = function (string) {
        string = string.replace(/\r\n/g,"\n");
        var utftext = "";
        for (var n = 0; n < string.length; n++) {
          var c = string.charCodeAt(n);
          if (c < 128) {
          utftext += String.fromCharCode(c);
          } else if((c > 127) && (c < 2048)) {
          utftext += String.fromCharCode((c >> 6) | 192);
          utftext += String.fromCharCode((c & 63) | 128);
          } else {
          utftext += String.fromCharCode((c >> 12) | 224);
          utftext += String.fromCharCode(((c >> 6) & 63) | 128);
          utftext += String.fromCharCode((c & 63) | 128);
          }

        }
        return utftext;
    }

    // private method for UTF-8 decoding
    _utf8_decode = function (utftext) {
        var string = "";
        var i = 0;
        var c = c1 = c2 = 0;
        while ( i < utftext.length ) {
          c = utftext.charCodeAt(i);
          if (c < 128) {
          string += String.fromCharCode(c);
          i++;
          } else if((c > 191) && (c < 224)) {
          c2 = utftext.charCodeAt(i+1);
          string += String.fromCharCode(((c & 31) << 6) | (c2 & 63));
          i += 2;
          } else {
          c2 = utftext.charCodeAt(i+1);
          c3 = utftext.charCodeAt(i+2);
          string += String.fromCharCode(((c & 15) << 12) | ((c2 & 63) << 6) | (c3 & 63));
          i += 3;
          }
        }
        return string;
    }
}
```

http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/scripts.bundle.js

```
/**
 * @class mApp  Metronic App class
 */

var mApp = function() {

    /**
    * Initializes bootstrap tooltip
    */
    var initTooltip = function(el) {
        var skin = el.data('skin') ? 'm-tooltip--skin-' + el.data('skin') : '';
        var width = el.data('width') == 'auto' ? 'm-tooltop--auto-width' : '';
        var triggerValue = el.data('trigger') ? el.data('trigger') : 'hover';

        el.tooltip({
          trigger: triggerValue,
          template: '<div class="m-tooltip ' + skin + ' ' + width + ' tooltip" role="tooltip">\
          <div class="arrow"></div>\
          <div class="tooltip-inner"></div>\
          </div>'
        });
    }

    /**
    * Initializes bootstrap tooltips
    */
    var initTooltips = function() {
        // init bootstrap tooltips
        $('[data-toggle="m-tooltip"]').each(function() {
          initTooltip($(this));
        });
    }

    /**
    * Initializes bootstrap popover
    */
    var initPopover = function(el) {
        var skin = el.data('skin') ? 'm-popover--skin-' + el.data('skin') : '';
        var triggerValue = el.data('trigger') ? el.data('trigger') : 'hover';

        el.popover({
          trigger: triggerValue,
          template: '\
          <div class="m-popover ' + skin + ' popover" role="tooltip">\
          <div class="arrow"></div>\
          <h3 class="popover-header"></h3>\
          <div class="popover-body"></div>\
          </div>'
        });
    }

    /**
    * Initializes bootstrap popovers
    */
    var initPopovers = function() {
        // init bootstrap popover
        $('[data-toggle="m-popover"]').each(function() {
          initPopover($(this));
        });
    }

    /**
    * Initializes bootstrap file input
    */
    var initFileInput = function() {
        // init bootstrap popover
        $('.custom-file-input').on('change',function(){
          var fileName = $(this).val();
          $(this).next('.custom-file-label').addClass("selected").html(fileName);
        });
    }

    /**
    * Initializes metronic portlet
    */
    var initPortlet = function(el, options) {
        // init portlet tools
        el.mPortlet(options);
    }

    /**
    * Initializes metronic portlets
    */
    var initPortlets = function() {
        // init portlet tools
        $('[data-portlet="true"]').each(function() {
          var el = $(this);

          if ( el.data('portlet-initialized') !== true ) {
          initPortlet(el, {});
          el.data('portlet-initialized', true);
          }
        });
    }

    /**
    * Initializes scrollable contents
    */
    var initScrollables = function() {
        $('[data-scrollable="true"]').each(function(){
          var maxHeight;
          var height;
          var el = $(this);

          if (mUtil.isInResponsiveRange('tablet-and-mobile')) {
          if (el.data('mobile-max-height')) {
          maxHeight = el.data('mobile-max-height');
          } else {
          maxHeight = el.data('max-height');
          }

          if (el.data('mobile-height')) {
          height = el.data('mobile-height');
          } else {
          height = el.data('height');
          }
          } else {
          maxHeight = el.data('max-height');
          height = el.data('max-height');
          }

          if (maxHeight) {
          el.css('max-height', maxHeight);
          }
          if (height) {
          el.css('height', height);
          }

          mApp.initScroller(el, {});
        });
    }

    /**
    * Initializes bootstrap alerts
    */
    var initAlerts = function() {
        // init bootstrap popover
        $('body').on('click', '[data-close=alert]', function() {
          $(this).closest('.alert').hide();
        });
    }

    /**
    * Initializes Metronic custom tabs
    */
    var initCustomTabs = function() {
        // init bootstrap popover
        $('[data-tab-target]').each(function() {
          if ($(this).data('tabs-initialized') == true ) {
          return;
          }

          $(this).click(function(e) {
          e.preventDefault();

          var tab = $(this);
          var tabs = tab.closest('[data-tabs="true"]');
          var contents = $( tabs.data('tabs-contents') );
          var content = $( tab.data('tab-target') );

          tabs.find('.m-tabs__item.m-tabs__item--active').removeClass('m-tabs__item--active');
          tab.addClass('m-tabs__item--active');

          contents.find('.m-tabs-content__item.m-tabs-content__item--active').removeClass('m-tabs-
content__item--active');
...
```

http://127.0.0.1:8090/opus-front-sso/framework/ui-themes/common/metronic/js/vendors.bundle.js

```
/*!
 * jQuery JavaScript Library v3.2.1
 * https://jquery.com/
 *
 * Includes Sizzle.js
 * https://sizzlejs.com/
 *
 * Copyright JS Foundation and other contributors
 * Released under the MIT license
 * https://jquery.org/license
 *
 * Date: 2017-03-20T18:59Z
 */
( function( global, factory ) {

 "use strict";

 if ( typeof module === "object" && typeof module.exports === "object" ) {

         // For CommonJS and CommonJS-like environments where a proper `window`
         // is present, execute the factory and get jQuery.
         // For environments that do not have a `window` with a `document`
         // (such as Node.js), expose a factory as module.exports.
         // This accentuates the need for the creation of a real `window`.
         // e.g. var jQuery = require("jquery")(window);
         // See ticket #14549 for more info.
         module.exports = global.document ?
                 factory( global, true ) :
                 function( w ) {
                         if ( !w.document ) {
                                 throw new Error( "jQuery requires a window with a document" );
                                }
                         return factory( w );
                 }       ;
 } else {
         factory( global );
        }

// Pass this if window is not defined yet
} )( typeof window !== "undefined" ? window : this, function( window, noGlobal ) {

// Edge <= 12 - 13+, Firefox <=18 - 45+, IE 10 - 11, Safari 5.1 - 9+, iOS 6 - 9.1
// throw exceptions when non-strict code (e.g., ASP.NET 4.5) accesses strict mode
// arguments.callee.caller (trac-13335). But as of jQuery 3.0 (2016), strict mode should be common
// enough that all such attempts are guarded in a try block.
"use strict";

var arr = [];

var document = window.document;

var getProto = Object.getPrototypeOf;

var slice = arr.slice;

var concat = arr.concat;

var push = arr.push;

var indexOf = arr.indexOf;

var class2type = {};

var toString = class2type.toString;

var hasOwn = class2type.hasOwnProperty;

var fnToString = hasOwn.toString;

var ObjectFunctionString = fnToString.call( Object );

var support = {};



 function DOMEval( code, doc ) {
         doc = doc || document;

         var script = doc.createElement( "script" );

         script.text = code;
         doc.head.appendChild( script ).parentNode.removeChild( script );
        }
/* global Symbol */
// Defining this global in .eslintrc.json would create a danger of using the global
// unguarded in another place, it seems safer to define global only for this module



var
 version = "3.2.1",

 // Define a local copy of jQuery
 jQuery = function( selector, context ) {

         // The jQuery object is actually just the init constructor 'enhanced'
         // Need init if jQuery is called (just allow error to be thrown if not included)
         return new jQuery.fn.init( selector, context );
 },

 // Support: Android <=4.0 only
 // Make sure we trim BOM and NBSP
 rtrim = /^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,

 // Matches dashed string for camelizing
 rmsPrefix = /^-ms-/,
 rdashAlpha = /-([a-z])/g,

 // Used by jQuery.camelCase as callback to replace()
 fcamelCase = function( all, letter ) {
         return letter.toUpperCase();
 };

jQuery.fn = jQuery.prototype = {

 // The current version of jQuery being used
 jquery: version,

 constructor: jQuery,

 // The default length of a jQuery object is 0
 length: 0,

 toArray: function() {
         return slice.call( this );
 },

 // Get the Nth element in the matched element set OR
 // Get the whole matched element set as a clean array
 get: function( num ) {

         // Return all the elements in a clean array
         if ( num == null ) {
                 return slice.call( this );
                }

         // Return just the one element from the set
         return num < 0 ? this[ num + this.length ] : this[ num ];
 },

 // Take an array of elements and push it onto the stack
 // (returning the new matched element set)
 pushStack: function( elems ) {

         // Build a new jQuery matched element set
         var ret = jQuery.merge( this.constructor(), elems );

         // Add the old object onto the stack (as a reference)
         ret.prevObject = this;

         // Return the newly-formed element set
         return ret;
 },

 // Execute a callback for every element in the matched set.
 each: function( callback ) {
         return jQuery.each( this, callback );
 },

 map: function( callback ) {
         return this.pushStack( jQuery.map( this, function( elem, i ) {
                 return callback.call( elem, i, elem );
         } ) );
 },

 slice: function() {
         return this.pushStack( slice.apply( this, arguments ) );
 },

 first: function() {
         return this.eq( 0 );
 },

 last: function() {
         return this.eq( -1 );
 },
 eq: function( i ) {
        var len = this.length,
                j = +i + ( i < 0 ? len : 0 );
        return this.pushStack( j >= 0 && j < len ? [ this[ j ] ] : [] );
 },

 end: function() {
        return this.prevObject || this.constructor();
 },

 // For internal use only.
 // Behaves like an Array's method, not like a jQuery method.
 push: push,
 sort: arr.sort,
 splice: arr.splice
};

jQuery.extend = jQuery.fn.extend = function() {
 var optio...
```

http://127.0.0.1:8000/xmjg/common/tool/common-merge.js

```
/**
 * 外部js调用
 */
var commonWindow = {
    //打开页面
    toWindowForReturn: function (url, pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
//          pageObj.commonWindowAction.doWindowForReturn(encodeURI(url));
                 console.log(encodeURI(url))
          pageObj.commonWindowAction.doWindowForReturn(encodeURI(url));
        }
    },


    //打开页面  不支持返回
    toWindowNotReturn: function (url, pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
          pageObj.commonWindowAction.doWindowNotReturn(url);
        }
    },

    //返回上一页面
    returnParentWindow: function (pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
          pageObj.commonWindowAction.doReturnParentWindow();
        }
    },
    //跳转到对应页面(传入的url与之前的iframe地址一致的时候 退回到对应iframe,如果不存在 则调用toWindowForReturn)
    jumpWindowForIframe: function (url, pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
          pageObj.commonWindowAction.doJumpWindowForIframe(url);
        }
    },
    //获取对应的页面  pageFlag (max-top-page: 最顶级页面;)
    getWindowObj: function (pageFlag) {
        if (!pageFlag) {
          pageFlag = "max-top-page";
        }
        var obj = window.self;
        var whileFlag = true;
        while (whileFlag) {

          if (obj.document.getElementById("page-level-flag-in")) {
          //最顶级页面
          if (obj.document.getElementById("page-level-flag-in").value == pageFlag) {
          return obj;
          }
          }
          if (whileFlag) {
          if (obj.window.parent != obj.window) {
          obj = obj.window.parent;
          } else {
          whileFlag = false;
          }
          }
        }
        return window.self;
    },
};

//===========================================================================================================
=================

var commonWindowAction = {
    doWindowForReturn: function (url) {
        var maxDataIndex = 0;
        var $lastIframe;
        $(".content-url-iframe").each(function () {
          var thisDataIndex = parseInt($(this).attr("data-index"));
          if (maxDataIndex < thisDataIndex) {
          maxDataIndex = thisDataIndex;
          }
          if (maxDataIndex == thisDataIndex) {
          $lastIframe = $(this);
          }
          commonWindowAction.doRemoveClass($(this), "curr-url-iframe");
        });
        if ($lastIframe) {
          var timestamp = (new Date()).valueOf();
          var key = "contentZframe-id-" + timestamp + "-" + (maxDataIndex + 1);
          $lastIframe.after("<iframe allowfullscreen  id=\"" + key + "\" width=\"100%\" height=\"100%\"
src=\"\" frameborder=\"0\" class=\"content-url-iframe  curr-url-iframe\" data-index=\"" + (maxDataIndex + 1)
+ "\"></iframe>");
          $("#" + key).attr("src", url);
        }
        console.log(url)
        commonWindowAction.removeIframeOrHide(true);

    },
    doWindowNotReturn: function (url) {
        $(".content-url-iframe").each(function () {
                if($(this).hasClass("curr-url-iframe")){
                        if(url.indexOf("?")<=-1){
                                url+="?";
                        }else{
                                url+="&";
                        }
                        url+="notHaveReturnFlag=yes";
                        $(this).attr("src", url);
                        $(this).attr("id","contentZframe");
                        $(this).attr("data-index","0");
                }else{
          commonWindowAction.doRemoveClass($(this), "curr-url-iframe");
          }
        });
        commonWindowAction.removeIframeOrHide(false);
    },
    //执行返回上一页
    doReturnParentWindow: function () {
        var $lastIframe;
        var maxDataIndex = 0;

        $(".curr-url-iframe").each(function (i) {
          if (i == 0) {
          if ($(this).attr("data-index") == "0") {
          return;
          }
          maxDataIndex = parseInt($(this).attr("data-index")) - 1;
          $lastIframe = $(this);
          }
        })
        $(".content-url-iframe").each(function () {
         if ($lastIframe.attr("src") == $(this).attr("src")) {
           maxDataIndex = parseInt($(this).attr("data-index")) - 1;
```

```
            return false;
          }
        });
        if (maxDataIndex <= 0) {
          maxDataIndex = 0;
          $(".content-url-iframe").each(function () {
          var thisDataIndex = parseInt($(this).attr("data-index"));
          if (maxDataIndex == thisDataIndex) {
          $(this).show();
          commonWindowAction.doAddClass($(this), "curr-url-iframe");
          } else {
          commonWindowAction.doRemoveClass($(this), "curr-url-iframe");
          }
  ...
```

http://127.0.0.1:8000/xmjg/opus/front/blue/index.html

```
    var isWhite = '';
```

http://127.0.0.1:8000/xmjg/opus/front/blue/index.html

```
    var ctx = '/xmjg/';    // var ctx = 'http://192.168.30.45:8080/opus-front/';    var designSize = 1920; //
设计图尺寸    var wW =  document.documentElement.clientWidth;// 窗口宽度    var rem = wW * 100 / designSize;
//1rem = 100px  为了好计算    document.documentElement.style.fontSize = rem + 'px';    window.resize=function
() {// 绑定到窗口的这个事件中        var designSize = 1920; // 设计图尺寸        var wW =
document.documentElement.clientWidth;// 窗口宽度        var rem = wW * 100 / designSize;
document.documentElement.style.fontSize = rem + 'px';    };
```

http://127.0.0.1:8000/xmjg/opus/front/blue/index.html

```
      initWhite();
```

http://127.0.0.1:8000/xmjg/agcloud/framework/js-lib/jquery-v1/jquery.min.js

```
/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?
b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return
b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=
[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l=
{},m="1.12.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-
/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype=
{jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return
null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var
b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return
n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return
a.call(b,c,b)}))},slice:function(){return this.pushStack(e.apply(this,arguments))},first:function(){return
this.eq(0)},last:function(){return this.eq(-1)},eq:function(a){var b=this.length,c=+a+(0>a?b:0);return
this.pushStack(c>=0&&b>c?[this[c]]:[])},end:function(){return
this.prevObject||this.constructor()},push:g,sort:c.sort,splice:c.splice},n.extend=n.fn.extend=function(){var
a,b,c,d,e,f,g=arguments[0]||{},h=1,i=arguments.length,j=!1;for("boolean"==typeof g&&(j=g,g=arguments[h]||
{},h++),"object"==typeof g||n.isFunction(g)||(g={}),h===i&&(g=this,h--);i>h;h++)if(null!=
(e=arguments[h]))for(d in e)a=g[d],c=e[d],g!==c&&(j&&c&&(n.isPlainObject(c)||(b=n.isArray(c)))?(b?
(b=!1,f=a&&n.isArray(a)?a:[]):f=a&&n.isPlainObject(a)?a:{},g[d]=n.extend(j,f,c)):void 0!==c&&(g[d]=c));return
g},n.extend({expando:"jQuery"+(m+Math.random()).replace(/\D/g,""),isReady:!0,error:function(a){throw new
Error(a)},noop:function(){},isFunction:function(a)
{return"function"===n.type(a)},isArray:Array.isArray||function(a)
{return"array"===n.type(a)},isWindow:function(a){return null!=a&&a==a.window},isNumeric:function(a){var
b=a&&a.toString();return!n.isArray(a)&&b-parseFloat(b)+1>=0},isEmptyObject:function(a){var b;for(b in
a)return!1;return!0},isPlainObject:function(a){var
b;if(!a||"object"!==n.type(a)||a.nodeType||n.isWindow(a))return!1;try{if(a.constructor&&!k.call(a,"constructo
r")&&!k.call(a.constructor.prototype,"isPrototypeOf"))return!1}catch(c){return!1}if(!l.ownFirst)for(b in
a)return k.call(a,b);for(b in a);return void 0===b||k.call(a,b)},type:function(a){return null==a?
a+"":"object"==typeof a||"function"==typeof a?i[j.call(a)]||"object":typeof a},globalEval:function(b)
{b&&n.trim(b)&&(a.execScript||function(b){a.eval.call(a,b)})(b)},camelCase:function(a){return
a.replace(p,"ms-").replace(q,r)},nodeName:function(a,b){return
a.nodeName&&a.nodeName.toLowerCase()===b.toLowerCase()},each:function(a,b){var c,d=0;if(s(a))
{for(c=a.length;c>d;d++)if(b.call(a[d],d,a[d])===!1)break}else for(d in
a)if(b.call(a[d],d,a[d])===!1)break;return a},trim:function(a){return null==a?"":
(a+"").replace(o,"")},makeArray:function(a,b){var c=b||[];return null!=a&&(s(Object(a))?
n.merge(c,"string"==typeof a?[a]:a):g.call(c,a)),c},inArray:function(a,b,c){var d;if(b){if(h)return
h.call(b,a,c);for(d=b.length,c=c?0>c?Math.max(0,d+c):c:0;d>c;c++)if(c in b&&b[c]===a)return c}return-
1},merge:function(a,b){var c=+b.length,d=0,e=a.length;while(c>d)a[e++]=b[d++];if(c!==c)while(void
0!==b[d])a[e++]=b[d++];return a.length=e,a},grep:function(a,b,c){for(var d,e=
[],f=0,g=a.length,h=!c;g>f;f++)d=!b(a[f],f),d!==h&&e.push(a[f]);return e},map:function(a,b,c){var d,e,g=0,h=
[];if(s(a))for(d=a.length;d>g;g++)e=b(a[g],g,c),null!=e&&h.push(e);else for(g in
a)e=b(a[g],g,c),null!=e&&h.push(e);return f.apply([],h)},guid:1,proxy:function(a,b){var
c,d,f;return"string"==typeof b&&(f=a[b],b=a,a=f),n.isFunction(a)?(c=e.call(arguments,2),d=function(){return
a.apply(b||this,c.concat(e.call(arguments)))},d.guid=a.guid=a.guid||n.guid++,d):void 0},now:function()
{return+new Date},support:l}),"function"==typeof Symbol&&
(n.fn[Symbol.iterator]=c[Symbol.iterator]),n.each("Boolean Number String Function Array Date RegExp Object
Error Symbol".split(" "),function(a,b){i["[object "+b+"]"]=b.toLowerCase()});function s(a){var
b=!!a&&"length"in
a&&a.length,c=n.type(a);return"function"===c||n.isWindow(a)?!1:"array"===c||0===b||"number"==typeof
b&&b>0&&b-1 in a}var t=function(a){var b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u="sizzle"+1*new
Date,v=a.document,w=0,x=0,y=ga(),z=ga(),A=ga(),B=function(a,b){return a===b&&(l=!0),0},C=1<<31,D=
{}.hasOwnProperty,E=[],F=E.pop,G=E.push,H=E.push,I=E.slice,J=function(a,b){for(var
c=0,d=a.length;d>c;c++)if(a[c]===b)return c;return-
1},K="checked|selected|async|autofocus|autoplay|controls|defer|disabled|hidden|ismap|loop|multiple|open|reado
nly|required|scoped",L="[\\x20\\t\\r\\n\\f]",M="(?:\\\\.|[\\w-]|[^\\x00-\\xa0])+",N="\\["+L+"*("+M+")
(?:"+L+"*([*^$|!~]?=)"+L+"*(?:'((?:\\\\.|[^\\\\'])*)'|\"((?:\\\\....
```

http://127.0.0.1:8000/xmjg/agcloud/framework/js-lib/element-2/element.js

```
!function(e,t){"object"==typeof exports&&"object"==typeof module?
module.exports=t(require("vue")):"function"==typeof define&&define.amd?define("ELEMENT",
["vue"],t):"object"==typeof exports?exports.ELEMENT=t(require("vue")):e.ELEMENT=t(e.Vue)}("undefined"!=typeof
self?self:this,function(e){return function(e){var t={};function i(n){if(t[n])return t[n].exports;var r=t[n]=
{i:n,l:!1,exports:{}};return e[n].call(r.exports,r,r.exports,i),r.l=!0,r.exports}return
i.m=e,i.c=t,i.d=function(e,t,n){i.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:n})},i.r=function(e)
{"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,
{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},i.t=function(e,t){if(1&t&&
(e=i(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var
n=Object.create(null);if(i.r(n),Object.defineProperty(n,"default",
{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var r in e)i.d(n,r,function(t){return
e[t]}.bind(null,r));return n},i.n=function(e){var t=e&&e.__esModule?function(){return e.default}:function()
{return e};return i.d(t,"a",t),t},i.o=function(e,t){return
Object.prototype.hasOwnProperty.call(e,t)},i.p="/dist/",i(i.s=48)}([function(t,i)
{t.exports=e},function(e,t,i){var n=i(12);e.exports=function(e,t,i){return void 0===i?
n(e,t,!1):n(e,i,!1!==t)}},function(e,t,i){var n;!function(r){"use strict";var s={},o=/d{1,4}|M{1,4}|yy(?:yy)?
|S{1,3}|Do|ZZ|([HhMsDm])\1?|[aA]|"[^"]*"|'[^']*'/g,a=/\d\d?/,l=/[0-9]*['a-z\u00A0-\u05FF\u0700-\uD7FF\uF900-
\uFDCF\uFDF0-\uFFEF]+|[\u0600-\u06FF\/]+(\s*?[\u0600-\u06FF]+){1,2}/i,u=function(){};function c(e,t){for(var
i=[],n=0,r=e.length;n<r;n++)i.push(e[n].substr(0,t));return i}function h(e){return function(t,i,n){var
r=n[e].indexOf(i.charAt(0).toUpperCase()+i.substr(1).toLowerCase());~r&&(t.month=r)}}function d(e,t)
{for(e=String(e),t=t||2;e.length<t;)e="0"+e;return e}var p=
["Sunday","Monday","Tuesday","Wednesday","Thursday","Friday","Saturday"],f=
["January","February","March","April","May","June","July","August","September","October","November","December
"],m=c(f,3),v=c(p,3);s.i18n={dayNamesShort:v,dayNames:p,monthNamesShort:m,monthNames:f,amPm:
["am","pm"],DoFn:function(e){return e+["th","st","nd","rd"][e%10>3?0:(e-e%10!=10)*e%10]}};var g=
{D:function(e){return e.getDay()},DD:function(e){return d(e.getDay())},Do:function(e,t){return
t.DoFn(e.getDate())},d:function(e){return e.getDate()},dd:function(e){return
d(e.getDate())},ddd:function(e,t){return t.dayNamesShort[e.getDay()]},dddd:function(e,t){return
t.dayNames[e.getDay()]},M:function(e){return e.getMonth()+1},MM:function(e){return
d(e.getMonth()+1)},MMM:function(e,t){return t.monthNamesShort[e.getMonth()]},MMMM:function(e,t){return
t.monthNames[e.getMonth()]},yy:function(e){return String(e.getFullYear()).substr(2)},yyyy:function(e){return
e.getFullYear()},h:function(e){return e.getHours()%12||12},hh:function(e){return
d(e.getHours()%12||12)},H:function(e){return e.getHours()},HH:function(e){return
d(e.getHours())},m:function(e){return e.getMinutes()},mm:function(e){return d(e.getMinutes())},s:function(e)
{return e.getSeconds()},ss:function(e){return d(e.getSeconds())},S:function(e){return
Math.round(e.getMilliseconds()/100)},SS:function(e){return
d(Math.round(e.getMilliseconds()/10),2)},SSS:function(e){return d(e.getMilliseconds(),3)},a:function(e,t)
{return e.getHours()<12?t.amPm[0]:t.amPm[1]},A:function(e,t){return e.getHours()<12?
t.amPm[0].toUpperCase():t.amPm[1].toUpperCase()},ZZ:function(e){var t=e.getTimezoneOffset();return(t>0?"-
":"+")+d(100*Math.floor(Math.abs(t)/60)+Math.abs(t)%60,4)}},b={d:[a,function(e,t){e.day=t}],M:
[a,function(e,t){e.month=t-1}],yy:[a,function(e,t){var i=+(""+(new
Date).getFullYear()).substr(0,2);e.year=""+(t>68?i-1:i)+t}],h:[a,function(e,t){e.hour=t}],m:[a,function(e,t)
{e.minute=t}],s:[a,function(e,t){e.second=t}],yyyy:[/\d{4}/,function(e,t){e.year=t}],S:[/\d/,function(e,t)
{e.millisecond=100*t}],SS:[/\d{2}/,function(e,t){e.millisecond=10*t}],SSS:[/\d{3}/,function(e,t)
{e.millisecond=t}],D:[a,u],ddd:[l,u],MMM:[l,h("monthNamesShort")],MMMM:[l,h("monthNames")],a:
[l,function(e,t,i){var n=t.toLowerCase();n===i.amPm[0]?e.isPm=!1:n===i.amPm[1]&&(e.isPm=!0)}],ZZ:[/[\+\-
]\d\d:?\d\d/,function(e,t){var i,n=(t+"").match(/([\+\-]|\d\d)/gi);n&&
(i=60*n[1]+parseInt(n[2],10),e.timezoneOffset="+"===n[0]?i:-
i)}]};b.DD=b.D,b.dddd=b.ddd,b.Do=b.dd=b.d,b.mm=b.m,b.hh=b.H=b.HH=b.h,b.MM=b.M,b.ss=b.s,b.A=b.a,s.masks=
{default:"ddd MMM dd yyyy HH:mm:ss",shortDate:"M/D/yy",mediumDate:"MMM d, yyyy",longDate:"MMMM d,
yyyy",fullDate:"dddd, MMMM d,
yyyy",shortTime:"HH:mm",mediumTime:"HH:mm:ss",longTime:"HH:mm:ss.SSS"},s.format=function(e,t,i){var
n=i||s.i18n;if("number"==typeof e&&(e=new Date(e)),"[object
Date]"!==Object.prototype.toString.call(e)||isNaN(e.getTime()))throw new Error("Invalid Date in
fecha.format");return(t=s.masks[t]||t||s.masks.default).replace(o,function(t){return t in g?g[t]
(e,n):t.slice(1,t.length-1)})},s.parse=function(e,t,i){var n=i||s....
```

http://127.0.0.1:8000/xmjg/agcloud/framework/js-lib/agcloud-lib/js/common.js

```
var access_token = localStorage.getItem("access_token");
var client_auth = '';
var date = new Date(); // 日期初始化
var BaseUrl = ''; // ajax请求基础路径
var that = new Vue();

function formatDate(date, fmt) {
    if (/(y+)/.test(fmt)) {
      fmt = fmt.replace(RegExp.$1, (date.getFullYear() + '').substr(4 - RegExp.$1.length));
    }
    var o = {
      'M+': date.getMonth() + 1,
      'd+': date.getDate(),
      'h+': date.getHours(),
      'm+': date.getMinutes(),
      's+': date.getSeconds()
    };
    for (var k in o) {
        if (new RegExp('('+k+')').test(fmt)) {
          var str = o[k] + '';
          fmt = fmt.replace(RegExp.$1, (RegExp.$1.length === 1) ? str : padLeftZero(str));
          }
    }
    return fmt;
}

/**
*  确认弹框
  header：头部信息默认为“提示”,
  msg：提示信息默认为空,
  confirmButtonText：确认按钮文本，cancelButtonText：取消按钮文本,
  type：弹出框类型默认info,
  center：bool值 弹出框是否居中默认为false
  succFun 确认回调
  errFun  取消回调
*/
function confirmMsg(header,msg,succFun,errFun,confirmButtonText,cancelButtonText,type,center,useHtml) {
  that.$confirm(msg?msg:'', header?header:'提示', {
    confirmButtonText: confirmButtonText?confirmButtonText:'',
    cancelButtonText: cancelButtonText?cancelButtonText:'',
    type: type?type:'warning',
    center: center?center:false,
    dangerouslyUseHTMLString: useHtml == true?true:false,
    callback: function(action,instance) {
      if(action=='confirm'){
        succFun();
      } else{
        errFun();
      }
    },
  })
}
```

```
/**
*    操作消息提示
 header：头部信息默认为“提示”，
 msg：提示信息默认为空，
 confirmButtonText：确认按钮文本，
 type：弹出框类型默认info，
 center：bool值 弹出框是否居中默认为false
 callback 回调
*/
function  alertMsg(header,msg,confirmButtonText,type,center,callback,useHtml) {
    that.$alert(msg?msg:'', header?header:'提示', {
      confirmButtonText: confirmButtonText?confirmButtonText:'确定',
      type: type?type:'info',
      center: center?center:false,
      dangerouslyUseHTMLString: useHtml == true?true:false,
      callback: function (action) {
        if(!callback){
          return;
        } else if(action=='confirm') {
          callback();
        }

      }
    });
}


/**
* 请求服务器;
* module  模块名称必填
* @param  param 参数
* @cb 回调函数
*/
function request(module,param,cbSun,cbErr){
    requestProxy({url:param.url, type:param.type,
data:param.data,async:param.async,ContentType:param.ContentType,timeout: param.timeout},cbSun,cbErr);
}

/**
* 请求参数:
* @param  param { url type data timeout} callback
*/
function requestProxy(param,cbSun,cbErr){
  if(param.type=='get'){
    if(param.data){
      param.data.time = new Date().getTime();
    }else {
      param.data = {
        time: new Date().getTime()
      };
    }
  }
    $.ajax({
      type: param.type || 'post',
      dataType: "json",
      data: param.data,
      url: BaseUrl + param.url,
      headers: {
          'Content-Type' :param.ContentType || 'application/x-www-form-urlencoded;',
          'Authorization': 'bearer '+access_token
      },
      xhrFields: {
        withCredentials: true
      },
      async: typeof param.async === "undefined"?true:param.async,
      crossDomain: true,
      timeout: param.timeout || 30000,
      success:function (res) {
        if(typeof cbSun === "function") cbSun(res)
      },
      error:function (err, textStatus) {
        typeof cbErr === "function" && cbErr(err);
        if(err.status == '401' && err.responseJSON.clientModel == 'rsServer'){
          client_auth = err.responseJSON.clientAuth;
          var url = window.location.href;
          var serverUrl = err.responseJSON.ssoServerUrl;
          var b = new Base64();
          var baseUrl = b.encode(url);
          window.location.href = '/framework-ui/src/main/resources/static/agcloud/login/login.html?
reBackurl='+baseUrl+'&client_auth='+client_auth+'&serverUrl='+serverUrl;
        } else if (textStatus==="timeout"){
          that.$message.error('请求超时，请重试');
        } else if (err.status == '401') {
          // 2020-05-27 去掉该错误信息
          // that.$message({
          //   message: err.message?err.message:''+'未获取到登录信息，请刷新页面！',
          //   type: 'error'
          // });
        }
      }
    });
}

function padLeftZero(str) {
  return ('00' + str).substr(str.length);
}
function Base64() {

  // private property
  _keyStr = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";

  // public method for encoding
  this.encode = function (input) {
    var output = "";
    var chr1, chr2, chr3, enc1, enc2, enc3, enc4;
    var i = 0;
    input = _utf8_encode(input);
    while (i < input.length) {
      chr1 = input.charCodeAt(i++);
      chr2 = input.charCodeAt(i++);
      chr3 = input.charCodeAt(i++);
      enc1 = chr1 >> 2;
      enc2 = ((chr1 & 3) << 4) | (chr2 >> 4);
      enc3 = ((chr2 & 15) << 2) | (chr3 >> 6);
      enc4 = chr3 & 63;
      if (isNaN(chr2)) {
        enc3 = enc4 = 64;
      } el...
```

http://127.0.0.1:8000/xmjg/agcloud/framework/ui-schemes/dark-blue/js/index.js

```
/*
 * @Author: ZL
 * @Date:   2019/05/15
 * @Last Modified by:   ZL
 * @Last Modified time: $ $
 */
var vm = new Vue({
    el: '#portal',
    data: function () {
        var _that = this;
        var checkSame = function (rule, value, callback) {
          if (value === '') {
          callback(new Error('请再次输入密码'));
          }else if (value.toString().trim().length<3) {
          callback(new Error('密码不能小于3个字符'));
          }else if (value !== _that.editPasswordData.newPassword) {
          callback(new Error('两次输入密码不一致！'));
          } else {
          callback();
          }
        };
        var checkDiffer = function (rule, value, callback) {
          if (value === '') {
          callback(new Error('请输入密码'));
          } else if (value.toString().trim().length<3) {
          callback(new Error('密码不能小于3个字符'));
          } else if (value == _that.editPasswordData.oldPassword) {
          callback(new Error('新密码和原密码不能相同！'));
          } else {
          callback();
          }
        };
        var checkOldPass = function (rule, value, callback) {
          if (value === '') {
          callback(new Error('请输入原密码'));
          } else {
          request('opus-admin', {
          url: ctx+'opus/front/om/users/passwordCheckout',
          data: {
          oldPassword: sm3(hex_md5(value)),
          proPassword: sm3(new SM4Util().encryptData_ECB(value))
          },
          type: 'get'
          }, function (data) {
          if(data.success){
          callback();
          }else {
          callback(new Error(data.message ? data.message : '原密码错误'));
          }
          })
          }
        };
        return {
          headerData: [], // 头部菜单所有data
          headerActive: 0,  // 头部菜单active状态
          curWidth: (document.documentElement.clientWidth || document.body.clientWidth),//当前屏幕宽度
          curHeight: (document.documentElement.clientHeight || document.body.clientHeight),//当前屏幕高度
          showMenuMore: false,  // 展示更多菜单默认隐藏
          menuCount: 1, // 头部菜单展示条数 menuCount+1
          loginName: '', // 用户登陆名
          userName: '', // 用户名
          userId: '',  // 用户id
          hideHeaderData: [], // 头部菜单隐藏data
          headerDataShow: [], // 头部菜单展示data
          showMoreItem: false, // 是否展示隐藏的头部菜单
          topOrgId: '',
          userSex: '',
          iframeUrl: '',
          editPasswordFlag: false, // 是否展示修改密码弹窗
          editPasswordData: {
          oldPassword:'',
          newPassword: '',
          newPasswordCheck: ''
          }, // 修改密码data
          newPasswordCheck: '', // 再次确认新密码
          editPasswordRule: {
          oldPassword: [
          { required: true, validator: checkOldPass, trigger: 'blur' },
          ],
          newPassword: [
          { validator: checkDiffer, required: true, trigger: 'blur' }
          ],
          newPasswordCheck: [
          { validator: checkSame, required: true,trigger: 'blur' }
          ]
          },  // 修改密码校验
          systemName: '',    //系统标题名称
          showLodingMask:false
        }
    },
    mounted: function () {
        var _that = this;
        window.addEventListener("resize", function() {
          vm.curWidth=document.documentElement.clientWidth;
          vm.curHeight = document.documentElement.clientHeight;
          vm.setHeaderShow();
        });
        //在document挂载onlick事件
        document.addEventListener("click",this.displayMenuPopover);
        // 监听子页面的传递过来的数据
        if(window.addEventListener){
          window.addEventListener('message',_that.onMessage,false);
        }else{
          if(window.attachEvent){
          window.attachEvent("onmessage", _that.onMessage);
          }
        }
        _that.getUserIndo();
        //获取系统标题
        _that.getSystemName();

    },
    methods: {
        getUserIndo: function () { // 获取用户登陆信息
          var _that = this;
          request('opus-admin', {
          url: ctx+'opus/front/om/users/currOpusLoginUser',
          // url: '../../../../../static/agcloud/framework/ui-schemes/dark-blue/js/user_1.json',
          type: 'get',
          }, function (data) {
          if(data.success){
          _that.loginName = data.content.user.loginName;
          _that.userName = data.content.user.userName;
          _that.userId = data.content.user.userId;
          _that.topOrgId = data.content.currentOrgId
          _that.getHeaderData();
          _that.getUserAllInfo(data.content.user....
```

http://127.0.0.1:8000/xmjg/agcloud/login/js/sm3-sm4-md5-base64-merge.js

```
/*
 * JavaScript SM3
 * https://github.com/jiaxingzheng/JavaScript-SM3
 *
 * Copyright 2017, Zheng Jiaxing
 *
 * Licensed under the MIT license:
 * http://www.opensource.org/licenses/MIT
 *
 * Refer to
 * http://www.oscca.gov.cn/UpFile/20101222141857786.pdf
 */


// 左补0到指定长度
function leftPad(str, totalLength) {
  const len = str.length;
  return Array(totalLength > len ? ((totalLength - len) + 1) : 0).join(0) + str;
}

// 二进制转化为十六进制
function binary2hex(binary) {
  const binaryLength = 8;
  let hex = '';
  for (let i = 0; i < binary.length / binaryLength; i += 1) {
    hex += leftPad(parseInt(binary.substr(i * binaryLength, binaryLength), 2).toString(16), 2);
  }
  return hex;
}

// 十六进制转化为二进制
function hex2binary(hex) {
  const hexLength = 2;
  let binary = '';
  for (let i = 0; i < hex.length / hexLength; i += 1) {
    binary += leftPad(parseInt(hex.substr(i * hexLength, hexLength), 16).toString(2), 8);
  }
  return binary;
}

// 普通字符串转化为二进制
function str2binary(str) {
  let binary = '';
  for (const ch of str) {
    binary += leftPad(ch.codePointAt(0).toString(2), 8);
  }
  return binary;
}

// 循环左移
function rol(str, n) {
  return str.substring(n % str.length) + str.substr(0, n % str.length);
}

// 二进制运算
function binaryCal(x, y, method) {
  const a = x || '';
  const b = y || '';
  const result = [];
  let prevResult;
  // for (let i = 0; i < a.length; i += 1) { // 小端
  for (let i = a.length - 1; i >= 0; i -= 1) { // 大端
    prevResult = method(a[i], b[i], prevResult);
    result[i] = prevResult[0];
  }
  // console.log(`x     :${x}\ny     :${y}\nresult:${result.join('')}\n`);
  return result.join('');
}

// 二进制异或运算
function xor(x, y) {
  return binaryCal(x, y, (a, b) => [(a === b ? '0' : '1')]);
}

// 二进制与运算
function and(x, y) {
  return binaryCal(x, y, (a, b) => [(a === '1' && b === '1' ? '1' : '0')]);
}

// 二进制或运算
function or(x, y) {
  return binaryCal(x, y, (a, b) => [(a === '1' || b === '1' ? '1' : '0')]);// a === '0' && b === '0' ? '0' :
'1'
}

// 二进制与运算
function add(x, y) {
  const result = binaryCal(x, y, (a, b, prevResult) => {
    const carry = prevResult ? prevResult[1] : '0' || '0';
    if (a !== b) return [carry === '0' ? '1' : '0', carry];// a,b不等时,carry不变，结果与carry相反
    // a,b相等时，结果等于原carry，新carry等于a
    return [carry, a];
  });
  // console.log('x: ' + x + '\ny: ' + y + '\n=  ' + result + '\n');
  return result;
}

// 二进制非运算
function not(x) {
  return binaryCal(x, undefined, a => [a === '1' ? '0' : '1']);
}

function calMulti(method) {
  return (...arr) => arr.reduce((prev, curr) => method(prev, curr));
}

// function xorMulti(...arr) {
//   return arr.reduce((prev, curr) => xor(prev, curr));
// }

// 压缩函数中的置换函数 P1(X) = X xor (X <<< 9) xor (X <<< 17)
function P0(X) {
  return calMulti(xor)(X, rol(X, 9), rol(X, 17));
}

// 消息扩展中的置换函数 P1(X) = X xor (X <<< 15) xor (X <<< 23)
function P1(X) {
  return calMulti(xor)(X, rol(X, 15), rol(X, 23));
}

// 布尔函数，随j的变化取不同的表达式
function FF(X, Y, Z, j) {
  return j >= 0 && j <= 15 ? calMulti(xor)(X, Y, Z) : calMulti(or)(and(X, Y), and(X, Z), and(Y, Z));
}

// 布尔函数，随j的变化取不同的表达式
function GG(X, Y, Z, j) {
  return j >= 0 && j <= 15 ? calMulti(xor)(X, Y, Z) : or(and(X, Y), and(not(X), Z));
}
```

```
// 常量，随j的变化取不同的值
function T(j) {
  return j >= 0 && j <= 15 ? hex2binary('79cc4519') : hex2binary('7a879d8a');
}

// 压缩函数
function CF(V, Bi) {
  // 消息扩展
  const wordLength = 32;
  const W = [];
  const M = [];// W'

  // 将消息分组B划分为16个字W0， W1，…… ，W15 （字为长度为32的比特串）
  for (let i = 0; i < 16; i += 1) {
    W.push(Bi.substr(i * wordLength, wordLength));
  }

  // W[j] <- P1(W[j-16] xor W[j-9] xor (W[j-3] <<< 15)) xor (W[j-13] <<< 7) xor W[j-6]
  for (let j = 16; j < 68; j += 1) {
    W.push(calMulti(xor)(
      P1(calMulti(xor)(W[j - 16], W[j - 9], rol(W[j - 3], 15))),
      rol(W[j - 13], 7),
      W[j - 6]
    ));
  }

  // W'[j] = W[j] xor W[j+4]
  for (let j = 0; j < 64; j += 1) {
    M.push(xor(W[j], W[j + 4]));
  }

  // 压缩
  const wordRegister = [];// 字寄存器
  for (let j = 0; j < 8; j += 1) {
    wordRegister.push(V.substr(j * wordLength, wordLength));
  }

  let A = wordRegister[0];
  let B = wordRegister[1];
  let C = wordRegister[2];
  let D = wordRegister[3];
  let E = wordRegister[4];
  let F = wordRegister[5];
  let G = wordRegister[6];
  let H = wordRegister[7];

  // 中间变量
  let SS1;
  let SS2;
  let TT1;
  let TT2;
  for (let j = 0; j < 64; j += 1) {
    SS1 = rol(calMulti(add)(rol(A, 12), E, rol(T(j), j)), 7);
    SS2 = xor(SS1, rol(A, 12));

    TT1 = calMulti(add)(FF(A, B, C, j), D, SS2, M[j]);
    TT2 = calMulti(add)(GG(E, F, G, j), H, SS1, W[j]);

    D = C;
    C = rol(B, 9);
    B = A;
    A = TT1;
    H = G;
    G = rol(F, 19);
    F = E;
    E = P0(TT2);
  }

  return xor(Array(A, B, C, D, E, F, G, H).join(''), V);
}

// sm3 hash算法 http://www.oscca.gov.cn/News/20...
```

http://127.0.0.1:8000/xmjg/agcloud/framework/js-lib/vue-v2/vue.js

```
/*!
 * Vue.js v2.6.10
 * (c) 2014-2019 Evan You
 * Released under the MIT License.
 */
(function (global, factory) {
  typeof exports === 'object' && typeof module !== 'undefined' ? module.exports = factory() :
  typeof define === 'function' && define.amd ? define(factory) :
  (global = global || self, global.Vue = factory());
}(this, function () { 'use strict';

  /*  */

  var emptyObject = Object.freeze({});

  // These helpers produce better VM code in JS engines due to their
  // explicitness and function inlining.
  function isUndef (v) {
    return v === undefined || v === null
  }

  function isDef (v) {
    return v !== undefined && v !== null
  }

  function isTrue (v) {
    return v === true
  }

  function isFalse (v) {
    return v === false
  }

  /**
   * Check if value is primitive.
   */
  function isPrimitive (value) {
    return (
      typeof value === 'string' ||
      typeof value === 'number' ||
      // $flow-disable-line
      typeof value === 'symbol' ||
      typeof value === 'boolean'
    )
  }

  /**
   * Quick object check - this is primarily used to tell
   * Objects from primitive values when we know the value
   * is a JSON-compliant type.
   */
  function isObject (obj) {
    return obj !== null && typeof obj === 'object'
  }

  /**
   * Get the raw type string of a value, e.g., [object Object].
   */
  var _toString = Object.prototype.toString;

  function toRawType (value) {
    return _toString.call(value).slice(8, -1)
  }

  /**
   * Strict object type check. Only returns true
   * for plain JavaScript objects.
   */
  function isPlainObject (obj) {
    return _toString.call(obj) === '[object Object]'
  }

  function isRegExp (v) {
    return _toString.call(v) === '[object RegExp]'
  }
```

```
/**
 * Check if val is a valid array index.
 */
function isValidArrayIndex (val) {
  var n = parseFloat(String(val));
  return n >= 0 && Math.floor(n) === n && isFinite(val)
}

function isPromise (val) {
  return (
    isDef(val) &&
    typeof val.then === 'function' &&
    typeof val.catch === 'function'
  )
}

/**
 * Convert a value to a string that is actually rendered.
 */
function toString (val) {
  return val == null
    ? ''
    : Array.isArray(val) || (isPlainObject(val) && val.toString === _toString)
      ? JSON.stringify(val, null, 2)
      : String(val)
}

/**
 * Convert an input value to a number for persistence.
 * If the conversion fails, return original string.
 */
function toNumber (val) {
  var n = parseFloat(val);
  return isNaN(n) ? val : n
}

/**
 * Make a map and return a function for checking if a key
 * is in that map.
 */
function makeMap (
  str,
  expectsLowerCase
) {
  var map = Object.create(null);
  var list = str.split(',');
  for (var i = 0; i < list.length; i++) {
    map[list[i]] = true;
  }
  return expectsLowerCase
    ? function (val) { return map[val.toLowerCase()]; }
    : function (val) { return map[val]; }
}

/**
 * Check if a tag is a built-in tag.
 */
var isBuiltInTag = makeMap('slot,component', true);

/**
 * Check if an attribute is a reserved attribute.
 */
var isReservedAttribute = makeMap('key,ref,slot,slot-scope,is');

/**
 * Remove an item from an array.
 */
function remove (arr, item) {
  if (arr.length) {
    var index = arr.indexOf(item);
    if (index > -1) {
      return arr.splice(index, 1)
    }
  }
}

/**
```

```
   * Check whether an object has the property.
   */
  var hasOwnProperty = Object.prototype.hasOwnProperty;
  function hasOwn (obj, key) {
    return hasOwnProperty.call(obj, key)
  }

  /**
   * Create a cached version of a pure function.
   */
  function cached (fn) {
    var cache = Object.create(null);
    return (function cachedFn (str) {
      var hit = cache[str];
      return hit || (cache[str] = fn(str))
    })
  }

  /**
   * Camelize a hyphen-delimited string.
   */
  var camelizeRE = /-(\w)/g;
  var camelize = cached(function (str) {
    return str.replace(camelizeRE, function (_, c) { return c ? c.toUpperCase() : ''; })
  });

  /**
   * Capitalize a string.
   */
  var capitalize = cached(function (str) {
    return str.charAt(0).toUpperCase() + str.slice(1)
  });

  /**
   * Hyphenate a camelCase string.
   */
  var hyphenateRE = /\B([A-Z])/g;
  var hyphenate = cached(function (str) {
    return str.replace(hyphenateRE, '-$1').toLowerCase()
  });

  /**
   * Simple bind polyfill for environments that do not support it,
   * e.g., PhantomJS 1.x. Technically, we don't need this anymore
   * since native bind is now performant enough in most browsers.
   * But removing it would mean breaking code that was able to run in
   * PhantomJS 1.x, so this must be kept for backward compatibility...
```

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/jquery-2.1.0.min.js

```
/*! jQuery v2.1.0 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license
//@ sourceMappingURL=jquery-2.1.0.min.map
*/
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?
b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return
b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=
[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k="".trim,l=
{},m=a.document,n="2.1.0",o=function(a,b){return new o.fn.init(a,b)},p=/^-ms-/,q=/-([\da-
z])/gi,r=function(a,b){return b.toUpperCase()};o.fn=o.prototype=
{jquery:n,constructor:o,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return
null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var
b=o.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return
o.each(this,a,b)},map:function(a){return this.pushStack(o.map(this,function(b,c){return
a.call(b,c,b)}))},slice:function(){return this.pushStack(d.apply(this,arguments))},first:function(){return
this.eq(0)},last:function(){return this.eq(-1)},eq:function(a){var b=this.length,c=+a+(0>a?b:0);return
this.pushStack(c>=0&&b>c?[this[c]]:[])},end:function(){return
this.prevObject||this.constructor(null)},push:f,sort:c.sort,splice:c.splice},o.extend=o.fn.extend=function()
{var a,b,c,d,e,f,g=arguments[0]||{},h=1,i=arguments.length,j=!1;for("boolean"==typeof g&&
(j=g,g=arguments[h]||{},h++),"object"==typeof g||o.isFunction(g)||(g={}),h===i&&(g=this,h--
);i>h;h++)if(null!=(a=arguments[h]))for(b in a)c=g[b],d=a[b],g!==d&&(j&&d&&(o.isPlainObject(d)||
(e=o.isArray(d)))?(e?(e=!1,f=c&&o.isArray(c)?c:[]):f=c&&o.isPlainObject(c)?c:{},g[b]=o.extend(j,f,d)):void
0!==d&&(g[b]=d));return g},o.extend({expando:"jQuery"+
(n+Math.random()).replace(/\D/g,""),isReady:!0,error:function(a){throw new Error(a)},noop:function()
{},isFunction:function(a){return"function"===o.type(a)},isArray:Array.isArray,isWindow:function(a){return
null!=a&&a===a.window},isNumeric:function(a){return a-parseFloat(a)>=0},isPlainObject:function(a)
{if("object"!==o.type(a)||a.nodeType||o.isWindow(a))return!1;try{if(a.constructor&&!j.call(a.constructor.prot
otype,"isPrototypeOf"))return!1}catch(b){return!1}return!0},isEmptyObject:function(a){var b;for(b in
a)return!1;return!0},type:function(a){return null==a?a+"":"object"==typeof a||"function"==typeof a?
h[i.call(a)]||"object":typeof a},globalEval:function(a){var b,c=eval;a=o.trim(a),a&&(1===a.indexOf("use
strict")?
(b=m.createElement("script"),b.text=a,m.head.appendChild(b).parentNode.removeChild(b)):c(a))},camelCase:funct
ion(a){return a.replace(p,"ms-").replace(q,r)},nodeName:function(a,b){return
a.nodeName&&a.nodeName.toLowerCase()===b.toLowerCase()},each:function(a,b,c){var
d,e=0,f=a.length,g=s(a);if(c){if(g){for(;f>e;e++)if(d=b.apply(a[e],c),d===!1)break}else for(e in
a)if(d=b.apply(a[e],c),d===!1)break}else if(g){for(;f>e;e++)if(d=b.call(a[e],e,a[e]),d===!1)break}else for(e
in a)if(d=b.call(a[e],e,a[e]),d===!1)break;return a},trim:function(a){return
null==a?"":k.call(a)},makeArray:function(a,b){var c=b||[];return null!=a&&(s(Object(a))?
o.merge(c,"string"==typeof a?[a]:a):f.call(c,a)),c},inArray:function(a,b,c){return null==b?-
1:g.call(b,a,c)},merge:function(a,b){for(var c=+b.length,d=0,e=a.length;c>d;d++)a[e++]=b[d];return
a.length=e,a},grep:function(a,b,c){for(var d,e=
[],f=0,g=a.length,h=!c;g>f;f++)d=!b(a[f],f),d!==h&&e.push(a[f]);return e},map:function(a,b,c){var
d,f=0,g=a.length,h=s(a),i=[];if(h)for(;g>f;f++)d=b(a[f],f,c),null!=d&&i.push(d);else for(f in
a)d=b(a[f],f,c),null!=d&&i.push(d);return e.apply([],i)},guid:1,proxy:function(a,b){var
c,e,f;return"string"==typeof b&&(c=a[b],b=a,a=c),o.isFunction(a)?(e=d.call(arguments,2),f=function(){return
a.apply(b||this,e.concat(d.call(arguments)))},f.guid=a.guid=a.guid||o.guid++,f):void
0},now:Date.now,support:l}),o.each("Boolean Number String Function Array Date RegExp Object Error".split("
"),function(a,b){h["[object "+b+"]"]=b.toLowerCase()});function s(a){var
b=a.length,c=o.type(a);return"function"===c||o.isWindow(a)?!1:1===a.nodeType&&b?!0:"array"===c||0===b||"numbe
r"==typeof b&&b>0&&b-1 in a}var t=function(a){var b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s="sizzle"+-new
Date,t=a.document,u=0,v=0,w=eb(),x=eb(),y=eb(),z=function(a,b){return a===b&&
(j=!0),0},A="undefined",B=1<<31,C={}.hasOwnProperty,D=
[],E=D.pop,F=D.push,G=D.push,H=D.slice,I=D.indexOf||function(a){for(var
b=0,c=this.length;c>b;b++)if(this[b]===a)return b;return-
1},J="checked|selected|async|autofocus|autoplay|controls|defer|disabled|hidden|ismap|loop|multiple|open|reado
nly|required|scoped",K="[\\x20\\t\\r\\n\\f]",L="(?:\\\\.|[\\w-]|[^\\x00-\\xa0])+",M=L.replace("w","w#"),N="\\
["+K+"*("+L+")"+K+"*(?:([*^$|!~]?=)"+K+"*(?:(['\"])((?:\\\\.|[^\\\\])*?)\\3|("+M+")|)|)"+K+"*\\]",O=":("+L+")
(?:\\((['\"])((?:\\\\.|[^\\\\])*?)\\3|((?:\\\\.|[^\\\\()[\\]]|"+N.replace(3,8)+")*)|.*)\\)|)",P=new R...
```

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/numberAnimate.js

```
/**
 * Created by GYFlasher on 2017-12-08.
 */
/**
 * 滚动数字 (依赖jq)
 * @param el 用来显示滚动字幕的容器class 或 id
 * @param option 配置参数 width: 数字的宽 (无单位),fontSize: 字体大小（无单位）, color: 文字颜
色,autoSizeContainerWidth: 自动计算容器宽度
 * @returns {Object}
 */
function numberAnimate(el,option) {
    $(el).html('');
    this.container = $(el);
    this.option = option;
    this.container.css({
        position: "relative",
        padding: "0",
        'overflow': "hidden"
    });
    var height = this.container.height();
    this.subWidth = Number(option.width)-2;
    this.subHeight = height+10;
    this.autoSizeContainerWidth = option.autoSizeContainerWidth;
    this.col = '<span class="g-num-item" href="0">' +
        '<i class="g-wheel-item g-wheel-item-0"><a>0</a></i>' +
        '<i class="g-wheel-item g-wheel-item-1"><a>1</a></i>' +
        '<i class="g-wheel-item g-wheel-item-2"><a>2</a></i>' +
        '<i class="g-wheel-item g-wheel-item-3"><a>3</a></i>' +
        '<i class="g-wheel-item g-wheel-item-4"><a>4</a></i>' +
        '<i class="g-wheel-item g-wheel-item-5"><a>5</a></i>' +
        '<i class="g-wheel-item g-wheel-item-6"><a>6</a></i>' +
        '<i class="g-wheel-item g-wheel-item-7"><a>7</a></i>' +
        '<i class="g-wheel-item g-wheel-item-8"><a>8</a></i>' +
        '<i class="g-wheel-item g-wheel-item-9"><a>9</a></i>' +
        '<i class="g-wheel-item g-wheel-item-10"><a>.</a></i>' +
        '</span>';
```

```
}
numberAnimate.prototype.run = function (value,param) {
     // console.log("old = " + this.currentValue + "new = " + value);
    var self = this;
    this.currentValue = value;
    var valueString = value.toString();
    var itemLength = 11;
    var angle = 360 / itemLength;
    var h = self.subHeight / Math.tan((angle * 0.5) * (2 * Math.PI/360));
    if (self.autoSizeContainerWidth) {
        self.container.css({
          "width": (valueString.length * self.subWidth)/100 + "rem"
        });
    }
    var oldLength = self.container.children(".g-num-item").length;

    if (valueString.length > oldLength) {
        for (var i = 0; i < valueString.length - oldLength; i++) {
          self.container.append(self.col);
          self.container.children(".g-num-item").eq(oldLength + i).css({
          right: (self.subWidth * (oldLength + i))/100 + "rem"
          });
          var num = 0;
          self.oldValueString = num.toString() + self.oldValueString;
        }
    }else if (valueString.length < oldLength) {
        for (var i = 0; i < oldLength - valueString.length; i++) {
          self.container.children(".g-num-item:last").remove();
          var newStr = self.oldValueString.substr(1, self.oldValueString.length - 1);
          self.oldValueString = newStr;
        }
    }
    //白屏版
    var bgColor = '#fff';
    if (screen != "3") {
        bgColor = '#22355c'
    }
    if(oldLength == 0 || this.currentValue != self.oldValueString){
        $(".g-num-item").css({
          position: "absolute",
          top:  (-(h - self.subHeight) * 0.6)/100 + "rem",
          width:  self.subWidth/100 + "rem",
          height:  h/100 + "rem",
          display:'inline-block',
          transformStyle:' preserve-3d',
          '-webkit-transform-style':' preserve-3d',
          '-ms-transform-style': 'preserve-3d'
        });
        $(".g-wheel-item").css({
          width: self.subWidth/100 + "rem",
          height: h/100 + "rem",
          position: 'absolute',
          left: 0,
          top: 0,
          border: '0px solid gainsboro',
          background:bgColor,
          transformStyle:' preserve-3d',
          '-webkit-transform-style':' preserve-3d',
          '-ms-transform-style': 'preserve-3d'
        });
        $(".g-wheel-item a").css({
          width: self.subWidth/100 + "rem",
          height: (self.subHeight)/100 + "rem",
          lineHeight: (self.subHeight+10)/100 + "rem",
          textAlign: "center",
          fontSize: self.option.fontSize/100 + "rem",
          color: self.option.color,
          display: "block",
          fontStyle: "normal",
          transform: 'translateY(-'+ (self.subHeight * 0.5)/100 +'rem) rotateX(90deg)',
          backgroundColor: bgColor,
        });

        for (var i = 0; i < itemLength; i++) {
          $(".g-wheel-item-" + i).css({
          transform: "rotateX(" + (-90 - i * angle) + "deg)",
          height: h/100 + "rem"
          });
        }
    }
    setTimeout(function () {
        if (valueString.length !== self.container.children(".g-num-item").length) {
          console.log("%c%s","color:red;", "数字位数和数字条个数不相等");
          // debugger
        }
        for (var i = 0; i < valueString.length; i++) {
          var rotateAngle  = 0;
          var value = parseInt(valueString[i]);

          var lastValue = parseInt(self.oldValue...
```

http://127.0.0.1:8000/xmjg/common/tool/date/js/bootstrap.min.js

```
/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under the MIT license
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){"use
strict";var b=a.fn.jquery.split(" ")[0].split(".");if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>3)throw
new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4")}
(jQuery),+function(a){"use strict";function b(){var a=document.createElement("bootstrap"),b=
{WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd
otransitionend",transition:"transitionend"};for(var c in b)if(void
0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var
c=!1,d=this;a(this).one("bsTransitionEnd",function(){c=!0});var e=function()
{c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this},a(function()
{a.support.transition=b(),a.support.transition&&(a.event.special.bsTransitionEnd=
{bindType:a.support.transition.end,delegateType:a.support.transition.end,handle:function(b)
{if(a(b.target).is(this))return b.handleObj.handler.apply(this,arguments)}})})}(jQuery),+function(a){"use
strict";function b(b){return this.each(function(){var
c=a(this),e=c.data("bs.alert");e||c.data("bs.alert",e=new d(this)),"string"==typeof b&&e[b].call(c)})}var
c='[data-dismiss="alert"]',d=function(b)
{a(b).on("click",c,this.close)};d.VERSION="3.3.7",d.TRANSITION_DURATION=150,d.prototype.close=function(b)
{function c(){g.detach().trigger("closed.bs.alert").remove()}var e=a(this),f=e.attr("data-target");f||
(f=e.attr("href"),f=f&&f.replace(/.*(?=#[^\s]*$)/,""));var g=a("#"===f?[]:f);b&&b.preventDefault(),g.length||
(g=e.closest(".alert")),g.trigger(b=a.Event("close.bs.alert")),b.isDefaultPrevented()||
(g.removeClass("in"),a.support.transition&&g.hasClass("fade")?
g.one("bsTransitionEnd",c).emulateTransitionEnd(d.TRANSITION_DURATION):c())};var
e=a.fn.alert;a.fn.alert=b,a.fn.alert.Constructor=d,a.fn.alert.noConflict=function(){return
a.fn.alert=e,this},a(document).on("click.bs.alert.data-api",c,d.prototype.close)}(jQuery),+function(a){"use
strict";function b(b){return this.each(function(){var d=a(this),e=d.data("bs.button"),f="object"==typeof
b&&b;e||d.data("bs.button",e=new c(this,f)),"toggle"==b?e.toggle():b&&e.setState(b)})}var c=function(b,d)
{this.$element=a(b),this.options=a.extend({},c.DEFAULTS,d),this.isLoading=!1};c.VERSION="3.3.7",c.DEFAULTS=
{loadingText:"loading..."},c.prototype.setState=function(b){var
c="disabled",d=this.$element,e=d.is("input")?"val":"html",f=d.data();b+="Text",null==f.resetText&&d.data("res
etText",d[e]()),setTimeout(a.proxy(function(){d[e](null==f[b]?this.options[b]:f[b]),"loadingText"==b?
(this.isLoading=!0,d.addClass(c).attr(c,c).prop(c,!0)):this.isLoading&&
(this.isLoading=!1,d.removeClass(c).removeAttr(c).prop(c,!1))},this),0)},c.prototype.toggle=function(){var
a=!0,b=this.$element.closest('[data-toggle="buttons"]');if(b.length){var
c=this.$element.find("input");"radio"==c.prop("type")?(c.prop("checked")&&
(a=!1),b.find(".active").removeClass("active"),this.$element.addClass("active")):"checkbox"==c.prop("type")&&
(c.prop("checked")!==this.$element.hasClass("active")&&
(a=!1),this.$element.toggleClass("active")),c.prop("checked",this.$element.hasClass("active")),a&&c.trigger("
change")}else this.$element.attr("aria-
pressed",!this.$element.hasClass("active")),this.$element.toggleClass("active")};var
d=a.fn.button;a.fn.button=b,a.fn.button.Constructor=c,a.fn.button.noConflict=function(){return
a.fn.button=d,this},a(document).on("click.bs.button.data-api",'[data-toggle^="button"]',function(c){var
d=a(c.target).closest(".btn");b.call(d,"toggle"),a(c.target).is('input[type="radio"],
input[type="checkbox"]')||(c.preventDefault(),d.is("input,button")?
d.trigger("focus"):d.find("input:visible,button:visible").first().trigger("focus"))}).on("focus.bs.button.dat
a-api blur.bs.button.data-api",'[data-toggle^="button"]',function(b)
{a(b.target).closest(".btn").toggleClass("focus",/^focus(in)?$/.test(b.type))})}(jQuery),+function(a){"use
strict";function b(b){return this.each(function(){var
d=a(this),e=d.data("bs.carousel"),f=a.extend({},c.DEFAULTS,d.data(),"object"==typeof b&&b),g="string"==typeof
b?b:f.slide;e||d.data("bs.carousel",e=new c(this,f)),"number"==typeof b?e.to(b):g?e[g]
():f.interval&&e.pause().cycle()})}var c=function(b,c)
{this.$element=a(b),this.$indicators=this.$element.find(".carousel-
indicators"),this.options=c,this.paused=null,this.sliding=null,this.interval=null,this.$active=null,this.$ite
ms=null,this.options.keyboard&&this.$element.on("keydown.bs.carousel",a.proxy(this.keydown,this)),"hover"==th
is.options.pause&&!("ontouchstart"in
document.documentElement)&&this.$element.on("mouseenter.bs.carousel",a.proxy(this.pause,this)).on("mouseleave
.bs.carousel",a.proxy(this.cycle,this))};c.VERSION="3.3.7",c.TRANSITION_DURATION=600,c.DEFAULTS=
{interval:5e3,pause:"hover",wrap:!0,keyboard:!0},...
```

http://127.0.0.1:8000/xmjg/common/tool/date/js/bootstrap-datepicker.min.js

```
/*!
 * Datepicker for Bootstrap v1.6.4 (https://github.com/eternicode/bootstrap-datepicker)
 *
 * Copyright 2012 Stefan Petre
 * Improvements by Andrew Rowls
 * Licensed under the Apache License v2.0 (http://www.apache.org/licenses/LICENSE-2.0)
 */
!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):a("object"==typeof exports?
require("jquery"):jQuery)}(function(a,b){function c(){return new
Date(Date.UTC.apply(Date,arguments))}function d(){var a=new Date;return
c(a.getFullYear(),a.getMonth(),a.getDate())}function e(a,b){return
a.getUTCFullYear()===b.getUTCFullYear()&&a.getUTCMonth()===b.getUTCMonth()&&a.getUTCDate()===b.getUTCDate()}f
unction f(a){return function(){return this[a].apply(this,arguments)}}function g(a){return
a&&!isNaN(a.getTime())}function h(b,c){function d(a,b){return b.toLowerCase()}var e,f=a(b).data(),g={},h=new
RegExp("^"+c.toLowerCase()+"([A-Z])");c=new RegExp("^"+c.toLowerCase());for(var i in f)c.test(i)&&
(e=i.replace(h,d),g[e]=f[i]);return g}function i(b){var c={};if(q[b]||(b=b.split("-")[0],q[b])){var
d=q[b];return a.each(p,function(a,b){b in d&&(c[b]=d[b])}),c}}var j=function(){var b={get:function(a){return
this.slice(a)[0]},contains:function(a){for(var
b=a&&a.valueOf(),c=0,d=this.length;d>c;c++)if(this[c].valueOf()===b)return c;return-1},remove:function(a)
{this.splice(a,1)},replace:function(b){b&&(a.isArray(b)||(b=
[b]),this.clear(),this.push.apply(this,b))},clear:function(){this.length=0},copy:function(){var a=new
j;return a.replace(this),a}};return function(){var c=[];return c.push.apply(c,arguments),a.extend(c,b),c}}
(),k=function(b,c){a(b).data("datepicker",this),this._process_options(c),this.dates=new
j,this.viewDate=this.o.defaultViewDate,this.focusDate=null,this.element=a(b),this.isInput=this.element.is("in
put"),this.inputField=this.isInput?
this.element:this.element.find("input"),this.component=this.element.hasClass("date")?this.element.find(".add-
on, .input-group-addon,
.btn"):!1,this.hasInput=this.component&&this.inputField.length,this.component&&0===this.component.length&&
(this.component=!1),this.isInline=!this.component&&this.element.is("div"),this.picker=a(r.template),this._che
ck_template(this.o.templates.leftArrow)&&this.picker.find(".prev").html(this.o.templates.leftArrow),this._che
ck_template(this.o.templates.rightArrow)&&this.picker.find(".next").html(this.o.templates.rightArrow),this._b
uildEvents(),this._attachEvents(),this.isInline?this.picker.addClass("datepicker-
inline").appendTo(this.element):this.picker.addClass("datepicker-dropdown dropdown-
menu"),this.o.rtl&&this.picker.addClass("datepicker-
rtl"),this.viewMode=this.o.startView,this.o.calendarWeeks&&this.picker.find("thead .datepicker-title, tfoot
.today, tfoot .clear").attr("colspan",function(a,b){return
parseInt(b)+1}),this._allow_update=!1,this.setStartDate(this._o.startDate),this.setEndDate(this._o.endDate),t
his.setDaysOfWeekDisabled(this.o.daysOfWeekDisabled),this.setDaysOfWeekHighlighted(this.o.daysOfWeekHighlight
ed),this.setDatesDisabled(this.o.datesDisabled),this.fillDow(),this.fillMonths(),this._allow_update=!0,this.u
pdate(),this.showMode(),this.isInline&&this.show()};k.prototype={constructor:k,_resolveViewName:function(a,c)
{return 0===a||"days"===a||"month"===a?0:1===a||"months"===a||"year"===a?1:2===a||"years"===a||"decade"===a?
2:3===a||"decades"===a||"century"===a?3:4===a||"centuries"===a||"millennium"===a?
4:c===b?!1:c},_check_template:function(c){try{if(c===b||""===c)return!1;if((c.match(/[<>]/g)||
[]).length<=0)return!0;var d=a(c);return d.length>0}catch(e){return!1}},_process_options:function(b)
{this._o=a.extend({},this._o,b);var e=this.o=a.extend({},this._o),f=e.language;q[f]||(f=f.split("-")
[0],q[f]||
(f=o.language)),e.language=f,e.startView=this._resolveViewName(e.startView,0),e.minViewMode=this._resolveView
Name(e.minViewMode,0),e.maxViewMode=this._resolveViewName(e.maxViewMode,4),e.startView=Math.min(e.startView,e
.maxViewMode),e.startView=Math.max(e.startView,e.minViewMode),e.multidate!==!0&&
(e.multidate=Number(e.multidate)||!1,e.multidate!==!1&&
(e.multidate=Math.max(0,e.multidate))),e.multidateSeparator=String(e.multidateSeparator),e.weekStart%=7,e.wee
kEnd=(e.weekStart+6)%7;var g=r.parseFormat(e.format);e.startDate!==-(1/0)&&(e.startDate?e.startDate
instanceof Date?
e.startDate=this._local_to_utc(this._zero_time(e.startDate)):e.startDate=r.parseDate(e.startDate,g,e.language
,e.assumeNearbyYear):e.startDate=-(1/0)),e.endDate!==1/0&&(e.endDate?e.endDate instanceof Date?
e.endDate=this._local_to_utc(this._zero_time(e.endDate)):e.endDate=r.parseDate(e.endDate,g,e.language,e.assum
eNearbyYear):e.endDate=1/0),e.daysOfWeekDisabled=e.daysOfWeekDisabled||[],a.isArray(e.daysOfWeekDisabled)||
(e.daysOfWeekDisabled=e.daysOfWeekDisabled.split(/[,\s]*/)),e.daysOfWeekDisabled=a.map(e.daysOfWeekDisabled,f
unction(a){return parseInt(a,10)}),e.daysOfWeekHighlighted=e.daysOfWeekHighlighted||
[],a.isArray(e.daysOfWeekHighlighted)||(e.daysOfWeekHighlighted=e.daysOfWeekHighlighted.split(/[,\s]*/)),...
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
    var isWhite = '';//pc版首页    var ctx='/xmjg/';    var name = '';    var xzqhdm= "";    var loginXzqhdm=
"" ? "" : "china";    var loginProvince = "" ? "" : "china";   // var oldflag = "";    var oldflag =
"true";console.log(oldflag);    var oldStartDate = "";    var oldEndDate = "";    var bigScreenFolder=""; //
大屏css 目录，如果是普通屏（默认）则该值为空    var provinceCode="";    //var projectManager=parent.projectManager;
var defaultEndDate="",defaultStartDate="";    var provinceParam={};    var params = "";    var initHeartBeat
="";    var initStartDate="";//获取配置文件中统计时间的配置参数
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
    var date = new Date();var dateStr =    date.getFullYear() + "-" + ("0" + (date.getMonth() + 1)).slice(-2)
+ "-"+ ("0" + (date.getDate())).slice(-2);var startTime = dateStr.substr(0,5)+"01-01";var endDateStr =
dateStr;    Date.prototype.format = function(fmt) {        var o = {          "M+" : this.getMonth()+1,
//月份          "d+" : this.getDate(),          //日          "h+" : this.getHours(),          //小时
"m+" : this.getMinutes(),          //分          "s+" : this.getSeconds(),          //秒          "q+" :
Math.floor((this.getMonth()+3)/3), //季度          "S"  : this.getMilliseconds()          //毫秒        };
if(/(y+)/.test(fmt)) {          fmt=fmt.replace(RegExp.$1, (this.getFullYear()+"").substr(4 -
RegExp.$1.length));        }        for(var k in o) {          if(new RegExp("("+ k +")").test(fmt)){
fmt = fmt.replace(RegExp.$1, (RegExp.$1.length==1) ? (o[k]) : (("00"+ o[k]).substr((""+ o[k]).length)));
}        }        return fmt;    }    var initStartDate='2018-06-01';//获取配置文件中统计时间的配置参数
$(function () {$(".loading").show();//一秒后消失loading图标setTimeout(function () {$(".loading").hide()},1000);
var date = new Date();        var nowDate='';        var nowYearStart = date.getFullYear() + "-01-01";
//tab栏        $('.stage-tab-tit a').click(function(e) {          var selfIndex = $(this).index();
$(this).addClass('active').siblings().removeClass('active');
$(this).parent().siblings().children('div:eq(' + selfIndex +
')').addClass('active').siblings().removeClass('active');          if($(this).text()=="办件总量"){
$("#sumyqxm").css('color','#007BFF');          $("#spjdyqxm li p b ").css('color','#007BFF');          }
var texxt = $(this).text();          if( texxt =='审批用时'){          scrollEl('pjys');          } else
if(texxt =='跨度用时'){          scrollEl('kdys');          } else if(texxt =='最长用时'){
scrollEl('zcys');          }if(texxt=="最长用时"){$(this).parent().parent().find('div').eq(0).html("最长用时
(天)");}else if(texxt=="审批用时" || texxt=="跨度用时"){$(this).parent().parent().find('div').eq(0).html("平均用
时(天)");}        });        // 新增想项目数前五名（个） 省排名 城市排名 点击事件$('.stage-tab-tit2
a').click(function(e) {          $(".loading").show();var selfIndex =
$(this).index();$(this).addClass('active').siblings().removeClass('active');$(this).parent().siblings().child
ren('div:eq(' + selfIndex + ')').addClass('active').siblings().removeClass('active');console.log('index = '+
selfIndex);var texxt = $(this).text();if( texxt =='省排名')
{setMonthNewProjectTop5('',getStartDate(),getEndDate());} else if(texxt =='师市排名')
{setMonthNewProjectTop5('getTopFiveCity',getStartDate(),getEndDate());}          setTimeout(function () {
$(".loading").hide()          },1000);});        // 各城市项目逾期率排名 省排名 城市排名 点击事件        $('.stage-
tab-tit3 a').click(function(e) {          $(".loading").show();          var selfIndex = $(this).index();
$(this).addClass('active').siblings().removeClass('active');
$(this).parent().siblings().children('div:eq(' + selfIndex +
')').addClass('active').siblings().removeClass('active');          var texxt = $(this).text();          if(
texxt =='省排名'){
getCityItemOverTimeSort('getProvinceItemOverTimeSort',getStartDate(),getEndDate());          } else if(texxt
=='师市排名'){          getCityItemOverTimeSort('city',getStartDate(),getEndDate());          }
setTimeout(function () {          $(".loading").hide()          },1000);        });
$('#dateStart').val(startTime);        $('#dateEnd').val(endDateStr);        //执行初始化方法
setTimeout("doOnloadInit()",5);//开始时间初始化$('#dateStart').datepicker({autoclose : true, //自动关闭
beforeShowDay : $.noop, //在显示日期之前调用的函数calendarWeeks : false, //是否显示今年是第几周clearBtn : false, //
显示清除按钮daysOfWeekDisabled : [], //星期几不可选forceParse : true, //是否强制转换不符合格式的字符串format : 'yyyy-
mm-dd', //日期格式keyboardNavigation : true, //是否显示箭头导航language : 'zh-CN', //语言minViewMode :
0,orientation : "auto", //方向rtl : false,//startDate : -Infinity, //日历开始日期startDate :"2018-06-
01",endDate:dateStr,startView : 0, //开始显示todayBtn : false, //今天按钮todayHighlight : true, //今天高亮
weekStart : 0//星期几是开始}).on('changeDate', function(e) {var start = $("#dateStart").val();$('.js-
endTime').datepicker('setStartDate', new Date(start));});//结束时间初始化$('#dateEnd').datepicker({autoclose :
true, //自动关闭beforeShowDay : $.noop, //在显示日期之前调用的函数calendarWeeks : false, //是否显示今年是第几周
clearBtn : false, //显示清除按钮daysOfWeekDisabled : [], //星期几不可选forceParse : true, //是否强制转换不符合格式的
字符串format : 'yyyy-mm-dd', //日期格式keyboardNavigation : true, //是否显示箭头导航language : 'zh-CN', //语言
minViewMode : 0,orientation : "auto", //方向rtl : false,//startDate : -Infinity, //日历开始日期startDate
:startTime,endDate:"2099-12-31",startView : 0, //开始显示todayBtn : false, //今天按钮todayHighlight : true, //今
天高...
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
skipPage();
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
;
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toStageRankPage('5','0')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toRankingPage(1)
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toProjectStageRankPage('8','0')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toProjectStageRankPage('8','1')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toProjectStageRankPage('8','2')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toProjectStageRankPage('8','3')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toProjectStageRankPage('8','4')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toProjectStageRankPage('8','5')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toProjectStageRankPage('9','0')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toProjectStageRankPage('9','1')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toProjectStageRankPage('9','2')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toProjectStageRankPage('9','3')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toProjectStageRankPage('9','4')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toProjectStageRankPage('9','5')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toPingJunYongShiPage()
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toStageRankPage(1,5,'政府投资工程建设项目（房屋建筑类）')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toStageRankPage(2,5,'政府投资工程建设项目（房屋建筑类）')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toStageRankPage(3,5,'政府投资工程建设项目（房屋建筑类）')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toStageRankPage('4','1')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toStageRankPage('4','2')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toStageRankPage('4','3')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toStageRankPage('4','4')
```

http://127.0.0.1:8000/xmjg/supervisionInspection/dg-jdkh-main.do

```
toStageRankPage('4','5')
```

http://127.0.0.1:8000/xmjg/common/tool/cityselect/js/auto_area.js

```
var localDataCitiesCanselect = [];
var auto_area = {
    run: function () {// 运行应用
        var run = $('.data-search input[name=searcharea]'), runList = $('.searchList'), ac_menu =
$('.searchList .area_menu');
        var def_text = '请搜索...';
        run.val(def_text);
        run.focus(function () {
          if (this.value == def_text) this.value = '';
        }).blur(function () {
          if (this.value == '') this.value = def_text;
          auto_area.delay(function () { runList.hide() }, 300);//延时，等待选择事件执行完成
        }).bind('keyup', function () {
          auto_area.appRunList(runList, run.val());
        }).keydown(function (e) {
          if (e.keyCode == 13) setTimeout(auto_area.appRunExec, 200);
        });
    },
    delay: function (f, t) {
        { if (typeof f != "function") return; var o = setTimeout(f, t); this.clear = function () {
clearTimeout(o) } }
    },
    appRunList: function (runList, v) {//自动搜索应用
        if (v == '') {
          runList.hide();
          return;
        }
        var canselects   = __LocalDataCities.category["canselect"]; //不存在时 可选所有
        var i, temp = '', n = 0, loaded = {};
        //搜索以关键词开头的应用
        for (i in searchValue) {
          if (isNaN(i) || loaded[i] || !searchValue[i].name) {
          continue;
          }
          runSearchCode = searchValue[i].code
                if(canselects){
                        if(canselects[runSearchCode]==undefined || canselects[runSearchCode]=='undefined'){
                                continue;
                        }
                }
          runSearchName = searchValue[i].name;
          runSearchPinyin = searchValue[i].pinyin;
          runSearchPy = searchValue[i].py;
          if (runSearchName.indexOf(v) >= 0 || runSearchPinyin.indexOf(v) >= 0 || runSearchPy.indexOf(v) >= 0
|| runSearchPinyin.toLowerCase().indexOf(v) >= 0 || runSearchPy.toLowerCase().indexOf(v) >= 0) {
          loaded[i] = 1;
          temp += '<a class="area_menu" href="javascript:;" data-flag=1 data-code="' + runSearchCode + '"
data-name="' + runSearchName + '" onclick="selectProvince(\'sub\',this,\'\')"><em>' +
runSearchPinyin.replace(v, "<b>" + v + "</b>") + '</em>' + runSearchName.replace(v, "<b>" + v + "</b>") +
'</a>';
          if (++n > 10) break;
          }
        }
        if (temp) {// 搜索到应用则显示
          runList.show().html(temp);
        } else {
          runList.hide().html('');
        }
    },

    appRunExec: function () {// 运行按纽点击
        ac_menu = $('.searchList .area_menu');
        if (ac_menu.length > 0) {
          ac_menu.eq(0).trigger('click');
        }
    },
};
/**
 * 城市选择插件 中可选城市数据构造
 * @param dataObj
 * @returns
 */
function setCanSelectCityDataForCityTool(dataObj){

    var xxxCode="";
    for(var i=0;i<dataObj.length;i++){
        xxxCode=dataObj[i]["XZQHDM"];
        localDataCitiesCanselect[xxxCode]=dataObj[i]["CNT"];
        /*if(i<30){
          //项目数最多的30个城市 设置为热点城市
          localDataCitiesHotcities.push(xxxCode);
        }*/
        if(xxxCode.indexOf("6590") > -1){
          //新疆兵团
          xxxCode=xxxCode.substring(0,3)+"100";// 省编码
        }else{
          xxxCode=xxxCode.substring(0,2)+"0000";// 省编码
        }
        if(localDataCitiesCanselect[xxxCode]==undefined || localDataCitiesCanselect[xxxCode]=='undefined'){
          localDataCitiesCanselect[xxxCode]="a";
        }
    }
    __LocalDataCities.category["canselect"]=localDataCitiesCanselect;
    // __LocalDataCities.category["hotcities"]=localDataCitiesHotcities;
}
```

http://127.0.0.1:8000/xmjg/common/tool/cityselect/js/city_data.js

```
//执行 analysis-info!CreateCityData.action 方式生成最新城市数据
//生成的文件路径为 D:\city_data.js，请手动替换/common/tool/cityselect/js/city_data.js 中的内容
var __LocalDataCities={"list":{"110000":["北京","Beijing","BJ"],"120000":["天津","Tianjin","TJ"],"130000":["河
北","Hebei","HB"],"130100":["石家庄","Shijiazhuang","SJZ"],"130181":["辛集市","Xinjishi","XJS"],"130200":["唐
山","Tangshan","TS"],"130300":["秦皇岛","Qinhuangdao","QHD"],"130400":["邯郸","Handan","HD"],"130500":["邢
台","Xingtai","XT"],"130600":["保定","Baoding","BD"],"130682":["定州市","Dingzhoushi","DZS"],"130700":["张家
口","Zhangjiakou","ZJK"],"130800":["承德","Chengde","CD"],"130900":["沧州","Cangzhou","CZ"],"131000":["廊
坊","Langfang","LF"],"131100":["衡水","Hengshui","HS"],"131200":["雄安","Xionganxinqu","XAXQ"],"140000":["山
西","Shanxi","SX"],"140100":["太原","Taiyuan","TY"],"140200":["大同","Datong","DT"],"140300":["阳
泉","Yangquan","YQ"],"140400":["长治","Zhangzhi","CZ"],"140500":["晋城","Jincheng","JC"],"140600":["朔
州","Shuozhou","SZ"],"140700":["晋中","Jinzhong","JZ"],"140800":["运城","Yuncheng","YC"],"140900":["忻
州","Xinzhou","XZ"],"141000":["临汾","Linfen","LF"],"141100":["吕梁","Lüliang","LL"],"150000":["内蒙
古","Neimenggu","NMG"],"150100":["呼和浩特","Huhehaote","HHHT"],"150200":["包头","Baotou","BT"],"150300":["乌
海","Wuhai","WH"],"150400":["赤峰","Chifeng","CF"],"150500":["通辽","Tongliao","TL"],"150600":["鄂尔多
斯","Eerduosi","EEDS"],"150700":["呼伦贝尔","Hulunbeier","HLBE"],"150800":["巴彦淖
尔","Bayannaoer","BYNE"],"150900":["乌兰察布","Wulanchabu","WLCB"],"152200":["兴安","Xingan","XA"],"152500":
["锡林郭勒","Xilinguole","XLGL"],"152900":["阿拉善","Alashan","ALS"],"210000":["辽宁","Liaoning","LN"],"210100":
["沈阳","Shenyang","SY"],"210200":["大连","Dalian","DL"],"210300":["鞍山","Anshan","AS"],"210400":["抚
顺","Fushun","FS"],"210500":["本溪","Benxi","BX"],"210600":["丹东","Dandong","DD"],"210700":["锦
州","Jinzhou","JZ"],"210800":["营口","Yingkou","YK"],"210900":["阜新","Fuxin","FX"],"211000":["辽
阳","Liaoyang","LY"],"211100":["盘锦","Panjin","PJ"],"211200":["铁岭","Tieling","TL"],"211300":["朝
阳","Chaoyang","CY"],"211400":["葫芦岛","Huludao","HLD"],"220000":["吉林","Jilin","JL"],"220100":["长
春","Zhangchun","CC"],"220200":["吉林","Jilin","JL"],"220300":["四平","Siping","SP"],"220400":["辽
源","Liaoyuan","LY"],"220500":["通化","Tonghua","TH"],"220600":["白山","Baishan","BS"],"220700":["松
原","Songyuan","SY"],"220800":["白城","Baicheng","BC"],"222400":["延边","Yanbian","YB"],"230000":["黑龙
江","Heilongjiang","HLJ"],"230100":["哈尔滨","Haerbin","HEB"],"230200":["齐齐哈尔","Qiqihaer","QQHE"],"230300":
["鸡西","Jixi","JX"],"230400":["鹤岗","Hegang","HG"],"230500":["双鸭山","Shuangyashan","SYS"],"230600":["大
庆","Daqing","DQ"],"230700":["伊春","Yichun","YC"],"230800":["佳木斯","Jiamusi","JMS"],"230900":["七台
河","Qitaihe","QTH"],"231000":["牡丹江","Mudanjiang","MDJ"],"231100":["黑河","Heihe","HH"],"231200":["绥
化","Suihua","SH"],"232700":["大兴安岭","Daxinganling","DXAL"],"310000":["上海","Shanghai","SH"],"320000":["江
苏","Jiangsu","JS"],"320100":["南京","Nanjing","NJ"],"320200":["无锡","Wuxi","WX"],"320300":["徐
州","Xuzhou","XZ"],"320400":["常州","Changzhou","CZ"],"320500":["苏州","Suzhou","SZ"],"320600":["南
通","Nantong","NT"],"320700":["连云港","Lianyungang","LYG"],"320800":["淮安","Huaian","HA"],"320900":["盐
城","Yancheng","YC"],"321000":["扬州","Yangzhou","YZ"],"321100":["镇江","Zhenjiang","ZJ"],"321200":["泰
州","Taizhou","TZ"],"321300":["宿迁","Xiuqian","SQ"],"330000":["浙江","Zhejiang","ZJ"],"330100":["杭
州","Hangzhou","HZ"],"330200":["宁波","Ningbo","NB"],"330300":["温州","Wenzhou","WZ"],"330400":["嘉
兴","Jiaxing","JX"],"330500":["湖州","Huzhou","HZ"],"330600":["绍兴","Shaoxing","SX"],"330700":["金
华","Jinhua","JH"],"330800":["衢州","Quzhou","QZ"],"330900":["舟山","Zhoushan","ZS"],"331000":["台
州","Taizhou","TZ"],"331100":["丽水","Lishui","LS"],"340000":["安徽","Anhui","AH"],"340100":["合
肥","Hefei","HF"],"340200":["芜湖","Wuhu","WH"],"340300":["蚌埠","Bangbu","BB"],"340400":["淮
南","Huainan","HN"],"340500":["马鞍山","Maanshan","MAS"],"340600":["淮北","Huaibei","HB"],"340700":["铜
陵","Tongling","TL"],"340800":["安庆","Anqing","AQ"],"341000":["黄山","Huangshan","HS"],"341100":["滁
州","Chuzhou","CZ"],"341200":["阜阳","Fuyang","FY"],"341300":["宿州","Xiuzhou","SZ"],"341400":["巢湖
市","Chaohushi","CHS"],"341500":["六安","Liuan","LA"],"341600":["亳州","Bozhou","BZ"],"341700":["池
州","Chizhou","CZ"],"341800":["宣城","Xuancheng","XC"],"350000":["福建","Fujian","FJ"],"350100":["福
州","Fuzhou","FZ"],"350128":["平潭综合实验区","Pingtanzongheshiyanqu","PTZHSYQ"],"350200":["厦
门","Shamen","SM"],"350300":["莆田","Putian","PT"],"350400":["三明","Sanming","SM"],"350500":["泉
州","Quanzhou","QZ"],"350600":["漳州","Zhangzhou","ZZ"],"350700":["南平","Nanping","NP"],"350800":["龙
岩","Longyan","LY"],"350900":["宁德","Ningde","ND"],"360000":["江西","Jiangxi","JX"],"360100":["南
昌","Nanchang","NC"],"360200":["景德镇","Jingdezhen","JDZ"],"360300":["萍乡","Pingxiang","PX"],"360400":["九
江","Jiujiang","JJ"],"360500":["新余","Xinyu","XY"],"360600":["鹰潭","Yingtan","YT"],"360700":["赣
州","Ganzhou","GZ"],"360800":["吉安","Jian","JA"],"360900":["宜春","Yichun","YC"],"361000":["抚
州","Fuzhou","FZ"],"361100":["上饶","Shangrao","SR"],"361298":["赣江新区","Ganjiangxinqu","GJXQ"],"370000":["山
东","Shandong","SD"],"370100...
```

http://127.0.0.1:8000/xmjg/common/tool/cityselect/js/areadata.js

```
var strVarCity = '';
strVarCity += '<div class="aui_state_box"><div class="aui_state_box_bg"></div>';
strVarCity += '  <div class="aui_alert_zn aui_outer">';
strVarCity += '    <table class="aui_border" >';
strVarCity += '      <tbody>';
strVarCity += '        <tr>';
strVarCity += '          <td class="aui_c">';
strVarCity += '          <div class="aui_inner">';
strVarCity += '          <table class="aui_dialog">';
strVarCity += '          <tbody>';
strVarCity += '          <tr>';
strVarCity += '          <td class="aui_header" colspan="2" style="text-align: left;"><div
class="aui_titleBar">';
strVarCity += '          <div class="aui_title" style="cursor: move;" id="title-div-t">选择师市</div>';
strVarCity += '          <a href="javascript:;" class="aui_close" onclick="Close()">×</a>';
strVarCity += '          </div>';
strVarCity += '          </td>';
strVarCity += '          </tr>';
strVarCity += '          <tr>';
strVarCity += '          <tr>';
strVarCity += '          <td class="aui_icon" style="display: none;">';
strVarCity += '          <div class="aui_iconBg" style="background: transparent none repeat scroll 0% 0%;">
</div></td>';
strVarCity += '          <td class="aui_main" style="width: auto; height: auto;">';
strVarCity += '          <div class="aui_content" style="padding: 0px; position:relative">';
strVarCity += '          <div id="aui_content_div" style="width: 1000px; position:relative;">';
strVarCity += '          <div class="data-result"><em>最多选择 <strong class="ff-ss">2000</strong> 项</em>
</div>';
strVarCity += '          <div class="data-error" style="display: none;">最多只能选择 3 项</div>';
strVarCity += '          <div class="data-search" id="searchRun"><input class="run" name="searcharea"/><div
class="searchList run"></div></div>';
strVarCity += '          <div class="data-clear-select" id="clearSelect" style="display: none;"><a
class="clear-btn"  href="#"  onclick="removeAll_area()">清除</a></div>';
strVarCity += '          <div class="data-tabs">';
strVarCity += '          <ul>';
strVarCity += '          <li onclick="removenode_area(this)" data-selector="tab-all" class="active
js_SelectAllJyts" ><a href="javascript:;"><span class="ff-span">全部</span><em></em></a></li>';
strVarCity += '          </ul>';
strVarCity += '          </div>';
strVarCity += '          <div class="data-container data-container-city">';
strVarCity += '          </div>';
strVarCity += '          </div>';
strVarCity += '          </div>';
strVarCity += '          </div>';
strVarCity += '          </td>';
strVarCity += '          </tr>';
strVarCity += '          <tr>';
strVarCity += '          <td class="aui_footer" colspan="2">';
strVarCity += '          <div class="aui_buttons">';
strVarCity += '          <button class="aui-btn aui-btn-light" onclick="Close()" type="button">取消
</button>';
strVarCity += '          <button class="aui-btn aui-btn-light"  onclick="save_City()"  type="button">确定
</button>';
strVarCity += '          </div>';
strVarCity += '          </td>';
strVarCity += '          </tr>';
strVarCity += '          </tbody>';
strVarCity += '          </table>';
strVarCity += '          </div></td>';
strVarCity += '        </tr>';
strVarCity += '      </tbody>';
strVarCity += '    </table>';
strVarCity += '  </div>';
strVarCity += '</div>';

// 全局变量
var datatype        = "";
var dataCityinput   = null;
var saveCityCallBack =null;
var searchValue     = searchdata();
var maxSelectCnt=   0; //选择最多数 0 表示所有  如: data-max-select-cnt="5" 最多选择5个
var selectLevel    =""; //数据选择级别(cp:可选城市和省, province:选择省，其他任何值:选择城市)默认选择城市  如：data-
select-level="province" 选择省份
var canSelectCity="";
var wholeCountry="no"; //是否可选全国（什么都不选点确定 表示全国） 如: data-whole-country="yes" 什么都不选点确定 表示全
国
var _provinceCodeV=""; //data-province-code='350000'  //指定只能选择某个省份的城市，值为城市省编码
var _provinceNameV="";

var selectInfo = {  //单选 点击过程选择的数据
    province:"",
    provinceCode:"",
    city:"",
    cityCode:""
}

$(document).on('click', '.area-duoxuan', function () {
    appendCity(this, 'duoxuan');
});

$(document).on('click', '.area-danxuan', function () {
    appendCity(this, 'danxuan');
});

initPilotCity();
/**
 * 初始化试点城市
 */
function initPilotCity(){
    if(typeof ctx != "undefined" ? true : false){   //参数存在则获取试点城市
        $.ajax({
          type : "POST",
          url :ctx+"/analysis-info!getPilotCity.action",
          data:{},
          dataType : ...
```

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/dg-jdkh-main.js

```
var common_stages = "立项用地规划许可,工程建设许可,施工许可,竣工验收,并行推进".split(",");
var OLD_DATA_OBJ = null;
var heartBeatParams = {};
var checkDataFalg = 0; // 0:心跳未启动，1:心跳方法正在执行，2:正在等待下次心跳执行
var checkDataval = null;
var currDateStr = "";
var cityNameMap;
var pillar1 = '';
var scrollId = {}; //平均用时滚动id
var scrollData = '';//平均用时数据

/**
 * 页面初始化
 * @returns
 */

function doOnloadInit() {
    //显示加载动画
    $(".loading").show();
    provinceParam["mapProvince"]='china';
    provinceParam["mapName"]='china';
    provinceParam["districtType"]='province';
    //数据初始化
    dataInit();
    //返回按钮
    $("#back-btn").click(function () {
        //清空滚动旧值
         BYXZXMSOldVal = '-';
         QGYSLXMZSOldVal = '-';
         jdxmzsOldVal = '-';
         jdxmWrapValArr = ['-', '-', '-', '-', '-',"-"];

        //清空单机地图存的行政区域编码
        $("#choose_province_code").val('');

        //一张蓝图隐藏
        $(".js-yzltBtn").hide();
        //返回按钮隐藏
        $(this).css("display", "none");

        // 新增项目总数前五名：省排名、城市排名按钮显示，"新增项目总数前五名"样式靠左
        $("#XZXMSQWM").css("text-align","left");
        $("#XZXMSQWM-province").css("display","");
        $("#XZXMSQWM-city").css("display","");

        // 各城市项目逾期排名：省排名、城市排名按钮显示，"各城市项目逾期排名"样式靠左
        $("#GCSXMYQPM").css("text-align","left");
        $("#GCSXMYQPM-province").css("display","");
        $("#GCSXMYQPM-city").css("display","");
        //查询全国数据
        searchNationMap();
    });
    //全国已受理项目总数
    $("#qg_pro").click(function () {
        toProjectStageRankPage("8", "0");
    });
    // 办件总量
    $("#qg_pro_month").click(function () {
        toStageRankPage('12', '0');
    });
    commonFunction.doSaveFunctionLog({"functionUrl": window.location.href, "functionName": "监督检测-全国首
页"});
}
//查询按钮
function timeSearch() {
    if (provinceCode == "") {
        searchNationMap();
    } else {
        searchProviceMap();
    }
    BYXZXMSOldVal = '-';
    QGYSLXMZSOldVal = '-';
    jdxmzsOldVal = '-';
    jdxmWrapValArr = ['-', '-', '-', '-', '-',"-"];
}

/**
 * 省地图数据查询
 * @returns
 */
function searchProviceMap() {
    var startDateVal = getStartDate();
    var endDateVal = getEndDate();
    changeTitle(provinceParam["mapName"], endDateVal.substring(0, 4) + "年" + endDateVal.substring(5, 7) +
"月");//改变标题
    nationTotal("", provinceCode, startDateVal, endDateVal);
    loadData(provinceParam["mapProvince"], provinceParam["mapName"], provinceParam["districtType"],
startDateVal, endDateVal);
}

/**
 * 全国地图数据查询
 * @returns
 */
function searchNationMap() {
    var startDateVal = getStartDate();
    var endDateVal = getEndDate();
    provinceParam["mapProvince"]='china';
    provinceParam["mapName"]='china';
    provinceParam["districtType"]='province';
    nationTotal("", "", startDateVal, endDateVal);
    loadData('china', 'china', 'province', startDateVal, endDateVal);
    changeTitle("", endDateVal.substring(0, 4) + "年" + endDateVal.substring(5, 7) + "月");//改变标题
}

/**
 * 全国/省 数据查询
 * @param name
 * @param code
 * @param startDate
 * @param endDate
 * @returns
 */
function nationTotal(name, code, startDate, endDate) {
    if (code) {
        provinceCode = code;
        $("#XZXMSQWM-province").hide();
        $("#XZXMSQWM-city").hide();
        $("#GCSXMYQPM-province").hide();
        $("#GCSXMYQPM-city").hide();
    } else {
        provinceCode = "";
    }
    // stopHeartBeat();//todo 注释原有的心跳检测 待完成新的整合心跳逻辑
    // heartBeatParams = {name: name, province: code, beginDate: startDate, endDate: endDate};
    // $.ajax({
```

```
    //     url: ctx + '/xmjg-project-info!getProjectNationTotal.action',
    //     type: "get",
    //     data: heartBeatParams,
    //     dataType: "json",
    //     async: true,
    //     success: function (result) {
    //         debugger
    //         setData(result, false); //数据设置
    //     }
    // });

    getYslAndXzblxms(code, startDate, endDate);//全国已受理项目数 新增办件量 逾期项目数


/*    getSPPJSLCS(code, startDate, endDate);//审批平均受理次数（次）
    getGJDBLQK(code, startDate, endDate);//各阶段审批办理情况（个）
    getCityItemOverTimeSort(code, startDate, endDate);//各城市项目逾期率排名
    getJdzbxms(code, startDate, endDate);//各阶在办项目数(个）
    getJdbjs(code, startDate, endDate);//各阶办件数(个）*/

    //合并上述5个方法
    getMergeData(code, startDate, endDate);






    setMonthNewProjectTop5(code, startDate, endDate); //新增项目数前五名
    getPjysByTjjssj(code, startDate, endDate);//各阶段平均用时

    // getYqxms(code,startDate,endDate);//全国逾期项目数 TODO 页面待完成

     if (initHeartBeat) {//todo 注释原有的心跳检测 待完成新的整合心跳逻辑
         doHeartBeat(); //开启定时心条检测
     }
}

/**
 * 多项数据合并获取
 * 审批平均受理次数（次）、各阶段审批办理情况（个）、各城市项目逾期率排名、各阶在办项目数(个）、各阶办件数(个）
 * @param startDate
 * @param endDate
 */
function getMergeData(provinceCodeAA, startDate, endDate) {
    $.ajax({
        url: ctx + 'supervisionInspection/getMergeData.do',
        type: "get",
        data: {xzqhdm: provinceCodeAA, startDate: startDa...
```

http://127.0.0.1:8000/xmjg/region/vue.min.js

```
/*!
 * Vue.js v2.5.16
 * (c) 2014-2018 Evan You
 * Released under the MIT License.
 */
!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?module.exports=t():"function"==typeof
define&&define.amd?define(t):e.Vue=t()}(this,function(){"use strict";var y=Object.freeze({});function M(e)
{return null==e}function D(e){return null!=e}function S(e){return!0===e}function T(e){return"string"==typeof
e||"number"==typeof e||"symbol"==typeof e||"boolean"==typeof e}function P(e){return
null!==e&&"object"==typeof e}var r=Object.prototype.toString;function l(e){return"[object
Object]"===r.call(e)}function i(e){var t=parseFloat(String(e));return
0<=t&&Math.floor(t)===t&&isFinite(e)}function t(e){return null==e?"":"object"==typeof e?
JSON.stringify(e,null,2):String(e)}function F(e){var t=parseFloat(e);return isNaN(t)?e:t}function s(e,t)
{for(var n=Object.create(null),r=e.split(","),i=0;i<r.length;i++)n[r[i]]=!0;return t?function(e){return
n[e.toLowerCase()]}:function(e){return n[e]}}var c=s("slot,component",!0),u=s("key,ref,slot,slot-
scope,is");function f(e,t){if(e.length){var n=e.indexOf(t);if(-1<n)return e.splice(n,1)}}var
n=Object.prototype.hasOwnProperty;function p(e,t){return n.call(e,t)}function e(t){var
n=Object.create(null);return function(e){return n[e]||(n[e]=t(e))}}var o=/-(\w)/g,g=e(function(e){return
e.replace(o,function(e,t){return t?t.toUpperCase():""})}),d=e(function(e){return
e.charAt(0).toUpperCase()+e.slice(1)}),a=/\B([A-Z])/g,_=e(function(e){return e.replace(a,"-
$1").toLowerCase()});var v=Function.prototype.bind?function(e,t){return e.bind(t)}:function(n,r){function
```

```
e(e){var t=arguments.length;return t?1<t?n.apply(r,arguments):n.call(r,e):n.call(r)}return
e._length=n.length,e};function h(e,t){t=t||0;for(var n=e.length-t,r=new Array(n);n--;)r[n]=e[n+t];return
r}function m(e,t){for(var n in t)e[n]=t[n];return e}function b(e){for(var t=
{},n=0;n<e.length;n++)e[n]&&m(t,e[n]);return t}function $(e,t,n){}var O=function(e,t,n)
{return!1},w=function(e){return e};function C(t,n){if(t===n)return!0;var
e=P(t),r=P(n);if(!e||!r)return!e&&!r&&String(t)===String(n);try{var
i=Array.isArray(t),o=Array.isArray(n);if(i&&o)return t.length===n.length&&t.every(function(e,t){return
C(e,n[t])});if(i||o)return!1;var a=Object.keys(t),s=Object.keys(n);return
a.length===s.length&&a.every(function(e){return C(t[e],n[e])})}catch(e){return!1}}function x(e,t){for(var
n=0;n<e.length;n++)if(C(e[n],t))return n;return-1}function R(e){var t=!1;return function(){t||
(t=!0,e.apply(this,arguments))}}var E="data-server-rendered",k=["component","directive","filter"],A=
["beforeCreate","created","beforeMount","mounted","beforeUpdate","updated","beforeDestroy","destroyed","activ
ated","deactivated","errorCaptured"],j=
{optionMergeStrategies:Object.create(null),silent:!1,productionTip:!1,devtools:!1,performance:!1,errorHandler
:null,warnHandler:null,ignoredElements:
[],keyCodes:Object.create(null),isReservedTag:O,isReservedAttr:O,isUnknownElement:O,getTagNamespace:$,parsePl
atformTagName:w,mustUseProp:O,_lifecycleHooks:A};function N(e,t,n,r){Object.defineProperty(e,t,
{value:n,enumerable:!!r,writable:!0,configurable:!0})}var L=/[^\w.$]/;var
I,H="__proto__"in{},B="undefined"!=typeof window,U="undefined"!=typeof
WXEnvironment&&!!WXEnvironment.platform,V=U&&WXEnvironment.platform.toLowerCase(),z=B&&window.navigator.userA
gent.toLowerCase(),K=z&&/msie|trident/.test(z),J=z&&0<z.indexOf("msie 9.0"),q=z&&0<z.indexOf("edge/"),W=
(z&&z.indexOf("android"),z&&/iphone|ipad|ipod|ios/.test(z)||"ios"===V),G=(z&&/chrome\/\d+/.test(z),
{}.watch),Z=!1;if(B)try{var X={};Object.defineProperty(X,"passive",{get:function()
{Z=!0}}),window.addEventListener("test-passive",null,X)}catch(e){}var Y=function(){return void 0===I&&
(I=!B&&!U&&"undefined"!=typeof
global&&"server"===global.process.env.VUE_ENV),I},Q=B&&window.__VUE_DEVTOOLS_GLOBAL_HOOK__;function ee(e)
{return"function"==typeof e&&/native code/.test(e.toString())}var te,ne="undefined"!=typeof
Symbol&&ee(Symbol)&&"undefined"!=typeof Reflect&&ee(Reflect.ownKeys);te="undefined"!=typeof Set&&ee(Set)?
Set:function(){function e(){this.set=Object.create(null)}return e.prototype.has=function(e)
{return!0===this.set[e]},e.prototype.add=function(e){this.set[e]=!0},e.prototype.clear=function()
{this.set=Object.create(null)},e}();var re=$,ie=0,oe=function(){this.id=ie++,this.subs=
[]};oe.prototype.addSub=function(e){this.subs.push(e)},oe.prototype.removeSub=function(e)
{f(this.subs,e)},oe.prototype.depend=function()
{oe.target&&oe.target.addDep(this)},oe.prototype.notify=function(){for(var
e=this.subs.slice(),t=0,n=e.length;t<n;t++)e[t].update()},oe.target=null;var ae=[];function se(e)
{oe.target&&ae.push(oe.target),oe.target=e}function ce(){oe.target=ae.pop()}var le=function(e,t,n,r,i,o,a,s)
{this.tag=e,this.data=t,this.children=n,this.text=r,this.elm=i,this.ns=void
0,this.context=o,this.fnContext=void 0,this.fnOptions=void 0,this.fnScopeId=void
0,this.key=t&&t.key,this.componentOptions=a,this.componentInstance=void 0,this.parent=vo...
```

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/indexMap.js

```
var tjfs = "xmsl"; //地图统计切换
var projectManager=new Augur.ProjectManager();
var cityDataCache =projectManager.cityDataCache;
var myChart;
var date = new Date();
var dateStr = date.getFullYear() + "年" + (date.getMonth() + 1) + "月";
var provinceName = "";
var option;
var dataConfigSencondCity=null;
var visualMapShowOrClose = false;//色列显示控制 false：为不显示 true为显示
var visualMapFontSize = 15;//色列显示字体大小
var toolboxShow = false;//灯泡按钮 显示控制 false：为不显示 true为显示
var myBackBtnTitle ="开启";//灯泡提示 鼠标hover显示文字
var toolboxPosition="9%";//灯泡显示位置 默认设置为为大屏版本的8%
var toolboxIcon ='path://M512 841.142857C204.8 841.142857 21.942857 541.257143 14.628571 533.942857L0
512l14.628571-21.942857C21.942857 475.428571 204.8 182.857143 512 182.857143s490.057143 299.885714 497.371429
307.2l14.628571 21.942857-14.628571 21.942857c-7.314286 7.314286-190.171429 307.2-497.371429 307.2zM87.771429
512c43.885714 58.514286 197.485714 256 424.228571 256s380.342857-197.485714 424.228571-256c-43.885714-
58.514286-197.485714-256-424.228571-256S131.657143 453.485714 87.771429 512z,'+
    'path://M512 694.857143C409.6 694.857143 329.142857 614.4 329.142857 512S409.6 329.142857 512 329.142857
694.857143 409.6 694.857143 512 614.4 694.857143 512 694.857143z m0-292.571429c-58.514286 0-109.714286 51.2-
109.714286 109.714286S453.485714 621.714286 512 621.714286 621.714286 570.514286 621.714286 512 570.514286
402.285714 512 402.285714z';
var sjXzqhdm ="";//省级行政区划代码 用于切换展示时使用（ 默认为空，即展示全国 ）
var nameAbbr ="";

var app = new Vue({
    el: '#jdkh',
    data: {
        showone:false,
        showtwo:false,
        showthd:false,
        dateRangeValue: [],
        cloud_tit: '', //"已接入"标题
        dialogVisible:false,//通知弹窗
    },
    watch:{
        cloud_tit:function(newVal,oldVal){
          if ($("#indexMap-tit").text().indexOf("兵团") <-1){return;}
          if(newVal!=''){
          this.cloud_tit=newVal.replace('城市','师市');
          }
        }
    },
    methods:{
        confirmedInfo: function () {
          var _that = this;
          $.ajax({
          url: ctx + "/monitorEarlyWarning/earlyWarningRecord/noticeToConfirm.do",
          data: "",
          async: true,
          type : "get", // 数据发送方式
          dataType : "json", // 接受数据格式
          success : function(data) {
          if (data.length>0){
          _that.dialogVisible=true;
          }
          if(data){
          indexObjArr = new Array();
          _that.INDEXoptions = [];
          for (var i = 0; i < data.length ; i++) {
          var indexObj = new Object();
          indexObj.YJTSXX = data[i].YJTSXX;
          indexObjArr.push(indexObj);
          _that.dateRangeValue.push(data[i].YJTSXX);
          }

          }
          }
          });
        },

        allToConfirm: function(){
          var _that = this;
          $.ajax({
          url: ctx + "/monitorEarlyWarning/earlyWarningRecord/allToConfirm.do",
          async: false,
          type : "post", // 数据发送方式
          dataType : "json", // 接受数据格式
          error : function(result) {
          _that.$message({
          message: result.message ? result.message : '请求后台出错，请稍后重试',
          type: 'error'
          ,customClass:'zZindex'
          });
          },
          success : function(data) {
          debugger;
          if(data){
          _that.dialogEditTable1 = false;
          setTimeout(function () {
          _that.searchData();
          },500);
          _that.$message({
          type: 'success',
          message: '确认成功'
          ,customClass:'zZindex'
          });
          }else{
          _that.$message({
          type: 'error',
          message: data.msg?data.msg:"确认失败！"
          ,customClass: 'zZindex'
          });
          }
          }
          });
        },
        toWarningRecord: function (){
          var url = ctx + "monitorEarlyWarning/earlyWarningRecord/index.do?intoWay=1";
          commonWindow.toWindowForReturn(url);
        }


    },
    mounted:function(){
        this.confirmedInfo();
    }
})

/**
 * 数据初始化
 * @returns
 */
function dataInit(){
    //先初始化myChart
    myChart = echarts.init(document.getElementById('indexMap'));
    mapShowConfig();//地图标注控制显示全称还简称
    //判断用户行政区划信息用以加载对应数据
    getUserDistrict();
    initCitySelectPlugin();
    //地图单击事件
    myChar...
```

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/echarts.min.js

```
/*
* Licensed to the Apache Software Foundation (ASF) under one
* or more contributor license agreements.  See the NOTICE file
* distributed with this work for additional information
* regarding copyright ownership.  The ASF licenses this file
* to you under the Apache License, Version 2.0 (the
* "License"); you may not use this file except in compliance
* with the License.  You may obtain a copy of the License at
*
*   http://www.apache.org/licenses/LICENSE-2.0
*
* Unless required by applicable law or agreed to in writing,
* software distributed under the License is distributed on an
* "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY
* KIND, either express or implied.  See the License for the
* specific language governing permissions and limitations
* under the License.
*/


!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports):"function"==typeof
define&&define.amd?define(["exports"],e):e(t.echarts={})}(this,function(t){"use strict";function e(t,e)
{"createCanvas"===t&&(v_=null),g_[t]=e}function i(t){if(null==t||"object"!=typeof t)return t;var
e=t,n=l_.call(t);if("[object Array]"===n){if(!O(t)){e=[];for(var o=0,a=t.length;o<a;o++)e[o]=i(t[o])}}else
if(s_[n]){if(!O(t)){var r=t.constructor;if(t.constructor.from)e=r.from(t);else{e=new r(t.length);for(var
o=0,a=t.length;o<a;o++)e[o]=i(t[o])}}}else if(!r_[n]&&!O(t)&&!M(t)){e={};for(var s in t)t.hasOwnProperty(s)&&
(e[s]=i(t[s]))}return e}function n(t,e,o){if(!w(e)||!w(t))return o?i(e):t;for(var a in
e)if(e.hasOwnProperty(a)){var
r=t[a],s=e[a];!w(s)||!w(r)||y(s)||y(r)||M(s)||M(r)||b(s)||b(r)||O(s)||O(r)?!o&&a in t||
(t[a]=i(e[a],!0)):n(r,s,o)}return t}function o(t,e){for(var
i=t[0],o=1,a=t.length;o<a;o++)i=n(i,t[o],e);return i}function a(t,e){for(var i in e)e.hasOwnProperty(i)&&
(t[i]=e[i]);return t}function r(t,e,i){for(var n in e)e.hasOwnProperty(n)&&(i?null!=e[n]:null==t[n])&&
(t[n]=e[n]);return t}function s(){return v_||(v_=m_().getContext("2d")),v_}function l(t,e){if(t)
{if(t.indexOf)return t.indexOf(e);for(var i=0,n=t.length;i<n;i++)if(t[i]===e)return i}return-1}function
u(t,e){function i(){}var n=t.prototype;i.prototype=e.prototype,t.prototype=new i;for(var o in
n)t.prototype[o]=n[o];t.prototype.constructor=t,t.superClass=e}function h(t,e,i){r(t="prototype"in t?
t.prototype:t,e="prototype"in e?e.prototype:e,i)}function c(t){if(t)return"string"!=typeof
t&&"number"==typeof t.length}function d(t,e,i){if(t&&e)if(t.forEach&&t.forEach===h_)t.forEach(e,i);else
if(t.length===+t.length)for(var n=0,o=t.length;n<o;n++)e.call(i,t[n],n,t);else for(var a in
t)t.hasOwnProperty(a)&&e.call(i,t[a],a,t)}function f(t,e,i){if(t&&e){if(t.map&&t.map===f_)return
t.map(e,i);for(var n=[],o=0,a=t.length;o<a;o++)n.push(e.call(i,t[o],o,t));return n}}function p(t,e,i,n)
{if(t&&e){if(t.reduce&&t.reduce===p_)return t.reduce(e,i,n);for(var
o=0,a=t.length;o<a;o++)i=e.call(n,i,t[o],o,t);return i}}function g(t,e,i){if(t&&e)
{if(t.filter&&t.filter===c_)return t.filter(e,i);for(var n=
[],o=0,a=t.length;o<a;o++)e.call(i,t[o],o,t)&&n.push(t[o]);return n}}function m(t,e){var
```

```
i=d_.call(arguments,2);return function(){return t.apply(e,i.concat(d_.call(arguments)))}}function v(t){var
e=d_.call(arguments,1);return function(){return t.apply(this,e.concat(d_.call(arguments)))}}function y(t)
{return"[object Array]"===l_.call(t)}function x(t){return"function"==typeof t}function _(t){return"[object
String]"===l_.call(t)}function w(t){var e=typeof t;return"function"===e||!!t&&"object"==e}function b(t)
{return!!r_[l_.call(t)]}function S(t){return!!s_[l_.call(t)]}function M(t){return"object"==typeof
t&&"number"==typeof t.nodeType&&"object"==typeof t.ownerDocument}function I(t){return t!==t}function T(t)
{for(var e=0,i=arguments.length;e<i;e++)if(null!=arguments[e])return arguments[e]}function D(t,e){return
null!=t?t:e}function A(t,e,i){return null!=t?t:null!=e?e:i}function C(){return
Function.call.apply(d_,arguments)}function L(t){if("number"==typeof t)return[t,t,t,t];var e=t.length;return
2===e?[t[0],t[1],t[0],t[1]]:3===e?[t[0],t[1],t[2],t[1]]:t}function k(t,e){if(!t)throw new Error(e)}function
P(t){return null==t?null:"function"==typeof t.trim?t.trim():t.replace(/^[\s\uFEFF\xA0]+|
[\s\uFEFF\xA0]+$/g,"")}function N(t){t[y_]=!0}function O(t){return t[y_]}function E(t){function e(t,e){i?
n.set(t,e):n.set(e,t)}var i=y(t),n=this;t instanceof E?t.each(e):t&&d(t,e)}function R(t){return new
E(t)}function z(t,e){for(var i=new t.constructor(t.length+e.length),n=0;n<t.length;n++)i[n]=t[n];var
o=t.length;for(n=0;n<e.length;n++)i[n+o]=e[n];return i}function B(){}function V(t,e){var i=new __(2);return
null==t&&(t=0),null==e&&(e=0),i[0]=t,i[1]=e,i}function G(t,e){return t[0]=e[0],t[1]=e[1],t}function W(t){var
e=new __(2);return e[0]=t[0],e[1]=t[1],e}function F(t,e,i){return t[0]=e,t[1]=i,t}function H(t,e,i){return
t[0]=e[0]+i[0],t[1]=e[1]+i[1],t}function Z(t,e,i,n){return t[0]=e[0]+i[0]*n,t[1]=e[1]+i[1]*n,t}function
U(t,e,i){return t[0]=e[0]-i[0],t[1]=e[1]-i[1],t}function X(t){return...
```

http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do

```
var ctx='/xmjg/';var bigScreenFolder="";var tjkssj="2020-01-01";var tjjssj="2020-12-29";var dateEnd = "2020-
12-29";var provinceCode="660000";var dataType="8";  //1:各城市各阶段平均用时（审批用时）; 2:各城市各阶段跨度用时; 3:各
城市各阶段最长用时; 4:各城市各阶段平均受理次数;5:本月新增项目数var stageType="0"; //0: 总数, 1: 立项用地规划许可; 2: 工程建
设许可; 3: 施工许可; 4: 竣工验收var splclx="";var splcmc="";var sfType="";//算法类型
```

http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do

```
    var isWhite = '';    var screen = (isWhite=="white"?3:0);    function initWhite(){        $.ajax({
type: "POST",          url: ctx+ '/xmjg/xmjg-project-info!getScreen.action?',          dataType: "json",
async:false,          success: function (result) {          screen = result;          if("3"==result){
var doc=document;          var link=doc.createElement("link");          link.setAttribute("rel",
"stylesheet");          link.setAttribute("type", "text/css");          link.setAttribute("href",
ctx+"/xmjg/css/white/common_new.css");          var heads = doc.getElementsByTagName("head");
if(heads.length)          heads[0].appendChild(link);          else
doc.documentElement.appendChild(link);          }          }        });    }
```

http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do

```
$(function(){doInit();          $("#goBackBtn").click(function () {
commonWindow.returnParentWindow();          });          $("#goBackProvinceBtn").click(function () {
//todo 返回按钮要重新请求 待优化返回逻辑          getAnalysisCityStageSlcsRankingData(null,"");          });
});
```

http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do

```
toStageProjectListPage(dataType,0,provinceCode,'','')
```

http://127.0.0.1:8000/xmjg/common/tool/projectManager.js

```
var Augur = Augur || {};
Augur.ProjectManager = function () {
    /**
     * 创建存储缓存的帮助器
     */
    this.cityDataCache=new Augur.Xmjg.CityDataCache();
}
```

http://127.0.0.1:8000/xmjg/common/tool/common-core.js

```
/**
 *
 */


var Augur = Augur || {}
Augur.Xmjg = Augur.Xmjg || {}
Augur.Xmjg.CityDataCache = function () {
    this.mapDataCache = {};
    this.storeMapDataCache = function (name, data) {
        this.mapDataCache[name] = data;
    };
    this.getMapDataCache = function (name) {
        return this.mapDataCache[name];
    }
}
Augur.CookieHelper = {
    setCookie: function (cookieKey, cookieValue) {
        var cookieArr = {};
        cookieArr[cookieKey] = cookieValue;
        this._saveCookieArr(cookieArr);
    },
    getCookie: function (key) {
        var keyValues = document.cookie.split(";");
        var keyValueDir = [];
        for (var i = 0; i < keyValues.length; i++) {
          var keyIndex = keyValues[i].indexOf('=');
          var name = keyValues[i].substr(0, keyIndex).trim();
          if (key === name)
          return keyValues[i].substr(keyIndex + 1);
        }
        return "";
    },
    getCookieAsBoolean: function (key, defaultValue) {
        if (defaultValue == undefined)
          defaultValue = false;
        var result = this.getCookie(key);
        if (result == "" || result == null)
          return defaultValue;
        if (result == "false" || result == "0")
          return false;
        if (result == "true" || result == "1")
          return true;
        return result;
    },
    saveBackground: function (scene, param) {
        scene = scene || "background";
        var cookieArr = {};
        cookieArr[scene] = param;
        this._saveCookieArr(cookieArr);
    },
    getBackground: function (scene) {
        scene = scene || "background";
        return this.getCookie(scene);
    },
    _saveCookieArr: function (keyValueDir) {
        var str = "";
        for (var name in keyValueDir) {
          str += name + "=" + keyValueDir[name] + ";";
        }
        var exdate = new Date();
        exdate.setDate(exdate.getDate() + 30);
        document.cookie = str + "expires=" + exdate.toGMTString();
    },
    _getCookieArr: function () {
        var keyValues = document.cookie.split(";");
        var keyValueDir = {};
        for (var i = 0; i < keyValues.length; i++) {
          if (keyValues[i].length < 1)
          continue;
          var keyIndex = keyValues[i].indexOf('=');
          var name = keyValues[i].substr(0, keyIndex).trim();
          var value = keyValues[i].substr(keyIndex + 1).trim();
          keyValueDir[name] = value;
        }
        return keyValueDir;
    }
};
/**
 *  需要引用
 * <script type="text/javascript" src="js/libs/jquery-3.1.0.min.js"></script>
 */
Augur.AjaxGetter = {
    getHtmlSegment: function (url, successCallback, failCallback, params) {
        var isJsp = Augur.UrlHelper.isJspUrl(url);
        var dataTypeValue = isJsp ? "JSONP" : "text";
        url = Augur.UrlHelper.getFilterredUrl(url);

        $.ajax({
          type: 'GET',
          scriptCharset: 'utf-8',
          url: url,
          data: null,
          dataType: dataTypeValue,
          processData: false,
          contentType: false,
          sender: this,
          success: function (args1) {
          successCallback(args1, url, params);
          },
          error: function (XMLHttpRequest, textStatus, errorThrown) {
          console.log("getHtmlSegment loadPage error");
          if (failCallback)
          failCallback(XMLHttpRequest, textStatus, errorThrown, params);
          else
          this.sender.defaultFailCallback(url, XMLHttpRequest, textStatus, errorThrown);
          }
        });
    },
    getHtmlSegmentByPost: function (url, data, successCallback, failCallback, params) {
        var isJsp = Augur.UrlHelper.isJspUrl(url);
        var dataTypeValue = isJsp ? "JSONP" : "text";
        url = Augur.UrlHelper.getFilterredUrl(url);

        $.ajax({
          type: 'POST',
          url: url,
          data: data,
          processData: true,
          contentType: false,
          sender: this,
          contentType: 'application/x-www-form-urlencoded',
          success: function (args1) {
          successCallback(args1, params);
          },
          error: function (XMLHttpRequest, textStatus, errorThrown) {
          console.log("getHtmlSegment loadPage error");
          if (failCallback)
          failCallback(XMLHttpRequest, textStatus, errorThrown);
          else
          this.sender.defaultFailCallback(url, XMLHttpRequest, textStatus, errorThrown);
          }
        });
    },
    defaultFailCallback: function (url, XMLHttpRequest, textStatus, errorThrown) {
        console.warn("无法访问 " + url, XMLHttpRequest, textStatus, errorThrown)
    },
    loadHtmlSegments: function (domElements) {
        var items = domElements;
        ...
```

http://127.0.0.1:8000/xmjg/common/tool/common.js

```
/**
 * 外部js调用
 */
var commonWindow = {
    //打开页面
    toWindowForReturn: function (url, pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
//          pageObj.commonWindowAction.doWindowForReturn(encodeURI(url));
                 console.log(encodeURI(url))
          pageObj.commonWindowAction.doWindowForReturn(encodeURI(url));
        }
    },


    //打开页面  不支持返回
    toWindowNotReturn: function (url, pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
          pageObj.commonWindowAction.doWindowNotReturn(url);
        }
    },

    //返回上一页面
    returnParentWindow: function (pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
          pageObj.commonWindowAction.doReturnParentWindow();
        }
    },
    //跳转到对应页面(传入的url与之前的iframe地址一致的时候 退回到对应iframe,如果不存在 则调用toWindowForReturn)
    jumpWindowForIframe: function (url, pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
          pageObj.commonWindowAction.doJumpWindowForIframe(url);
        }
    },
    //获取对应的页面  pageFlag (max-top-page：最顶级页面;)
    getWindowObj: function (pageFlag) {
        if (!pageFlag) {
          pageFlag = "max-top-page";
        }
        var obj = window.self;
        var whileFlag = true;
        while (whileFlag) {

          if (obj.document.getElementById("page-level-flag-in")) {
          //最顶级页面
          if (obj.document.getElementById("page-level-flag-in").value == pageFlag) {
          return obj;
          }
          }
          if (whileFlag) {
          if (obj.window.parent != obj.window) {
          obj = obj.window.parent;
          } else {
          whileFlag = false;
          }
          }
        }
        return window.self;
    },
};

//=============================================================================================================
=================

var commonWindowAction = {
    doWindowForReturn: function (url) {
        var maxDataIndex = 0;
        var $lastIframe;
        $(".content-url-iframe").each(function () {
          var thisDataIndex = parseInt($(this).attr("data-index"));
          if (maxDataIndex < thisDataIndex) {
```

```
          maxDataIndex = thisDataIndex;
          }
          if (maxDataIndex == thisDataIndex) {
          $lastIframe = $(this);
          }
          commonWindowAction.doRemoveClass($(this), "curr-url-iframe");
        });
        if ($lastIframe) {
          var timestamp = (new Date()).valueOf();
          var key = "contentZframe-id-" + timestamp + "-" + (maxDataIndex + 1);
          $lastIframe.after("<iframe allowfullscreen  id=\"" + key + "\" width=\"100%\" height=\"100%\" 
src=\"\" frameborder=\"0\" class=\"content-url-iframe  curr-url-iframe\" data-index=\"" + (maxDataIndex + 1) 
+ "\"></iframe>");
          $("#" + key).attr("src", url);
        }
        console.log(url)
        commonWindowAction.removeIframeOrHide(true);

    },
    doWindowNotReturn: function (url) {
        $(".content-url-iframe").each(function () {
                if($(this).hasClass("curr-url-iframe")){
                        if(url.indexOf("?")<=-1){
                                url+="?";
                        }else{
                                url+="&";
                        }
                        url+="notHaveReturnFlag=yes";
                        $(this).attr("src", url);
                        $(this).attr("id","contentZframe");
                        $(this).attr("data-index","0");
                }else{
          commonWindowAction.doRemoveClass($(this), "curr-url-iframe");
          }
        });
        commonWindowAction.removeIframeOrHide(false);
    },
    //执行返回上一页
    doReturnParentWindow: function () {
        var $lastIframe;
        var maxDataIndex = 0;

        $(".curr-url-iframe").each(function (i) {
          if (i == 0) {
          if ($(this).attr("data-index") == "0") {
          return;
          }
          maxDataIndex = parseInt($(this).attr("data-index")) - 1;
          $lastIframe = $(this);
          }
        })
        $(".content-url-iframe").each(function () {
         if ($lastIframe.attr("src") == $(this).attr("src")) {
           maxDataIndex = parseInt($(this).attr("data-index")) - 1;
           return false;
         }
        });
        if (maxDataIndex <= 0) {
          maxDataIndex = 0;
          $(".content-url-iframe").each(function () {
          var thisDataIndex = parseInt($(this).attr("data-index"));
          if (maxDataIndex == thisDataIndex) {
          $(this).show();
          commonWindowAction.doAddClass($(this), "curr-url-iframe");
          } else {
          commonWindowAction.doRemoveClass($(this), "curr-url-iframe");
          }
  ...
```

http://127.0.0.1:8000/xmjg/common/tool/date/js/bootstrap-datepicker.zh-CN.min.js

```
!function(a){a.fn.datepicker.dates["zh-CN"]={days:["星期日","星期一","星期二","星期三","星期四","星期五","星期
六"],daysShort:["周日","周一","周二","周三","周四","周五","周六"],daysMin:
```

```
["日","一","二","三","四","五","六"],months:["一月","二月","三月","四月","五月","六月","七月","八月","九月","十月","十一月","十二月"],monthsShort:["1月","2月","3月","4月","5月","6月","7月","8月","9月","10月","11月","12月"],today:"今日",clear:"清除",format:"yyyy年mm月dd日",titleFormat:"yyyy年mm月",weekStart:1}}(jQuery);
```

http://127.0.0.1:8000/xmjg/common/tool/date/js/dateQuery.js

```
var strVarDate = '';
strVarDate += '<div class="aui_state_box_date"><div class="aui_state_box_bg_date"></div>';
strVarDate += '  <div class="aui_alert_zn_date aui_outer_date">';
strVarDate += '    <table class="aui_border_date" style="border:2px solid #fff;">';
strVarDate += '      <tbody>';
strVarDate += '        <tr>';
strVarDate += '          <td>';
strVarDate += '          <div class="aui_inner_date">';
strVarDate += '          <table class="aui_dialog_date">';
strVarDate += '          <tbody>';
strVarDate += '          <tr>';
strVarDate += '          <td class="aui_header_date" colspan="2"><div class="aui_titleBar_date">';
strVarDate += '          <div class="aui_title_date" style="cursor: move;">时间选择</div>';
strVarDate += '          <a href="javascript:;" class="aui_close_date" onclick="date_cancel()">×</a>';
strVarDate += '          </div>';
strVarDate += '          </td>';
strVarDate += '          <td>';
strVarDate += '          </td>';
strVarDate += '          </tr>';
strVarDate += '          <tr>';
strVarDate += '          <td colspan="2">';
strVarDate += '                 <table>';
strVarDate += '                         <tr>';
strVarDate += '                                 <td >';/*style="width:100px;margin-left:5px;"*/
strVarDate += '                                         <select id="selectId"
onchange="date_selectChange()">';
strVarDate += '                                                 <option value ="1">按天</option>';
strVarDate += '                                                 <option value ="2" selected = "selected" >按
月</option>';
strVarDate += '                                                 <option value="3">按年</option>';
strVarDate += '                                         </select>';
strVarDate += '                                 </td>';
strVarDate += '                                 <td><input type="text" class="form-control selectData"
id="date_dateStart" name="date_dateStart"  /></td>';/* style="width:130px;"*/
strVarDate += '                                 <td class="end-tt">一</td>';
strVarDate += '                                 <td class="end-tt" ><input type="text" class="form-control
selectData" id="date_dateEnd" name="date_dateEnd" /></td>';/*style="width:130px;"*/
strVarDate += '                                 <td ></td>';/*style="width:100px;margin-left:5px;"*/
strVarDate += '                         </tr>';
strVarDate += '                 </table>';
strVarDate += '          </td>';
strVarDate += '          </tr>';
strVarDate += '          <tr>';
strVarDate += '          <td class="aui_footer_date" colspan="2">';
strVarDate += '          <div class="aui_buttons_date">';
strVarDate += '                 <button class="aui-btn_date aui-btn-light_date" onclick="date_cancel()"
type="button">取消</button>';
strVarDate += '                 <button class="aui-btn_date aui-btn-light_date" onclick="date_submit()"
type="button">确定</button>';
strVarDate += '          </div>';
strVarDate += '          </td>';
strVarDate += '          <td>';
strVarDate += '          </td>';
strVarDate += '          </tr>';
strVarDate += '          </tbody>';
strVarDate += '          </table>';
strVarDate += '          </div></td>';
strVarDate += '        </tr>';
strVarDate += '      </tbody>';
strVarDate += '    </table>';
strVarDate += '  </div>';
strVarDate += '</div>';

var dataSubmitFunction=null; //时间选择确定回调方法

//确定函数
function date_submit(){
 if(dataSubmitFunction!=null){
         dataSubmitFunction($('#date_dateStart').val(),$('#date_dateEnd').val());
        }
 date_cancel();
}
//取消函数
function date_cancel(){
 $(".aui_state_box_date").remove();
}
//点击控件按钮显示
function date_showDateSelect(submitFunction){
 if(submitFunction){
         dataSubmitFunction=submitFunction;
        }
 $('body').append(strVarDate);
 date_selectChange();
}

var monthEndDate = '';

/**
 * 点击控件按钮显示
 * @param dateFlag
 * @param startDate
 * @param endDate
 * @param submitFunction
 * @param nds
 * @param endDateStr 日历能选择的截止日期
 * @returns
 */
function date_showDateSelect1(dateFlag,startDate,endDate,submitFunction,nds,endDateStr){
 if(submitFunction){
         dataSubmitFunction=submitFunction;
        }
 $('body').append(strVarDate);
 if(dateFlag){
         date_selectChange(dateFlag,startDate,endDate,nds,endDateStr);
 }else{
         date_selectChange(null,startDate,endDate);
        }

    if(endDateStr){ //日历能选的最后日期
        monthEndDate = endDateStr.substr(0,7);
    }
}

//时间控件开始
$.fn.datepicker.dates['day'] = { //切换为中文显示
 days : [ "       周日", "周一", "周二", "周三", "周四", "周五", "周六", "周日" ],
 daysShort : [ "       日", "一", "二", "三", "四", "五", "六", "七" ],
 daysMin : [ "       日", "一", "二", "三", "四", "五", "六", "七" ],
 months : [ "       一月", "二月", "三月", "四月", "五月", "六月", "七月", "八月", "九月",
                        "十月", "十一月", "十二月" ],
 monthsShort : [ "       一月", "二月", "三月", "四月", "五月", "六月", "七月", "八月",
                        "九月", "十月", "十一", "十二" ],
 today : "       今天",
 clear : "       清除"
};
$.fn....
```

http://127.0.0.1:8000/xmjg/xmjg/xndc/js/common-charts.js

```
var cityCode;
/**
 * 加载柱状图 <多个柱子>
 * @param chartsParams{
 *   objId     <必须>
 *   legendData x主标数据分组 <必须>
 *   xAxisData  x坐标数据  <必须>
 *   seriesDatas y坐标数据  <必须>
 *   colorData  柱子颜色
 *   provideNumber  x坐标 文字一行长度
 *   ...
 * }
 * @param onclickFunction 点击方法
 * @returns
 */
function doBarCharts(chartsParams,onclickFunction){
 var legendData=chartsParams.legendData;
 var xAxisData=chartsParams.xAxisData;
 var seriesDatas=chartsParams.seriesDatas;
 var objId=chartsParams.objId;
 var seriesObj=[],zearVall=[];
 var barWidth="20%";
 var xAxisFontSize=14;
 var barFontSize = 12;
 var legendFontSize=15;
 var gridBbottom="5%";
 var tooltipFontSize=18;
 var color = "#fff";
 if(screen == "3"){
        color="#545C6A";
        }
/*      if(getBigScreen()=="bigscreen"){
          barWidth="20%";
          xAxisFontSize=24;
          legendFontSize=24;
          gridBbottom="10%";
 }*/
 if(getBigScreen()=="bigscreen" || bigScreenFolder == 'bigscreenTwo/'){
          barWidth="15%";
          xAxisFontSize=24;
          barFontSize=24;
          legendFontSize=24;
          gridBbottom="2%";
        }
 if(chartsParams.barWidth){
         barWidth=chartsParams.barWidth;
        }
 if(chartsParams.xAxisFontSize){
         xAxisFontSize=chartsParams.xAxisFontSize;
        }
 var vall=null;
 for(var i=0;i<legendData.length;i++){
         zearVall.push(0);
        }
 for(var i=0;i<seriesDatas.length;i++){
         if(seriesDatas==null || seriesDatas.length<=i-1 || seriesDatas[i]==undefined ||
seriesDatas[i]==null){
                 vall=zearVall;
         }else{
                 vall=seriesDatas[i];
                }
         seriesObj.push({name: legendData[i],type: 'bar',data: vall,barWidth: barWidth,
                 label: {normal: {
                                 show: true,
          rotate: 90,
          align: 'left',
          verticalAlign: 'middle',
                                 position:  "insideTop",//'top',*/
                                 textStyle: {color: color, fontSize: barFontSize}
                 }}});
        }
 var provideNumber=8;
 if(chartsParams.provideNumber){
         provideNumber=chartsParams.provideNumber;
        }
 var colorData=[];
 if(!chartsParams.colorData  || chartsParams.colorData.length<=0){
         if(legendData.length==1){
                 colorData=['#5d91dd'];
         }else if(legendData.length==2){
                 colorData=['#5d91dd','#6bc0d5'];
         }else if(legendData.length==3){
                 colorData=['#5d91dd','#6bc0d5','#9d66e8'];
         }else if(legendData.length==4){
                 colorData=['#5d91dd','#6bc0d5','#9d66e8','#ff6b6b'];
                }
 }else{
         colorData=chartsParams.colorData;
        }
```

```
    var pillar1 = echarts.init(document.getElementById(objId));
    var option = {
        color: colorData,
        tooltip : {
            trigger: 'axis',
            textStyle: {
             fontSize: tooltipFontSize
            },
            axisPointer : {          //        坐标轴指示器，坐标轴触发有效
              type : 'shadow'        //        默认为直线，可选为：'line' | 'shadow'
            }
        },
           legend: {
                   top: '2%',
            data: legendData,
            textStyle: {
              color: "#abcaf3",
              fontSize: legendFontSize
            },
            itemWidth: 18,
            itemHeight: 18,
            itemGap: 30
        },
        grid: {top: '15%',left: '4%', right: '4%',bottom: gridBbottom,containLabel: true},
        xAxis : [
            {
              type : 'category',
              data : xAxisData,
              axisTick: {
              show: false
              },
              splitLine: {
                      show: false
                     },
              axisLabel: {
                      textStyle: {
                      fontSize: xAxisFontSize,
                      color:color
                      },
                      formatter:function(params) {
             var newParamsName = "";
             var paramsNameNumber = params.length;
             var rowNumber = Math.ceil(paramsNameNumber / provideNumber);
             if (paramsNameNumber > provideNumber) {
             for (var p = 0; p < rowNumber; p++) {
             var tempStr = "";
             var start = p * provideNumber;
             var end = start + provideNumber;
             if (p == rowNumber - 1) {
             tempStr = params.substring(start, paramsNameNumber);
             } else {
             tempStr = params.substring(start, end) + "\n";
             }
             newParamsName += tempStr;
             }

             } else {
             newParamsName = params;
             }
             return newParamsName
             }
                    },
                    axisLine: {
                      lineStyle: {
                      color: '#336bbd',
                      width: '1'
                      }
                     }
            }
        ],
        yAxis : [
            {
              type : 'value',
              min: 0,
        ...
```

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/analysis-ranking-stage.js

```
/**
 *
 */
var cityObj={};
var dataObj;
var pageSize=27,pageNo=0;
var _ObjId="";
var xzqhdmss="";
var listStrCc="";
var dataDesc="";
var dw = "";
var dateTabTit = "";
var nowDate = new Date();
var selectTypeName="";
function doInit(){
    if(dataType=="6"){
        $("#stage-tab-tit-ttta").prepend('<select name="tjTypeVal" id="tjTypeVal"  class="analy-select"
onchange="getAnalysisCityStageSlcsRankingData(null,this.options[this.selectedIndex].text)">'+
          '<option value="1">已退件</option>'+
          '<option value="2">不予受理</option>'+
          '<option value="3">退件（已退件+不予受理）</option>'+
          '</select>');
    }else if(dataType=="7"){
        $("#stage-tab-tit-ttta").prepend('<select name="qtTypeVal" id="qtTypeVal"  class="analy-select"
onchange="getAnalysisCityStageSlcsRankingData(null,this.options[this.selectedIndex].text)">'+
          '<option value="0">其它</option>'+
          '<option value="1">补正</option>'+
          //'<option value="2">挂起</option>'+      //新版没有这两个字段,先注释掉
          '<option value="3">特别程序</option>'+
          //'<option value="4">过程补正</option>'+
          '</select>');
    }

 $('.div-arrow-left').click(function(){
         pageNo--;
         setData();
 });
 $('.div-arrow-right').click(function(){
         pageNo++;
         setData();
 });
 goToQgProjectListBtn();
 getAnalysisCityStageSlcsRankingData(null,"");
 if(dataDesc!=""){
         commonFunction.doSaveFunctionLog({"functionUrl":window.location.href,"functionName":"       监督检查-
"+dataDesc});
 }else{
         commonFunction.doSaveFunctionLog({"functionUrl":window.location.href,"functionName":"       监督检查-
项目排名页"});
        }
}

function goToQgProjectListBtn(){
    var btnTitle = "兵团";
    if(null != provinceCode && ''!=$.trim(provinceCode)){
        if("110000"==provinceCode || "120000"==provinceCode || "310000"==provinceCode ||
"500000"==provinceCode){
          btnTitle = "全市";
        }else{
          btnTitle = "兵团";
        }
    }
    if(8==dataType){
        $("#goQgxm").html("<i></i>查看"+btnTitle+"项目列表");
    }else if(12==dataType){
        $("#goQgbj").html("<i></i>查看"+btnTitle+"办件列表");
    }
}

/**
 * 各城市各阶段数据
 * @returns
 */
```

```
function getAnalysisCityStageSlcsRankingData(xzqhdm,selectType){
    var splcmcAlia = "";
    var dateEnds=dateEnd.split("-");
    $("#endDate").html(dateEnds[0]+"年"+dateEnds[1]+"月"+dateEnds[2]+"日");
    var startDays=tjkssj.split("-");
    $("#sDate").html(startDays[0]+"年"+startDays[1]+"月"+startDays[2]+"日");
    var showStageTitle = xzqhdm==null?((provinceCode && provinceCode!="")?'各师市':'各省'):"各师市";
    var showCityName = xzqhdm==null?((provinceCode && provinceCode!="")?'师市':'省份'):"师市";
    if(splcmc){
        splcmcAlia =showStageTitle+splcmc;
    }
    if(stageType=="0"){
        dataDesc=""+splcmcAlia;
    }else if(stageType=="1"){
       dataDesc=showStageTitle+"立项用地规划许可阶段";
    }else if(stageType=="2"){
        dataDesc=showStageTitle+"工程建设许可阶段";
    }else if(stageType=="3"){
        dataDesc=showStageTitle+"施工许可阶段";
    }else if(stageType=="4"){
        dataDesc=showStageTitle+"竣工验收阶段";
    }else if(stageType=="5"){
        dataDesc=showStageTitle+"并行推进阶段";
    }

    if(dataType=="1"){
        var showTitle = xzqhdm==null?((provinceCode && provinceCode!="")?'各师市审批平均用时排名':'各省审批平均用时
排名'):'各师市审批平均用时排名';
        dataDesc+=dataDesc==""?showTitle:"审批平均用时排名";
        dateTabTit="审批平均用时";
        $("#dw").html("工作日");
    }else if(dataType=="2"){
        var showTitle = xzqhdm==null?((provinceCode && provinceCode!="")?'各师市跨度平均用时排名':'各省跨度平均用时
排名'):'各师市跨度平均用时排名';
        dataDesc+=dataDesc==""?showTitle:"跨度平均用时排名";
        dateTabTit="跨度平均用时";
        $("#dw").html("自然日");
    }else if(dataType=="3"){
        var showTitle = xzqhdm==null?((provinceCode && provinceCode!="")?'各师市最长用时排名':'各省最长用时排
名'):'各师市最长用时排名';
        dataDesc+=dataDesc==""?showTitle:"最长用时排名";
        dateTabTit="最长用时";
        $("#dw").html("工作日");
    }else if(dataType=="4"){
        var showTitle = xzqhdm==null?((provinceCode && provinceCode!="")?'各师市审批平均受理次数排名':'各省审批平均
受理次数排名'):'各师市审批平均受理次数排名';
        dataDesc+=dataDesc==""?showTitle:"审批平均受理次数排名";
        dateTabTit="平均受理次数";
        $("#dw").html("次");
    }else if(dataType=="5"){
        dataDesc = xzqhdm==null?((provinceCode && provinceCode!="")?'各师市新增项目数排名':'各省新增项目数排
名'):'各师市新增项目数排名';
        dateTabTit="新增项目数";
        $("#dw").html("个");
        $("#sDate").html(startDays[0]+"年"+startDays[1]+"月"+startDays[2]+"日");
        tjkssj= startDays[0]+"-"+startDays[1]+"-"+startDays[2];
    }else if(dataType=="6"){
        selectTypeName ="已退件";
        if(selectType !=""){
          selectTypeName = selectType;
                }
        dataDesc = xzqhdm==null?((provinceCode && provinceCode!="")?'各师市'+selectTypeName+'办件数量排名':'各
省'+selectTypeName+'办件数量排名'):'各师市'+selectTypeName+'办件数量排名';
        dateTabTit=selectTypeName+"办件数量(个)";
        $("#dw").html("个");
    }else if(dataType=="7"){
        selectTypeNam...
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
          var ctx='/xmjg/';var bigScreenFolder="";var xzqhdms="";var tjkssj="2020-01-01";var tjjssj="2020-12-
29";var orderByFlag="";var dataType="8";var sfzb="";var sfbyxz="";var sfjgqqxt="";var spjd="";var blqk="";var
splclx="";var splcmc="";var sfyq="";var tjTypeVal="";var qtTypeVal = "";var splcbm="";var dateEnd = "2020-12-
```

```
29";var provinceCode="";var dataType="8";  //1:各阶段平均用时（审批用时）; 2:各阶段跨度用时; 3:各阶段最长用时; 4:各阶段
平均受理次数;var stageType="0"; //0：总数，1：立项用地规划许可；2：工程建设许可；3：施工许可；4：竣工验收          var
oldStartDate = "2020-01-01";          var oldEndDate = "2020-12-29";          var flag="1";          var
xzqhdm="660000"; //跳转带过来的行政区划代码 用于钻取标题显示          var name="";//跳转带过来的城市名称 用于钻取标题显示
var sfType = "";//算法类型
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
        $(function(){          //加hide loading          $(window.parent.document).find('#mask').hide();
loadSortIcon();          var dataType = $("#dataType").val();          if(12==dataType || 14==dataType ||
15==dataType){          $("#page_bjzl").text($("#bjl").val());          $("#page_bjzl").parent().show();
}        });        //排序方法        function orderByTitle(orderByName,th){          parent.orderNameId =
$(th).attr("id");          if(parent.orderClickName == orderByName){          parent.orderClickCount ++;
}else{          parent.orderClickCount = 1;          }          parent.orderClickName = orderByName;
if(parent.orderClickCount % 2 == 1){          orderByName += " DESC";          }          $('#zb-form
[name=orderByName]').val(orderByName);          search();        }        //动态加载排序图标        function
loadSortIcon(){          if(parent.orderNameId){          if(parent.orderClickCount % 2 == 1){          $("#"
+ parent.orderNameId).addClass('pt-arrow-down').removeClass('pt-arrow-up');          }else{          $("#" +
parent.orderNameId).addClass('pt-arrow-up').removeClass('pt-arrow-down');          }          }        }
//重写重置function toClearForm(){$("#xmdm").val("");$("#xmmc").val("");$("#jsddxzqh").val("");}
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
        function newsearch(){        var i=document.getElementById("pageSize").value;       var
n=document.getElementById("pageNo").value;       var m="811";        if(m<i){
document.getElementById("pageNo").value=1;        search();        }else{        var u=Math.ceil(m/i)
if(n>u){        $.messager.alert('提示','页数超出限制');        }else{        search();        }        }
}        $(function(){          $('#pageNo').bind('keypress', function (event) {          if (event.keyCode
== "13") {          //需要处理的事情var pageNo = $(this).val();          pageNo = parseInt(pageNo);
var pages = $(this).data('pages');    //最大页码          if(pageNo < 1) {          pageNo = 1;          }
if(pageNo > pages){          pageNo = pages;          }          jumpPage(pageNo);   //跳转页面          }
});        });
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
jumpPage(2)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
jumpPage(82)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickback()
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
search()
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
toClearForm();search();
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
orderByTitle('xmztbxsjspys',this)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660900,'2020-654225-78-01-011794')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-13-03-007890')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-47-01-007688')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660800,'2019-659001-70-03-008909')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-47-01-008940')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-78-01-005475')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-47-01-005747')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660700,'2020-654003-70-03-011382')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660200,'2020-652801-77-03-013365')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660600,'2020-659004-41-03-004577')
```

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/city-project-stage-list.js

```
/**
 *
 */
var listTitleStr="",dataDesc="",dwStr="工作日";
function doInit(){
    var titleShow ="";
    if(name=='china'){
        titleShow ="各省";
    }if(xzqhdm == null || xzqhdm == ""){
        titleShow ="兵团";
    }
    else{
        titleShow = getCityName(xzqhdm,name);
    }
 if(stageType=="0"){
         dataDesc=""
 }else if(stageType=="1"){
         dataDesc=titleShow+"       立项用地规划许可阶段";
 }else if(stageType=="2"){
         dataDesc=titleShow+"       工程建设许可阶段";
 }else if(stageType=="3"){
         dataDesc=titleShow+"       施工许可阶段";
 }else if(stageType=="4"){
         dataDesc=titleShow+"       竣工验收阶段";
 }else if(stageType=="5"){
        dataDesc=titleShow+"并行推进阶段";
    }
 if(dataType=="1"){
     if(sfyq != '1'){
          dataDesc+=dataDesc==""?titleShow+"项目列表":"项目列表";
        }else{
          dataDesc+=dataDesc==""?titleShow+"逾期项目列表":"逾期项目列表";
        }
 }else if(dataType=="2"){
         dataDesc+=dataDesc==""?titleShow+"       跨度用时项目列表":"跨度用时项目列表";
 }else if(dataType=="3"){
         dataDesc+=dataDesc==""?titleShow+"       最长用时项目列表":"最长用时项目列表";
 }else if(dataType=="4"){
         dataDesc+=dataDesc==""?titleShow+"       受理次数项目列表":"受理次数项目列表";
         dwStr="       次";
 }else if(dataType=="5"){
        dataDesc+=dataDesc==""?titleShow+"新增项目数项目列表":"新增项目数项目列表";
        dwStr="次";
    }else if(dataType=="6"){
         dataDesc+=dataDesc==""?titleShow+"       各阶段退件项目数项目列表":"退件项目数项目列表";
         dwStr="       次";
 }else if(dataType=="7"){
         dataDesc+=dataDesc==""?titleShow+"       各阶段其他项目数项目列表":"其他项目数项目列表";
         dwStr="       次";
 }else if(dataType=="8"||dataType=="11"){
         if(xzqhdm == null || xzqhdm == ""){
          dataDesc+=dataDesc==""?titleShow+"受理项目列表":"受理项目列表";
         }else{
          dataDesc+=dataDesc==""?titleShow+"受理项目数项目列表":"受理项目数项目列表";
        }
         dwStr="       次";
 }else if(dataType=="9"||dataType=="10"){
     var yqTitleStr = ""; //       城市首页左下角"各类型项目平均总用时(天)/逾期数(个)"逾期和非逾期的钻取都用
dataType=10，此处需求区分下
        if(sfyq == '1'){
          yqTitleStr = "逾期";
        }
        dataDesc+=dataDesc==""?titleShow+yqTitleStr+"项目列表":yqTitleStr+"项目列表";
         dwStr="       次";
 }else if(dataType=="12"){
        dataDesc+=dataDesc==""?titleShow+"办件总量项目列表":"办件总量项目列表";
        dwStr="次";
    }else if(dataType=="15"){
     if(blqk == 1){
          dataDesc+=dataDesc==""?titleShow+"常规办理情况项目数项目列表":"常规办理情况项目数项目列表";
        }else if(blqk == 2){
          dataDesc+=dataDesc==""?titleShow+"退件办理情况项目数项目列表":"退件办理情况项目数项目列表";
        }else if(blqk == 3){
          dataDesc+=dataDesc==""?titleShow+"其他办理情况项目数项目列表":"其他办理情况项目数项目列表";
        }
        dwStr="次";
    }
 if(splcmc){
        $(".tit-ddd").html(splcmc+"-"+dataDesc);
    }else{
        $(".tit-ddd").html(dataDesc);
    }
    var orderColumn = "TOTAL_CNT";
    if(stageType != "0"){
        orderColumn = "CNT_" + stageType;
    }
    var orderNameId = "orderStage"+orderColumn;
    var orderNameClass = "";
    if(parent.orderNameId && parent.orderNameId == orderNameId){
        if(parent.orderClickCount % 2 == 1){
          orderNameClass = 'pt-arrow-down';
        }else{
          orderNameClass = 'pt-arrow-up';
        }
    }
    // var orderBtn = '<span onclick="orderByTitle(\''+orderColumn+'\',this)" id="'+orderNameId+'"
class="order-img pt-arrow '+orderNameClass+'" style="vertical-align: -webkit-baseline-middle;"></span>';
    var orderBtn = '<span class="title-tip" style="display:inline-block;" title="四阶段各阶段用时之和，审批用时=阶
段一用时+阶段二用时+阶段三用时+阶段四用时"></span>\n' +
        '\t&nbsp;&nbsp;<span onclick="orderByTitle(\''+orderColumn+'\',this)" id="'+orderNameId+'"
class="order-img pt-arrow '+orderNameClass+'" style=""></span>';

 $("#sptitle").html("<span class='table-th-span'>"+dataDesc+"("+dwStr+")</span>" + orderBtn);
 var startDays=tjkssj.split("-");
 $("#sDate").html(startDays[0]+"       年"+startDays[1]+"月"+startDays[2]+"日");
 var dateEnds=dateEnd.split("-");
 $("#endDate").html(dateEnds[0]+"       年"+dateEnds[1]+"月"+dateEnds[2]+"日");
 if(dataDesc!=""){
         commonFunction.doSaveFunctionLog({"functionUrl":window.location.href,"functionName":"       监督检查-
"+dataDesc});
 }else{
         commonFunction.doSaveFunctionLog({"functionUrl":window.location.href,"functionName":"       监督检查-
项目信息查询"});
        }
 //       退件
    if(dataType=="6" ||
            ((dataType=="11" || dataType=="12" || dataType=="13" || dataType=="14" ||dataType=="15") &&
blqk=="2")){
        //添加办理状态查询条件
        $("#search_tr1").find("td:eq(4)").after('<td width="1%"> </td>'+
                                                         '<td width="5%" align="right">办理状态：</td>'+
                                                         '<td width="10%">'+
                                                         '<select name="tjTypeVal" id="tjTypeVal"
class="common-select-white">'+
                                                         '<option value="1">已退件</option>'+
                                                         '<option value="3">退件（已退件+不予受理）</option>'+
                                                         '<option value="2">不予受理</option>'+
                                                         '</select>'+
                                                         '</td>');
        if(tjTypeVal){
                $("#tjTypeVal").val(tjTypeVal);
        }
    }else if(dataType=="7" ||
                ((dataType=="11" || dataType=="12" || dataType=="13" || dataType=="14" ||dataType=="15") &&
blqk=="3")){
        //添加办理状态查询条件
        $(...
```

http://127.0.0.1:8000/xmjg/resources/js/common/validate.js

```
//验证是否为空
function check_blank(obj, obj_name){
   if(obj.value != ''){
          return true;
     }else{
         alert(obj_name + "所填不能为空！");
          obj.value = "";
         return false;
     }
}

//过滤输入字符的长度
function check_str_len(name,obj,maxLength){
 obj.value=obj.value.replace(/(^\s*)|(\s*$)/g, "");
 var newvalue = obj.value.replace(/[^\x00-\xff]/g, "**");
    var length11 = newvalue.length;
 if(length11>maxLength){
         alert(name+"       的长度不能超过"+maxLength+"个字符！");
         obj.value="";
         obj.focus();
 }
 }

//验证只能为数字
function checkNumber(obj){
 var reg = /^[0-9]+$/;
    if(obj.value!=""&&!reg.test(obj.value)){
                alert('只能输入数字！');
                obj.value = "";
                obj.focus();
                return false;
        }
}

//验证数字大小的范围

function check_num_value(obj_name,obj,minvalue,maxvalue){
 var reg = /^[0-9]+$/;
 if(obj.value!=""&&!reg.test(obj.value)){
         alert(obj_name+'       只能输入数字！');
                obj.value = "";
                obj.focus();
                return false;
 }else if(minvalue>obj.value||obj.value>maxvalue){
         alert(obj_name+"       的范围是"+minvalue+"-"+maxvalue+"!");
         obj.value="";
        obj.focus();
        return false;
        }

}
```

```
//验证只能是字母和数字
function checkZmOrNum(zmnum){
  var zmnumReg=/^[0-9a-zA-Z]*$/;
  if(zmnum.value!=""&&!zmnumReg.test(zmnum.value)){
     alert("只能输入是字母或者数字,请重新输入");
     zmnum.value="";
     zmnum.focus();
     return false;
  }
}

//验证双精度数字
function check_double(obj,obj_name){
 var reg = /^[0-9]+(\.[0-9]+)?$/;
 if(obj.value!=""&&!reg.test(obj.value)){
                alert(obj_name+'所填必须为有效的双精度数字');
                obj.value = "";
         obj.focus();
                return false;
        }
}

/**
 * 判断是否为正整数
 */
function isPositiveInt(value){
 var re = /^[1-9]+[0-9]*$/;
 if (!re.test(value))
         return false;
 else
         return true;
}

//验证邮政编码
function check_youbian(obj){
 var reg=/^\d{6}$/;
 if(obj.value!=""&&!reg.test(obj.value)){
                alert('邮政编码格式输入错误！');
                obj.value = "";
                obj.focus();
                return false;
        }
}

//验证邮箱格式
function check_email(obj){
 var reg = /^[a-zA-Z0-9_-]+(\.([a-zA-Z0-9_-])+)*@[a-zA-Z0-9_-]+[.][a-zA-Z0-9_-]+([.][a-zA-Z0-9_-
]+)*$/;
 if(obj.value!=""&&!reg.test(obj.value)){
         obj.select();
                alert('电子邮箱格式输入错误！');
                obj.value = "";
         obj.focus();
                return false;
        }
}

/*验证固定电话号码
  0\d{2,3}   代表区号
  [0\+]\d{2,3}   代表国际区号
 \d{7,8} 代表7－8位数字(表示电话号码)
 正确格式：区号-电话号码-分机号(全写|只写电话号码)
*/

function check_phone(obj){
 var reg=/^(([0\+]\d{2,3}-)?(0\d{2,3})-)?(\d{7,8})(-(\d{3,}))?$/;
 if(obj.value!=""&&!reg.test(obj.value)){
                alert('电话号码格式输入错误！');
                obj.value = "";
         obj.focus();
                return false;
        }
}

//验证手机号码(检验13,15,18开头的手机号！)
function check_telephone(obj){
 var reg= /^[1][358]\d{9}$/;
 if(obj.value!=""&&!reg.test(obj.value)){
```

```
                alert('手机号码格式输入错误！');
                obj.value = "";
         obj.focus();
                return false;
        }
}

//验证是否为中文
function isChinese(obj,obj_name){
 var reg=/^[\u0391-\uFFE5]+$/;
 if(obj.value!=""&&!reg.test(obj.value)){
                alert(obj_name+'必须输入中文！');
                obj.value = "";
         obj.focus();
                return false;
        }
}

//检验时间大小(与当前时间比较)
function checkDate(obj,obj_name){
 var obj_value=obj.value.replace(/-/g,"/");//       替换字符，变成标准格式(检验格式为：'2009-12-10')
 // var obj_value=obj.value.replace("-","/");//       替换字符，变成标准格式(检验格式为：'2010-12-10 11:12')
 var date1=new Date(Date.parse(obj_value));
 var date2=new Date();//       取今天的日期
 if(date1>date2){
         alert(obj_name+"       不能大于当前时间！");
         return false;
        }
}



//检验字符串不能为空
function notEmpty(val){
        return val.replace(/(^\s*)|(\s*$)/g, "").length>0;
}


//验证字符串是否为IP地址
function isIP(strIP) {
       var re=/^(\d+)\.(\d+)\.(\d+)\.(\d+)$/g //匹配IP地址的正则表达式
       if(re.test(strIP))
       {
          if( RegExp.$1 <256 && RegExp.$2<256 && RegExp.$3<256 && RegExp.$4<256)
          return true;
       }
       return false;
}
```

http://127.0.0.1:8000/xmjg/resources/js/common/public.js

```
/**
 * 页面初始化（初始化页面的多个form）
 */
function initPage(){
 var formsLen = document.forms.length;
 if(formsLen > 0){
         for(var i=0; i<formsLen-1; i++){
                 initForm(i);
                }
        }
}

/**
 * 初始化form
 * @index form的序号
 */
function initForm(index){
 var excludeElemType = ",button,submit,reset,image,hidden,"; //       设置非注册事件的控件类型
 var allElems = document.forms[index].elements;

 //       为指定输入控件注册回车事件
 registerEnterKey(allElems, excludeElemType);
 //       当页面初始化后设置页面第一个输入控件的鼠标焦点
 setFirstInputElemFocus(allElems, excludeElemType);

 //       为页面单行文本框或多行文本框注册获取焦点时选中文本的事件
 registerSelectText(allElems);
}

/**
 * 为页面输入控件注册回车事件，使得输入控件可以响应回车键
 */
function registerEnterKey(allElems, excludeElemType) {
 for(var i=0; i<allElems.length; i++){
         /       /若不属于非注册事件的控件类型，则为其注册事件
         if(excludeElemType.indexOf(','+allElems[i].type+',') == -1){
                 allElems[i].onkeydown = function(){

                         if(event.keyCode == 13 && event.srcElement.type != ''
                                 && excludeElemType.indexOf(','+event.srcElement.type+',') == -1){

                                 event.keyCode = 9; //       跳转至下一输入控件

                                 /       /若控件类型为单行文本框或多行文本框，则为其添加选中文本动作
                                 if(event.srcElement.type == 'text' || event.srcElement.type ==
'textarea')
                                         event.srcElement.select(); //       选中下一输入控件文本内容
                                }
                 }       ;
         }
        }
}

/**
 * 为页面单行文本框或多行文本框注册获取焦点时选中文本的事件
 */
function registerSelectText(allElems){
 for(var i=0; i<allElems.length; i++){
         /       /若控件类型为单行文本框或多行文本框，则为其添加选中文本动作
         if(allElems[i].type == 'text' || allElems[i].type == 'textarea'){
                 allElems[i].attachEvent("onfocus", func_textHandler(allElems[i]));
         }
        }
}

var func_textHandler = function(obj){
 return function(){
         textHandler(obj);
 }
}

/**
 * 选中输入框文本内容
 */
function textHandler(obj){
 obj.select();
}

/**
 * 当页面初始化后设置页面第一个输入控件的鼠标焦点
 */
function setFirstInputElemFocus(allElems, excludeElemType){
 for(var i=0; i<allElems.length; i++){
         if(excludeElemType.indexOf(allElems[i].type) == -1){
                 allElems[i].focus(); //       设置页面第一个输入控件焦点

                 /       /如果为单行文本框或多行文本框，则还要选中文本
                 if(allElems[i].type == 'text' || allElems[i].type == 'numberfield')
                         allElems[i].select();
                 return;
                }
        }
}

/**
 * 跳转至第几页
 */
function jumpPage(pageNo){
 checkPagePara();
 $("#pageNo").val(pageNo);
 document.forms[0].submit();
}

/**
 * agcloud跳转至第几页
 */
function agcloudJumpPage(pageNo){
    checkPagePara();
    $("#pageNum").val(pageNo);
    document.forms[0].submit();
}

/**
 * 查询方法
 */
function search(){
 //       检查分页参数是否设置正确
 var pattern = new RegExp("^[0-9]*$");
 if($("#ztzStart").val()!=null && $("#ztzStart").val()!=""){
         if(!pattern.test($("#ztzStart").val())){
                 alert("       总投资只能为数字!");
                 $("#ztzStart").val("");
                 return false;
                }
        }
 if($("#ztzEnd").val()!=null && $("#ztzEnd").val()!=""){
         if(!pattern.test($("#ztzEnd").val())){
         alert("       总投资只能为数字!");
         $("#ztzEnd").val("");
         return false;
        }
        }

 $("#pageNo").val('1');//       重置当前页
 $("#pageNum").val('1');//       重置当前页
 checkPagePara();
 document.forms[0].submit();
}


/**
 * 检查分页参数设置是否有误
 */
function checkPagePara(){
 //       如果分页参数设置有误则使用默认值
 if(!isPositiveInt($("#pageSize").val()) || !isPositiveInt($("#pageNo").val())){
         $("#pageSize").val('10');
         $("#pageNo").val('1');
 }else if($("#pageNo").val() > $("#totalPages").val()){
     $("#pageNo").val($("#totalPages").val());
        }
}

/**
 * 取消操作
 */
function cancelSubmit(){
 if(confirm("       确定不保存当前页面数据并退出吗？")){
         history.back();
 }else
         return;
}

/**
 * 去除单行文本框或多行文本框多余空格
 */
function trimInputText(){
 var inputElems = document.forms[0].getElementsByTagName("INPUT");
 for(var i=0; i<inputElems.length; i++){
         if(inputElems[i].type == "text" || inputElems[i].type == 'textarea'){
                 if(inputElems[i].value.length > 0){
                         inputElems[i].value = trim(inputElems[i].value);
                        }
         }
 }
}
```

```
/**
 * 清空表单
 */
function clearForm(){
 var excludeElementIds = ',pageSize,pageNo,orderDir,orderBy,checkall,'; //       无需执行清空操作的控件ID
 clearFormByCustom(excludeElementIds); //       清空表单
}

/**
 * 清空表单。excludeElementIds表示无需执行清空操作的控件ID，以逗号作全分隔
 */
function clearFormByCustom(excludeElementIds) {
 var formObj = document.forms[0];
 var formEl = formObj.elements;

 for (var i=0; i<formEl.length; i++) {
         var element = formEl[i];

         /       /特殊字段要忽略掉清空操作
         if (excludeElementIds != "" && excludeElementIds.indexOf("," + element.id + ",") != -1)
                 break;

         if (element.type == 'text')
                 element.value = '';
         if (element.type == 'textarea')
                 element.value = '';
         if (element.type == 'checkbox')
                 element.checked = false;
         if (element.type == 'radio')
                 element.checked = false;
         if (element.type == 'select-multiple')
                 element.selectedIndex = 0;
         if (element.type == 'select-one')
                 element.selectedIndex = 0;
        }
}

/**
 * URL跳转
 */
function openUrl(url) {
 window.location.href = url;
}

/**
 * 删除操作
 */
function del(url) {
 if(confirm("       真的要删除该记录吗？")) {
         openUrl(url);
        }
}

/**
 * 带删除提示的多条记录删除操作URL跳转
 */
function delMore...
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
        function newsearch(){        var i=document.getElementById("pageSize").value;       var
n=document.getElementById("pageNo").value;       var m="0";        if(m<i){
document.getElementById("pageNo").value=1;        search();        }else{        var u=Math.ceil(m/i)
if(n>u){        $.messager.alert('提示','页数超出限制');        }else{        search();        }        }
}        $(function(){          $('#pageNo').bind('keypress', function (event) {          if (event.keyCode
== "13") {          //需要处理的事情var pageNo = $(this).val();          pageNo = parseInt(pageNo);
var pages = $(this).data('pages');    //最大页码          if(pageNo < 1) {          pageNo = 1;          }
if(pageNo > pages){          pageNo = pages;          }          jumpPage(pageNo);   //跳转页面          }
});        });
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
jumpPage(1)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
jumpPage(0)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
        function newsearch(){        var i=document.getElementById("pageSize").value;       var
n=document.getElementById("pageNo").value;       var m="49";        if(m<i){
document.getElementById("pageNo").value=1;        search();        }else{        var u=Math.ceil(m/i)
if(n>u){        $.messager.alert('提示','页数超出限制');        }else{        search();        }        }
}        $(function(){          $('#pageNo').bind('keypress', function (event) {          if (event.keyCode
== "13") {          //需要处理的事情var pageNo = $(this).val();          pageNo = parseInt(pageNo);
var pages = $(this).data('pages');    //最大页码          if(pageNo < 1) {          pageNo = 1;          }
if(pageNo > pages){          pageNo = pages;          }          jumpPage(pageNo);   //跳转页面          }
});        });
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
jumpPage(3)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
jumpPage(5)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660700,'2020-654003-05-03-007790')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660700,'2020-650203-05-03-007781')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660700,&#39;2020-654003-82-03-011839&#39;)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660700,'2020-654003-44-01-011068')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660700,'2020-654003-59-01-011389')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660700,'2020-654003-05-03-007032')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660700,'2019-654003-80-01-003395')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660700,'2020-654003-82-03-006773')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660700,'2020-654003-41-03-015233')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660700,'2020-654003-50-03-013174')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
var ctx="/xmjg/";var xzqhdm ="660000";var startDate ="2020-01-01";var endDate ="2020-12-29";
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
var isClickQuery = false; //是否点击过查询并且没有取消查询$(function()
{//getCountXmfl();//getPageData("");//getPageProjectLifeCycleData("");getProjectCategoryCount("");});//------
------------生命周期点击方法-------------------- function clickSmzq(spjd,codeName){
//window.location.href="${ctx}/xm-ag-project-info!getCountBySMZQ.action?xmsmzqbz="+xmsmzqbz;
//window.location.href="${ctx}/xmjg-statis-show!selectByCycleOne.action?
codeName="+codeName+"&spjd="+spjd+"&name=zone&tongji=zone&tjtype=qy";//----2019-04-10 --王羽中
window.location.href="${ctx}/xmjg-statis-show!selectByCycleOne.action?
codeName="+codeName+"&spjd="+spjd+"&name=province&tongji=province&tjtype=qy"; }//------------------生命周期点击
方法 结束--------------------//------------------建设项目类型点击方法--------------------function clickXmfl(xmfl)
{  location.href="${ctx}/xmjg-statis-show!selectByJsxmlxOne.action?
jsxmlx="+xmfl+"&name=province&tongji=province&tjtype=qy"; }//----------------点击行业分类的方法-----------------
-----//点击某一项国民经济行业分类/* function ClickGmjjhyfl(code,name){if(isClickQuery){var xmlx =
$("#xmlx").combobox("getValue");//项目类型 var startNum = $("#startNum").val(); var endNum =
$("#endNum").val(); var queryParams="&xmlx="+xmlx+"&startNum="+startNum+"&endNum="+endNum;
window.location.href="${ctx}/xmjg-statis-show!gotoDlPageByMlcode.action?
tongji=hy&code="+code+"&codeName="+name+queryParams;}else{var name1 =
encodeURI(encodeURI(name));window.location.href="${ctx}/xmjg-statis-show!gotoDlPageByMlcode.action?
tongji=hy&code="+code+"&codeName="+name1;}} *///点击某一项国民经济行业分类function ClickGmjjhyfl(e,code,name){
if($(e).attr('num') != 0){window.location.href=ctx+"/xmjg-statis-show!getAjaxByHy_one.action?
tongji=hy&code="+code+"&codeName="+name+"&type=province&startDate="+startDate+"&endDate="+endDate+"&xzqhdm="+
xzqhdm;       };}//----------------点击行业分类方法 结束----------------------//--------------图标hover时的方法---
-----------//操作按钮(修改、删除)图标鼠标移入移出效果function setImgSrc(imgObj,type){var
imgSrc=imgObj.src;if(type=="over")
{imgObj.src=imgSrc.substring(0,imgSrc.indexOf(".png"))+"_hover.png";}else{imgObj.src=imgSrc.substring(0,imgSr
c.indexOf("_hover.png"))+".png";}}function showdiv() {  document.getElementById("bg").style.display ="block";
document.getElementById("show").style.display ="block"; } function hidediv() {
document.getElementById("bg").style.display ='none'; document.getElementById("show").style.display ='none'; }
function showMore(){$(".moreInfo").show();$("#showBtn").hide();$("#hideBtn").show();}function hideMore()
{$(".moreInfo").hide();$("#hideBtn").hide();$("#showBtn").show();}//--------------原来图标hover时的方法 结束----
---------- //----------------快捷入口的方法------------------ function clickSSZD(){
//window.location.href="${ctx}/dghyindex/index-dghy-content.jsp?menuId=1880&menuName=项目管理&pmenuId=1111";
window.location.href="${ctx}/xm-ag-project-info!getZXFL.action"; } function clickTZTJ(){
window.location.href="${ctx}/dghyindex/index-dghy-content.jsp?menuId=1966&menuName=统计分析&pmenuId=5555"; }
function clickXYXX(){ window.location.href="${ctx}/dghyindex/index-dghy-content.jsp?menuId=1880&menuName=项目
管理&pmenuId=2222"; } function clickZRDW(){ //window.location.href="${ctx}/dghyindex/index-dghy-content.jsp?
menuId=1880&menuName=项目管理&pmenuId=3333"; window.location.href="${ctx}/xm-ag-project-info!getZRDW.action";
} function clickZBLS(){ //window.location.href="${ctx}/dghyindex/index-dghy-content.jsp?menuId=1880&menuName=
项目管理&pmenuId=00000"; window.location.href="${ctx}/xm-ag-zbls-info!getZbls.action"; } function clickTZLQY()
{//投资类 window.location.href="${ctx}/dghyindex/index-dghy-content.jsp?menuId=1880&menuName=项目管理
&pmenuId=tzl"; } function clickJSLQY(){//建设类 window.location.href="${ctx}/dghyindex/index-dghy-content.jsp?
menuId=1880&menuName=项目管理&pmenuId=jsl"; } function clickSSLQY(){//实施类
window.location.href="${ctx}/dghyindex/index-dghy-content.jsp?menuId=1880&menuName=项目管理&pmenuId=ssl"; }
function clickCYL(){//产业链 window.location.href="${ctx}/xm-ag-project-info!getCYL.action"; } function
clickCYY(){//产业园 window.location.href="${ctx}/xm-ag-project-info!getCYY.action"; } function clickPmtj(){//
统计排名 //window.location.href="${ctx}/xmjg/xndc/pm_jsl_sy.jsp";
window.location.href="${ctx}/dghyindex/index-dghy-content.jsp?menuId=2023&menuName=统计排名&pmenuId=tjpm";
}//----------------快捷入口的方法 结束------------------ function query(){ var xmlx =
$("#xmlx").combobox("getValue");//项目类型 var startNum = $("#startNum").val(); var endNum =
$("#endNum").val(); var queryParams="&xmlx="+xmlx+"&startNum="+startNum+"&endNum="+endNum;
getPageData(queryParams); isClickQuery = true; }  function cancleQuery(){ $("#xmlx").combobox("setValue","");
$("#startNum").val(""); $("#endNum").val(""); getPageData(''); isClickQuery = false; }  function zhQuery(){
window.location.href="${ctx}/dghyindex/common-content.jsp?method=zhcx"; }
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
    var radius = [37, 50];    var labelBottom = {    normal : {        color: '#ccc',        label : {
show : true,          position : 'center'        },         labelLine : {          show : false        }    },
emphasis: {        color: 'rgba(0,0,0,0)'    }};/***加载项目类型数据*/function getCountXmfl(){  $.ajax({
//async:false,          //   url :"${ctx}/xmjg-statis-show!getProjectCountLx.action",  //后台处理程序
url :"${ctx}/xmjg-statis-show!getProjectCountLx_new.action",  //后台处理程序          type:"post",    //数据发送
方式          dataType:"json",   //接受数据格式          error: function(){          //alert("服务器没有返回数据，
可能服务器忙，请重试");          },          success: function(data){          var obj = eval(data);
var total = obj[0].xmcb+obj[0].xmsc+obj[0].qqsp+obj[0].gcghxk; //06 01 02 03          $("#czjz").html("
("+obj[0].czjz+")");          $("#czxx").html("("+obj[0].czxx+")");          $("#xxsh").html("
("+obj[0].xxsh+")");          $("#ybsh").html("("+obj[0].ybsh+")");          $("#dfsh").html("
("+obj[0].dfsh+")");          $("#qtlx").html("("+obj[0].qtlx+")");          }          });     }/**加载页面项
目生命周期数据*/function getPageProjectLifeCycleData(queryParams){     showdiv();$.ajax({          url
:"${ctx}/xmjg-statis-show!getProjectLifeCycleCount.action?xzqhdm="+xzqhdm+"&t="+Math.random()+queryParams,
//后台处理程序          type:"post",    //数据发送方式          dataType:"json",   //接受数据格式          error:
function(){          //alert("服务器没有返回数据，可能服务器忙，请重试");          },          success:
function(data){          //getCountXmfl(" ");//获取页面数据          //(两个ajax的原因，如要加载动画，则将前一个设置为
同步，或者将一个置于另一个success代码块中)          hidediv();          var obj = eval(data);          var total =
obj.xmcb+obj.xmsc+obj.qqsp+obj.gcghxk; //06 01 02 03          require.config({          paths: {
echarts:ctx+"/dghyindex/echarts/build/dist"          }          });    require(          [          'echarts',
'echarts/chart/bar', // 使用柱状图就加载bar模块，按需加载          'echarts/chart/pie' // 使用柱状图就加载pie模块，按
需加载          ],          function (ec) {          // 基于准备好的dom，初始化echarts图表        var myChart2 =
ec.init(document.getElementById('label'));         var labelTop = {    normal : {    color: '#FE8463',
label : {          show : true,          position : 'center',          formatter : '{b}',          textStyle:
{          baseline : 'bottom'          }        },        labelLine : {          show : false        }
}};var labelFromatter = {    normal : {    color: '#FE8463',        label : {          formatter : function
(params){          return total-params.value;          },          textStyle: {          baseline : 'top'
}        }    }};var option2 = {    legend: {        x : 'left',        y : 'left',        data:[
'立项用地规划许可阶段'        ]    },    series : [        {          type : 'pie',          center : ['50%',
'50%'],          radius : radius,          x: '0%', // for funnel          itemStyle : labelFromatter,
data : [          {name:'other', value:total-obj.xmcb, itemStyle : labelBottom},          {name:'立项用地规划许
可阶段', value:obj.xmcb,itemStyle : labelTop}          ]        }    ]};    // 为echarts对象加载数据
myChart2.setOption(option2);          var myChart3 = ec.init(document.getElementById('label2'));          var
labelTop = {    normal : {    color: '#27727B',        label : {          show : true,          position :
'center',          formatter : '{b}',          textStyle: {          baseline : 'bottom'          }        },
labelLine : {          show : false        }    }};var labelFromatter = {    normal : {    color: '#27727B',
label : {          formatter : function (params){          return total - params.value;          },
textStyle: {          baseline : 'top'          }        }    },};var option3 = {    legend: {        x :
'left',        y : 'left',        data:[          '工程建设许可'        ]    },    series : [        {
type : 'pie',          center : ['50%', '50%'],          radius : radius,          x: '0%', // for funnel
itemStyle : labelFromatter,          data : [          {name:'other', value:total-obj.xmsc, itemStyle :
labelBottom},          {name:'工程建设许可', value:obj.xmsc,itemStyle : labelTop}          ]        }    ]};
// 为echarts对象加载数据          myChart3.setOption(option3);          var myChart4 =
ec.init(document.getElementById('label3'));          var labelTop = {    normal : {    color: '#E87C25',
...
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
history.go(-1);
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('nlmyyimg','A','农、林、牧、渔业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
setImgSrc(this,'over')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
setImgSrc(this,'out')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('ckyimg','B','采矿业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('zzyimg','C','制造业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('drrsimg','D','电力、热力、燃气及水生产和供应业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('jzyimg','E','建筑业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('pfhlsyimg','F','批发和零售业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('jtyschhyzyimg','G','交通运输、仓储和邮政业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('zshcyyimg','H','住宿和餐饮业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('rjxximg','I','信息传输、软件和信息技术服务业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('jryimg','J','金融业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('fdcyimg','K','房地产业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('zlhswfwyimg','L','租赁和商务服务业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('kxyjhjsfwyimg','M','科学研究和技术服务业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('slhjhggssglyimg','N','水利、环境和公共设施管理业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('jmfwxlhqtfwyimg','O','居民服务、修理和其他服务业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('jyimg','P','教育')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('wshshgzimg','Q','卫生和社会工作')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('whtyhylyimg','R','文化、体育和娱乐业')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('ggglshbzhshzzimg','S','公共管理、社会保障和社会组织')
```

http://127.0.0.1:8000/xmjg/xmjg-statis-show!getSkipPage.action

```
ClickGmjjhyfl('gjzzimg','T','国际组织')
```

http://127.0.0.1:8000/xmjg/resources/js/dghy/index.js

```
//tab切换
function changeTab(obj){
 var tabLables = ["dbgz","dbxm","jbj","ybj"];
 for (var i=0;i<tabLables.length;i++){
         if(obj.id==tabLables[i]){
                 $("#"+tabLables[i]).removeClass().addClass("current");
                 $("#"+tabLables[i]+"Table").show();
         }else{
                 $("#"+tabLables[i]).removeClass();
                 $("#"+tabLables[i]+"Table").hide();
                }
        }
}
//点击更多
function moreBtn(){
 var tabLables = ["dbgz","dbxm","jbj","ybj"];
 var url = "index-dghy-content.jsp?menuId=1898";
 for (var i=0;i<tabLables.length;i++){
         if($("#"+tabLables[i]).hasClass("current")){
                 if(i==0){
                         url+="&pmenuId=1883";
                 }else if(i==1){
                         url+="&pmenuId=1887";
                        }
                }
        }
 location.href = url;
}
//签收任务
function wfSignTask(taskInstDbid, title){
 //window.open(ctx + '/task/work-task!signTask.action?instance.taskInstDbid=' + taskInstDbid);
 window.location=ctx+"/dghyindex/index-dghy-content.jsp?
menuId=1898&pmenuId=dzbpage&taskInstDbid="+taskInstDbid+"&title="+title;
}
//剩余天数
function remainderDay(duedate){
 var str;
 if(duedate){
         /       /截掉毫秒数
         if(duedate.length>19) duedate = duedate.substr(duedate,19);
         var dueDate = new Date(Date.parse(duedate.replace(/-/g,"/")));
         var nowDateTime = new Date();
         var days = Math.round((dueDate-nowDateTime)/(24*60*60*1000));
         var cla;
         if(days>0&&days<=3){
                 cla="list_time_orange";
                 str = "<span class='"+cla+"'>       余"+days+"天</span>";
         }else if(days<=0){
                 cla="list_time_red";
                 str = "<span class='"+cla+"'>       超"+Math.abs(days)+"天</span>";
         }else{
                 cla="list_time_green";
                 str = "<span class='"+cla+"'>       余"+days+"天</span>";
                }
         return str;
        }
 return "";
}
//累计正常、异常、提醒件数量
function countStatePercent(today,duedate){
 if(duedate){
         var dueDate = new Date(Date.parse(duedate.replace(/-/g,"/")));
         var days = Math.round((dueDate-today)/(24*60*60*1000));
         if(days>0&&days<=3){
                 txj++;
         }else if(days<=0){
                 ycj++;
         }else{
                 zcj++;
                }
 }else{
         zcj++
        }
}
//正常件
 var circle1 = {
     paper: null,
         percent: null,
     init: function() {
         //       初始化Raphael画布
         this.paper = Raphael("progress1", 60, 60);

         //       把底图先画上去
         this.paper.image("../resources/css/dghyindex/images/circlebg.png", 0, 0, 60, 60);

         //       进度比例，0到1，在本例中我们画65%
         //       需要注意，下面的算法不支持画100%，要按99.99%来画
         //var percent = 0.65,
          var drawPercent = this.percent >= 1 ? 0.9999 : this.percent;

         //       开始计算各点的位置，见后图
         //r1       是内圆半径，r2是外圆半径
         var r1 = 23,
           r2 = 30,
           PI = Math.PI,
           p1 = {
           x: 30,
           y: 60
           },
           p4 = {
           x: p1.x,
           y: p1.y - r2 + r1
           },
           p2 = {
           x: p1.x + r2 * Math.sin(2 * PI * (1 - drawPercent)),
           y: p1.y - r2 + r2 * Math.cos(2 * PI * (1 - drawPercent))
           },
           p3 = {
           x: p4.x + r1 * Math.sin(2 * PI * (1 - drawPercent)),
           y: p4.y - r1 + r1 * Math.cos(2 * PI * (1 - drawPercent))
           },
           path = [
           'M', p1.x, ' ', p1.y,
           'A', r2, ' ', r2, ' 0 ', this.percent > 0.5 ? 1 : 0, ' 1 ', p2.x, ' ', p2.y,
           'L', p3.x, ' ', p3.y,
           'A', r1, ' ', r1, ' 0 ', this.percent > 0.5 ? 1 : 0, ' 0 ', p4.x, ' ', p4.y,
           'Z'
           ].join('');

         //       用path方法画图形，由两段圆弧和两条直线组成，画弧线的算法见后 www.it165.net
         this.paper.path(path)
           //       填充渐变色，从#3f0b3f到#ff66ff
           .attr({
           "stroke-width": 0.5,
           "stroke": "#39a219",
           "fill": "#39a219"
           });

         //       显示进度文字
         $("#progressText1").text(Math.round(this.percent * 100) + "%");
     }

  };
 //       提醒件
 var circle2 = {
     paper: null,
         percent: null,
     init: function() {
         //       初始化Raphael画布
         this.paper = Raphael("progress2", 60, 60);

         //       把底图先画上去
         this.paper.image("../resources/css/dghyindex/images/circlebg.png", 0, 0, 60, 60);

         //       进度比例，0到1，在本例中我们画65%
         //       需要注意，下面的算法不支持画100%，要按99.99%来画
         //var percent = 0.65,
          var drawPercent = this.percent >= 1 ? 0.9999 : this.percent;

         //       开始计算各点的位置，见后图
         //r1       是内圆半径，r2是外圆半径
         var r1 = 23,
           r2 = 30,
           PI = Math.PI,
           p1 = {
           x: 30,
           y: 60
           },
           p4 = {
           x: p1.x,
           y: p1.y - r2 + r1
           },
           p2 = {
           x: p1.x + r2 * Math.sin(2 * PI * (1 - drawPercent)),
           y: p1.y - r2 + r2 * Math.cos(2 * PI * (1 - drawPercent))
           },
           p3 = {
           x: p4.x + r1 * Math.sin(2 * PI * (1 - drawPercent)),
           y: p4.y - r1 + r1 * Math.cos(2 * PI * (1 - drawPercent))
           },
  ...
```

http://127.0.0.1:8000/xmjg/dghyindex/js/index-dghy-main.js

```
//正常件，提醒件，异常件数量
var zcj=0,txj=0,ycj=0;

//待办列表
function loadDbList(){
 $.ajax({
         type: "post",
         url:"summary/wf-task-summary!getDbSummary.action",
         data:{"sort":"create","dir":"DESC","start":0,"limit":10},
         dataType:"json",
         success:function(res){
                 if(res.totalItems>0){
                         $("#dban").html(res.totalItems);//       显示待办总记录数
                 }else{
                         $("#dban").hide();
                        }
                }
 });
}

//查询在办总记录数
function loadZbList(){
 $.ajax({
         type:"post",
         url:"summary/wf-task-summary!getZbSummary.action",
         data:{"sort":"create","dir":"DESC","start":0,"limit":10},
         dataType:"json",
         success:function(res){
                 if(res.totalItems>0){
                         $("#zaiban").html(res.totalItems);//       显示在办总记录数
                 }else{
                         $("#zaiban").hide();
                        }
                }
 });
}

//待在办列表
function loadDZbList(){
 $.ajax({
         type: "post",
         url:"summary/wf-task-summary!getDZbSummary.action",
         data:{"sort":"create","dir":"DESC","start":0,"limit":10},
         dataType:"json",
         success:function(res){
                 $.each(res.result,function(index,obj){
                         var newRow = "<tr><td width='30%' align='center'><a href='#'
style='color:#000;' onclick='wfSignTask("+obj.taskInstDbid+","+'"'+obj.busMemo1+'"'+")'>"+obj.busMemo1+"</a>
</td><td width='15%' align='center'>"+obj.templateName+"</td><td width='20%'
align='center'>"+obj.activityChineseName+"</td><td width='10%'>"+remainderDay(obj.duedate)+"</td><td
width='25%' align='center'>到达时间 : "+obj.create+"</td></tr>";
                         $("#dbgzTable").append(newRow);
                 })       ;

                 if((res.totalItems)>0){
                         $("#dzbTabCount").html(res.totalItems);//       显示页签待在办总记录数
                 }else{
                         $("#dzbTabCount").hide();
                        }
                }
 });
}

//查询所有待办，累计正常，异常，提醒件
function loadDzbStatistics(){
 $.ajax({
         type: "post",
         url:"summary/wf-task-summary!getDZbSummary.action",
         data:{"sort":"create","dir":"DESC","start":0,"limit":10000},
         dataType:"json",
         success:function(res){
                 var total=res.totalItems,today=new Date();
                 $.each(res.result,function(index,obj){
                         countStatePercent(today,obj.duedate);
                 })       ;

                 $("#zcjnum").text(zcj);
                 $("#txjnum").text(txj);
                 $("#ycjnum").text(ycj);
                 circle1.percent=(total==0?0:zcj/total);
             circle1.init();
                 circle2.percent=(total==0?0:txj/total);
             circle2.init();
                 circle3.percent=(total==0?0:ycj/total);
             circle3.init();
                }
 });
}

//催办列表
function loadDubanList(){
 $.ajax({
         type: "post",
         url:"wf/remind/wf-remind!list.action",
         data:{"sort":"remindDate","dir":"ASC","start":0,"limit":10},
         dataType:"json",
         success:function(res){
                 $.each(res.result,function(index,obj){
                         var newRow = "<tr><td width='20%' align='center'>"+obj.busMemo1+"</td><td
width='10%' align='center'>催办人: "+obj.reminderName+"</td><td width='20%'
align='center'>"+obj.activityChineseName+"</td><td width='20%' align='center'>提醒内容: "+obj.content+"</td>
<td width='20%' align='center'>提醒日期: "+obj.remindDate+"</td><td width='10%' align='center'><input
type='button' value='马上处理' onclick='wfSignTask("+obj.taskInstDbid+","+'"'+obj.activityChineseName+'"'+")'
/></td></tr>";
                         $("#dbxmTable").append(newRow);
                 })       ;
                 if(res.totalItems>0){
                         $("#duban").html(res.totalItems);//       显示督办总记录数
                         $("#dbTabCount").html(res.totalItems);//       显示页签督办总记录数
                 }else{
                         $("#duban").hide();
                         $("#dbTabCount").hide();
                        }
                }
 });
}

//加载我的会议
function loadMyConferenceList(){
 $.ajax({
         method:"post",
         url:"dg-hyreceive!myDgHyreceiveList.action?isHome=home",
         success:function(data){
                 if(data && data.length>0){
                         var hyHtml="";
                         var count=3;
                         if(data.length<=3)
```

```
                                 count=data.length;
                         for(var i=0;i<count;i++){
                                 hyHtml+="<li><p><a href='${ctx}/hygl/my-hytz-main.jsp?url=dg-
hyreceive!input.action?hyid="+data[i].hyid+"&title=会议通知'>"+data[i].dgHyglForm.hyzt+"</a></p>
<span>"+data[i].dgHyglForm.hysj+"</span></li>";
                                }
                         $("#myHyInfo").html(hyHtml);
                        }
                }
 });
}

//加载会议纪要
function loadMySummaryList(){
 $.ajax({
         method:"post",
         url:"dg-hyjy!myDgHyjyList.action?isHome=home",
         success:function(data){
                 if(data && data.length>0){
                         var hyjyHtmlLeft="";
                         for(var i=0;i<data.length;i++){
                                 hyjyHtmlLeft+="<div class='con_list'><p class='list_tit'><a
href='${ctx}/hygl/my-hytz-main.jsp?url=dg-hyreceive!input.action?
hyid="+data[i].hyid+"&hyjyid="+data[i].id+"&title=会议纪要'>"+data[i].dgHyglForm.hyzt+"</a></p><p
class='list_date'>"+data[i].lrr+"&nbsp;&nbsp;&nbsp;"+data[i].lrsj+"</p></div>";
                                }
                         $("#hyjyDivLeft").html(hyjyHtmlLeft);
                        }
                }
 });
}

//多规新闻
function loadNewsList(){
 $.ajax({
         type:"post",
         url:ctx+"/xm-ag-project-notice!listJson.action?type=1",
         success:function(data){
                 var newsHtmls="";
                 $.each(data,function(index,newsdata){
                         var imgPath=ctx+newsdata.titlePicPath;
                         var url = ctx+"/xm-ag-project-notice!viewNews.action?id="+newsdata.id;
                         var newsHtml = "<li><span  class='news_pic'><a href='"+url+"'
target='_blank'><img src='"+imgPath+"' width='129' height='89'></a></span>"+
                                                    "<..       .
```

http://127.0.0.1:8000/xmjg/resources/easyui/easycore.js

```
/*
var bootPATH = typeof(ctx) == 'undefined' ? '../../../..' : ctx;*/
var bootPATH  = ctx+'resources/easyui/';
document.write('<script src="' + bootPATH + 'jquery.min.js" type="text/javascript"></script>');
document.write('<script src="' + bootPATH + 'jquery.easyui.min.js" type="text/javascript"></script>');
document.write('<script src="' + bootPATH + 'locale/easyui-lang-zh_CN.js" type="text/javascript"></script>');
document.write('<link rel="stylesheet" type="text/css" href="' + bootPATH + 'themes/icon.css"/>');
document.write('<link rel="stylesheet" type="text/css" href="' + bootPATH + 'themes/default/easyui.css"/>');
```

http://127.0.0.1:8000/xmjg/dghyindex/js/dghy-public.js

```
//二级菜单鼠标悬浮效果
function setMenuImg(imgObj,type){
 var imgSrc=imgObj.src;
 if(type=="over"){
         imgObj.src=imgSrc.replace(".png","_hover.png");
 }else{
         imgObj.src=imgSrc.replace("_hover.png",".png");
        }
}
```

```
function redirectUrl(url,title,failedData){
         if($("#mainTabs").tabs("exists",title)){
                 $("#mainTabs").tabs("select",title);
                 var currTab = $("#mainTabs").tabs("getSelected",title);
                 $('#mainTabs').tabs('update', {
                        tab : currTab,
                        options : {
                                content : currTab.content
                        }
                });
         }else{
                 //url = "/xmzh/xm-ag-project-info!getProjectByFaild.action?data="+failedData;
                 $("#mainTabs").tabs("add",{
                         title:title,
                         closable:true,
                         content:"<iframe allowfullscreen  id='iframeMain' src='"+url+"'
frameborder='0' width='100%' height='90%' />"
                 })       ;
                }
}

/**
 * 跳转至第几页
 */
function jumpPage(pageNo){
 checkPagePara();
 $("#pageNo").val(pageNo);
 document.forms[0].submit();
}

/**
 * 查询方法
 */
function search(){
 //       检查分页参数是否设置正确
 checkPagePara();
 document.forms[0].submit();
}
/**
 * 判断是否为正整数
 */
function isPositiveInt(value){
 var re = /^[1-9]+[0-9]*]*$/;
 if (!re.test(value))
         return false;
 else
         return true;
}

/**
 * 检查分页参数设置是否有误
 */
function checkPagePara(){
 //       如果分页参数设置有误则使用默认值
 if(!isPositiveInt($("#pageSize").val()) || !isPositiveInt($("#pageNo").val())){
         $("#pageSize").val('10');
         $("#pageNo").val('1');
        }
}
```

http://127.0.0.1:8000/xmjg/resources/easyui/locale/easyui-lang-zh_CN.js

```
if ($.fn.pagination){
 $.fn.pagination.defaults.beforePageText = '       第';
 $.fn.pagination.defaults.afterPageText = '       共{pages}页';
 $.fn.pagination.defaults.displayMsg = '       显示{from}到{to},共{total}记录';
}
if ($.fn.datagrid){
 $.fn.datagrid.defaults.loadMsg = '       正在处理，请稍待。。。';
}
if ($.fn.treegrid && $.fn.datagrid){
 $.fn.treegrid.defaults.loadMsg = $.fn.datagrid.defaults.loadMsg;
}
if ($.messager){
 $.messager.defaults.ok = '       确定';
 $.messager.defaults.cancel = '       取消';
}
$.map(['validatebox','textbox','filebox','searchbox',
         'combo','combobox','combogrid','combotree',
         'datebox','datetimebox','numberbox',
         'spinner','numberspinner','timespinner','datetimespinner'], function(plugin){
 if ($.fn[plugin]){
         $.fn[plugin].defaults.missingMessage = '       该输入项为必输项';
        }
});
if ($.fn.validatebox){
 $.fn.validatebox.defaults.rules.email.message = '       请输入有效的电子邮件地址';
 $.fn.validatebox.defaults.rules.url.message = '       请输入有效的URL地址';
 $.fn.validatebox.defaults.rules.length.message = '       输入内容长度必须介于{0}和{1}之间';
 $.fn.validatebox.defaults.rules.remote.message = '       请修正该字段';
}
if ($.fn.calendar){
 $.fn.calendar.defaults.weeks = ['       日','一','二','三','四','五','六'];
 $.fn.calendar.defaults.months = ['       一月','二月','三月','四月','五月','六月','七月','八月','九月','十月','十一
月','十二月'];
}
if ($.fn.datebox){
 $.fn.datebox.defaults.currentText = '       今天';
 $.fn.datebox.defaults.closeText = '       关闭';
 $.fn.datebox.defaults.okText = '       确定';
 $.fn.datebox.defaults.formatter = function(date){
         var y = date.getFullYear();
         var m = date.getMonth()+1;
         var d = date.getDate();
         return y+'-'+(m<10?('0'+m):m)+'-'+(d<10?('0'+d):d);
 };
 $.fn.datebox.defaults.parser = function(s){
         if (!s) return new Date();
         var ss = s.split('-');
         var y = parseInt(ss[0],10);
         var m = parseInt(ss[1],10);
         var d = parseInt(ss[2],10);
         if (!isNaN(y) && !isNaN(m) && !isNaN(d)){
                 return new Date(y,m-1,d);
         } else {
                 return new Date();
                }
 };
}
if ($.fn.datetimebox && $.fn.datebox){
 $.extend($.fn.datetimebox.defaults,{
         currentText: $.fn.datebox.defaults.currentText,
         closeText: $.fn.datebox.defaults.closeText,
         okText: $.fn.datebox.defaults.okText
 });
}
if ($.fn.datetimespinner){
 $.fn.datetimespinner.defaults.selections = [[0,4],[5,7],[8,10],[11,13],[14,16],[17,19]]
}
```

http://127.0.0.1:8000/xmjg/resources/js/jquery/jquery.js

```
/*! jQuery v1.7.1 jquery.com | jquery.org/license */
(function(a,b){function cy(a){return f.isWindow(a)?a:a.nodeType===9?a.defaultView||a.parentWindow:!1}function
cv(a){if(!ck[a]){var b=c.body,d=f("<"+a+">").appendTo(b),e=d.css("display");d.remove();if(e==="none"||e==="")
{cl||
(cl=c.createElement("iframe"),cl.frameBorder=cl.width=cl.height=0),b.appendChild(cl);if(!cm||!cl.createElemen
t)cm=(cl.contentWindow||cl.contentDocument).document,cm.write((c.compatMode==="CSS1Compat"?"<!doctype
html>":"")+"<html>
<body>"),cm.close();d=cm.createElement(a),cm.body.appendChild(d),e=f.css(d,"display"),b.removeChild(cl)}ck[a]
=e}return ck[a]}function cu(a,b){var c={};f.each(cq.concat.apply([],cq.slice(0,b)),function()
{c[this]=a});return c}function ct(){cr=b}function cs(){setTimeout(ct,0);return cr=f.now()}function cj()
{try{return new a.ActiveXObject("Microsoft.XMLHTTP")}catch(b){}}function ci(){try{return new
a.XMLHttpRequest}catch(b){}}function cc(a,c){a.dataFilter&&(c=a.dataFilter(c,a.dataType));var
```

```
d=a.dataTypes,e={},g,h,i=d.length,j,k=d[0],l,m,n,o,p;for(g=1;g<i;g++){if(g===1)for(h in a.converters)typeof
h=="string"&&(e[h.toLowerCase()]=a.converters[h]);l=k,k=d[g];if(k==="*")k=l;else if(l!=="*"&&l!==k){m=l+"
"+k,n=e[m]||e["* "+k];if(!n){p=b;for(o in e){j=o.split(" ");if(j[0]===l||j[0]==="*"){p=e[j[1]+" "+k];if(p)
{o=e[o],o===!0?n=p:p===!0&&(n=o);break}}}}!n&&!p&&f.error("No conversion from "+m.replace(" "," to
")),n!==!0&&(c=n?n(c):p(o(c)))}}return c}function cb(a,c,d){var
e=a.contents,f=a.dataTypes,g=a.responseFields,h,i,j,k;for(i in g)i in d&&
(c[g[i]]=d[i]);while(f[0]==="*")f.shift(),h===b&&(h=a.mimeType||c.getResponseHeader("content-
type"));if(h)for(i in e)if(e[i]&&e[i].test(h)){f.unshift(i);break}if(f[0]in d)j=f[0];else{for(i in d)
{if(!f[0]||a.converters[i+" "+f[0]]){j=i;break}k||(k=i)}j=j||k}if(j){j!==f[0]&&f.unshift(j);return
d[j]}}function ca(a,b,c,d){if(f.isArray(b))f.each(b,function(b,e){c||bE.test(a)?d(a,e):ca(a+"["+(typeof
e=="object"||f.isArray(e)?b:"")+"]",e,c,d)});else if(!c&&b!=null&&typeof b=="object")for(var e in b)ca(a+"
["+e+"]",b[e],c,d);else d(a,b)}function b_(a,c){var d,e,g=f.ajaxSettings.flatOptions||{};for(d in
c)c[d]!==b&&((g[d]?a:e||(e={}))[d]=c[d]);e&&f.extend(!0,a,e)}function b$(a,c,d,e,f,g)
{f=f||c.dataTypes[0],g=g||{},g[f]=!0;var h=a[f],i=0,j=h?h.length:0,k=a===bT,l;for(;i<j&&(k||!l);i++)l=h[i]
(c,d,e),typeof l=="string"&&(!k||g[l]?l=b:(c.dataTypes.unshift(l),l=b$(a,c,d,e,l,g)));(k||!l)&&!g["*"]&&
(l=b$(a,c,d,e,"*",g));return l}function bZ(a){return function(b,c){typeof b!="string"&&
(c=b,b="*");if(f.isFunction(c)){var
d=b.toLowerCase().split(bP),e=0,g=d.length,h,i,j;for(;e<g;e++)h=d[e],j=/^\+/.test(h),j&&
(h=h.substr(1)||"*"),i=a[h]=a[h]||[],i[j?"unshift":"push"](c)}}}function bC(a,b,c){var d=b==="width"?
a.offsetWidth:a.offsetHeight,e=b==="width"?bx:by,g=0,h=e.length;if(d>0){if(c!=="border")for(;g<h;g++)c||(d-
=parseFloat(f.css(a,"padding"+e[g]))||0),c==="margin"?d+=parseFloat(f.css(a,c+e[g]))||0:d-
=parseFloat(f.css(a,"border"+e[g]+"Width"))||0;return
d+"px"}d=bz(a,b,b);if(d<0||d==null)d=a.style[b]||0;d=parseFloat(d)||0;if(c)for(;g<h;g++)d+=parseFloat(f.css(a
,"padding"+e[g]))||0,c!=="padding"&&(d+=parseFloat(f.css(a,"border"+e[g]+"Width"))||0),c==="margin"&&
(d+=parseFloat(f.css(a,c+e[g]))||0);return d+"px"}function bp(a,b){b.src?
f.ajax({url:b.src,async:!1,dataType:"script"}):f.globalEval((b.text||b.textContent||b.innerHTML||"").replace(
bf,"/*$0*/")),b.parentNode&&b.parentNode.removeChild(b)}function bo(a){var
b=c.createElement("div");bh.appendChild(b),b.innerHTML=a.outerHTML;return b.firstChild}function bn(a){var b=
(a.nodeName||"").toLowerCase();b==="input"?bm(a):b!=="script"&&typeof
a.getElementsByTagName!="undefined"&&f.grep(a.getElementsByTagName("input"),bm)}function bm(a)
{if(a.type==="checkbox"||a.type==="radio")a.defaultChecked=a.checked}function bl(a){return typeof
a.getElementsByTagName!="undefined"?a.getElementsByTagName("*"):typeof a.querySelectorAll!="undefined"?
a.querySelectorAll("*"):[]}function bk(a,b){var c;if(b.nodeType===1)
{b.clearAttributes&&b.clearAttributes(),b.mergeAttributes&&b.mergeAttributes(a),c=b.nodeName.toLowerCase();if
(c==="object")b.outerHTML=a.outerHTML;else if(c!=="input"||a.type!=="checkbox"&&a.type!=="radio")
{if(c==="option")b.selected=a.defaultSelected;else
if(c==="input"||c==="textarea")b.defaultValue=a.defaultValue}else a.checked&&
(b.defaultChecked=b.checked=a.checked),b.value!==a.value&&
(b.value=a.value);b.removeAttribute(f.expando)}}function bj(a,b){if(b.nodeType===1&&!!f.hasData(a)){var
c,d,e,g=f._data(a),h=f._data(b,g),i=g.events;if(i){delete h.handle,h.events={};for(c in
i)for(d=0,e=i[c].length;d<e;d++)f.event.add(b,c+(i[c][d].namespace?".":"")+i[c][d].namespace,i[c][d],i[c]
[d].data)}h.data&&(h.data=f.extend({},h.data))}}function bi(a,b){return f.nodeName(a,"table")?
a.getElementsByTagName("tbody")[0]||a.appendChild(a.ownerDocument.createElement("tbody")):a}function U(a){var
b=V.split("|"),c=a.createDocumentFragment();if(c.createElement)while(b.length)c.creat...
```

http://127.0.0.1:8000/xmjg/resources/easyui/jquery.min.js

```
/*! jQuery v1.11.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?
b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return
b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=
[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k=
{},l="1.11.1",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,o=/^-ms-
/,p=/-([\da-z])/gi,q=function(a,b){return b.toUpperCase()};m.fn=m.prototype=
{jquery:l,constructor:m,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return
null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var
b=m.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return
m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){return
a.call(b,c,b)}))},slice:function(){return this.pushStack(d.apply(this,arguments))},first:function(){return
this.eq(0)},last:function(){return this.eq(-1)},eq:function(a){var b=this.length,c=+a+(0>a?b:0);return
this.pushStack(c>=0&&b>c?[this[c]]:[])},end:function(){return
this.prevObject||this.constructor(null)},push:f,sort:c.sort,splice:c.splice},m.extend=m.fn.extend=function()
{var a,b,c,d,e,f,g=arguments[0]||{},h=1,i=arguments.length,j=!1;for("boolean"==typeof g&&
(j=g,g=arguments[h]||{},h++),"object"==typeof g||m.isFunction(g)||(g={}),h===i&&(g=this,h--
);i>h;h++)if(null!=(e=arguments[h]))for(d in e)a=g[d],c=e[d],g!==c&&(j&&c&&(m.isPlainObject(c)||
(b=m.isArray(c)))?(b?(b=!1,f=a&&m.isArray(a)?a:[]):f=a&&m.isPlainObject(a)?a:{},g[d]=m.extend(j,f,c)):void
0!==c&&(g[d]=c));return g},m.extend({expando:"jQuery"+
(l+Math.random()).replace(/\D/g,""),isReady:!0,error:function(a){throw new Error(a)},noop:function()
{},isFunction:function(a){return"function"===m.type(a)},isArray:Array.isArray||function(a)
{return"array"===m.type(a)},isWindow:function(a){return null!=a&&a==a.window},isNumeric:function(a)
{return!m.isArray(a)&&a-parseFloat(a)>=0},isEmptyObject:function(a){var b;for(b in
a)return!1;return!0},isPlainObject:function(a){var
b;if(!a||"object"!==m.type(a)||a.nodeType||m.isWindow(a))return!1;try{if(a.constructor&&!j.call(a,"constructo
r")&&!j.call(a.constructor.prototype,"isPrototypeOf"))return!1}catch(c){return!1}if(k.ownLast)for(b in
a)return j.call(a,b);for(b in a);return void 0===b||j.call(a,b)},type:function(a){return null==a?
a+"":"object"==typeof a||"function"==typeof a?h[i.call(a)]||"object":typeof a},globalEval:function(b)
{b&&m.trim(b)&&(a.execScript||function(b){a.eval.call(a,b)})(b)},camelCase:function(a){return
a.replace(o,"ms-").replace(p,q)},nodeName:function(a,b){return
a.nodeName&&a.nodeName.toLowerCase()===b.toLowerCase()},each:function(a,b,c){var
d,e=0,f=a.length,g=r(a);if(c){if(g){for(;f>e;e++)if(d=b.apply(a[e],c),d===!1)break}else for(e in
a)if(d=b.apply(a[e],c),d===!1)break}else if(g){for(;f>e;e++)if(d=b.call(a[e],e,a[e]),d===!1)break}else for(e
in a)if(d=b.call(a[e],e,a[e]),d===!1)break;return a},trim:function(a){return null==a?"":
(a+"").replace(n,"")},makeArray:function(a,b){var c=b||[];return null!=a&&(r(Object(a))?
m.merge(c,"string"==typeof a?[a]:a):f.call(c,a)),c},inArray:function(a,b,c){var d;if(b){if(g)return
g.call(b,a,c);for(d=b.length,c=c?0>c?Math.max(0,d+c):c:0;d>c;c++)if(c in b&&b[c]===a)return c}return-
1},merge:function(a,b){var c=+b.length,d=0,e=a.length;while(c>d)a[e++]=b[d++];if(c!==c)while(void
0!==b[d])a[e++]=b[d++];return a.length=e,a},grep:function(a,b,c){for(var d,e=
[],f=0,g=a.length,h=!c;g>f;f++)d=!b(a[f],f),d!==h&&e.push(a[f]);return e},map:function(a,b,c){var
d,f=0,g=a.length,h=r(a),i=[];if(h)for(;g>f;f++)d=b(a[f],f,c),null!=d&&i.push(d);else for(f in
a)d=b(a[f],f,c),null!=d&&i.push(d);return e.apply([],i)},guid:1,proxy:function(a,b){var
c,e,f;return"string"==typeof b&&(f=a[b],b=a,a=f),m.isFunction(a)?(c=d.call(arguments,2),e=function(){return
a.apply(b||this,c.concat(d.call(arguments)))},e.guid=a.guid=a.guid||m.guid++,e):void 0},now:function()
{return+new Date},support:k}),m.each("Boolean Number String Function Array Date RegExp Object Error".split("
"),function(a,b){h["[object "+b+"]"]=b.toLowerCase()});function r(a){var
b=a.length,c=m.type(a);return"function"===c||m.isWindow(a)?!1:1===a.nodeType&&b?!0:"array"===c||0===b||"numbe
r"==typeof b&&b>0&&b-1 in a}var s=function(a){var b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u="sizzle"+-new
Date,v=a.document,w=0,x=0,y=gb(),z=gb(),A=gb(),B=function(a,b){return a===b&&
(l=!0),0},C="undefined",D=1<<31,E={}.hasOwnProperty,F=
[],G=F.pop,H=F.push,I=F.push,J=F.slice,K=F.indexOf||function(a){for(var
b=0,c=this.length;c>b;b++)if(this[b]===a)return b;return-
1},L="checked|selected|async|autofocus|autoplay|controls|defer|disabled|hidden|ismap|loop|multiple|open|reado
nly|required|scoped",M="[\\x20\\t\\r\\n\\f]",N="(?:\\\\.|[\\w-]|[^\\x00-\\xa0])+",O=N.replace("...
```

http://127.0.0.1:8000/xmjg/resources/easyui/jquery.easyui.min.js

```
/**
 * jQuery EasyUI 1.4.2
 *
 * Copyright (c) 2009-2015 www.jeasyui.com. All rights reserved.
 *
 * Licensed under the GPL license: http://www.gnu.org/licenses/gpl.txt
 * To use it on other terms please contact us at info@jeasyui.com
 *
 */
(function($){
$.parser={auto:true,onComplete:function(_1){
},plugins:
["draggable","droppable","resizable","pagination","tooltip","linkbutton","menu","menubutton","splitbutton","p
rogressbar","tree","textbox","filebox","combo","combobox","combotree","combogrid","numberbox","validatebox","
searchbox","spinner","numberspinner","timespinner","datetimespinner","calendar","datebox","datetimebox","slid
er","layout","panel","datagrid","propertygrid","treegrid","datalist","tabs","accordion","window","dialog","fo
rm"],parse:function(_2){
var aa=[];
for(var i=0;i<$.parser.plugins.length;i++){
var _3=$.parser.plugins[i];
var r=$(".easyui-"+_3,_2);
if(r.length){
if(r[_3]){
r[_3]();
}else{
aa.push({name:_3,jq:r});
}
}
}
if(aa.length&&window.easyloader){
var _4=[];
for(var i=0;i<aa.length;i++){
_4.push(aa[i].name);
}
easyloader.load(_4,function(){
for(var i=0;i<aa.length;i++){
var _5=aa[i].name;
var jq=aa[i].jq;
jq[_5]();
}
$.parser.onComplete.call($.parser,_2);
});
}else{
$.parser.onComplete.call($.parser,_2);
}
},parseValue:function(_6,_7,_8,_9){
_9=_9||0;
var v=$.trim(String(_7||""));
var _a=v.substr(v.length-1,1);
if(_a=="%"){
v=parseInt(v.substr(0,v.length-1));
if(_6.toLowerCase().indexOf("width")>=0){
v=Math.floor((_8.width()-_9)*v/100);
}else{
v=Math.floor((_8.height()-_9)*v/100);
}
}else{
v=parseInt(v)||undefined;
}
return v;
},parseOptions:function(_b,_c){
var t=$(_b);
var _d={};
var s=$.trim(t.attr("data-options"));
if(s){
if(s.substring(0,1)!="{"){
s="{"+s+"}";
}
_d=(new Function("return "+s))();
}
$.map(["width","height","left","top","minWidth","maxWidth","minHeight","maxHeight"],function(p){
var pv=$.trim(_b.style[p]||"");
if(pv){
if(pv.indexOf("%")==-1){
pv=parseInt(pv)||undefined;
}
_d[p]=pv;
}
});
if(_c){
var _e={};
for(var i=0;i<_c.length;i++){
var pp=_c[i];
if(typeof pp=="string"){
_e[pp]=t.attr(pp);
}else{
for(var _f in pp){
var _10=pp[_f];
if(_10=="boolean"){
_e[_f]=t.attr(_f)?(t.attr(_f)=="true"):undefined;
}else{
if(_10=="number"){
_e[_f]=t.attr(_f)=="0"?0:parseFloat(t.attr(_f))||undefined;
}
}
}
}
}
$.extend(_d,_e);
}
return _d;
}};
$(function(){
var d=$("<div style=\"position:absolute;top:-1000px;width:100px;height:100px;padding:5px\">
</div>").appendTo("body");
$._boxModel=d.outerWidth()!=100;
d.remove();
if(!window.easyloader&&$.parser.auto){
$.parser.parse();
}
});
$.fn._outerWidth=function(_11){
if(_11==undefined){
if(this[0]==window){
return this.width()||document.body.clientWidth;
}
return this.outerWidth()||0;
}
return this._size("width",_11);
```

```
};
$.fn._outerHeight=function(_12){
if(_12==undefined){
if(this[0]==window){
return this.height()||document.body.clientHeight;
}
return this.outerHeight()||0;
}
return this._size("height",_12);
};
$.fn._scrollLeft=function(_13){
if(_13==undefined){
return this.scrollLeft();
}else{
return this.each(function(){
$(this).scrollLeft(_13);
});
}
};
$.fn._propAttr=$.fn.prop||$.fn.attr;
$.fn._size=function(_14,_15){
if(typeof _14=="string"){
if(_14=="clear"){
return this.each(function(){
$(this).css({width:"",minWidth:"",maxWidth:"",height:"",minHeight:"",maxHeight:""});
});
}else{
if(_14=="fit"){
return this.each(function(){
_16(this,this.tagName=="BODY"?$("body"):$(this).parent(),true);
});
}else{
if(_14=="unfit"){
return this.each(function(){
_16(this,$(this).parent(),false);
});
}else{
if(_15==undefined){
return _17(this[0],_14);
}else{
return this.each(function(){
_17(this,_14,_15);
});
}
}
}
}
}else{
return this.each(function(){
_15=_15||$(this).parent();
$.extend(_14,_16(this,_15,_14.fit)||{});
var r1=_18(this,"width",_15,_14);
var r2=_18(this,"height",_15,_14);
if(r1||r2){
$(this).addClass("easyui-fluid");
}else{
$(this).removeClass("easyui-fluid");
}
});
}
function _16(_19,_1a,fit){
if(!_1a.length){
return false;
}
var t=$(_19)[0];
var p=_1a[0];
var _1b=p.fcount||0;
if(fit){
if(!t.fitted){
t.fitted=true;
p.fcount=_1b+1;
$(p).addClass("panel-noscroll");
if(p.tagName=="BODY"){
$("html").addClass("panel-fit");
}
}
return {width:($(p).width()||1),height:($(p).height()||1)};
}else{
```

```
if(t.fitted){
t.fitted=false;
p.fcount=_1b-1;
if(p.fcount==0){
$(p).removeClass("panel-noscroll");
if(p.tagName=="BODY"){
$("html").removeClass("panel-fit");
}
}
}
return false;
}
};
function _18(_1c,_1d,_1e,_1f){
var t=$(_1c);
var p=_1d;
var p1=p.substr(0,1).toUpperCase()+p.substr(1);
var min=$.parser.parseValue("min"+p1,_1f["min"+p1],_1e);
var max=$.parser.parseValue("max"+p1,_1f["max"+p1],_1e);
var val=$.parser.parseValue(p,_1f[p],_1e);
var _20=(String(_1f[p]||"").indexOf("%")>=0?true:false);
if(!isNaN(val)){
var v=Math.min(Math.max(...
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
    var ctx= "/xmjg/";    var xzqhdm="660100";    var flag = "1";    var oldStartDate = "2020-01-01";    var
oldEndDate = "2020-12-29";    var province="";    var city="660100";    var name="一师阿拉尔市";    var
defaultEndDate="",defaultStartDate="";    var bigScreenFolder="";    var provinceCode = "";    var OrgName =
"管理员";    var districtAdminFlag = "1";    var initHeartBeat = "";    //是否是省级用户、管理员用户var
isAdminUser = "true";var isProvinceUser = "false";    var initStartDate="2018-06-01";//获取配置文件中统计时间的配
置参数var sfType="";//算法类型
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
//一张蓝图切换    /* $('.full-screen-btn').click(function(e) {
$(this).toggleClass('active');$('#blueprint').toggleClass('active');    }); */$(function () {
doInit();          //城市登陆 不显示返回按钮          if(OrgName == "师市" || districtAdminFlag =="2"){
$("#city-screen-back-btn").hide();          }          var date = new Date();          var dateStr =
date.getFullYear() + "-" + ("0" + (date.getMonth() + 1)).slice(-2) + "-"+ ("0" + (date.getDate())).slice(-2);
var startTime = dateStr.substr(0,5)+"01-01";          var endDateStr = dateStr;          //开始时间初始化
$('#dateStart').datepicker({          autoclose : true, //自动关闭          beforeShowDay : $.noop, //在显示日期
之前调用的函数          calendarWeeks : false, //是否显示今年是第几周          clearBtn : false, //显示清除按钮
daysOfWeekDisabled : [], //星期几不可选          forceParse : true, //是否强制转换不符合格式的字符串          format
: 'yyyy-mm-dd', //日期格式          keyboardNavigation : true, //是否显示箭头导航          language : 'zh-CN', //
语言          minViewMode : 0,          orientation : "auto", //方向          rtl : false,
//startDate : -Infinity, //日历开始日期          startDate :"2018-06-01",          endDate:dateStr,
startView : 0, //开始显示          todayBtn : false, //今天按钮          todayHighlight : true, //今天高亮
weekStart : 0          //星期几是开始          }).on('changeDate', function(e) {          var start =
$("#dateStart").val();          $('.js-endTime').datepicker('setStartDate', new Date(start));          });
//结束时间初始化          $('#dateEnd').datepicker({          autoclose : true, //自动关闭
beforeShowDay : $.noop, //在显示日期之前调用的函数          calendarWeeks : false, //是否显示今年是第几周
clearBtn : false, //显示清除按钮          daysOfWeekDisabled : [], //星期几不可选          forceParse : true, //
是否强制转换不符合格式的字符串          format : 'yyyy-mm-dd', //日期格式          keyboardNavigation : true, //是否
显示箭头导航          language : 'zh-CN', //语言          minViewMode : 0,          orientation : "auto", //方向
rtl : false,          //startDate : -Infinity, //日历开始日期          startDate :startTime,
endDate:"2099-12-31",          startView : 0, //开始显示          todayBtn : false, //今天按钮
todayHighlight : true, //今天高亮          weekStart : 0          }).on('changeDate',function(e){          var
end = $("#dateEnd").val();          $('.js-startTime').datepicker('setEndDate', new Date(end));
});//tab栏$('.stage-tab-tit a').unbind('click').click(function(e) {var selfIndex =
$(this).index()$(this).addClass('active').siblings().removeClass('active');$(this).parent().siblings().childr
en('div:eq(' + selfIndex + ')').addClass('active').siblings().removeClass('active');/*if($(this).text()=="逾
期项目数"){$("#jdyqxmzs").css('color','#ff3333');$("#jdyqxms li p b ").css('color','#ff3333');}*/var texxt =
$(this).text();if( texxt =='审批用时'){scrollEl('pjys');} else if(texxt =='跨度用时'){scrollEl('kdys');} else
if(texxt =='最长用时'){scrollEl('zcys');}//最长用时去掉平均字样if(texxt == "最长用时")
{$(this).parent().parent().find('div').eq(0).html("最长用时(天)");}else if(texxt == "审批用时" || texxt == "跨度
用时"){$(this).parent().parent().find('div').eq(0).html("平均用时(天)");}});$(".systems-list
li").mouseover(function(){$(this).children().children("span").addClass("on");});$(".systems-list
```

```
li").mouseout(function(){$(this).children().children("span").removeClass("on");})$(".systems-
top").mouseover(function(){$(this).children().children("span").addClass("on");});$(".systems-
top").mouseout(function(){$(this).children().children("span").removeClass("on");});//查询按钮点击事件
$("#ts_search").click(function(){timeSearch();});//重置按钮$("#timeReset").click(function()
{$('#dateStart').val(startTime);$('#dateEnd').val(endDateStr);$(".loading").show();//一秒后消失loading图标
setTimeout(function ()
{$(".loading").hide()},1000);//$("#loading").css('display','block');setTimeout("timeSearch()",5);});
});          var app = new Vue({          el: '#cityPage',          data: {          showone:false,
showtwo:false,          showthd:false,          showFour:false,dialogVisible:false,          dateRangeValue:
[],          },methods:{confirmedInfo: function () {var _that = this;$.ajax({url: ctx +
"/monitorEarlyWarning/earlyWarningRecord/noticeToConfirm.do",data: "",async: true,type : "get", // 数据发送方式
dataType : "json", // 接受数据格式success : function(data) {if (data.length>0)
{_that.dialogVisible=true;}if(data){indexObjArr = new ...
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
void(0);
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
intoOneSystem();
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
intoYgck();
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
intoYzbd();
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
intoYtjz();
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
acceptedItems('11','1','660100','','','','','','','')
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
acceptedItems('13','1','660100','','','','','1','','')
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
toStageProjectListPage('1','5')
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
toStageProjectListPage('12','5')
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
toStageProjectListPage('2','5')
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
toStageProjectListPage('4','1')
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
toStageProjectListPage('4','2')
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
toStageProjectListPage('4','3')
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
toStageProjectListPage('4','4')
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
toStageProjectListPage('4','5')
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
changeDavescrollTop('glxxm-pjys-data11','city-index-table1',false)
```

http://127.0.0.1:8000/xmjg/city-page/getCsrk.action

```
changeDavescrollTop('glxxm-pjys-data11','city-index-table1',true)
```

http://127.0.0.1:8000/xmjg/xmjg/xndc/js/bootstrap-datepicker.zh-CN.min.js

```
!function(a){a.fn.datepicker.dates["zh-CN"]={
    days:["星期日","星期一","星期二","星期三","星期四","星期五","星期六"],
    daysShort:["周日","周一","周二","周三","周四","周五","周六"],
    daysMin:["日","一","二","三","四","五","六"],months:["一月","二月","三月","四月","五月","六月","七月","八月","九
月","十月","十一月","十二月"],monthsShort:["1月","2月","3月","4月","5月","6月","7月","8月","9月","10月","11月","12
月"],today:"今日",clear:"清除",format:"yyyy年mm月dd日",titleFormat:"yyyy年mm月",weekStart:1}}(jQuery);
```

http://127.0.0.1:8000/xmjg/xmjg/xndc/js/bootstrap-datepicker.min.js

```
/*!
 * Datepicker for Bootstrap v1.6.4 (https://github.com/eternicode/bootstrap-datepicker)
 *
 * Copyright 2012 Stefan Petre
 * Improvements by Andrew Rowls
 * Licensed under the Apache License v2.0 (http://www.apache.org/licenses/LICENSE-2.0)
 */
!function(a){"function"==typeof define&&define.amd?define(["jquery"],a):a("object"==typeof exports?
require("jquery"):jQuery)}(function(a,b){function c(){return new
Date(Date.UTC.apply(Date,arguments))}function d(){var a=new Date;return
c(a.getFullYear(),a.getMonth(),a.getDate())}function e(a,b){return
a.getUTCFullYear()===b.getUTCFullYear()&&a.getUTCMonth()===b.getUTCMonth()&&a.getUTCDate()===b.getUTCDate()}f
unction f(a){return function(){return this[a].apply(this,arguments)}}function g(a){return
a&&!isNaN(a.getTime())}function h(b,c){function d(a,b){return b.toLowerCase()}var e,f=a(b).data(),g={},h=new
RegExp("^"+c.toLowerCase()+"([A-Z])");c=new RegExp("^"+c.toLowerCase());for(var i in f)c.test(i)&&
(e=i.replace(h,d),g[e]=f[i]);return g}function i(b){var c={};if(q[b]||(b=b.split("-")[0],q[b])){var
d=q[b];return a.each(p,function(a,b){b in d&&(c[b]=d[b])}),c}}var j=function(){var b={get:function(a){return
this.slice(a)[0]},contains:function(a){for(var
b=a&&a.valueOf(),c=0,d=this.length;d>c;c++)if(this[c].valueOf()===b)return c;return-1},remove:function(a)
{this.splice(a,1)},replace:function(b){b&&(a.isArray(b)||(b=
[b]),this.clear(),this.push.apply(this,b))},clear:function(){this.length=0},copy:function(){var a=new
j;return a.replace(this),a}};return function(){var c=[];return c.push.apply(c,arguments),a.extend(c,b),c}}
(),k=function(b,c){a(b).data("datepicker",this),this._process_options(c),this.dates=new
j,this.viewDate=this.o.defaultViewDate,this.focusDate=null,this.element=a(b),this.isInput=this.element.is("in
put"),this.inputField=this.isInput?
this.element:this.element.find("input"),this.component=this.element.hasClass("date")?this.element.find(".add-
on, .input-group-addon,
.btn"):!1,this.hasInput=this.component&&this.inputField.length,this.component&&0===this.component.length&&
(this.component=!1),this.isInline=!this.component&&this.element.is("div"),this.picker=a(r.template),this._che
ck_template(this.o.templates.leftArrow)&&this.picker.find(".prev").html(this.o.templates.leftArrow),this._che
ck_template(this.o.templates.rightArrow)&&this.picker.find(".next").html(this.o.templates.rightArrow),this._b
uildEvents(),this._attachEvents(),this.isInline?this.picker.addClass("datepicker-
inline").appendTo(this.element):this.picker.addClass("datepicker-dropdown dropdown-
menu"),this.o.rtl&&this.picker.addClass("datepicker-
rtl"),this.viewMode=this.o.startView,this.o.calendarWeeks&&this.picker.find("thead .datepicker-title, tfoot
.today, tfoot .clear").attr("colspan",function(a,b){return
parseInt(b)+1}),this._allow_update=!1,this.setStartDate(this._o.startDate),this.setEndDate(this._o.endDate),t
his.setDaysOfWeekDisabled(this.o.daysOfWeekDisabled),this.setDaysOfWeekHighlighted(this.o.daysOfWeekHighlight
ed),this.setDatesDisabled(this.o.datesDisabled),this.fillDow(),this.fillMonths(),this._allow_update=!0,this.u
pdate(),this.showMode(),this.isInline&&this.show()};k.prototype={constructor:k,_resolveViewName:function(a,c)
{return 0===a||"days"===a||"month"===a?0:1===a||"months"===a||"year"===a?1:2===a||"years"===a||"decade"===a?
2:3===a||"decades"===a||"century"===a?3:4===a||"centuries"===a||"millennium"===a?
4:c===b?!1:c},_check_template:function(c){try{if(c===b||""===c)return!1;if((c.match(/[<>]/g)||
[]).length<=0)return!0;var d=a(c);return d.length>0}catch(e){return!1}},_process_options:function(b)
{this._o=a.extend({},this._o,b);var e=this.o=a.extend({},this._o),f=e.language;q[f]||(f=f.split("-")
[0],q[f]||
(f=o.language)),e.language=f,e.startView=this._resolveViewName(e.startView,0),e.minViewMode=this._resolveView
```

```
Name(e.minViewMode,0),e.maxViewMode=this._resolveViewName(e.maxViewMode,4),e.startView=Math.min(e.startView,e
.maxViewMode),e.startView=Math.max(e.startView,e.minViewMode),e.multidate!==!0&&
(e.multidate=Number(e.multidate)||!1,e.multidate!==!1&&
(e.multidate=Math.max(0,e.multidate))),e.multidateSeparator=String(e.multidateSeparator),e.weekStart%=7,e.wee
kEnd=(e.weekStart+6)%7;var g=r.parseFormat(e.format);e.startDate!==-(1/0)&&(e.startDate?e.startDate
instanceof Date?
e.startDate=this._local_to_utc(this._zero_time(e.startDate)):e.startDate=r.parseDate(e.startDate,g,e.language
,e.assumeNearbyYear):e.startDate=-(1/0)),e.endDate!==1/0&&(e.endDate?e.endDate instanceof Date?
e.endDate=this._local_to_utc(this._zero_time(e.endDate)):e.endDate=r.parseDate(e.endDate,g,e.language,e.assum
eNearbyYear):e.endDate=1/0),e.daysOfWeekDisabled=e.daysOfWeekDisabled||[],a.isArray(e.daysOfWeekDisabled)||
(e.daysOfWeekDisabled=e.daysOfWeekDisabled.split(/[,\s]*/)),e.daysOfWeekDisabled=a.map(e.daysOfWeekDisabled,f
unction(a){return parseInt(a,10)}),e.daysOfWeekHighlighted=e.daysOfWeekHighlighted||
[],a.isArray(e.daysOfWeekHighlighted)||(e.daysOfWeekHighlighted=e.daysOfWeekHighlighted.split(/[,\s]*/)),...
```

http://127.0.0.1:8000/xmjg/region/vue.js

```
/*!
 * Vue.js v2.6.10
 * (c) 2014-2019 Evan You
 * Released under the MIT License.
 */
(function (global, factory) {
    typeof exports === 'object' && typeof module !== 'undefined' ? module.exports = factory() :
        typeof define === 'function' && define.amd ? define(factory) :
          (global = global || self, global.Vue = factory());
}(this, function () { 'use strict';

    /*  */

    var emptyObject = Object.freeze({});

    // These helpers produce better VM code in JS engines due to their
    // explicitness and function inlining.
    function isUndef (v) {
        return v === undefined || v === null
    }

    function isDef (v) {
        return v !== undefined && v !== null
    }

    function isTrue (v) {
        return v === true
    }

    function isFalse (v) {
        return v === false
    }

    /**
     * Check if value is primitive.
     */
    function isPrimitive (value) {
        return (
          typeof value === 'string' ||
          typeof value === 'number' ||
          // $flow-disable-line
          typeof value === 'symbol' ||
          typeof value === 'boolean'
        )
    }

    /**
     * Quick object check - this is primarily used to tell
     * Objects from primitive values when we know the value
     * is a JSON-compliant type.
     */
    function isObject (obj) {
        return obj !== null && typeof obj === 'object'
    }

    /**
     * Get the raw type string of a value, e.g., [object Object].
     */
    var _toString = Object.prototype.toString;

    function toRawType (value) {
        return _toString.call(value).slice(8, -1)
    }

    /**
     * Strict object type check. Only returns true
     * for plain JavaScript objects.
     */
    function isPlainObject (obj) {
        return _toString.call(obj) === '[object Object]'
    }

    function isRegExp (v) {
        return _toString.call(v) === '[object RegExp]'
    }

    /**
     * Check if val is a valid array index.
     */
    function isValidArrayIndex (val) {
        var n = parseFloat(String(val));
        return n >= 0 && Math.floor(n) === n && isFinite(val)
    }

    function isPromise (val) {
        return (
          isDef(val) &&
          typeof val.then === 'function' &&
          typeof val.catch === 'function'
        )
    }

    /**
     * Convert a value to a string that is actually rendered.
     */
    function toString (val) {
        return val == null
          ? ''
          : Array.isArray(val) || (isPlainObject(val) && val.toString === _toString)
          ? JSON.stringify(val, null, 2)
          : String(val)
    }

    /**
     * Convert an input value to a number for persistence.
     * If the conversion fails, return original string.
     */
    function toNumber (val) {
        var n = parseFloat(val);
        return isNaN(n) ? val : n
    }

    /**
     * Make a map and return a function for checking if a key
     * is in that map.
     */
    function makeMap (
        str,
        expectsLowerCase
    ) {
        var map = Object.create(null);
        var list = str.split(',');
        for (var i = 0; i < list.length; i++) {
          map[list[i]] = true;
        }
        return expectsLowerCase
          ? function (val) { return map[val.toLowerCase()]; }
          : function (val) { return map[val]; }
    }

    /**
     * Check if a tag is a built-in tag.
     */
    var isBuiltInTag = makeMap('slot,component', true);
```

```
    /**
     * Check if an attribute is a reserved attribute.
     */
    var isReservedAttribute = makeMap('key,ref,slot,slot-scope,is');

    /**
     * Remove an item from an array.
     */
    function remove (arr, item) {
        if (arr.length) {
          var index = arr.indexOf(item);
          if (index > -1) {
          return arr.splice(index, 1)
          }
        }
    }

    /**
     * Check whether an object has the property.
     */
    var hasOwnProperty = Object.prototype.hasOwnProperty;
    function hasOwn (obj, key) {
        return hasOwnProperty.call(obj, key)
    }

    /**
     * Create a cached version of a pure function.
     */
    function cached (fn) {
        var cache = Object.create(null);
        return (function cachedFn (str) {
          var hit = cache[str];
          return hit || (cache[str] = fn(str))
        })
    }

    /**
     * Camelize a hyphen-delimited string.
     */
    var camelizeRE = /-(\w)/g;
    var camelize = cached(function (str) {
        return str.replace(camelizeRE, function (_, c) { return c ? c.toUpperCase() : ''; })
    });

    /**
     * Capitalize a string.
     */
    var capitalize = cached(function (str) {
        return str.charAt(0).toUpperCase() + str.slice(1)
    });

    /**
     * Hyphenate a camelCase string.
     */
    var hyph...
```

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-table-zh-CN.js

```
/**
 * Bootstrap Table Chinese translation
 * Author: Zhixin Wen<wenzhixin2010@gmail.com>
 */
(function ($) {
    'use strict';

    $.fn.bootstrapTable.locales['zh-CN'] = {
        formatLoadingMessage: function () {
          return '正在加载,请稍候……';
        },
        formatRecordsPerPage: function (pageNumber) {
          return '每页显示 ' + pageNumber + ' 条记录';
        },
        formatShowingRows: function (pageFrom, pageTo, totalRows) {
          return '显示第 ' + pageFrom + ' 到第 ' + pageTo + ' 条记录，总共 ' + totalRows + ' 条记录';
        },
        formatSearch: function () {
          return '搜索';
        },
        formatNoMatches: function () {
          return '没有找到匹配的记录';
        },
        formatPaginationSwitch: function () {
          return '隐藏/显示分页';
        },
        formatRefresh: function () {
          return '刷新';
        },
        formatToggle: function () {
          return '切换';
        },
        formatColumns: function () {
          return '列';
        }
    };

    $.extend($.fn.bootstrapTable.defaults, $.fn.bootstrapTable.locales['zh-CN']);

})(jQuery);
```

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/city-page.js

```
var common_stages="立项用地规划许可,工程建设许可,施工许可,竣工验收,并行推进".split(",");
var OLD_DATA_OBJ=null,OLD_DATA_OBJ1=null;
var heartBeatParams={};
var checkDataFalg=0; // 0:心跳未启动，1:心跳方法正在执行，2:正在等待下次心跳执行
var checkDataval=null;
var currDateStr=null;
var currDate=null;
var myChart;
var tjfs="xmsl";  //地图统计切换
var visualMapShowOrClose = false;//色列显示控制 false：为不显示 true为显示
var myBackBtnTitle ="开启";//灯泡提示 鼠标hover显示文字
var scrollId = {}; //平均用时滚动id
var scrollData = '';//平均用时数据
var bxtj;
var toolboxIcon ='path://M512 841.142857C204.8 841.142857 21.942857 541.257143 14.628571 533.942857L0
512l14.628571-21.942857C21.942857 475.428571 204.8 182.857143 512 182.857143s490.057143 299.885714 497.371429
307.2l14.628571 21.942857-14.628571 21.942857c-7.314286 7.314286-190.171429 307.2-497.371429 307.2zM87.771429
512c43.885714 58.514286 197.485714 256 424.228571 256s380.342857-197.485714 424.228571-256c-43.885714-
58.514286-197.485714-256-424.228571-256S131.657143 453.485714 87.771429 512z,'+
'path://M512 694.857143C409.6 694.857143 329.142857 614.4 329.142857 512S409.6 329.142857 512 329.142857
694.857143 409.6 694.857143 512 614.4 694.857143 512 694.857143z m0-292.571429c-58.514286 0-109.714286 51.2-
109.714286 109.714286S453.485714 621.714286 512 621.714286 621.714286 570.514286 621.714286 512 570.514286
402.285714 512 402.285714z';
Date.prototype.format = function(fmt) {
    var o = {
        "M+" : this.getMonth()+1,          //月份
        "d+" : this.getDate(),          //日
        "h+" : this.getHours(),          //小时
        "m+" : this.getMinutes(),          //分
        "s+" : this.getSeconds(),          //秒
        "q+" : Math.floor((this.getMonth()+3)/3), //季度
        "S"  : this.getMilliseconds()          //毫秒
    };
    if(/(y+)/.test(fmt)) {
        fmt=fmt.replace(RegExp.$1, (this.getFullYear()+"").substr(4 - RegExp.$1.length));
    }
    for(var k in o) {
        if(new RegExp("("+ k +")").test(fmt)){
          fmt = fmt.replace(RegExp.$1, (RegExp.$1.length==1) ? (o[k]) : (("00"+ o[k]).substr((""+
o[k]).length)));
        }
    }
    return fmt;
}
```

```
/**
 * 初始化
 * @returns
 */
function doInit(){
 //        初始化查询时间控件
 initSearchDate();
 //        初始化城市选择
 initCitySelect();
 defaultEndDate=currDateStr;
 //       获取配置的 开始时间 为空 取 2018-06-01
    var date = new Date();
    var nowDate='';
    var nowYearStart = date.getFullYear() + "-01-01";
    //设置默认选项
    $("#dropdown-menu-li").append('<li class="divider"></li>');
    $("#dropdown-menu-li").append('<li><a href="#" class="js-timeOne" data-startdate="nowYearStart"' +
        'data-enddate="nowDate">' + new Date(nowYearStart).format("yyyy年MM月dd日") +'-至今（本年度）</a>
</li>');
    $("#dropdown-menu-li").append('<li class="divider"></li>');
    $("#dropdown-menu-li").append('<li><a href="#" class="js-timeOne" data-startdate="initStartDate"' +
        'data-enddate="nowDate">' + new Date(initStartDate).format("yyyy年MM月dd日") +'-至今</a></li>');
    $.ajax({
        url :ctx + '/bsc/dic/code/lgetItemsByTypeCode.do',
        type : "get",
        data : {
          typeCode : "TJ_DATE_CONFIG",
          flag : false,
        },
        dataType : "json",
        async : false,
        success : function(result) {
          if(result && result.length > 0){
          $("#dropdown-menu-li .divider").remove();
          $("#dropdown-menu-li .js-timeOne").remove();
          for(var i = 0 ; i < result.length ; i ++){
          var values = result[i].value.split("&");
          if(values.length == 2){
          if(values[0] == "initStartDate" || values[0] == "nowDate" || values[0] == "nowYearStart"){
          values[0] = eval(values[0]);
          }
          if(values[1] == "initStartDate" || values[1] == "nowDate" || values[1] == "nowYearStart"){
          values[1] = eval(values[1]);
          }
          result[i].label = result[i].label.replace("nowYearStart",new Date(nowYearStart).format("yyyy年MM月
dd日"))
          result[i].label = result[i].label.replace("nowDate",date.format("yyyy年MM月dd日"))
          result[i].label = result[i].label.replace("initStartDate",new Date(initStartDate).format("yyyy年MM
月dd日"))
          $("#dropdown-menu-li").append('<li class="divider"></li>');
          $("#dropdown-menu-li").append('<li><a href="#" class="js-timeOne" data-startdate="' + values[0] +'"
' +
          'data-enddate="' + values[1] + '">' + result[i].label +'</a></li>');
          }

          }
          $('.js-timeOne').click(function(){
          var startDate = $(this).data("startdate");
          var enddate = $(this).data("enddate");
          spreadTimeSearch(startDate,enddate)
          });
          }else{
  ...
```

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-table.js

```
/**
 * @author zhixin wen <wenzhixin2010@gmail.com>
 * version: 1.9.0
 * https://github.com/wenzhixin/bootstrap-table/
 */

!function ($) {
    'use strict';

    // TOOLS DEFINITION
    // ======================

    var cachedWidth = null;

    // it only does '%s', and return '' when arguments are undefined
    var sprintf = function (str) {
        var args = arguments,
          flag = true,
          i = 1;

        str = str.replace(/%s/g, function () {
          var arg = args[i++];

          if (typeof arg === 'undefined') {
          flag = false;
          return '';
          }
          return arg;
        });
        return flag ? str : '';
    };

    var getPropertyFromOther = function (list, from, to, value) {
        var result = '';
        $.each(list, function (i, item) {
          if (item[from] === value) {
          result = item[to];
          return false;
          }
          return true;
        });
        return result;
    };

    var getFieldIndex = function (columns, field) {
        var index = -1;

        $.each(columns, function (i, column) {
          if (column.field === field) {
          index = i;
          return false;
          }
          return true;
        });
        return index;
    };

    // http://jsfiddle.net/wenyi/47nz7ez9/3/
    var setFieldIndex = function (columns) {
        var i, j, k,
          totalCol = 0,
          flag = [];

        for (i = 0; i < columns[0].length; i++) {
          totalCol += columns[0][i].colspan || 1;
        }

        for (i = 0; i < columns.length; i++) {
          flag[i] = [];
          for (j = 0; j < totalCol; j++) {
          flag[i][j] = false;
          }
        }

        for (i = 0; i < columns.length; i++) {
          for (j = 0; j < columns[i].length; j++) {
          var r = columns[i][j],
          rowspan = r.rowspan || 1,
          colspan = r.colspan || 1,
          index = $.inArray(false, flag[i]);

          if (colspan === 1) {
          r.fieldIndex = index;
          // when field is undefined, use index instead
          if (typeof r.field === 'undefined') {
```

```
          r.field = index;
          }
          }

          for (k = 0; k < rowspan; k++) {
          flag[i + k][index] = true;
          }
          for (k = 0; k < colspan; k++) {
          flag[i][index + k] = true;
          }
          }
        }
    };

    var getScrollBarWidth = function () {
        if (cachedWidth === null) {
          var inner = $('<p/>').addClass('fixed-table-scroll-inner'),
          outer = $('<div/>').addClass('fixed-table-scroll-outer'),
          w1, w2;

          outer.append(inner);
          $('body').append(outer);

          w1 = inner[0].offsetWidth;
          outer.css('overflow', 'scroll');
          w2 = inner[0].offsetWidth;

          if (w1 === w2) {
          w2 = outer[0].clientWidth;
          }

          outer.remove();
          cachedWidth = w1 - w2;
        }
        return cachedWidth;
    };

    var calculateObjectValue = function (self, name, args, defaultValue) {
        var func = name;

        if (typeof name === 'string') {
          // support obj.func1.func2
          var names = name.split('.');

          if (names.length > 1) {
          func = window;
          $.each(names, function (i, f) {
          func = func[f];
          });
          } else {
          func = window[name];
          }
        }
        if (typeof func === 'object') {
          return func;
        }
        if (typeof func === 'function') {
          return func.apply(self, args);
        }
        if (!func && typeof name === 'string' && sprintf.apply(this, [name].concat(args))) {
          return sprintf.apply(this, [name].concat(args));
        }
        return defaultValue;
    };

    var compareObjects = function (objectA, objectB, compareLength) {
        // Create arrays of property names
        var objectAProperties = Object.getOwnPropertyNames(objectA),
          objectBProperties = Object.getOwnPropertyNames(objectB),
          propName = '';

        if (compareLength) {
          // If number of properties is different, objects are not equivalent
          if (objectAProperties.length !== objectBProperties.length) {
          return false;
          }
        }
        for (var i = 0; i < objectAProperties.length; i++) {
          propName = objectAProperties[i];

          // If the property is not in the object B properties, continue with the next property
          if ($.inAr...
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
          var ctx='/xmjg/';var bigScreenFolder="";var xzqhdms="";var tjkssj="2020-01-01";var tjjssj="2020-12-
29";var orderByFlag="";var dataType="12";var sfzb="";var sfbyxz="";var sfjgqqxt="";var spjd="";var
blqk="";var splclx="";var splcmc="";var sfyq="";var tjTypeVal="";var qtTypeVal = "";var splcbm="";var dateEnd
= "2020-12-29";var provinceCode="";var dataType="12";  //1:各阶段平均用时（审批用时）; 2:各阶段跨度用时; 3:各阶段最长
用时; 4:各阶段平均受理次数;var stageType="0"; //0：总数，1：立项用地规划许可；2：工程建设许可；3：施工许可；4：竣工验收
var oldStartDate = "2020-01-01";          var oldEndDate = "2020-12-29";          var flag="2";          var
xzqhdm="660100"; //跳转带过来的行政区划代码 用于钻取标题显示          var name="一师阿拉尔市";//跳转带过来的城市名称 用于
钻取标题显示var sfType = "";//算法类型
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
        function newsearch(){        var i=document.getElementById("pageSize").value;       var
n=document.getElementById("pageNo").value;       var m="160";        if(m<i){
document.getElementById("pageNo").value=1;         search();        }else{        var u=Math.ceil(m/i)
if(n>u){        $.messager.alert('提示','页数超出限制');        }else{        search();        }        }
}        $(function(){          $('#pageNo').bind('keypress', function (event) {          if (event.keyCode
== "13") {          //需要处理的事情var pageNo = $(this).val();          pageNo = parseInt(pageNo);
var pages = $(this).data('pages');    //最大页码          if(pageNo < 1) {          pageNo = 1;          }
if(pageNo > pages){          pageNo = pages;          }          jumpPage(pageNo);   //跳转页面          }
});        });
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
jumpPage(16)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660100,'2020-659002-48-01-000022')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660100,'2019-659002-46-01-008189')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660100,'2019-659002-45-03-008271')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660100,'2020-659002-50-01-012203')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660100,'2019-659002-78-01-003968')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660100,'2020-659002-47-01-013581')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660100,'2020-659002-59-03-011516')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660100,'2020-659002-70-03-011405')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660100,'2019-659002-94-01-009280')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660100,'2020-659002-78-01-010429')
```

http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do

```
var ctx='/xmjg/';var bigScreenFolder="";var tjkssj="2020-01-01";var tjjssj="2020-12-29";var dateEnd = "2020-
12-29";var provinceCode="660000";var dataType="5";  //1:各城市各阶段平均用时（审批用时）; 2:各城市各阶段跨度用时; 3:各
城市各阶段最长用时; 4:各城市各阶段平均受理次数;5:本月新增项目数var stageType="0"; //0：总数，1：立项用地规划许可；2：工程建
设许可；3：施工许可；4：竣工验收var splclx="";var splcmc="";var sfType="";//算法类型
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
        //用于子页面排序的变量        var orderClickName = "";        var orderClickCount = 0;        var
orderNameId;        var ctx = '/xmjg/';        var oldStartDate = "2020-01-01";        var oldEndDate =
"2020-12-29";        var bigScreenFolder=""; //大屏css 目录，如果是普通屏（默认）则该值为空        var
defaultSelect ="${currentCityName}";        var dqcs="660100";        var xzqhdm = "660100";        var name
= decodeURIComponent("%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82");        var xmlx="";
var djzt="";//该状态位默认为2，正在办理  ，  -1: 代表正在使用及时率、超期率的统计        var pm_count = ""; //统计排名状
态, 1:  及时率、2: 超期率        var dqspjd = "";        var splclxData ;        var provinceCode = "";
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
spreadTimeSearch('2019-01-01')
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
spreadTimeSearch('2018-06-01')
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
showOpenhistoryFj()
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
shuJuJiCha(this)
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
showProInfo_img('zt1','正常件','','2');namechange('正常件');
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
showProInfo_img('zt3','异常件','','5');namechange('异常件');
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
showProInfo_img('zt4','不予受理退件','','9');namechange('不予受理退件');
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
showProInfo_img('zt5','过程督察','','10');namechange('过程督察');
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
javascript:showProInfo1('pm1',ctx+'xmjg-project-info!topmjsl.action?endtype=1','工程建设项目审批办结及时率排
名');Tjpmchange('工程建设项目审批办结及时率排名');
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
javascript:showProInfo2('pm2',ctx+'xmjg-project-info!topmjsl.action?endtype=2','工程建设项目审批超期率排
名');Tjpmchange('工程建设项目审批超期率排名');
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
closeMap()
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
backPrePage()
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
changeToMap()
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
changeToMap(1)
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
changeTab('0')
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
showProInfo_xmlx('','备案类');
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
submitSearch()
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
toClearForm()
```

http://127.0.0.1:8000/xmjg/csrk/oneSystemByMd.do

```
toHighSearch()
```

http://127.0.0.1:8000/xmjg/xmjg/xndc/js/dg-md-xndc-main.js

```
var date = new Date();
var currDateStr =date.Format('yyyy-MM-dd')
var defaultEnd = getDefaultEnd();
//获取本月的下一个月
var dateStr = date.getFullYear() + "-" + ("0" + (date.getMonth() + 1)).slice(-2) + "-"+ ("0" +
(date.getDate())).slice(-2);
var from = "";
var radius = [25,40];
var labelBottom = {
    normal : {
        color: '#aaa',
        label : {
          show : true,
          position : 'top'
        },
        labelLine : {
          show : false
        }
    },
    emphasis: {
        color: 'rgba(0,0,0,0)'
    }
};

$(function(){
    $("#cityName").text(decodeURI(name));
    getSxlx();
    $('#dateSelect').datepicker({
        autoclose : true, //自动关闭
        calendarWeeks : false, //是否显示今年是第几周
        clearBtn : false, //显示清除按钮
        daysOfWeekDisabled : [], //星期几不可选
        forceParse : true, //是否强制转换不符合格式的字符串
        format : 'yyyy-mm-dd', //日期格式
        keyboardNavigation : true, //是否显示箭头导航
        language : 'zh-CN', //语言
        startView: 'months', //开始视图层，为月视图层
        maxViewMode:'years', //最大视图层，为年视图层
        minViewMode:'months', //最小视图层，为月视图层startView: 'months', //开始视图层，为月视图层
        orientation : "auto", //方向
        rtl : false,
        //startDate : -Infinity, //日历开始日期
        startDate :"2018-06-01",
        endDate : dateStr, //日历结束日期
        todayBtn : false, //今天按钮
        todayHighlight : true, //今天高亮
        weekStart : 0
        //星期几是开始
    }).on('changeDate', function(ev){
        //$("#dateStart").val($("#dateStart").val().substring(0,4)+"-
"+$("#dateStart").val().substring(5,7)+"-01");
        $("#dateStart").datepicker('update',ev.date);
        $("#showDateStart").text($("#dateStart").val());

        if(getMonthEnd()==defaultEnd){
          $('#dateEnd').val(dateStr);
        }else{
          $('#dateEnd').val(getMonthEnd());
        }
        $("#showDateEnd").text($("#dateEnd").val());
/*        if($("#dateStart").val()=="2018-06-01"||$("#dateStart").val()=="2019-01-01"){
          //alert("dddddd");
          initEndDatepicker();
        }else{
          $('#dateEnd').datepicker("destroy");
        }*/
        $("#dropdown-switchDate").attr("class","dropdown");
        if("-1" == djzt){   //统计及时率、超期率
          if("1" == pm_count){
          showProInfo1('pm1',ctx+'xmjg-project-info!topmjsl.action?endtype=1','工程建设项目审批办结及时率排名');
          } else {
          showProInfo2('pm2',ctx+'xmjg-project-info!topmjsl.action?endtype=2','工程建设项目审批超期率排名');
          }
          return;
        }
        dqCs();
        dqCs2();
    });


    /**
     * 初始化时间控件下拉列表
     */
   /* var dateList = getStatisticalTimeInterval();
    var html='';
    for (var i = 0;i<=dateList.length-1;i++){
        var startDate = new Date(dateList[i].TJKSSJ).Format('yyyy-MM-dd');
        var endDate   = new Date(dateList[i].TJJSSJ).Format('yyyy-MM-dd');
        var showStartDate = new Date(dateList[i].TJKSSJ).Format('yyyy年MM月dd日');
        var showEndDate   = new Date(dateList[i].TJJSSJ).Format('yyyy年MM月dd日');
        html ='<li class="divider"></li>\n' +
          '<li><a href="javascript:spreadTimeSearch(\''+startDate+'\',\''+endDate+'\')">'+showStartDate+'-
'+showEndDate+'</a></li>'
        $("#dropdown-menu-li").append(html)
    }*/


/*    if($("#dateStart").val()=="2018-06-01"||$("#dateStart").val()=="2019-01-01"){
        initEndDatepicker();
    }*/
    //加载默认时间
    $("#dateStart").datepicker('update',oldStartDate);

    $("#showDateStart").text($("#dateStart").val());

    if(oldEndDate == defaultEnd){//显示当前日期
        $("#dateEnd").datepicker('setDate',dateStr);
    }else{
        $("#dateEnd").datepicker('setDate',oldEndDate);
    }
    $("#showDateEnd").text($("#dateEnd").val());


    document.getElementById("xmblqkDiv").style.display ="none";
    document.getElementById("bjjslDiv").style.display ="none";
    document.getElementById("cqlDiv").style.display ="none";
    autoHeight();
    //from = sessionStorage.getItem("from");
    dqCs();
    dqCs2();
});


/**
 * 跨月查询，传入一个时间段，如果结束时间为空则取当前时间
 */
function spreadTimeSearch(dateStart,dateEnd) {
    $("#dateStart").datepicker('update',dateStart);
    $("#showDateStart").text($("#dateStart").val());
    $('#dateEnd').datepicker("destroy");
    if(dateEnd){
        $('#dateEnd').val(dateEnd);
        $('#showDateEnd').text(dateEnd);
    }else {
        $('#dateEnd').val(currDateStr);
        $('#showDateEnd').text(currDateStr);
    }
    if("-1" == djzt){   //统计及时率、超期率
        if("1" == pm_count){
          showProInfo1('pm1',ctx+'xmjg-project-info!topmjsl.action?endtype=1','工程建设项目审批办结及时率排名');
        } else {
          showProInfo2('pm2',ctx+'xmjg-project-info!topmjsl.action?endtype=2','工程建设项目审批超期率排名');
        }
        return;
    }

    dqCs();
    dqCs2();

}


function autoHeight(){
    var iframe = document.getElementById("xndc_content_frame");
    var cli...
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
        var ctx = '/xmjg/';        var zb_order = 0; //在办数排序（默认值（0）; 0：升序; 1：降序）        var
bj_order = 0; //办结数排序（默认值（0）; 0：升序; 1：降序）        var yj_order = 0; //逾期数排序（默认值（0）; 0：升
序; 1：降序）        var bx_order = 0; //并行数排序（默认值（0）; 0：升序; 1：降序）        var tj_order = 0; //退件
数排序（默认值（0）; 0：升序; 1：降序）        var xzqhdm= "660100";        var name = "";        var
currentCityName ="";        var oldStartDate = "";        var oldEndDate = "";
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
        $(function(){
if($(window.parent.document).find("#xndc_content_frame").prop("id")=="xndc_content_frame"){
$("#SY").attr("target","_parent");          }          loadSortIcon();          pageNumKeyPress();        });
function pageNumKeyPress(){          $('#pageNum').bind('keypress', function (event) {          if
(event.keyCode == "13") {          //需要处理的事情          var pageNo = $(this).val();          pageNo =
parseInt(pageNo);          var pages = $(this).data('pages');    //最大页码          if(pageNo < 1) {
pageNo = 1;          }          if(pageNo > pages){          pageNo = pages;          }
agcloudJumpPage(pageNo);   //跳转页面          }          });        }        //操作按钮(修改、删除)图标鼠标移入移出
效果        function setImgSrc(imgObj,type){          var imgSrc=imgObj.src;          if(type=="over"){
imgObj.src=imgSrc.substring(0,imgSrc.indexOf(".png"))+"_hover.png";          }else{
imgObj.src=imgSrc.substring(0,imgSrc.indexOf("_hover.png"))+".png";          }        }        function
clickView(xzqhdm,xmdm){          //parent.window.location.href="xmjg-project-info!projectInfo.action?
id="+id;// var name ="${name}";          var djzt="";          var pageNo="1";          //获取搜索框的数据值
var searchXmdm = window.parent.document.getElementById("xmdm").value;          var searchXmmc =
window.parent.document.getElementById("xmmc").value;          var searchSpjdSearch =
window.parent.document.getElementById("spjdSearch").value;          var searchWhetherBinglian =
window.parent.document.getElementById("whether_binglian").value;          /*          var url=ctx+"/xmjg-
project-info!projectInfo.action?
xzqhdm="+xzqhdm+"&xmdm="+xmdm+"&currentPageNo="+pageNo+"&currentCityName="+currentCityName+"&name="+name+"&dj
zt="+djzt+
"&searchXmdm="+searchXmdm+"&searchXmmc="+searchXmmc+"&searchSpjdSearch="+searchSpjdSearch+"&searchWhetherBing
lian="+searchWhetherBinglian+"&startDate="+oldStartDate+"&endDate="+oldEndDate+"&intoWay=1";//intoWay:进入到流
程展示页面的方式：1表示从一个系统中进入，2表示从综合查询页面进入          */          var basePath = ctx;          var
url="mid-xmjg-project-info!projectInfo.action?
xzqhdm="+xzqhdm+"&xmdm="+xmdm+"&currentPageNo="+pageNo+"&currentCityName="+currentCityName+"&name="+name+"&dj
zt="+djzt+
"&searchXmdm="+searchXmdm+"&searchXmmc="+searchXmmc+"&searchSpjdSearch="+searchSpjdSearch+"&searchWhetherBing
```

```
lian="+searchWhetherBinglian+"&startDate="+oldStartDate+"&endDate="+oldEndDate+"&intoWay=1";
commonWindow.toWindowForReturn(basePath+url);          /*          parent.window.open(url);*/
//commonWindow.toWindowForReturn(url);          //parent.window.location.href=url;  //currentPageNo 当前的页数
currentCityName 当前选择的审批流程类型          //parent.window.location.href="xmjg-project-
info!projectInfo.action?
id="+id+"&currentPageNo="+${currentPageNo}+"&currentCityName="+currentCityName+"&name="+name;//currentPageNo
当前的页数 currentCityName 当前选择的审批流程类型        }        function locationmap(xmdm){//
$(window.parent.document.getElementById("Map")).css('display','block');$(window.parent.document.getElementByI
d("rightTjDiv")).css('display','none');
$(window.parent.document.getElementById("changetomap")).click();          setTimeout(function(){          var
win = window.parent.document.getElementById("dtzs_content_frame").contentWindow;          var data =
{type:1,value:{xmdm:xmdm}};          win.postMessage(JSON.stringify(data),"*");          }, 1000);        }
function toClearForm(){          //clearForm();          $("#xmdm").val("");          $("#xmmc").val("");
search();        }        //排序方法        function orderByTitle(orderByName,th){          parent.orderNameId
= $(th).attr("id");          if(parent.orderClickName == orderByName){          parent.orderClickCount ++;
}else{          parent.orderClickCount = 1;          }          parent.orderClickName = orderByName;
var cur_xmlx = parent.xmlx;          var cur_djzt = parent.djzt;          var cur_splcmc = parent.sub_splcmc;
var cur_splcbm = parent.sub_splcbm;          if(parent.orderClickCount % 2 == 1){          orderByName +=
"DESC";          }          var spjdUrl;          if($("#dateEnd",parent.document).val() == parent.dateStr){
spjdUrl=ctx+"projectInfo/qbMdxmList.do?
name="+parent.name+"&orderByName="+orderByName+"&djzt="+cur_djzt+"&splclx="+cur_xmlx+"&xzqhdm="+parent.xzqhdm
+"&splcmc="+cur_splcmc+"&splcbm="+cur_splcbm+"&currentPageNo=1&currentCityName="+cur_splcmc+"&startDate="+$("
#dateStart",parent.document).val().substring(0,4)+"-"+$("#dateStart",parent.document).val().substring(5,7)+"-
01"+"&endDate="+parent.defaultEnd;          }else{     ...
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
locationmap('2020-659002-96-01-002388')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
locationmap('2020-659002-30-03-011603')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
locationmap('2020-659002-83-01-002426')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
locationmap('2020-659002-78-01-010429')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
locationmap('2020-659002-83-01-003027')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
locationmap('2020-659002-90-01-010407')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
locationmap('2020-659002-47-03-007738')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
locationmap('2020-659002-77-01-006122')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
locationmap('2020-659002-47-01-011373')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
locationmap('2020-659002-70-03-015314')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
agcloudJumpPage(2)
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
agcloudJumpPage(16)
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
orderByTitle('orderByZB',this)
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
orderByTitle('orderByBJ',this)
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
orderByTitle('orderByYQ',this)
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
orderByTitle('orderByBX',this)
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
orderByTitle('orderByTJ',this)
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
clickView('660100','2020-659002-96-01-002388')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
clickView('660100','2020-659002-30-03-011603')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
clickView('660100','2020-659002-83-01-002426')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
clickView('660100','2020-659002-78-01-010429')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
clickView('660100','2020-659002-83-01-003027')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
clickView('660100','2020-659002-90-01-010407')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
clickView('660100','2020-659002-47-03-007738')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
clickView('660100','2020-659002-77-01-006122')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
clickView('660100','2020-659002-47-01-011373')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
clickView('660100','2020-659002-70-03-015314')
```

http://127.0.0.1:8000/xmjg/xmjg-one-window!getYgck.action

```
    var ctx = '/xmjg/';    var xzqhdm="660100";    var bigScreenFolder = "";
```

http://127.0.0.1:8000/xmjg/xmjg-one-window!getYgck.action

```
$(function () {    var name='%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82';
$("#cityName").text(decodeURIComponent(name));var height = $(document.body).height()-45;$(".article-
con").css("height",height+'px');getXmjgEditor();$("#back_id").click(function () {
commonWindow.returnParentWindow();    });if(bigScreenFolder == 'bigscreenTwo/'){
$("#titie_div_id").hide();        $(".article-tit span").show();        $("#back_id").css({width:
'100px',height:'40px','line-height':'40px','font-size':'25px'})}});function getXmjgEditor(){$.ajax({type:
"POST",url: ctx+ '/xmjg-one-window!getXmjgEditor.action?xzqhdm='+xzqhdm,dataType: "json",success: function
(result) {$("#content").html(result.content);}});}
```

http://127.0.0.1:8000/xmjg/xmjg-one-window!getYgck.action

```
      var name='%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82';      $(".article-tit").html('<span
style="display: none">'+decodeURIComponent(name)+'</span>"一个窗口"');
```

http://127.0.0.1:8000/xmjg/xmjg/xndc/js/DateUtils.js

```
var now = new Date();          //当前日期
var nowDayOfWeek = now.getDay();         //今天本周的第几天
var nowDay = now.getDate();          //当前日
var nowMonth = now.getMonth();          //当前月
var nowYear = now.getYear();          //当前年
nowYear += (nowYear < 2000) ? 1900 : 0;  //

var lastMonthDate = new Date();  //上月日期
lastMonthDate.setDate(1);
lastMonthDate.setMonth(lastMonthDate.getMonth()-1);
var lastYear = lastMonthDate.getYear();
var lastMonth = lastMonthDate.getMonth();

//格式化日期：yyyy-MM-dd
function formatDate(date) {
    var myyear = date.getFullYear();
    var mymonth = date.getMonth()+1;
    var myweekday = date.getDate();

    if(mymonth < 10){
        mymonth = "0" + mymonth;
    }
    if(myweekday < 10){
        myweekday = "0" + myweekday;
    }
    return (myyear+"-"+mymonth + "-" + myweekday);
}

//获得某月的天数
function getMonthDays(myMonth){
    var monthStartDate = new Date(nowYear, myMonth, 1);
    var monthEndDate = new Date(nowYear, myMonth + 1, 1);
    var   days   =   (monthEndDate   -   monthStartDate)/(1000   *   60   *   60   *   24);
    return   days;
}

//获得本季度的开始月份
function getQuarterStartMonth(){
    var quarterStartMonth = 0;
    if(nowMonth<3){
        quarterStartMonth = 0;
    }
    if(2<6){
        quarterStartMonth = 3;
    }
    if(5<9){
        quarterStartMonth = 6;
    }
    if(nowMonth>8){
        quarterStartMonth = 9;
    }
    return quarterStartMonth;
}

//今天
function getCurrentDate(){
 var currentDate = new Date(nowYear, nowMonth, nowDay);
 return formatDate(currentDate)
}

//本周的开始日期
function getWeekStartDate(){
 var weekStartDate = new Date(nowYear, nowMonth, nowDay - nowDayOfWeek);
 return formatDate(weekStartDate);
}

//本周的结束日期
function getWeekEndDate(){
 var weekEndDate = new Date(nowYear, nowMonth, nowDay + (6 - nowDayOfWeek));
 return formatDate(weekEndDate);
}

//上周的开始日期
function getUpWeekStartDate(){
 var upWeekStartDate = new Date(nowYear, nowMonth, nowDay - nowDayOfWeek -7);
 return formatDate(upWeekStartDate);
}

//上周的结束日期
function getUpWeekEndDate(){
 var upWeekEndDate = new Date(nowYear, nowMonth, nowDay + (6 - nowDayOfWeek - 7));
 return formatDate(upWeekEndDate);
}

//本月的开始日期
function getMonthStartDate(){
 var monthStartDate = new Date(nowYear, nowMonth, 1);
 return formatDate(monthStartDate);
}

//本月的结束日期
function getMonthEndDate(){
 var monthEndDate = new Date(nowYear, nowMonth, getMonthDays(nowMonth));
 return formatDate(monthEndDate);
}

//本年的开始日期
function getYearStartDate(){
 var yearStartDate = new Date(nowYear, 0, 1);
 return formatDate(yearStartDate);
}

//本年的结束日期
function getYearEndDate(){
 var yearEndDate = new Date(nowYear, 11, 31);
 return formatDate(yearEndDate);
}
```

http://127.0.0.1:8000/xmjg/xmjg/ygck/js/ygck.js

```
function qhcs(){
 $("#panel").show();
}
function close(){
}

function sfList(){
 $.ajax({
         type:"post",
         url:"${ctx}/xmjg-project-info!getJsonData.action",
         success:function(zmList){
                 var cszm="";
            var str = "<ul>";
            for(var i in zmList){
                    cszm+="<a herf=\"#"+zmList[i]['sfzm']+"\" style=\"margin-right:
15px;cursor:pointer;\">"+zmList[i]['sfzm']+"</a>";
                    str+="<li>"+zmList[i]['sfzm']+"</li>" ;
                    var sfList=zmList[i]['sfList'];
                    for(var j in sfList){
                            str+="<li style='margin-left:50px'><ul><li>"+sfList[j]['name']+"</li><li
style='margin-left:100px'>";
                            var csList=sfList[j]['csList'];
                            for(var m in csList){
                                    str+="<a href='${ctx}/xmjg-project-info!getYgck.action?
xzqhdm="+csList[m]['city']+"&name="+csList[m]['name']+"&cityName=${cityName}' style=\"margin-right:
5px;cursor:pointer;\">"+csList[m]['name'] +"</a>";
                                   }
                            str+="</li></ul></li>";
                    }
            }
            str+="</ul>";
            $("#sfList").html(str);
            $("#zmList").html(cszm);
            $("#sfList").show();
                }
 });
}

function csList(){
 $.ajax({
         type:"post",
         url:"${ctx}/xmjg-project-info!getJsonCityData.action",
         success:function(zmList){
            var cszm="";
            var str = "<ul>";
```

```
      for(var i in zmList){
          cszm+="<a herf=\"#"+zmList[i]['cszm']+"\" style=\"margin-right:
10px;cursor:pointer;\">"+zmList[i]['cszm']+"</a>";
          str+="<li name="+zmList[i]['cszm']+">"+zmList[i]['cszm']+"</li><li style='margin-
left:50px'><ul><li>" ;
          var csList=zmList[i]['csList'];
          for(var j in csList){
              str+="<a href='${ctx}/xmjg-project-info!getYgck.action?xzqhdm="+csList[j]
['city']+"&name="+csList[j]['name']+"&cityName=${cityName}' style=\"margin-right:
5px;cursor:pointer;\">"+csList[j]['name'] +"</a>";
          }
          str+="</li></ul></li>";
      }
      str+="</ul>";
      $("#sfList").html(str);
      $("#zmList").html(cszm);
      $("#sfList").show();
        }
 });
}

function getImgList(ctx) {

  $.ajax({
    type: "post",
    url: ctx+"/xmjgEditor/getImgList.do",
    success: function (imgList) {
        $("#editForm").height($("#editor").height()+$(".ygck_nav").height());
        $(".js-showImgWrap").remove();

     var html = "<ul class='js-showImgWrap showImgWrap'></ul>";
        $(html).insertAfter("#editForm");
     if(imgList.length !="" || imgList.length !="0"){
        var html2= "";
     for(var i=0; i<imgList.length; i++){
        var url = ctx+imgList[i].imgUrl;
     console.log(ctx+imgList[i].imgUrl);
     html2 += '<li id="'+imgList[i].realFileName+'">'
                     +'<img src="'+url+'" style="float: left">'
                     +'<p style="float: left;margin-left: 10px;"><span
style="width: 30%;">'+imgList[i].showileName+'</span><span class="js-deleteImg" style="margin-left: 50px;">删
除</span></p>'
                     +'</li>';
     $(html2).appendTo(".js-showImgWrap");
     }
            }

        $(".js-deleteImg").click(function () {
            var data = $(this).parent().parent().attr("id");
            var obj = {
                "realFileName":data
                }
     $.ajax({
     type: "post",
     url: ctx + "/xmjgEditor/getImgList.do",
                data:obj,
     success: function (res) {
        console.log(res);
     getImgList(ctx);
     }
     });
     });

    }
  });
}
```

http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action

```
  var ctx= "/xmjg/";var xzqhdm='660100';var
name=decodeURIComponent('%E4%B8%80%E5%B8%88%E9%98%BF%E6%8B%89%E5%B0%94%E5%B8%82');//var basePath = "
<%=basePath%>";//使用本系统的rest服务    var basePath = "hello";//使用本系统的rest服务    var bigScreenFolder="";
var spjdbh = '';    var switchBgbh = '';
```

http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action

```
$(function () {var messageOpts = {        "closeButton" : false,//是否显示关闭按钮        "debug" : false,//是否
使用debug模式        "positionClass" : "toast-top-center",//弹出窗的位置        "onclick" : null,
"showDuration" : "1000",//显示的动画时间        "hideDuration" : "1000",//消失的动画时间        "timeOut" :
"2000",//展现时间        "extendedTimeOut" : "1000",//加长展示时间        "showEasing" : "swing",//显示时的动画缓冲
方式        "hideEasing" : "linear",//消失时的动画缓冲方式        "showMethod" : "fadeIn",//显示时的动画方式
"hideMethod" : "fadeOut" //消失时的动画方式    };    toastr.options = messageOpts;});
```

http://127.0.0.1:8000/xmjg/xmjg-one-form!getYzbd.action

```
$(function(){    $(".js-name").html('<span style="font-size: 0.3rem">'+decodeURIComponent(name)+'"一张表
单"</span><a id="backid" href="javascript:">返  回</a>');dqCs();    $("#backid").click(function () {
commonWindow.returnParentWindow();    });})function dqCs(){$.ajax({        url :ctx+"/xmjg-project-
info!getSplcByXzqhdm.action?xzqhdm="+xzqhdm,  //后台处理程序  获取当前城市项目分类        type:"post",    //数据发
送方式          dataType:"json",   //接受数据格式          error: function(){        },        success:
function(data){        if(data!=null && data!='underfine' && data.length > 0){      xapaList = eval(data);
splclxData = eval(data);      var str = '<ul class="form-tab1">'; var bz=0;      for(var
i=0;i<data.length;i++){      var zm=   xapaList[i].splcmc.split("");      for(var j=0;j<zm.length;j++){
if(zm[j]=="(" || zm[j]=="（"){      bz=1;      }      }      var arr;      if(bz==1){          arr =
xapaList[i].splcmc.split("(");if(arr.length == 1){   arr = xapaList[i].splcmc.split("（");}var splcmc =
arr[0] + "</br>(" + arr[1].substring(0,arr[1].length-1)+")";      }else{      arr=xapaList[i].splcmc;var
splcmc = arr;      }      bz = 0;          if(i==0){          str+='<a
onclick="showProInfo(\''+xapaList[i].splcmc+'\',\''+xapaList[i].splcbm+'\',\'xmlx'+i+'\',\''+xapaList[i].splc
mc+'\',\''+xapaList[i].splclx+'\',\'1\',\''+xapaList[i].splcbbh+'\'); "><li data-splcbbh="' +
xapaList[i].splcbbh +'" id="xmlx'+i+'" class="on" data-splcbm="' + xapaList[i].splcbm +'">'+splcmc+'</li>
</a>';          }else{          str+='<a
onclick="showProInfo(\''+xapaList[i].splcmc+'\',\''+xapaList[i].splcbm+'\',\'xmlx'+i+'\',\''+xapaList[i].splc
mc+'\',\''+xapaList[i].splclx+'\',\'1\',\''+xapaList[i].splcbbh+'\'); "><li data-splcbbh="' +
xapaList[i].splcbbh + '" id="xmlx'+i+'" data-splcbm="' + xapaList[i].splcbm +'">'+splcmc+'</li></a>';
}      }      str+='</ul>';$('.inner-container').empty();$('.inner-
container').html(str);getspjd(xzqhdm,xapaList[0].splclx,xapaList[0].splcbbh,xapaList[0].splcmc,xapaList[0].sp
lcbm,"","");        }else{          $('.inner-container').empty();          $('.inner-container').html('<div
style="text-align: center">暂无数据</div>');          $('.city-detail-con .form-tabs-
con').css("display","none");}}          })};function showProInfo(splcmc,splcbm,id,val,lx,zt,splcbbh)
{$(".form-tab1 .on").each(function(){$(this).removeClass("on");});$('#'+id).addClass("on");selfIndex1 =
parseInt(id.substring(4,5));if(lx!=null&&lx!=""){xmlx=lx;}else  if(!$("#xmlx-count").val()==1){xmlx=$("#xmlx-
count").val();}if(zt!=null&&zt!=""){djzt=zt;}getspjd(xzqhdm,xmlx,splcbbh,splcmc,splcbm,"","");}//获取不同类型项
目的审批阶段function getspjd(xzqhdm,xmlx,splcbbh,splcmc,splcbm,startDate,endDate){    $.ajax({type : "GET", url
:encodeURI(ctx+"/xmjg-project-info!getSpjdByxmlx.action?
xzqhdm="+xzqhdm+"&splclx="+xmlx+"&splcbbh="+splcbbh+"&splcmc="+splcmc   +"&splcbm="+splcbm),dataType :
'json', success : function(resulttemp) {          var tempList;          var objTemp;          $.ajax({
url :encodeURI(ctx+'/xmjg-project-info!getGeLeiXingXiangMuCanShuByXzqhdm.action'),          type : "get",
data : {          xzqhdm : xzqhdm,          splcbm : splcbm,          splcbbh : splcbbh,          splclx :
xmlx,          startDate:startDate,          endDate:endDate          },          dataType : "json",
async : false,          success : function(result) {          if(result!=null&&result.list!=null){
tempList = result.list;          objTemp = tempList[0];          }          }          });
if(resulttemp == null || resulttemp.length == 0){          $(".form-tab2").empty();          $(".form-
tab2").html('<div style="text-align: center">暂无数据</div>');          $(".tab2-item").css("display","none");
return;          }          $(".tab2-item").css("display","block");var title="";var count="";var spjds="";var
spjdsmc="";if(resulttemp.length>0){$(".form-tab2").empty();    var result = new Array();    for(var
i=0;i<resulttemp.length;i++){       var arr = resulttemp[i].spjdmc.split("(");       if(arr.length == 1){
arr = resulttemp[i].spjdmc.split("（");       }       var spjdmc = arr[0].split("阶段")[0];
if(spjdmc!="并行推进")          result[i]=resulttemp[i];    }    var jdCount=result.length+1;    var
jdtitleLength=0;          if(jdCount>5){        var divwidth=100/(result.length+1);
divwidth=Math.floor(divwidth)+2;        jdtitleLength=10;     }else{        var divwidth=100/(result.length);
divwidth=Math.floor(divwidth);    }    var width=divwidth+'%';    var str = "";    for(var
i=0;i<result.length;i++){    if(i<4){    var forIndex = result[i].dybzspjdxh;    }
spjds+=result[i].dybzspjdxh+",";       spj...
```

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap.js

```
/*!
```

```
 * Bootstrap v3.3.5 (http://getbootstrap.com)
 * Copyright 2011-2015 Twitter, Inc.
 * Licensed under the MIT license
 */

if (typeof jQuery === 'undefined') {
  throw new Error('Bootstrap\'s JavaScript requires jQuery')
}

+function ($) {
  'use strict';
  var version = $.fn.jquery.split(' ')[0].split('.')
  if ((version[0] < 2 && version[1] < 9) || (version[0] == 1 && version[1] == 9 && version[2] < 1)) {
    throw new Error('Bootstrap\'s JavaScript requires jQuery version 1.9.1 or higher')
  }
}(jQuery);

/* ========================================================================
 * Bootstrap: transition.js v3.3.5
 * http://getbootstrap.com/javascript/#transitions
 * ========================================================================
 * Copyright 2011-2015 Twitter, Inc.
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 * ======================================================================== */


+function ($) {
  'use strict';

  // CSS TRANSITION SUPPORT (Shoutout: http://www.modernizr.com/)
  // ============================================================

  function transitionEnd() {
    var el = document.createElement('bootstrap')

    var transEndEventNames = {
      WebkitTransition : 'webkitTransitionEnd',
      MozTransition    : 'transitionend',
      OTransition      : 'oTransitionEnd otransitionend',
      transition       : 'transitionend'
    }

    for (var name in transEndEventNames) {
      if (el.style[name] !== undefined) {
        return { end: transEndEventNames[name] }
      }
    }

    return false // explicit for ie8 (  ._.)
  }

  // http://blog.alexmaccaw.com/css-transitions
  $.fn.emulateTransitionEnd = function (duration) {
    var called = false
    var $el = this
    $(this).one('bsTransitionEnd', function () { called = true })
    var callback = function () { if (!called) $($el).trigger($.support.transition.end) }
    setTimeout(callback, duration)
    return this
  }

  $(function () {
    $.support.transition = transitionEnd()

    if (!$.support.transition) return

    $.event.special.bsTransitionEnd = {
      bindType: $.support.transition.end,
      delegateType: $.support.transition.end,
      handle: function (e) {
        if ($(e.target).is(this)) return e.handleObj.handler.apply(this, arguments)
      }
    }
  })

}(jQuery);

/* ========================================================================
 * Bootstrap: alert.js v3.3.5
 * http://getbootstrap.com/javascript/#alerts
 * ========================================================================
 * Copyright 2011-2015 Twitter, Inc.
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 * ======================================================================== */


+function ($) {
  'use strict';

  // ALERT CLASS DEFINITION
  // ======================

  var dismiss = '[data-dismiss="alert"]'
  var Alert   = function (el) {
    $(el).on('click', dismiss, this.close)
  }

  Alert.VERSION = '3.3.5'

  Alert.TRANSITION_DURATION = 150

  Alert.prototype.close = function (e) {
    var $this    = $(this)
    var selector = $this.attr('data-target')

    if (!selector) {
      selector = $this.attr('href')
      selector = selector && selector.replace(/.*(?=#[^\s]*$)/, '') // strip for ie7
    }

    var $parent = $(selector)

    if (e) e.preventDefault()

    if (!$parent.length) {
      $parent = $this.closest('.alert')
    }

    $parent.trigger(e = $.Event('close.bs.alert'))

    if (e.isDefaultPrevented()) return

    $parent.removeClass('in')

    function removeElement() {
      // detach from parent, fire event then clean up data
      $parent.detach().trigger('closed.bs.alert').remove()
    }

    $.support.transition && $parent.hasClass('fade') ?
      $parent
        .one('bsTransitionEnd', removeElement)
        .emulateTransitionEnd(Alert.TRANSITION_DURATION) :
      removeElement()
  }


  // ALERT PLUGIN DEFINITION
  // =======================

  function Plugin(option) {
    return this.each(function () {
      var $this = $(this)
      var data  = $this.data('bs.alert')

      if (!data) $this.data('bs.alert', (data = new Alert(this)))
      if (typeof option == 'string') data[option].call($this)
    })
  }

  var old = $.fn.alert

  $.fn.alert             = Plugin
  $.fn.alert.Constructor = Alert
  // ALERT NO CONFLICT
  // =================

  $.fn.alert.noConflict = function () {
    $.fn.alert = old
    return this
  }


  // ALERT DATA-API
  // ==============

  $(document).on('click.bs.alert.data-api', dismiss, Alert.prototype.close)

}(jQuery);

/* ========================================================================
 * Bootstrap: button.js v3.3.5
 * http://getbootstrap.com/javascript/#buttons
 * ==========================================================...
```

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-datetimepicker.js

```
/* =========================================================
 * bootstrap-datetimepicker.js
 * =========================================================
 * Copyright 2012 Stefan Petre
 *
 * Improvements by Andrew Rowls
 * Improvements by Sébastien Malot
 * Improvements by Yun Lai
 * Improvements by Kenneth Henderick
 * Improvements by CuGBabyBeaR
 * Improvements by Christian Vaas <auspex@auspex.eu>
 *
 * Project URL : http://www.malot.fr/bootstrap-datetimepicker
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 * http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 * ========================================================= */

(function(factory){
    if (typeof define === 'function' && define.amd)
        define(['jquery'], factory);
    else if (typeof exports === 'object')
        factory(require('jquery'));
    else
        factory(jQuery);

}(function($, undefined){

    // Add ECMA262-5 Array methods if not supported natively (IE8)
    if (!('indexOf' in Array.prototype)) {
        Array.prototype.indexOf = function (find, i) {
          if (i === undefined) i = 0;
          if (i < 0) i += this.length;
          if (i < 0) i = 0;
          for (var n = this.length; i < n; i++) {
          if (i in this && this[i] === find) {
          return i;
          }
          }
          return -1;
        }
    }

    // Add timezone abbreviation support for ie6+, Chrome, Firefox
    function timeZoneAbbreviation() {
        var abbreviation, date, formattedStr, i, len, matchedStrings, ref, str;
        date = (new Date()).toString();
        formattedStr = ((ref = date.split('(')[1]) != null ? ref.slice(0, -1) : 0) || date.split(' ');
        if (formattedStr instanceof Array) {
          matchedStrings = [];
          for (var i = 0, len = formattedStr.length; i < len; i++) {
          str = formattedStr[i];
          if ((abbreviation = (ref = str.match(/\b[A-Z]+\b/)) !== null) ? ref[0] : 0) {
          matchedStrings.push(abbreviation);
          }
          }
          formattedStr = matchedStrings.pop();
        }
        return formattedStr;
    }

    function UTCDate() {
        return new Date(Date.UTC.apply(Date, arguments));
    }

    // Picker object
    var Datetimepicker = function (element, options) {
        var that = this;

        this.element = $(element);

        // add container for single page application
        // when page switch the datetimepicker div will be removed also.
        this.container = options.container || 'body';

        this.language = options.language || this.element.data('date-language') || 'en';
        this.language = this.language in dates ? this.language : this.language.split('-')[0]; // fr-CA
fallback to fr
        this.language = this.language in dates ? this.language : 'en';
        this.isRTL = dates[this.language].rtl || false;
        this.formatType = options.formatType || this.element.data('format-type') || 'standard';
        this.format = DPGlobal.parseFormat(options.format || this.element.data('date-format') ||
dates[this.language].format || DPGlobal.getDefaultFormat(this.formatType, 'input'), this.formatType);
        this.isInline = false;
        this.isVisible = false;
        this.isInput = this.element.is('input');
        this.fontAwesome = options.fontAwesome || this.element.data('font-awesome') || false;

        this.bootcssVer = options.bootcssVer || (this.isInput ? (this.element.is('.form-control') ? 3 : 2) :
( this.bootcssVer = this.element.is('.input-group') ? 3 : 2 ));

        this.component = this.element.is('.date') ? ( this.bootcssVer === 3 ? this.element.find('.input-
group-addon .glyphicon-th, .input-group-addon .glyphicon-time, .input-group-addon .glyphicon-remove, .input-
group-addon .glyphicon-calendar, .input-group-addon .fa-calendar, .input-group-addon .fa-clock-o').parent() :
this.element.find('.add-on .icon-th, .add-on .icon-time, .add-on .icon-calendar, .add-on .fa-calendar, .add-
on .fa-clock-o').parent()) : false;
        this.componentReset = this.element.is('.date') ? ( this.bootcssVer === 3 ? this.element.find('.input-
group-addon .glyphicon-remove, .input-group-addon .fa-times').parent():this.element.find('.add-on .icon-
remove, .add-on .fa-times').parent()) : false;
        this.hasInput = this.component && this.element.find('input').length;
        if (this.component && this.component.length === 0) {
      ...
```

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrapValidator.js

```
/*!
 * BootstrapValidator (http://bootstrapvalidator.com)
 * The best jQuery plugin to validate form fields. Designed to use with Bootstrap 3
 *
 * @version     v0.5.3, built on 2014-11-05 9:14:18 PM
 * @author      https://twitter.com/nghuuphuoc
 * @copyright   (c) 2013 - 2014 Nguyen Huu Phuoc
 * @license     Commercial: http://bootstrapvalidator.com/license/
 *          Non-commercial: http://creativecommons.org/licenses/by-nc-nd/3.0/
 */
if (typeof jQuery === 'undefined') {
    throw new Error('BootstrapValidator requires jQuery');
}

(function($) {
    var version = $.fn.jquery.split(' ')[0].split('.');
    if ((+version[0] < 2 && +version[1] < 9) || (+version[0] === 1 && +version[1] === 9 && +version[2] < 1))
{
        throw new Error('BootstrapValidator requires jQuery version 1.9.1 or higher');
    }
}(window.jQuery));

(function($) {
    var BootstrapValidator = function(form, options) {
        this.$form   = $(form);
        this.options = $.extend({}, $.fn.bootstrapValidator.DEFAULT_OPTIONS, options);

        this.$invalidFields = $([]);    // Array of invalid fields
        this.$submitButton  = null;     // The submit button which is clicked to submit form
        this.$hiddenButton  = null;

        // Validating status
        this.STATUS_NOT_VALIDATED = 'NOT_VALIDATED';
        this.STATUS_VALIDATING    = 'VALIDATING';
        this.STATUS_INVALID       = 'INVALID';
        this.STATUS_VALID         = 'VALID';

        // Determine the event that is fired when user change the field value
        // Most modern browsers supports input event except IE 7, 8.
        // IE 9 supports input event but the event is still not fired if I press the backspace key.
        // Get IE version
        // https://gist.github.com/padolsey/527683/#comment-7595
        var ieVersion = (function() {
          var v = 3, div = document.createElement('div'), a = div.all || [];
          while (div.innerHTML = '<!--[if gt IE '+(++v)+']><br><![endif]-->', a[0]) {}
          return v > 4 ? v : !v;
        }());

        var el = document.createElement('div');
        this._changeEvent = (ieVersion === 9 || !('oninput' in el)) ? 'keyup' : 'input';

        // The flag to indicate that the form is ready to submit when a remote/callback validator returns
        this._submitIfValid = null;

        // Field elements
        this._cacheFields = {};

        this._init();
    };

    BootstrapValidator.prototype = {
        constructor: BootstrapValidator,

        /**
         * Init form
         */
        _init: function() {
          var that    = this,
          options = {
          autoFocus:      this.$form.attr('data-bv-autofocus'),
          container:      this.$form.attr('data-bv-container'),
          events: {
          formInit:         this.$form.attr('data-bv-events-form-init'),
          formError:        this.$form.attr('data-bv-events-form-error'),
          formSuccess:      this.$form.attr('data-bv-events-form-success'),
          fieldAdded:       this.$form.attr('data-bv-events-field-added'),
          fieldRemoved:     this.$form.attr('data-bv-events-field-removed'),
          fieldInit:        this.$form.attr('data-bv-events-field-init'),
          fieldError:       this.$form.attr('data-bv-events-field-error'),
          fieldSuccess:     this.$form.attr('data-bv-events-field-success'),
          fieldStatus:      this.$form.attr('data-bv-events-field-status'),
          validatorError:   this.$form.attr('data-bv-events-validator-error'),
          validatorSuccess: this.$form.attr('data-bv-events-validator-success')
          },
          excluded:       this.$form.attr('data-bv-excluded'),
          feedbackIcons: {
          valid:      this.$form.attr('data-bv-feedbackicons-valid'),
          invalid:    this.$form.attr('data-bv-feedbackicons-invalid'),
          validating: this.$form.attr('data-bv-feedbackicons-validating')
          },
          group:          this.$form.attr('data-bv-group'),
          live:          this.$form.attr('data-bv-live'),
          message:        this.$form.attr('data-bv-message'),
          onError:        this.$form.attr('data-bv-onerror'),
          onSuccess:      this.$form.attr('data-bv-onsuccess'),
          submitButtons:  this.$form.attr('data-bv-submitbuttons'),
          threshold:      this.$form.attr('data-bv-threshold'),
          trigger:        this.$form.attr('data-bv-trigger'),
          verbose:        this.$form.attr('data-bv-verbose'),
          fields:         ...
```

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-common.js

```
/**
 *
 */


/**
 * 确认框
 * @param msg
 * @param doFunction
 * @returns
 */
function doConfirmAction(msg,doFunction){
 if($("#doConfirmDiv").length>0){
         $("#doConfirmDiv").remove();
        }
 var htmlStr='<div class="modal fade" style="top:30%;z-index:10001;"  id="doConfirmDiv"> ';
 htmlStr+='  <div class="modal-dialog">  ';
 htmlStr+='  <div class="modal-content message_align"> ';
 htmlStr+='  <div class="modal-header">  ';
 htmlStr+='   <h4 class="modal-title" id="doConfirmName"></h4>  ';
 htmlStr+='  </div>  ';
 htmlStr+='   <div class="modal-footer">  ';
 htmlStr+='     <input type="hidden" id="url"/> ';
 htmlStr+='     <button type="button" name="sureDelete"  class="btn btn-primary btn-success" data-
dismiss="modal" id="doConfirmAction">确定</button>';
 htmlStr+='     <button type="button" class="btn btn-default"  data-dismiss="modal">       取消</button>  ';
 htmlStr+='   </div>  ';
 htmlStr+='   </div>';
 htmlStr+='   </div>';
 htmlStr+='  </div>';
 $("body").append(htmlStr);
 $('#doConfirmName').html(msg);
 $('#doConfirmDiv').modal('show');
 $("#doConfirmAction").on("click",function(){
         doFunction();
 });
}
```

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-editable.js

```
/*! X-editable - v1.5.1
* In-place editing with Twitter Bootstrap, jQuery UI or pure jQuery
* http://github.com/vitalets/x-editable
* Copyright (c) 2013 Vitaliy Potapov; Licensed MIT */
/**
Form with single input element, two buttons and two states: normal/loading.
Applied as jQuery method to DIV tag (not to form tag!). This is because form can be in loading state when
spinner shown.
Editableform is linked with one of input types, e.g. 'text', 'select' etc.

@class editableform
@uses text
```

```
@uses textarea
**/
(function ($) {
    "use strict";

    var EditableForm = function (div, options) {
        this.options = $.extend({}, $.fn.editableform.defaults, options);
        this.$div = $(div); //div, containing form. Not form tag. Not editable-element.
        if(!this.options.scope) {
          this.options.scope = this;
        }
        //nothing shown after init
    };

    EditableForm.prototype = {
        constructor: EditableForm,
        initInput: function() {  //called once
          //take input from options (as it is created in editable-element)
          this.input = this.options.input;

          //set initial value
          //todo: may be add check: typeof str === 'string' ?
          this.value = this.input.str2value(this.options.value);

          //prerender: get input.$input
          this.input.prerender();
        },
        initTemplate: function() {
          this.$form = $($.fn.editableform.template);
        },
        initButtons: function() {
          var $btn = this.$form.find('.editable-buttons');
          $btn.append($.fn.editableform.buttons);
          if(this.options.showbuttons === 'bottom') {
          $btn.addClass('editable-buttons-bottom');
          }
        },
        /**
        Renders editableform

        @method render
        **/
        render: function() {
          //init loader
          this.$loading = $($.fn.editableform.loading);
          this.$div.empty().append(this.$loading);

          //init form template and buttons
          this.initTemplate();
          if(this.options.showbuttons) {
          this.initButtons();
          } else {
          this.$form.find('.editable-buttons').remove();
          }

          //show loading state
          this.showLoading();

          //flag showing is form now saving value to server.
          //It is needed to wait when closing form.
          this.isSaving = false;

          /**
          Fired when rendering starts
          @event rendering
          @param {Object} event event object
          **/
          this.$div.triggerHandler('rendering');

          //init input
          this.initInput();

          //append input to form
          this.$form.find('div.editable-input').append(this.input.$tpl);

          //append form to container
          this.$div.append(this.$form);
          //render input
          $.when(this.input.render())
          .then($.proxy(function () {
          //setup input to submit automatically when no buttons shown
          if(!this.options.showbuttons) {
          this.input.autosubmit();
          }

          //attach 'cancel' handler
          this.$form.find('.editable-cancel').click($.proxy(this.cancel, this));

          if(this.input.error) {
          this.error(this.input.error);
          this.$form.find('.editable-submit').attr('disabled', true);
          this.input.$input.attr('disabled', true);
          //prevent form from submitting
          this.$form.submit(function(e){ e.preventDefault(); });
          } else {
          this.error(false);
          this.input.$input.removeAttr('disabled');
          this.$form.find('.editable-submit').removeAttr('disabled');
          var value = (this.value === null || this.value === undefined || this.value === '') ?
this.options.defaultValue : this.value;
          this.input.value2input(value);
          //attach submit handler
          this.$form.submit($.proxy(this.submit, this));
          }

          /**
          Fired when form is rendered
          @event rendered
          @param {Object} event event object
          **/
          this.$div.triggerHandler('rendered');

          this.showForm();

          //call postrender method to perform actions required visibility of form
          if(thi...
```

http://127.0.0.1:8000/xmjg/bootstrap/js/jquery.eeyellow.Timeline.js

```
; (function ($, window, document, undefined) {
    //'use strict';
    var pluginName = 'vivaTimeline';//Plugin名稱

    //Timeline建構式
    var Timeline = function (element, opt) {
        //私有變數
        this.target = element;
        this.carouselInterval;
        this.checkImgLoad;
        this.imgLoad = false;
        //初始化
        this._init(opt);

        this._event();

    }

    //ImportKML2D預設參數
    Timeline.options = {
        carousel: true,
        carouselTime: 10000
    }

    //Timeline私有方法
    Timeline.prototype = {
        //初始化
        _init: function (_opt) {
          //合併自訂參數與預設參數
          var self = this;
          self.options = $.extend(true, {}, Timeline.options, _opt);
```

```
  self.target
  .find('.events-body')
  .each(function(){
  var rowcount = $(this).find('.row').length;
  if(rowcount > 1) {
  var html = "<ol>";
  for(var i = 0; i < rowcount; i++){
  html += "<li data-target='" + i + "'></li>";
  }
  html += "</ol>";
  $(this)
  .siblings('.events-footer')
  .html(html)
  .find('li')
  .first()
  .addClass('active');
  }
  });

  self.target
  .find('.events-body')
  .each(function(){
  $(this)
  .find('.row')
  .first()
  .show()
  .siblings()
  .hide();
  });

  self.target
  .find('img').on('load', function(){
  self.target
  .find('.events-body')
  .each(function(){
  var maxHeight = 0;
  $(this)
  .find('.row')
  .each(function(){
  if($(this).height() > maxHeight){
  maxHeight = $(this).height();
  }
  });
  $(this).find('.row').height(maxHeight);
  });
  });
},

//綁定事件
_event: function () {
  var self = this;
  self.target
  .find('.events-header')
  .click(function(){
  $(this)
  .siblings('.events-body').slideToggle()
  .end()
  .siblings('.events-footer').toggle();
  });

  self.target
  .find('.events-footer li')
  .click(function(){
  self._carousel($(this));
  });

  if(self.options.carousel){
  self.carouselInterval = setInterval(function(){
  self._carousel();
  }, self.options.carouselTime);

  self.target
  .find('.events')
  .hover(function(){
  clearInterval(self.carouselInterval);
  self.carouselInterval = null;
```

```
          }, function(){
          if(self.carouselInterval == undefined){
          self.carouselInterval = setInterval(function(){
          self._carousel();
          }, self.options.carouselTime);
          }
          });
          }
        },

        //自動輪播
        _carousel: function(_container) {
          var self = this;
          if(_container == undefined){
          self.target
          .find('.events-footer .active')
          .each(function(){
          var nextTarget;
          if($(this).is(':last-child')){
          nextTarget = $(this).siblings().first();
          }
          else{
          nextTarget = $(this).next();
          }
          self._carousel(nextTarget);
          });
          }
          else{
          var target = _container.data().target;

          _container
          .addClass('active')
          .siblings()
       ...
```

http://127.0.0.1:8000/xmjg/bootstrap/js/toastr.js

```
/*
 * Toastr
 * Copyright 2012-2015
 * Authors: John Papa, Hans Fjällemark, and Tim Ferrell.
 * All Rights Reserved.
 * Use, reproduction, distribution, and modification of this code is subject to the terms and
 * conditions of the MIT license, available at http://www.opensource.org/licenses/mit-license.php
 *
 * ARIA Support: Greta Krafsig
 *
 * Project: https://github.com/CodeSeven/toastr
 */
/* global define */
(function (define) {
    define(['jquery'], function ($) {
        return (function () {
          var $container;
          var listener;
          var toastId = 0;
          var toastType = {
          error: 'error',
          info: 'info',
          success: 'success',
          warning: 'warning'
          };

          var toastr = {
          clear: clear,
          remove: remove,
          error: error,
          getContainer: getContainer,
          info: info,
          options: {},
          subscribe: subscribe,
          success: success,
          version: '2.1.3',
          warning: warning
          };

          var previousToast;

          return toastr;

          ////////////////

          function error(message, title, optionsOverride) {
          return notify({
          type: toastType.error,
          iconClass: getOptions().iconClasses.error,
          message: message,
          optionsOverride: optionsOverride,
          title: title
          });
          }

          function getContainer(options, create) {
          if (!options) { options = getOptions(); }
          $container = $('#' + options.containerId);
          if ($container.length) {
          return $container;
          }
          if (create) {
          $container = createContainer(options);
          }
          return $container;
          }

          function info(message, title, optionsOverride) {
          return notify({
          type: toastType.info,
          iconClass: getOptions().iconClasses.info,
          message: message,
          optionsOverride: optionsOverride,
          title: title
          });
          }

          function subscribe(callback) {
          listener = callback;
          }

          function success(message, title, optionsOverride) {
          return notify({
          type: toastType.success,
          iconClass: getOptions().iconClasses.success,
          message: message,
          optionsOverride: optionsOverride,
          title: title
          });
          }

          function warning(message, title, optionsOverride) {
          return notify({
          type: toastType.warning,
          iconClass: getOptions().iconClasses.warning,
          message: message,
          optionsOverride: optionsOverride,
          title: title
          });
          }

          function clear($toastElement, clearOptions) {
          var options = getOptions();
          if (!$container) { getContainer(options); }
          if (!clearToast($toastElement, options, clearOptions)) {
          clearContainer(options);
          }
          }

          function remove($toastElement) {
          var options = getOptions();
          if (!$container) { getContainer(options); }
          if ($toastElement && $(':focus', $toastElement).length === 0) {
          removeToast($toastElement);
```

```
            return;
            }
            if ($container.children().length) {
            $container.remove();
            }
            }

            // internal functions

            function clearContainer (options) {
            var toastsToClear = $container.children();
            for (var i = toastsToClear.length - 1; i >= 0; i--) {
            clearToast($(toastsToClear[i]), options);
            }
            }

            function clearToast ($toastElement, options, clearOptions) {
            var force = clearOptions && clearOptions.force ? clearOptions.force : false;
            if ($toastElement && (force || $(':focus', $toastElement).length === 0)) {
            $toastElement[options.hideMethod]({
            duration: options.hideDuration,
            easing: options.hideEasing,
            complete: function () { removeToast($toastElement); }
            });
            return true;
            }
            ...
```

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-treeview.js

```
/* =========================================================
 * bootstrap-treeview.js v1.2.0
 * =========================================================
 * Copyright 2013 Jonathan Miles
 * Project URL : http://www.jondmiles.com/bootstrap-treeview
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 * http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 * ========================================================= */

;(function ($, window, document, undefined) {

 /*global jQuery, console*/

 'use strict';

 var pluginName = 'treeview';

 var _default = {};

 _default.settings = {

         injectStyle: true,

         levels: 2,

         expandIcon: 'glyphicon glyphicon-plus',
         collapseIcon: 'glyphicon glyphicon-minus',
         emptyIcon: 'glyphicon',
         nodeIcon: '',
         selectedIcon: '',
         checkedIcon: 'glyphicon glyphicon-check',
         uncheckedIcon: 'glyphicon glyphicon-unchecked',
         color: undefined, // '#000000',
         backColor: undefined, // '#FFFFFF',
         borderColor: undefined, // '#dddddd',
         onhoverColor: '#F5F5F5',
         selectedColor: '#FFFFFF',
         selectedBackColor: '#428bca',
         searchResultColor: '#D9534F',
         searchResultBackColor: undefined, //'#FFFFFF',

         enableLinks: false,
         highlightSelected: true,
         highlightSearchResults: true,
         showBorder: true,
         showIcon: true,
         showCheckbox: false,
         showTags: false,
         multiSelect: false,

         // Event handlers
         onNodeChecked: undefined,
         onNodeCollapsed: undefined,
         onNodeDisabled: undefined,
         onNodeEnabled: undefined,
         onNodeExpanded: undefined,
         onNodeSelected: undefined,
         onNodeUnchecked: undefined,
         onNodeUnselected: undefined,
         onSearchComplete: undefined,
         onSearchCleared: undefined
 };

 _default.options = {
         silent: false,
         ignoreChildren: false
 };

 _default.searchOptions = {
         ignoreCase: true,
         exactMatch: false,
         revealResults: true
 };

 var Tree = function (element, options) {

         this.$element = $(element);
         this.elementId = element.id;
         this.styleId = this.elementId + '-style';

         this.init(options);

         return {

                 // Options (public access)
                 options: this.options,

                 // Initialize / destroy methods
                 init: $.proxy(this.init, this),
                 remove: $.proxy(this.remove, this),

                 // Get methods
                 getNode: $.proxy(this.getNode, this),
                 getParent: $.proxy(this.getParent, this),
                 getSiblings: $.proxy(this.getSiblings, this),
                 getSelected: $.proxy(this.getSelected, this),
                 getUnselected: $.proxy(this.getUnselected, this),
                 getExpanded: $.proxy(this.getExpanded, this),
                 getCollapsed: $.proxy(this.getCollapsed, this),
                 getChecked: $.proxy(this.getChecked, this),
                 getUnchecked: $.proxy(this.getUnchecked, this),
                 getDisabled: $.proxy(this.getDisabled, this),
                 getEnabled: $.proxy(this.getEnabled, this),

                 // Select methods
                 selectNode: $.proxy(this.selectNode, this),
                 unselectNode: $.proxy(this.unselectNode, this),
                 toggleNodeSelected: $.proxy(this.toggleNodeSelected, this),

                 // Expand / collapse methods
                 collapseAll: $.proxy(this.collapseAll, this),
                 collapseNode: $.proxy(this.collapseNode, this),
                 expandAll: $.proxy(this.expandAll, this),
                 expandNode: $.proxy(this.expandNode, this),
                 toggleNodeExpanded: $.proxy(this.toggleNodeExpanded, this),
                 revealNode: $.proxy(this.revealNode, this),

                 // Expand / collapse methods
                 checkAll: $.proxy(this.checkAll, this),
                 checkNode: $.proxy(this.checkNode, this),
                 uncheckAll: $.proxy(this.uncheckAll, this),
                 uncheckNode: $.proxy(this.uncheckNode, this),
                 toggleNodeChecked: $.proxy(this.toggleNodeChecked, this),

                 // Disable / enable methods
                 disableAll: $.proxy(this.disableAll, this),
                 disableNode: $.proxy(this.disableNode, this),
                 enableAll: $.proxy(this.enableAll, this),
                 enableNode: $.proxy(this.enableNode, this),
                 toggleNodeDisabled: $.proxy(this.toggleNodeDisabled, this),

                 // Search methods
                 search: $.proxy(this.search, this),
                 searchById: $.proxy(this.searchById, this),
                 clearSearch: $.proxy(this.clearSearch, this)
         }       ;
 };

 Tree.prototype.init = function (options) {

         this.tree = [];
         this.nodes = [];

         if (options.data) {
                 if (typeof options.data === 'string') {
                         options.data = $.parseJSON(options.data);
                        }
                 this.tree = $.extend(true, [], options.data);
                 delete options.data;
                }
         this.options = $.extend({}, _default.settings, options);

         this.destroy();
         this.subscribeEvents();
         this.setInitialStates({ nodes: this.tree }, 0...
```

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-select.js

```
(function ($) {
  'use strict';

  //<editor-fold desc="Shims">
  if (!String.prototype.includes) {
    (function () {
      'use strict'; // needed to support `apply`/`call` with `undefined`/`null`
      var toString = {}.toString;
      var defineProperty = (function () {
        // IE 8 only supports `Object.defineProperty` on DOM elements
        try {
          var object = {};
          var $defineProperty = Object.defineProperty;
          var result = $defineProperty(object, object, object) && $defineProperty;
        } catch (error) {
        }
        return result;
      }());
      var indexOf = ''.indexOf;
      var includes = function (search) {
        if (this == null) {
          throw new TypeError();
        }
        var string = String(this);
        if (search && toString.call(search) == '[object RegExp]') {
```

```
        throw new TypeError();
      }
      var stringLength = string.length;
      var searchString = String(search);
      var searchLength = searchString.length;
      var position = arguments.length > 1 ? arguments[1] : undefined;
      // `ToInteger`
      var pos = position ? Number(position) : 0;
      if (pos != pos) { // better `isNaN`
        pos = 0;
      }
      var start = Math.min(Math.max(pos, 0), stringLength);
      // Avoid the `indexOf` call if no match is possible
      if (searchLength + start > stringLength) {
        return false;
      }
      return indexOf.call(string, searchString, pos) != -1;
    };
    if (defineProperty) {
      defineProperty(String.prototype, 'includes', {
        'value': includes,
        'configurable': true,
        'writable': true
      });
    } else {
      String.prototype.includes = includes;
    }
  }());
}

if (!String.prototype.startsWith) {
  (function () {
    'use strict'; // needed to support `apply`/`call` with `undefined`/`null`
    var defineProperty = (function () {
      // IE 8 only supports `Object.defineProperty` on DOM elements
      try {
        var object = {};
        var $defineProperty = Object.defineProperty;
        var result = $defineProperty(object, object, object) && $defineProperty;
      } catch (error) {
      }
      return result;
    }());
    var toString = {}.toString;
    var startsWith = function (search) {
      if (this == null) {
        throw new TypeError();
      }
      var string = String(this);
      if (search && toString.call(search) == '[object RegExp]') {
        throw new TypeError();
      }
      var stringLength = string.length;
      var searchString = String(search);
      var searchLength = searchString.length;
      var position = arguments.length > 1 ? arguments[1] : undefined;
      // `ToInteger`
      var pos = position ? Number(position) : 0;
      if (pos != pos) { // better `isNaN`
        pos = 0;
      }
      var start = Math.min(Math.max(pos, 0), stringLength);
      // Avoid the `indexOf` call if no match is possible
      if (searchLength + start > stringLength) {
        return false;
      }
      var index = -1;
      while (++index < searchLength) {
        if (string.charCodeAt(start + index) != searchString.charCodeAt(index)) {
        return false;
        }
      }
      return true;
    };
    if (defineProperty) {
      defineProperty(String.prototype, 'startsWith', {
        'value': startsWith,
        'configurable': true,
        'writable': true
      });
    } else {
      String.prototype.startsWith = startsWith;
    }
  }());
}

if (!Object.keys) {
  Object.keys = function (
    o, // object
    k, // key
    r  // result array
    ){
    // initialize object and result
    r=[];
    // iterate over object keys
    for (k in o)
        // fill result array with non-prototypical keys
      r.hasOwnProperty.call(o, k) && r.push(k);
    // return result
    return r;
  };
}

// set data-selected on select element if the value has been programmatically selected
// prior to initialization of bootstrap-select
// * consider removing or replacing an alternative method *
var valHooks = {
  useDefault: false,
  _set: $.valHooks.select.set
};

$.valHooks.select.set = function(elem, value) {
  if (value && !valHooks.useDefault) $(elem).data('selected', true);

  return valHooks._set.apply(this, arguments);
};

var changed_arguments = null;

var EventIsSupported = (function() {
  try {
    new Event('change');
    return true;
  } catch (e) {
    return false;
  }
})();

$.fn.triggerNative = function (eventName) {
  var el = this[0],
      event;

  if (el.dispatchEvent) { // for modern browsers & IE9+
    if (EventIsSupported) {
      // Fo...
```

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-table-editable.js

```
/**
 * @author zhixin wen <wenzhixin2010@gmail.com>
 * extensions: https://github.com/vitalets/x-editable
 */

!function ($) {

    'use strict';

    $.extend($.fn.bootstrapTable.defaults, {
        editable: true,
        onEditableInit: function () {
          return false;
        },
        onEditableSave: function (field, row, oldValue, $el) {
          return false;
        },
        onEditableShown: function (field, row, $el, editable) {
          return false;
        },
        onEditableHidden: function (field, row, $el, reason) {
          return false;
        }
    });

    $.extend($.fn.bootstrapTable.Constructor.EVENTS, {
        'editable-init.bs.table': 'onEditableInit',
        'editable-save.bs.table': 'onEditableSave',
        'editable-shown.bs.table': 'onEditableShown',
        'editable-hidden.bs.table': 'onEditableHidden'
    });

    var BootstrapTable = $.fn.bootstrapTable.Constructor,
        _initTable = BootstrapTable.prototype.initTable,
        _initBody = BootstrapTable.prototype.initBody;

    BootstrapTable.prototype.initTable = function () {
        var that = this;
        _initTable.apply(this, Array.prototype.slice.apply(arguments));

        if (!this.options.editable) {
          return;
        }

        $.each(this.columns, function (i, column) {
          if (!column.editable) {
          return;
          }

          var _formatter = column.formatter;
          column.formatter = function (value, row, index) {
          var result = _formatter ? _formatter(value, row, index) : value;

          return ['<a href="javascript:void(0)"',
          ' data-name="' + column.field + '"',
          ' data-pk="' + row[that.options.idField] + '"',
          ' data-value="' + result + '"',
          '>' + '</a>'
          ].join('');
          };
        });
    };

    BootstrapTable.prototype.initBody = function () {
        var that = this;
        _initBody.apply(this, Array.prototype.slice.apply(arguments));

        if (!this.options.editable) {
          return;
        }

        $.each(this.columns, function (i, column) {
          if (!column.editable) {
          return;
          }

          that.$body.find('a[data-name="' + column.field + '"]').editable(column.editable)
          .off('save').on('save', function (e, params) {
          var data = that.getData(),
          index = $(this).parents('tr[data-index]').data('index'),
          row = data[index],
          oldValue = row[column.field];

          row[column.field] = params.submitValue;
          that.trigger('editable-save', column.field, row, oldValue, $(this));
          });
          that.$body.find('a[data-name="' + column.field + '"]').editable(column.editable)
          .off('shown').on('shown', function (e, editable) {
          var data = that.getData(),
          index = $(this).parents('tr[data-index]').data('index'),
          row = data[index];
          that.trigger('editable-shown', column.field, row, $(this), editable);
          });
          that.$body.find('a[data-name="' + column.field + '"]').editable(column.editable)
          .off('hidden').on('hidden', function (e, reason) {
          var data = that.getData(),
          index = $(this).parents('tr[data-index]').data('index'),
          row = data[index];

          that.trigger('editable-hidden', column.field, row, $(this), reason);
          });
        });
        this.trigger('editable-init');
    };

}(jQuery);
```

http://127.0.0.1:8000/xmjg/bootstrap/js/bootstrap-combotree.js

```
/**
 * Created by CherryDream on 2016/9/1.
 */
(function ($) {
    $.fn.bootstrapCombotree = function (options, param) {
        if(typeof options === 'string')
        {
          return bootstrapCombotree.prototype[options](this, param);
        }
        options = options || {};
        this.each(function () {
          // var Value = new Array();

          var state = $.data(this, 'bootstrapCombotree');
          if(state)
          {
          $.extend(state.options, options);
          }
          else
          {
          $.data(this, 'bootstrapCombotree', {
          options : $.extend({}, $.fn.bootstrapCombotree.defaults, options)
          });
          }
          // $.data(this, "text", Text);
          // $.data(this, "value", value);
          var btComboTree = new bootstrapCombotree().init(this);
        })
    };
    var bootstrapCombotree = function(){
        this.Text = new Array();
        this.value = new Array();
        this.$Tree = undefined;
        this.$Button = undefined;
        this.$hidden = undefined;
        this.init = function (target) {
          var options = $.data(target, "bootstrapCombotree").options;
          $(target).empty();
          //写html标签
          if (options.width == undefined) {
          target.innerHTML = '<div class="btn-group">'
          + '<button type="button" class="btn btn-default dropdown-toggle"   data-toggle="dropdown" title=' +
options.defaultLable + '>'
          + options.defaultLable + '<span class="caret"></span>'
          + '</button>'
          + '<input type="hidden" name="' + options.name + '"/> '
          + '<div class="dropdown-menu" style="width: 400%"></div>'
          + '</div>';
          }
          else {
          target.innerHTML = '<div class="btn-group">'
          + '<button type="button" class="btn btn-default dropdown-toggle"  data-toggle="dropdown" title=' +
options.defaultLable + '>'
          + options.defaultLable + '<span class="caret"></span>'
          + '</button>'
          + '<input type="hidden" name="' + options.name + '"/> '
          + '<div class="dropdown-menu" style="width: ' + options.width + 'px;"></div>'
          + '</div>';
          }
          this.$Tree = $(target).find(".dropdown-menu");//Tree对象
          this.$Button = $(target).find("button");//button对象
          this.$hidden = $(target).find("input[type='hidden']");//隐藏域
          //渲染bootstrap-treeview
          var _this = this;
          this.$Tree.treeview({
          data: options.data,
          showIcon: options.showIcon,
          showCheckbox: true,
          onNodeChecked: function (event, node) {
          options.onBeforeCheck(node);
          if($(target).data("value") != undefined)
          {
          this.Text = $(target).data("Text");
          this.value = $(target).data("value");
          }

          if(_this.$Button[0].innerText == options.defaultLable)
          {
          _this.$Button[0].innerText = '';
          }
          _this.setCheck(node) ;
          _this.setCheckparent(node);
          if (_this.Text.length <= options.maxItemsDisplay) {
          _this.$Button[0].innerHTML = _this.Text + '<span class="caret"></span>';
          _this.$Button.attr("title", _this.Text);
          }
          else {
          _this.$Button[0].innerHTML = _this.Text.length + '项被选中  <span class="caret"></span>';
          _this.$Button.attr("title", _this.Text.length + '项被选中');
          }
          _this.$hidden.val(_this.value);
          if (options.onCheck != undefined) {
          options.onCheck(node);
          }
          },
          onNodeUnchecked: function (event, node) {
          options.onBeforeUnCheck(node);
          if($(target).data("value") != undefined)
          {
          this.Text = $(target).data("Text");
          this.value = $(target).data("value");
          }
          _this.setUnCheck(node);
          _this.setunCheckparent(node);
          if (_this.Text.length == 0) {
          _this.$Button[0].innerHTML = options.defaultLable + '<span class="caret"></span>';
          _this.$Button.attr("title", options.defaultLable);
          }
          else {
          if (_this.Text.length <= options.maxItemsDisplay) {
          ...
```

http://127.0.0.1:8000/xmjg/adswf/engine/public/public.js

```
/**
 * 页面初始化（初始化页面的多个form）
 */
function initPage(){
 var formsLen = document.forms.length;
 if(formsLen > 0){
         for(var i=0; i<formsLen-1; i++){
                 initForm(i);
                }
        }
}

/**
```

```
 * 初始化form
 * @index form的序号
 */
function initForm(index){
 var excludeElemType = ",button,submit,reset,image,hidden,"; //       设置非注册事件的控件类型
 var allElems = document.forms[index].elements;

 //       为指定输入控件注册回车事件
 registerEnterKey(allElems, excludeElemType);

 //       当页面初始化后设置页面第一个输入控件的鼠标焦点
 setFirstInputElemFocus(allElems, excludeElemType);

 //       为页面单行文本框或多行文本框注册获取焦点时选中文本的事件
 registerSelectText(allElems);
}

/**
 * 为页面输入控件注册回车事件，使得输入控件可以响应回车键
 */
function registerEnterKey(allElems, excludeElemType) {
 for(var i=0; i<allElems.length; i++){
         /       /若不属于非注册事件的控件类型，则为其注册事件
         if(excludeElemType.indexOf(','+allElems[i].type+',') == -1){
                 allElems[i].onkeydown = function(){

                         if(event.keyCode == 13 && event.srcElement.type != ''
                                 && excludeElemType.indexOf(','+event.srcElement.type+',') == -1){

                                 event.keyCode = 9; //       跳转至下一输入控件

                                 /       /若控件类型为单行文本框或多行文本框，则为其添加选中文本动作
                                 if(event.srcElement.type == 'text' || event.srcElement.type ==
'textarea')
                                         event.srcElement.select(); //       选中下一输入控件文本内容
                                }
                 }       ;
         }
        }
}

/**
 * 为页面单行文本框或多行文本框注册获取焦点时选中文本的事件
 */
function registerSelectText(allElems){
 for(var i=0; i<allElems.length; i++){
         /       /若控件类型为单行文本框或多行文本框，则为其添加选中文本动作
         if(allElems[i].type == 'text' || allElems[i].type == 'textarea'){
                 allElems[i].attachEvent("onfocus", func_textHandler(allElems[i]));
         }
        }
}

var func_textHandler = function(obj){
 return function(){
         textHandler(obj);
 }
}

/**
 * 选中输入框文本内容
 */
function textHandler(obj){
 obj.select();
}

/**
 * 当页面初始化后设置页面第一个输入控件的鼠标焦点
 */
function setFirstInputElemFocus(allElems, excludeElemType){
 for(var i=0; i<allElems.length; i++){
         if(excludeElemType.indexOf(allElems[i].type) == -1){
                 allElems[i].focus(); //       设置页面第一个输入控件焦点

                 /       /如果为单行文本框或多行文本框，则还要选中文本
                 if(allElems[i].type == 'text' || allElems[i].type == 'numberfield')
                         allElems[i].select();
                 return;
```

```
                }
        }
}

/**
 * 跳转至第几页
 */
function jumpPage(pageNo){
 checkPagePara();
 $("#pageNo").val(pageNo);
 document.forms[0].submit();
}

/**
 * 查询方法
 */
function search(){
 //       检查分页参数是否设置正确
 checkPagePara();
 document.forms[0].submit();
}


/**
 * 检查分页参数设置是否有误
 */
function checkPagePara(){
 //       如果分页参数设置有误则使用默认值
 if(!isPositiveInt($("#pageSize").val()) || !isPositiveInt($("#pageNo").val())){
         $("#pageSize").val('10');
         $("#pageNo").val('1');
        }
}

/**
 * 取消操作
 */
function cancelSubmit(){
 if(confirm("       确定不保存当前页面数据并退出吗？")){
         history.back();
 }else
         return;
}

/**
 * 去除单行文本框或多行文本框多余空格
 */
function trimInputText(){
 var inputElems = document.forms[0].getElementsByTagName("INPUT");
 for(var i=0; i<inputElems.length; i++){
         if(inputElems[i].type == "text" || inputElems[i].type == 'textarea'){
                 if(inputElems[i].value.length > 0){
                         inputElems[i].value = trim(inputElems[i].value);
                        }
         }
 }
}

/**
 * 清空表单
 */
function clearForm(){
 var excludeElementIds = ',pageSize,pageNo,order,orderBy,checkall,'; //       无需执行清空操作的控件ID
 clearFormByCustom(excludeElementIds); //       清空表单
}

/**
 * 清空表单。excludeElementIds表示无需执行清空操作的控件ID，以逗号作全分隔
 */
function clearFormByCustom(excludeElementIds) {
 var formObj = document.forms[0];
 var formEl = formObj.elements;

 for (var i=0; i<formEl.length; i++) {
         var element = formEl[i];

         /       /特殊字段要忽略掉清空操作
         if (excludeElementIds != "" && excludeElementIds.indexOf("," + element.id + ",") != -1)
```

```
                 break;

         if (element.type == 'text')
                 element.value = '';
         if (element.type == 'textarea')
                 element.value = '';
         if (element.type == 'checkbox')
                 element.checked = false;
         if (element.type == 'radio')
                 element.checked = false;
         if (element.type == 'select-multiple')
                 element.selectedIndex = 0;
         if (element.type == 'select-one')
                 element.selectedIndex = 0;
        }
}

/**
 * URL跳转
 */
function openUrl(url) {
 window.location.href = url;
}

/**
 * 删除操作
 */
function del(url) {
 if(confirm("       真的要删除该记录吗？")) {
         openUrl(url);
        }
}

/**
 * 带删除提示的多条记录删除操作URL跳转
 */
function delMore(url) {
 //       检查标记，让标记>0
 if (getCheckedNum(document.forms[0].ids) == 0){
         alert("       请先选择要删除的记录！");
         return;
        }

 if(confirm("       真的要删除选中的记录吗？")) {
         document.forms[0].action = url;
         document.forms[0].submit();
        }
}

/**
 * 全选/全不选函数
 * @param checkboxName 需要被设置的checkbox或checkbox数组控件的name属性所指定的名称
 * @param checkallObj 全选checkbox控件元素
 */
function checkAll(checkboxName, checkallObj){
 var ids = document.getElementsByName(checkboxName);
 if(ids != null){
         var ischeckall = checkallObj.checked;
         /       /如果ids为一项checkbox
         if(ids.type == "checkbox"){
                 ids.checked = ischeckall;
                 return;
                }
         /       /如果ids为checkbox数组
         for(var i=0; i<ids.length; i++){
                 ids[i].checked = ischeckall;
                }
        }
}

/**
 * 取得列表中ch...
```

http://127.0.0.1:8000/xmjg/resources/js/common/tool.js

```
/**
 * 改变样式
 */
function changeStyle(elemId, className){
 document.getElementById(elemId).className = className;
}

/**
 * 居中打开新窗口
 */
function openCenterWindow(url, width, height){
 var x = (screen.availWidth - width) / 2;
 var y = (screen.availHeight - height) / 2;
 var param = "left="+x+",top="+y+",width="+width+",height="+height;
 param +=
',toolbar=no,menubar=no,status=yes,locationbar=no,directories=no,scrollbars=yes,resizable=yes';
 var handle= window.open(url, '_blank', param);
 return handle;
}

/**
 * 居中打开新窗口
 */
function openCenterWindow(url){
 var param = "left=0,top=0,width="+screen.availWidth+",height="+screen.availHeight;
 param +=
',toolbar=no,menubar=no,status=yes,locationbar=no,directories=no,scrollbars=yes,resizable=yes';
 var handle= window.open(url, '_blank', param);
 return handle;
}

/**
 * 居中打开新窗口
 */
function openCenterWindow(url, name){
 var param = "left=0,top=0,width="+screen.availWidth+",height="+screen.availHeight;
 param +=
',toolbar=no,menubar=no,status=yes,locationbar=no,directories=no,scrollbars=yes,resizable=yes';
 var handle= window.open(url, name, param);
 return handle;
}

/**
 * 获取文件格式
 */
function getFileFormat(fileName){
 var pos = fileName.lastIndexOf(".");
 if(pos > 0){
         return fileName.substring(pos+1, fileName.length);
 }else
         return null;
}

/**
 * 判断文件格式是否为NTKO控件支持的文档格式
 */
function isNtkoSupportFormat(fileFormat){
 if(fileFormat != null && (
         fileFormat == 'doc' || fileFormat == 'docx'
         || fileFormat == 'xls' || fileFormat == 'xlsx'
         || fileFormat == 'ppt' || fileFormat == 'pptx'
         || fileFormat == 'vsd' || fileFormat == 'mpp'
         || fileFormat == 'wps'))
         return true;
 else
         return false;
}

//判断是否是IE浏览器
function checkIsIE(){
 if(-[1,]){
     alert("这不是IE浏览器！");
 }else{
     alert("这是IE浏览器！");
 }
}
```

```
/**
 * 去左空格
 */
function ltrim(s){
 return s.replace( /^\s*/, "");
}

/**
 * 去右空格
 */
function rtrim(s){
 return s.replace( /\s*$/, "");
}

/**
 * 去左右空格
 */
function trim(s){
   return str.replace(/(^\s*)|(\s*$)/g, "");
}

/**
 * 可以在一个任意深度的iframe中调用父iframe中的方法
 */
function getRootWindow(){
 var win = window;
 while (win != win.parent){
         win = win.parent;
 }
 return win;
}
```

http://127.0.0.1:8000/xmjg/adsfw/sysfile/public/attachment-operation.js

```
        /**
  *        添加附件
  * @param url        添加附件的url
  * @param redirectUrl        添加附件后跳转的url,
  *        redirectUrl       有两种取值:1.跳转到业务模块对应的url;
  *                                         2.       跳转到附件列表iframe对应的action,
如'/framework/sysfile/sys-file!showAttachmentsIframe.action'
  */
 function addAttachment(url, redirectUrl){
         if(document.getElementById('attachment').value.length > 0){
                 document.forms[0].action = url +"&redirectUrl="+redirectUrl;
                 document.forms[0].submit();
                }
         else
                 alert('       请选择要上传的附件!');

        }

 /**
  *        删除附件
  * @param fileName        要删除的附件的文件名
  * @param url        删除附件提交的url
  * @param redirectUrl        删除后跳转的url, 其取值同添加附件中redirectUrl
  */
 function deleteAttachment(fileName, url , redirectUrl){
         if(confirm("       确认要删除名为“" + fileName + "”的附件吗？")){
                 document.forms[0].action = url + '&redirectUrl=' + redirectUrl;
                 document.forms[0].submit();
                }
        }

 /**
  *        删除一个或者多个附件
  * @param url        删除一个或者多个附件提交的url
  * @param redirectUrl        删除后跳转的url, 其取值同添加附件中redirectUrl
  */
 function deleteAttachments(url, redirectUrl){
         document.forms[0].action = url + "?redirectUrl=" + redirectUrl;
         document.forms[0].submit();
```

```
       }

/**
 *        下载一个或者多个附件
 * @param url        下载一个或者多个附件提交的url
 */
function downloadAttachments(url){
        document.forms[0].action = url ;
        document.forms[0].submit();
       }

/**
 *        下载一个或者多个附件 iframe
 * @param url        下载一个或者多个附件提交的url
 * added by liuc 2015-02-09
 */
function downloadAttachmentsIframe(url){
        var grid = Ext.getCmp('attachmentGridPanel');
        var sel = grid.getSelectionModel().getSelections();
        if(sel.length > 0 ){
                var params = '?sysFileIds=' + sel[0].get(grid.keyField);
                for(var i=1; i<sel.length; i++){
                        params += '&sysFileIds=' + sel[i].get(grid.keyField)
                       }
                window.open(url+params);
               }

       }

/**
 *        删除一个或者多个附件, iframe
 * @param url        删除一个或者多个附件提交的url
 * @param redirectUrl        删除后跳转的url， 其取值同添加附件中redirectUrl
 */
function deleteAttachmentsIframe(url, redirectUrl){

        var grid = Ext.getCmp('attachmentGridPanel');
        var sel = grid.getSelectionModel().getSelections();
        if(sel.length > 0 ){
                var sysFileIds = grid.getSelKeyIds();
                Ext.Ajax.request({
                        url: url,
                        success: function(response, opts){
                                grid.store.reload();
                        }       ,
                        params: {
                                sysFileIds:sysFileIds,
                                redirectUrl: redirectUrl
                               }
                })       ;

               }
        else{
                alert('       请选择一个或者多个附件');
               }

       }

/**
 *        读取附件
 * @param url        读取附件的url
 * @param sysFileId        要读取的附件主键
 */
function readAttachment(url, sysFileId){
        if(sysFileId != null){
                document.forms[0].action = url;
                document.forms[0].submit();
               }
       }

/**
 * NTKO       在线编辑文档
 * @param url NTKO       在线编辑文档的url
 * @param sysFileId NTKO       在线编辑文档的主键
 * @param fileName NTKO       在线编辑文档的文件名
 */
function editOfficeDoc(url, sysFileId, fileName){
        if(sysFileId != null && isNtkoSupportFormat(getFileFormat(fileName))){
                openCenterWindow(url, 1050, 650);
               }
        else
                alert('       系统提示：选择的附件记录必须是NTKO控件所支持的Office文档格式，请重新选择！');
       }

/**
 *        通用的打开附件方法
 * @param url        打开附件的url
 * @param sysFileId        要打开的附件主键
 * @param fileName        要打开的附件主键的文件名
 */
function openAttachment(readAttachmentUrl, editOfficeDocUrl, sysFileId, fileName){
        if(isNtkoSupportFormat(getFileFormat(fileName)))
                editOfficeDoc(editOfficeDocUrl, sysFileId, fileName);
        else
                readAttachment(readAttachmentUrl, sysFileId);
       }
```

http://127.0.0.1:8000/xmjg/handsontable-master/dist/handsontable.full.js

```
/*!
 * (The MIT License)
 *
 * Copyright (c) 2012-2014 Marcin Warpechowski
 * Copyright (c) 2015 Handsoncode sp. z o.o. <hello@handsoncode.net>
 *
 * Permission is hereby granted, free of charge, to any person obtaining
 * a copy of this software and associated documentation files (the
 * 'Software'), to deal in the Software without restriction, including
 * without limitation the rights to use, copy, modify, merge, publish,
 * distribute, sublicense, and/or sell copies of the Software, and to
 * permit persons to whom the Software is furnished to do so, subject to
 * the following conditions:
 *
 * The above copyright notice and this permission notice shall be
 * included in all copies or substantial portions of the Software.
 *
 * THE SOFTWARE IS PROVIDED 'AS IS', WITHOUT WARRANTY OF ANY KIND,
 * EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
 * MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
 * IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
 * CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
 * TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
 * SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
 *
 * Version: 6.0.0
 * Release date: 27/09/2018 (built at 26/09/2018 12:54:09)
 */
(function webpackUniversalModuleDefinition(root, factory) {
 if(typeof exports === 'object' && typeof module === 'object')
         module.exports = factory();
 else if(typeof define === 'function' && define.amd)
         define("Handsontable", [], factory);
 else if(typeof exports === 'object')
         exports["Handsontable"] = factory();
 else
         root["Handsontable"] = factory();
})(typeof self !== 'undefined' ? self : this, function() {
return /******/ (function(modules) { // webpackBootstrap
/******/        // The module cache
/******/        var installedModules = {};
/******/
/******/        // The require function
/******/        function __webpack_require__(moduleId) {
/******/
/******/                // Check if module is in cache
/******/                if(installedModules[moduleId]) {
/******/                        return installedModules[moduleId].exports;
/******/                }
/******/                // Create a new module (and put it into the cache)
/******/                var module = installedModules[moduleId] = {
/******/                        i: moduleId,
/******/                                l: false,
/******/                                exports: {}
/******/                        };
/******/
/******/                        // Execute the module function
/******/                        modules[moduleId].call(module.exports, module, module.exports, __webpack_require__);
/******/
/******/                        // Flag the module as loaded
/******/                        module.l = true;
/******/
/******/                        // Return the exports of the module
/******/                        return module.exports;
/******/                }
/******/
/******/
/******/                // expose the modules object (__webpack_modules__)
/******/                __webpack_require__.m = modules;
/******/
/******/                // expose the module cache
/******/                __webpack_require__.c = installedModules;
/******/
/******/                // define getter function for harmony exports
/******/                __webpack_require__.d = function(exports, name, getter) {
/******/                        if(!__webpack_require__.o(exports, name)) {
/******/                                Object.defineProperty(exports, name, {
/******/                                        configurable: false,
/******/                                        enumerable: true,
/******/                                        get: getter
/******/                                });
/******/                        }
/******/                };
/******/
/******/                // getDefaultExport function for compatibility with non-harmony modules
/******/                __webpack_require__.n = function(module) {
/******/                        var getter = module && module.__esModule ?
/******/                                function getDefault() { return module['default']; } :
/******/                                function getModuleExports() { return module; };
/******/                        __webpack_require__.d(getter, 'a', getter);
/******/                        return getter;
/******/                };
/******/
/******/                // Object.prototype.hasOwnProperty.call
/******/                __webpack_require__.o = function(object, property) { return
Object.prototype.hasOwnProperty.call(object, property); };
/******/
/******/                // __webpack_public_path__
/******/                __webpack_require__.p = "";
/******/
/******/                // Load entry module and return exports
/******/                return __webpack_require__(__webpack_require__.s = 452);
/******/ })
/************************************************************************/
/******/ ([
/* 0 */
/***/ (function(module, exports, __webpack_require__) {

"use strict";


exports.__esModule = true;
exports.HTML_CHARACTERS = undefined;
exports.getParent = getParent;
exports.closest = closest;
exports.closestDown = closestDown;
exports.isChildOf = isChildOf;
exports.isChildOfWebComponentTable = isChildOfWebComponentTable;
exports.polymerWrap = polymerWrap;
exports.polymerUnwrap = polymerUnwrap;
exports.index = index;
exports.overlayContainsElement = overlayContainsElement;
exports.hasClass = hasClass;
exports.addClass = addClass;
exports.removeClass = removeClass;
exports.removeTextNodes = removeTextNodes;
exports.empty = empty;
exports.fastInnerHTML = fastInnerHTML;
exports.fastInnerText = fastInnerText;...
```

http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/web/viewer.js

```
/**
 * @licstart The following is the entire license notice for the
 * Javascript code in this page
 *
 * Copyright 2018 Mozilla Foundation
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 *     http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 *
 * @licend The above is the entire license notice for the
 * Javascript code in this page
 */

/******/ (function(modules) { // webpackBootstrap
/******/        // The module cache
/******/        var installedModules = {};
/******/
/******/        // The require function
/******/        function __webpack_require__(moduleId) {
/******/
/******/                // Check if module is in cache
/******/                if(installedModules[moduleId]) {
/******/                        return installedModules[moduleId].exports;
/******/                }
/******/                // Create a new module (and put it into the cache)
/******/                var module = installedModules[moduleId] = {
/******/                        i: moduleId,
/******/                        l: false,
/******/                        exports: {}
/******/                };
/******/
/******/                // Execute the module function
/******/                modules[moduleId].call(module.exports, module, module.exports, __webpack_require__);
/******/
/******/                // Flag the module as loaded
/******/                module.l = true;
/******/
/******/                // Return the exports of the module
/******/                return module.exports;
/******/        }
/******/
/******/
/******/        // expose the modules object (__webpack_modules__)
/******/        __webpack_require__.m = modules;
/******/
/******/        // expose the module cache
/******/        __webpack_require__.c = installedModules;
/******/
/******/        // define getter function for harmony exports
/******/        __webpack_require__.d = function(exports, name, getter) {
/******/                if(!__webpack_require__.o(exports, name)) {
/******/                        Object.defineProperty(exports, name, { enumerable: true, get: getter });
/******/                }
/******/        };
/******/
/******/        // define __esModule on exports
/******/        __webpack_require__.r = function(exports) {
/******/                if(typeof Symbol !== 'undefined' && Symbol.toStringTag) {
/******/                        Object.defineProperty(exports, Symbol.toStringTag, { value: 'Module' });
/******/                }
/******/                Object.defineProperty(exports, '__esModule', { value: true });
/******/        };
/******/
```

```
/******/        // create a fake namespace object
/******/        // mode & 1: value is a module id, require it
/******/        // mode & 2: merge all properties of value into the ns
/******/        // mode & 4: return value when already ns object
/******/        // mode & 8|1: behave like require
/******/        __webpack_require__.t = function(value, mode) {
/******/                if(mode & 1) value = __webpack_require__(value);
/******/                if(mode & 8) return value;
/******/                if((mode & 4) && typeof value === 'object' && value && value.__esModule) return
value;
/******/                var ns = Object.create(null);
/******/                __webpack_require__.r(ns);
/******/                Object.defineProperty(ns, 'default', { enumerable: true, value: value });
/******/                if(mode & 2 && typeof value != 'string') for(var key in value)
__webpack_require__.d(ns, key, function(key) { return value[key]; }.bind(null, key));
/******/                return ns;
/******/        };
/******/
/******/        // getDefaultExport function for compatibility with non-harmony modules
/******/        __webpack_require__.n = function(module) {
/******/                var getter = module && module.__esModule ?
/******/                        function getDefault() { return module['default']; } :
/******/                        function getModuleExports() { return module; };
/******/                __webpack_require__.d(getter, 'a', getter);
/******/                return getter;
/******/        };
/******/
/******/        // Object.prototype.hasOwnProperty.call
/******/        __webpack_require__.o = function(object, property) { return
Object.prototype.hasOwnProperty.call(object, property); };
/******/
/******/        // __webpack_public_path__
/******/        __webpack_require__.p = "";
/******/
/******/
/******/        // Load entry module and return exports
/******/        return __webpack_require__(__webpack_require__.s = 0);
/******/ })
/************************************************************************/
/******/ ([
/* 0 */
/***/ (function(module, exports, __webpack_require__) {

"use strict";


;
var pdfjsWebApp = void 0,
    pdfjsWebAppOptions = void 0;
{
  pdfjsWebApp = __webpack_require__(1);
  pdfjsWebAppOptions = __webpack_require__(12);
}
;
{
  __webpack_require__(38);
}
;
{
  __webpack_require__(43);
}
function getViewerConfiguration() {
  return {
    appContainer: document.body,
    mainContainer: document.getElementById('viewerContainer'),
    viewerContainer: document.getE...
```

http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/build/pdf.js

```
/**
 * @licstart The following is the entire license notice for the
 * Javascript code in this page
 *
 * Copyright 2018 Mozilla Foundation
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 *     http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 *
 * @licend The above is the entire license notice for the
 * Javascript code in this page
 */

(function webpackUniversalModuleDefinition(root, factory) {
 if(typeof exports === 'object' && typeof module === 'object')
         module.exports = factory();
 else if(typeof define === 'function' && define.amd)
         define("pdfjs-dist/build/pdf", [], factory);
 else if(typeof exports === 'object')
         exports["pdfjs-dist/build/pdf"] = factory();
 else
         root["pdfjs-dist/build/pdf"] = root.pdfjsLib = factory();
})(this, function() {
return /******/ (function(modules) { // webpackBootstrap
/******/        // The module cache
/******/        var installedModules = {};
/******/
/******/        // The require function
/******/        function __w_pdfjs_require__(moduleId) {
/******/
/******/                // Check if module is in cache
/******/                if(installedModules[moduleId]) {
/******/                        return installedModules[moduleId].exports;
/******/                }
/******/                // Create a new module (and put it into the cache)
/******/                var module = installedModules[moduleId] = {
/******/                        i: moduleId,
/******/                        l: false,
/******/                        exports: {}
/******/                };
/******/
/******/                // Execute the module function
/******/                modules[moduleId].call(module.exports, module, module.exports, __w_pdfjs_require__);
/******/
/******/                // Flag the module as loaded
/******/                module.l = true;
/******/
/******/                // Return the exports of the module
/******/                return module.exports;
/******/        }
/******/
/******/
/******/        // expose the modules object (__webpack_modules__)
/******/        __w_pdfjs_require__.m = modules;
/******/
/******/        // expose the module cache
/******/        __w_pdfjs_require__.c = installedModules;
/******/
/******/        // define getter function for harmony exports
/******/        __w_pdfjs_require__.d = function(exports, name, getter) {
/******/                if(!__w_pdfjs_require__.o(exports, name)) {
/******/                        Object.defineProperty(exports, name, { enumerable: true, get: getter });
/******/                }
/******/        };
/******/
/******/        // define __esModule on exports
/******/        __w_pdfjs_require__.r = function(exports) {
/******/                if(typeof Symbol !== 'undefined' && Symbol.toStringTag) {
/******/                        Object.defineProperty(exports, Symbol.toStringTag, { value: 'Module' });
/******/                }
/******/                Object.defineProperty(exports, '__esModule', { value: true });
/******/        };
/******/
```

```
/******/        // create a fake namespace object
/******/        // mode & 1: value is a module id, require it
/******/        // mode & 2: merge all properties of value into the ns
/******/        // mode & 4: return value when already ns object
/******/        // mode & 8|1: behave like require
/******/        __w_pdfjs_require__.t = function(value, mode) {
/******/                if(mode & 1) value = __w_pdfjs_require__(value);
/******/                if(mode & 8) return value;
/******/                if((mode & 4) && typeof value === 'object' && value && value.__esModule) return
value;
/******/                var ns = Object.create(null);
/******/                __w_pdfjs_require__.r(ns);
/******/                Object.defineProperty(ns, 'default', { enumerable: true, value: value });
/******/                if(mode & 2 && typeof value != 'string') for(var key in value)
__w_pdfjs_require__.d(ns, key, function(key) { return value[key]; }.bind(null, key));
/******/                return ns;
/******/        };
/******/
/******/        // getDefaultExport function for compatibility with non-harmony modules
/******/        __w_pdfjs_require__.n = function(module) {
/******/                var getter = module && module.__esModule ?
/******/                        function getDefault() { return module['default']; } :
/******/                        function getModuleExports() { return module; };
/******/                __w_pdfjs_require__.d(getter, 'a', getter);
/******/                return getter;
/******/        };
/******/
/******/        // Object.prototype.hasOwnProperty.call
/******/        __w_pdfjs_require__.o = function(object, property) { return
Object.prototype.hasOwnProperty.call(object, property); };
/******/
/******/        // __webpack_public_path__
/******/        __w_pdfjs_require__.p = "";
/******/
/******/
/******/        // Load entry module and return exports
/******/        return __w_pdfjs_require__(__w_pdfjs_require__.s = 0);
/******/ })
/************************************************************************/
/******/ ([
/* 0 */
/***/ (function(module, exports, __w_pdfjs_require...
```

http://127.0.0.1:8000/xmjg/xmjg/csrk/pdfShow/build/pdf.worker.js

```
/**
 * @licstart The following is the entire license notice for the
 * Javascript code in this page
 *
 * Copyright 2018 Mozilla Foundation
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 *     http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 *
 * @licend The above is the entire license notice for the
 * Javascript code in this page
 */

(function webpackUniversalModuleDefinition(root, factory) {
 if(typeof exports === 'object' && typeof module === 'object')
         module.exports = factory();
 else if(typeof define === 'function' && define.amd)
         define("pdfjs-dist/build/pdf.worker", [], factory);
 else if(typeof exports === 'object')
```

```
         exports["pdfjs-dist/build/pdf.worker"] = factory();
 else
         root["pdfjs-dist/build/pdf.worker"] = root.pdfjsWorker = factory();
})(this, function() {
return /******/ (function(modules) { // webpackBootstrap
/******/        // The module cache
/******/        var installedModules = {};
/******/
/******/        // The require function
/******/        function __w_pdfjs_require__(moduleId) {
/******/
/******/                // Check if module is in cache
/******/                if(installedModules[moduleId]) {
/******/                        return installedModules[moduleId].exports;
/******/                }
/******/                // Create a new module (and put it into the cache)
/******/                var module = installedModules[moduleId] = {
/******/                        i: moduleId,
/******/                        l: false,
/******/                        exports: {}
/******/                };
/******/
/******/                // Execute the module function
/******/                modules[moduleId].call(module.exports, module, module.exports, __w_pdfjs_require__);
/******/
/******/                // Flag the module as loaded
/******/                module.l = true;
/******/
/******/                // Return the exports of the module
/******/                return module.exports;
/******/        }
/******/
/******/
/******/        // expose the modules object (__webpack_modules__)
/******/        __w_pdfjs_require__.m = modules;
/******/
/******/        // expose the module cache
/******/        __w_pdfjs_require__.c = installedModules;
/******/
/******/        // define getter function for harmony exports
/******/        __w_pdfjs_require__.d = function(exports, name, getter) {
/******/                if(!__w_pdfjs_require__.o(exports, name)) {
/******/                        Object.defineProperty(exports, name, { enumerable: true, get: getter });
/******/                }
/******/        };
/******/
/******/        // define __esModule on exports
/******/        __w_pdfjs_require__.r = function(exports) {
/******/                if(typeof Symbol !== 'undefined' && Symbol.toStringTag) {
/******/                        Object.defineProperty(exports, Symbol.toStringTag, { value: 'Module' });
/******/                }
/******/                Object.defineProperty(exports, '__esModule', { value: true });
/******/        };
/******/
/******/        // create a fake namespace object
/******/        // mode & 1: value is a module id, require it
/******/        // mode & 2: merge all properties of value into the ns
/******/        // mode & 4: return value when already ns object
/******/        // mode & 8|1: behave like require
/******/        __w_pdfjs_require__.t = function(value, mode) {
/******/                if(mode & 1) value = __w_pdfjs_require__(value);
/******/                if(mode & 8) return value;
/******/                if((mode & 4) && typeof value === 'object' && value && value.__esModule) return
value;
/******/                var ns = Object.create(null);
/******/                __w_pdfjs_require__.r(ns);
/******/                Object.defineProperty(ns, 'default', { enumerable: true, value: value });
/******/                if(mode & 2 && typeof value != 'string') for(var key in value)
__w_pdfjs_require__.d(ns, key, function(key) { return value[key]; }.bind(null, key));
/******/                return ns;
/******/        };
/******/
/******/        // getDefaultExport function for compatibility with non-harmony modules
/******/        __w_pdfjs_require__.n = function(module) {
/******/                var getter = module && module.__esModule ?
/******/                        function getDefault() { return module['default']; } :
/******/                        function getModuleExports() { return module; };
/******/                __w_pdfjs_require__.d(getter, 'a', getter);
```

```
/******/                return getter;
/******/        };
/******/
/******/        // Object.prototype.hasOwnProperty.call
/******/        __w_pdfjs_require__.o = function(object, property) { return
Object.prototype.hasOwnProperty.call(object, property); };
/******/
/******/        // __webpack_public_path__
/******/        __w_pdfjs_require__.p = "";
/******/
/******/
/******/        // Load entry module and return exports
/******/        return __w_pdfjs_require__(__w_pdfjs_require__.s = 0);
/******/ })
/************************************************************************/
/******/ ([
/* 0 */
/***/ (function(module, ex...
```

http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do

```
var ctx="/xmjg/";var bigScreenFolder="";//var bigScreenFolder="bigscreenTwo";var tjkssj="2020-01-01";var
tjjssj="2020-12-29";var provinceCode="660000";var dateEnd = "2020-12-29";var dataType = "9";var stageType =
"0";var provinceDrillXzqhdm ='';
```

http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/analysis-ranking-overdue.do

```
$(function(){doInit();          $("#goBackBtn").click(function () {
commonWindow.returnParentWindow();          });          $("#goBackProvinceBtn").click(function () {
//todo 返回按钮要重新请求 待优化返回逻辑          provinceDrillXzqhdm='';
getAnalysisCityOverdueRankingData(null,true);          });});
```

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/analysis-ranking-overdue.js

```
/**
 *
 */
var cityObj={};
var dataObj;
var pageSize=27,pageNo=0;
var _ObjId="";
var xzqhdmss="";
var orderByFlag="1";
var listStrCc="";
var showStageTitle='';
function doInit(){
 var startDays=tjkssj.split("-");
 $("#startDay").html(startDays[0]+"       年"+startDays[1]+"月"+startDays[2]+"日");
 var dateEnds=dateEnd.split("-");
 $("#endDay").html(dateEnds[0]+"       年"+dateEnds[1]+"月"+dateEnds[2]+"日");

    $('.stage-tab-tit1 a').click(function(e) {
        var selfIndex = $(this).index()
        $(this).addClass('active').siblings().removeClass('active');
        $(this).parent().siblings().children('div:eq(' + selfIndex +
')').addClass('active').siblings().removeClass('active');
        $(".rank-title1").html(showStageTitle+$(this).html());
        var ss="个";
        if(selfIndex==0){
          ss="%";
        }
        $("#index-card-tit_id").html("单位: "+ss);
        var flag=selfIndex+1;
        tapCharts(flag);
    });
 $('.div-arrow-left').click(function(){
         pageNo--;
         setData();
 });
 $('.div-arrow-right').click(function(){
         pageNo++;
         setData();
 });
 getAnalysisCityOverdueRankingData(null,true);
 commonFunction.doSaveFunctionLog({"functionUrl":window.location.href,"functionName":"       监督检查-项目逾期率
排名"});
}

function tapCharts(flag){
 var isDefault = true;
 if(orderByFlag!=flag){
         orderByFlag=flag;
        isDefault = false;
         getAnalysisCityOverdueRankingData(provinceCode,isDefault);
        }
}

/**
 * 各城市项目逾期率排名
 * @returns
 */
function getAnalysisCityOverdueRankingData(xzqhdm,isDefalut){
 var ajaxParams={"tjkssj":tjkssj,"tjjssj":tjjssj,"orderByFlag":orderByFlag};
 if(xzqhdmss && xzqhdmss!=""){
         ajaxParams["xzqhdmss"]=xzqhdmss;
        }
    var showCityName = xzqhdm==null?((provinceCode && provinceCode!="")?'师市':'省份'):"师市";
    listStrCc="<tr><th width='10%'>排名</th><th width:12%;>"+showCityName+"</th><th width='22%'>项目数(个)</th>
<th width='25%'>逾期项目数(个)</th><th width='22%'>逾期率(%)</th></tr>";
    showStageTitle = xzqhdm==null?((provinceCode && provinceCode!="")?'各师市项目':'各省项目'):"各师市项目";
 //        加载进来或省级下钻时默认显示的标题
 if(isDefalut){
        var showTitle = xzqhdm==null?((provinceCode && provinceCode!="")?'各师市项目逾期率排名':'各省项目逾期率排
名'):'各师市项目逾期率排名';
        $(".rank-title1").html(showTitle);
        }
    //xzqhdm 值不为null 时 表示点击图表中的省继续钻取
    if(xzqhdm !=null){
        ajaxParams["provinceCode"]=xzqhdm;
        $("#goBackBtn").hide();
        $("#goBackProvinceBtn").show();
    }else{
        if(provinceCode && provinceCode!=""){
          ajaxParams["provinceCode"]=provinceCode;
        }
        $("#goBackBtn").show();
        $("#goBackProvinceBtn").hide();
    }

 $.ajax({
         type : "POST",
         url :ctx+"supervisionInspectionDrill/getAnalysisCityOverdueRankingData.do",
         data:ajaxParams,
         dataType : 'json',
         success : function(data) {
                 $(".rank-list-css").html(listStrCc);
                 echarts.init(document.getElementById("rank_lineBar11")).dispose();
                 if(data.result=="0"){
                         dataObj=data.data;
                         pageNo=0;
                         setData();
                 }else{
                         $(".div-arrow-left").hide();
                         $(".div-arrow-right").hide();
                        }
                }
 });
}

function setData(){
 var listStr="";
 $(".rank-list-css").html(listStrCc);
 var cityCodesss="",cityNamesss="";

 var xAxisData=[],seriesDatas=[],xAxisDataVal="";
 var index=1;
 var indexff=0,tableIndex=0;
 var startIndex=pageNo*pageSize;
 var length=(pageNo+1)*pageSize;
 var total=0;
 if(length>=dataObj.length){
         length=dataObj.length;
         $(".div-arrow-right").hide();
 }else{
         $(".div-arrow-right").show();
        }
 if(pageNo>0){
         $(".div-arrow-left").show();
 }else{
         $(".div-arrow-left").hide();
        }


 for(var i=startIndex;i<length;i++){
         total =+ i;
         if(i==startIndex){
                 cityCodesss=dataObj[i]["XZQHDM"];
                 cityNamesss=dataObj[i]["NAME"];
         }else{
                 cityCodesss+=","+dataObj[i]["XZQHDM"];
                 cityNamesss+=","+dataObj[i]["NAME"];
                }
        xAxisDataVal=dataObj[i]["NAME"];
        if(xAxisDataVal!=null
          &&xAxisDataVal.lastIndexOf("市") == xAxisDataVal.length){
          xAxisDataVal=xAxisDataVal.replace("市","");//x轴：去除dataObj里的市，保留城市名
        }
         cityObj[xAxisDataVal]=dataObj[i]["XZQHDM"];
         xAxisData.push(xAxisDataVal);
         if(orderByFlag=="1"){
                 seriesDatas.push(commonFunction.getDataNullIsZero(dataObj[i]
["OVERDUE_PER"]).toFixed(1));
         }else{
                 seriesDatas.push(commonFunction.getDataNullIsZero(dataObj[i]["OVERDUE_CNT"]));
                }
         if(indexff==0){
                 listStr=listStrCc;
                }
         if(commonFunction.getDataNullIsZero(dataObj[i]["OVERDUE_CNT"])==0){
                 listStr+="<tr><td width='10%'>"+(index+i)+"</td><td width='22%'>"+xAxisDataVal+"</td>
<td width='22%'>"+commonFunction.getDataNullIsZero(dataObj[i]["TOTAL_CNT"])+"</td><td width='25%'
class='red'>"+commonFunction.getDataNullIsZero(dataObj[i]["OVERDUE_CNT"])+"</td><td
width='22%'>"+commonFunction.getDataNullIsZero(dataObj[i]["OVERDUE_PER"])+"%</td></tr>";
         }else{
                 listStr+="<tr><td width='10%'>"+(index+i)+"</td><td width='22%'>"+xAx...
```

http://127.0.0.1:8000/xmjg/xmjg/supervisionInspection/js/common-charts.js

```
var cityCode;
/**
 * 加载柱状图 <多个柱子>
 * @param chartsParams{
 *   objId     <必须>
 *   legendData x主标数据分组 <必须>
 *   xAxisData  x坐标数据  <必须>
 *   seriesDatas y坐标数据  <必须>
 *   colorData  柱子颜色
 *   provideNumber  x坐标 文字一行长度
 *   ...
 * }
 * @param onclickFunction 点击方法
 * @returns
 */
function doBarCharts(chartsParams,onclickFunction){
 var legendData=chartsParams.legendData;
 var xAxisData=chartsParams.xAxisData;
 var seriesDatas=chartsParams.seriesDatas;
 var objId=chartsParams.objId;
 var seriesObj=[],zearVall=[];
 var barWidth="20%";
 var xAxisFontSize=14;
 var barFontSize = 12;
 var legendFontSize=15;
 var gridBbottom="5%";
 var tooltipFontSize=18;
 var color = "#fff";
 if(screen == "3"){
        color="#545C6A";
        }
/*      if(getBigScreen()=="bigscreen"){
          barWidth="20%";
          xAxisFontSize=24;
          legendFontSize=24;
          gridBbottom="10%";
 }*/
 if(getBigScreen()=="bigscreen" || bigScreenFolder == 'bigscreenTwo/'){
          barWidth="15%";
          xAxisFontSize=24;
          barFontSize=24;
          legendFontSize=24;
          gridBbottom="2%";
        }
 if(chartsParams.barWidth){
         barWidth=chartsParams.barWidth;
        }
 if(chartsParams.xAxisFontSize){
         xAxisFontSize=chartsParams.xAxisFontSize;
        }
 var vall=null;
 for(var i=0;i<legendData.length;i++){
         zearVall.push(0);
        }
 for(var i=0;i<seriesDatas.length;i++){
         if(seriesDatas==null || seriesDatas.length<=i-1 || seriesDatas[i]==undefined ||
seriesDatas[i]==null){
                 vall=zearVall;
         }else{
                 vall=seriesDatas[i];
                }
         seriesObj.push({name: legendData[i],type: 'bar',data: vall,barWidth: barWidth,
                 label: {normal: {
                                 show: true,
          rotate: 90,
          align: 'left',
          verticalAlign: 'middle',
                                 position:  "insideTop",//'top',*/
                                 textStyle: {color: color, fontSize: barFontSize}
                 }}});
        }
 var provideNumber=8;
 if(chartsParams.provideNumber){
         provideNumber=chartsParams.provideNumber;
        }
 var colorData=[];
 if(!chartsParams.colorData  || chartsParams.colorData.length<=0){
         if(legendData.length==1){
                 colorData=['#5d91dd'];
         }else if(legendData.length==2){
                 colorData=['#5d91dd','#6bc0d5'];
         }else if(legendData.length==3){
                 colorData=['#5d91dd','#6bc0d5','#9d66e8'];
         }else if(legendData.length==4){
                 colorData=['#5d91dd','#6bc0d5','#9d66e8','#ff6b6b'];
                }
 }else{
         colorData=chartsParams.colorData;
        }
 var pillar1 = echarts.init(document.getElementById(objId));
 var option = {
     color: colorData,
     tooltip : {
         trigger: 'axis',
         textStyle: {
          fontSize: tooltipFontSize
         },
         axisPointer : {          //        坐标轴指示器，坐标轴触发有效
           type : 'shadow'        //        默认为直线，可选为：'line' | 'shadow'
         }
     },
        legend: {
                top: '2%',
         data: legendData,
         textStyle: {
           color: "#abcaf3",
           fontSize: legendFontSize
         },
         itemWidth: 18,
         itemHeight: 18,
         itemGap: 30
     },
     grid: {top: '15%',left: '4%', right: '4%',bottom: gridBbottom,containLabel: true},
     xAxis : [
         {
           type : 'category',
           data : xAxisData,
           axisTick: {
           show: false
           },
           splitLine: {
                   show: false
                 },
           axisLabel: {
                   textStyle: {
                   fontSize: xAxisFontSize,
                   color:color
                   },
                   formatter:function(params) {
          var newParamsName = "";
          var paramsNameNumber = params.length;
          var rowNumber = Math.ceil(paramsNameNumber / provideNumber);
          if (paramsNameNumber > provideNumber) {
          for (var p = 0; p < rowNumber; p++) {
          var tempStr = "";
          var start = p * provideNumber;
          var end = start + provideNumber;
          if (p == rowNumber - 1) {
          tempStr = params.substring(start, paramsNameNumber);
          } else {
          tempStr = params.substring(start, end) + "\n";
          }
          newParamsName += tempStr;
          }

          } else {
          newParamsName = params;
          }
          return newParamsName
          }
                 },
                 axisLine: {
                   lineStyle: {
                   color: '#336bbd',
                   width: '1'
                   }
                  }
         }
     ],
     yAxis : [
         {
           type : 'value',
           min: 0,
     ...
```

http://127.0.0.1:8000/xmjg/supervisionInspectionDrill/getSupervisionInspectionDrillPage.do

```
    var ctx = '/xmjg/';    var provinceCode= "660000";    var StartDate_pjys = "2020-01-01";    var
EndDate_pjys = "2020-12-29";    var dateEnd =  "2020-12-29";    var bigScreenFolder="";    var jsgz2 = [
{           "index":0,           "splclx":1,           "splcmc":"政府投资工程建设项目（房屋建筑类）",
"spjds":[           {"pjys":13},           {"pjys":16},           {"pjys":15},           {"pjys":15},
{"pjys":22}           ],           "zpjys":83        },        {           "index":1,           "splclx":2,
"splcmc":"政府投资工程建设项目（线性工程类）",           "spjds":[           {"pjys": 15},           {"pjys": 20},
{"pjys": 20},           {"pjys": 16},           {"pjys": 21}           ],           "zpjys":95        },        {
"index":2,           "splclx":3,           "splcmc":"一般社会投资项目",           "spjds":[           {"pjys": 13},
{"pjys": 17},           {"pjys": 17},           {"pjys": 19},           {"pjys": 24}           ],
"zpjys":92        },        {           "index":3,           "splclx":4,           "splcmc":"小型社会投资项目",
"spjds":[           {"pjys": 11},           {"pjys": 15},           {"pjys": 15},           {"pjys": 19},
{"pjys": 24}           ],           "zpjys":86        },        {           "index":4,           "splclx":5,
"splcmc":"带方案出让用地的社会投资项目",           "spjds":[           {"pjys": 15},           {"pjys": 11},
{"pjys": 17},           {"pjys": 15},           {"pjys": 25}           ],           "zpjys":85        }    ];
var jsgz3 = [        {           "index":0,           "splclx":1,           "splcmc":"政府投资工程建设项目（房屋建筑
类）",           "spjds":[           {"pjys":29},           {"pjys":18},           {"pjys":10},
{"pjys":16},           {"pjys":24}           ],           "zpjys":99        },        {           "index":1,
"splclx":2,           "splcmc":"政府投资工程建设项目（线性工程类）",           "spjds":[           {"pjys": 25},
{"pjys": 13},           {"pjys": 15},           {"pjys": 11},           {"pjys": 22}           ],
"zpjys":89        },        {           "index":2,           "splclx":3,           "splcmc":"一般社会投资项目",
"spjds":[           {"pjys": 20},           {"pjys": 16},           {"pjys": 20},           {"pjys": 20},
{"pjys": 20}           ],           "zpjys":99        },        {           "index":3,           "splclx":4,
"splcmc":"小型社会投资项目",           "spjds":[           {"pjys": 15},           {"pjys": 7},           {"pjys":
8},           {"pjys": 12},           {"pjys": 11}           ],           "zpjys":56        },        {
"index":4,           "splclx":5,           "splcmc":"带方案出让用地的社会投资项目",           "spjds":[
{"pjys": 3},           {"pjys": 4},           {"pjys": 10},           {"pjys": 13},           {"pjys": 2}
],           "zpjys":33        }    ];    $(function () {        if(bigScreenFolder == 'bigscreenTwo/'){
$('body').css({'padding':"0 12.5%",'font-size': '28px'});           $(".pjysBack").css({border: '1px solid
#8daecd',background: '#336bbd','border-radius':'10px'});        }    })    /*项目实际审批用时使用投影算法，将各阶段
内的实际审批事项的审批时间在时间轴上投影，去除重复投影及没有投影的时间段剩下的时间作为各阶段审批用时，各阶段审批用时之和为项目审批
用时。完整阶段审批用时选取事项完整的阶段作为样本，基于样本阶段计算各阶段的审批用时，各阶段审批用时之和为项目审批用时。流程推算审批
用时将阶段内每个事项的审批用时按并联审批和串联审批的权重加权求和作为阶段的审批用时，各阶段审批用时之和为项目审批用时。*/    var
loading='';    var pjysVm = new Vue({        el:'#averageTime',        data:{           checked: false,//剔除异
常数据           gz1:true,           gz2:false,           gz3:false,           jsgzItemArr:['项目实际审批用时','完整
阶段审批用时','流程推算审批用时'],           showJsgz:['项目实际审批用时'],           titleArr:['立项用地规划许可','工程建
设许可','施工许可','竣工验收','并行审批'],           resData:"",           resDataNew:'',//剔除异常数据
resData2: jsgz2,//计算规则2           resData3: jsgz3,//计算规则2           isBigScreen: bigScreenFolder ==
'bigscreenTwo/'?true :false,           loading:'',           initOtherData:false,        },        watch:{
checked:function (val, newval) {           if(val && !this.initOtherData){           this.getInitData(1);
this.initOtherData = true;           }           }        },        methods:{           //返回
averageTimeBack:function () {           commonWindow.returnParentWindow();           },           //请求数据
getInitData:function (param) {           this.openFullScreen2();           var _that = this;           $.ajax({
url:ctx+"supervisionInspection/getPjysByTjjssj.do",           data:{           xzqhdm:provinceCode,
...
```

http://127.0.0.1:8000/xmjg/xmjg/sjjc/js/tool/common.js

```
/**
 * 外部js调用
 */
var commonWindow = {
    //打开页面
    toWindowForReturn: function (url, pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
//          pageObj.commonWindowAction.doWindowForReturn(encodeURI(url));
                console.log(encodeURI(url))
          pageObj.commonWindowAction.doWindowForReturn(encodeURI(url));

        }
    },


    //打开页面  不支持返回
    toWindowNotReturn: function (url, pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
          pageObj.commonWindowAction.doWindowNotReturn(url);
        }
    },

    //返回上一页面
    returnParentWindow: function (pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
          pageObj.commonWindowAction.doReturnParentWindow();
        }
    },
    //跳转到对应页面(传入的url与之前的iframe地址一致的时候 退回到对应iframe,如果不存在 则调用toWindowForReturn)
    jumpWindowForIframe: function (url, pageFlag) {
        var pageObj = commonWindow.getWindowObj(pageFlag);
        if (pageObj) {
          pageObj.commonWindowAction.doJumpWindowForIframe(url);
        }
    },
    //获取对应的页面  pageFlag (max-top-page: 最顶级页面;)
    getWindowObj: function (pageFlag) {
        if (!pageFlag) {
          pageFlag = "max-top-page";
        }
        var obj = window.self;
        var whileFlag = true;
        while (whileFlag) {
          if (obj.document.getElementById("page-level-flag-in")) {
          //最顶级页面
          if (obj.document.getElementById("page-level-flag-in").value == pageFlag) {
          return obj;
          }
          }
          if (whileFlag) {
          if (obj.window.parent != obj.window) {
          obj = obj.window.parent;
          } else {
          whileFlag = false;
          }
          }
        }
        return window.self;
    },
};

//===========================================================================================================
=================

var commonWindowAction = {
    doWindowForReturn: function (url) {
        var maxDataIndex = 0;
        var $lastIframe;
        $(".content-url-iframe").each(function () {
          var thisDataIndex = parseInt($(this).attr("data-index"));
          if (maxDataIndex < thisDataIndex) {
          maxDataIndex = thisDataIndex;
          }
          if (maxDataIndex == thisDataIndex) {
          $lastIframe = $(this);
          }
          commonWindowAction.doRemoveClass($(this), "curr-url-iframe");
        });
        if ($lastIframe) {
          var timestamp = (new Date()).valueOf();
          var key = "contentframe-id-" + timestamp + "-" + (maxDataIndex + 1);
          $lastIframe.after("<iframe allowfullscreen  id=\"" + key + "\" width=\"100%\" height=\"100%\"
src=\"\" frameborder=\"0\" class=\"content-url-iframe  curr-url-iframe\" data-index=\"" + (maxDataIndex + 1)
+ "\"></iframe>");
          $("#" + key).attr("src", url);
        }
        console.log(url)
        commonWindowAction.removeIframeOrHide(true);

    },
    doWindowNotReturn: function (url) {
        $(".content-url-iframe").each(function () {
                if($(this).hasClass("curr-url-iframe")){
                        if(url.indexOf("?")<=-1){
                                url+="?";
                        }else{
                                url+="&";
                        }
                        url+="notHaveReturnFlag=yes";
                        $(this).attr("src", url);
                        $(this).attr("id","contentframe");
                        $(this).attr("data-index","0");
                }else{
          commonWindowAction.doRemoveClass($(this), "curr-url-iframe");
          }
        });
        commonWindowAction.removeIframeOrHide(false);
    },
    //执行返回上一页
    doReturnParentWindow: function () {
        var $lastIframe;
        var maxDataIndex = 0;

        $(".curr-url-iframe").each(function (i) {
          if (i == 0) {
          if ($(this).attr("data-index") == "0") {
          return;
          }
          maxDataIndex = parseInt($(this).attr("data-index")) - 1;
          $lastIframe = $(this);
          }
        })
        $(".content-url-iframe").each(function () {
         if ($lastIframe.attr("src") == $(this).attr("src")) {
           maxDataIndex = parseInt($(this).attr("data-index")) - 1;
           return false;
         }
        });
        if (maxDataIndex <= 0) {
          maxDataIndex = 0;
          $(".content-url-iframe").each(function () {
          var thisDataIndex = parseInt($(this).attr("data-index"));
          if (maxDataIndex == thisDataIndex) {
          $(this).show();
          commonWindowAction.doAddClass($(this), "curr-url-iframe");
          } else {
          commonWindowAction.doRemoveClass($(this), "curr-url-iframe");
          }
    ...
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
          var ctx='/xmjg/';var bigScreenFolder="";var xzqhdms="";var tjkssj="2020-01-01";var tjjssj="2020-12-
29";var orderByFlag="";var dataType="1";var sfzb="1";var sfbyxz="";var sfjgqqxt="";var spjd="";var
blqk="";var splclx="";var splcmc="";var sfyq="";var tjTypeVal="";var qtTypeVal = "";var splcbm="";var dateEnd
= "2020-12-29";var provinceCode="";var dataType="1";  //1:各阶段平均用时（审批用时）; 2:各阶段跨度用时; 3:各阶段最长
用时; 4:各阶段平均受理次数;var stageType=""; //0: 总数，1: 立项用地规划许可; 2: 工程建设许可; 3: 施工许可; 4: 竣工验收
var oldStartDate = "2020-01-01";          var oldEndDate = "2020-12-29";          var flag="2";          var
xzqhdm="660300"; //跳转带过来的行政区划代码 用于钻取标题显示          var name="三师图木舒克市";//跳转带过来的城市名称 用
于钻取标题显示var sfType = "";//算法类型
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
        function newsearch(){        var i=document.getElementById("pageSize").value;       var
n=document.getElementById("pageNo").value;       var m="88";        if(m<i){
document.getElementById("pageNo").value=1;        search();        }else{        var u=Math.ceil(m/i)
if(n>u){        $.messager.alert('提示','页数超出限制');        }else{        search();        }        }
}        $(function(){          $('#pageNo').bind('keypress', function (event) {          if (event.keyCode
== "13") {          //需要处理的事情var pageNo = $(this).val();          pageNo = parseInt(pageNo);
var pages = $(this).data('pages');    //最大页码          if(pageNo < 1) {          pageNo = 1;          }
if(pageNo > pages){          pageNo = pages;          }          jumpPage(pageNo);   //跳转页面          }
});        });
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
jumpPage(9)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2019-659003-51-03-009674')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-44-01-012763')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-47-01-008657')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-83-01-006550')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-653127-78-01-002487')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-54-01-002173')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-47-01-012089')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-41-03-002603')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
          var ctx='/xmjg/';var bigScreenFolder="";var xzqhdms="";var tjkssj="2020-01-01";var tjjssj="2020-12-
29";var orderByFlag="";var dataType="15";var sfzb="1";var sfbyxz="";var sfjgqqxt="";var spjd="1";var
blqk="1";var splclx="";var splcmc="";var sfyq="";var tjTypeVal="";var qtTypeVal = "";var splcbm="";var
dateEnd = "2020-12-29";var provinceCode="";var dataType="15";  //1:各阶段平均用时（审批用时）; 2:各阶段跨度用时; 3:
各阶段最长用时; 4:各阶段平均受理次数;var stageType="1"; //0：总数，1：立项用地规划许可；2：工程建设许可；3：施工许可；4：竣
工验收          var oldStartDate = "2020-01-01";          var oldEndDate = "2020-12-29";          var
flag="1";          var xzqhdm="660000"; //跳转带过来的行政区划代码 用于钻取标题显示          var name="新疆生产建设兵
团";//跳转带过来的城市名称 用于钻取标题显示var sfType = "";//算法类型
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
        function newsearch(){        var i=document.getElementById("pageSize").value;       var
n=document.getElementById("pageNo").value;       var m="476";        if(m<i){
document.getElementById("pageNo").value=1;        search();        }else{        var u=Math.ceil(m/i)
if(n>u){        $.messager.alert('提示','页数超出限制');        }else{        search();        }        }
}        $(function(){          $('#pageNo').bind('keypress', function (event) {          if (event.keyCode
== "13") {          //需要处理的事情var pageNo = $(this).val();          pageNo = parseInt(pageNo);
var pages = $(this).data('pages');    //最大页码          if(pageNo < 1) {          pageNo = 1;          }
if(pageNo > pages){          pageNo = pages;          }          jumpPage(pageNo);   //跳转页面          }
});        });
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
jumpPage(48)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660700,'2020-654003-47-03-011814')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-47-01-008663')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(661400,'2020-653223-54-01-012667')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660900,'2020-654221-47-03-010351')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660900,'2019-654221-44-01-008942')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-44-01-013472')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660800,'2020-659001-01-03-006059')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(661300,'2020-652201-78-01-000269')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
          var ctx='/xmjg/';var bigScreenFolder="";var xzqhdms="";var tjkssj="2020-01-01";var tjjssj="2020-12-
29";var orderByFlag="";var dataType="15";var sfzb="";var sfbyxz="";var sfjgqqxt="";var spjd="1";var
blqk="3";var splclx="";var splcmc="";var sfyq="";var tjTypeVal="";var qtTypeVal = "0";var splcbm="";var
dateEnd = "2020-12-29";var provinceCode="";var dataType="15";  //1:各阶段平均用时（审批用时）; 2:各阶段跨度用时; 3:
各阶段最长用时; 4:各阶段平均受理次数;var stageType="1"; //0：总数，1：立项用地规划许可；2：工程建设许可；3：施工许可；4：竣
工验收          var oldStartDate = "2020-01-01";          var oldEndDate = "2020-12-29";          var
flag="2";          var xzqhdm="660300"; //跳转带过来的行政区划代码 用于钻取标题显示          var name="三师图木舒克
市";//跳转带过来的城市名称 用于钻取标题显示var sfType = "";//算法类型
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
        function newsearch(){        var i=document.getElementById("pageSize").value;       var
n=document.getElementById("pageNo").value;       var m="21";        if(m<i){
document.getElementById("pageNo").value=1;        search();        }else{        var u=Math.ceil(m/i)
if(n>u){        $.messager.alert('提示','页数超出限制');        }else{        search();        }        }
}        $(function(){          $('#pageNo').bind('keypress', function (event) {          if (event.keyCode
== "13") {          //需要处理的事情var pageNo = $(this).val();          pageNo = parseInt(pageNo);
var pages = $(this).data('pages');    //最大页码          if(pageNo < 1) {          pageNo = 1;          }
if(pageNo > pages){          pageNo = pages;          }          jumpPage(pageNo);   //跳转页面          }
});        });
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-77-01-007610')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-50-01-004476')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-47-01-008708')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-49-01-010969')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-47-01-008682')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-49-01-010968')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-49-01-010967')
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
clickView(660300,'2020-659003-47-01-008661')
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
        $(function(){
if($(window.parent.document).find("#xndc_content_frame").prop("id")=="xndc_content_frame"){
$("#SY").attr("target","_parent");           }           loadSortIcon();           pageNumKeyPress();         });
function pageNumKeyPress(){           $('#pageNum').bind('keypress', function (event) {           if
(event.keyCode == "13") {           //需要处理的事情           var pageNo = $(this).val();           pageNo =
parseInt(pageNo);           var pages = $(this).data('pages');    //最大页码           if(pageNo < 1) {
pageNo = 1;           }           if(pageNo > pages){           pageNo = pages;           }
agcloudJumpPage(pageNo);   //跳转页面           }           });         }         //操作按钮(修改、删除)图标鼠标移入移出
效果         function setImgSrc(imgObj,type){           var imgSrc=imgObj.src;           if(type=="over"){
imgObj.src=imgSrc.substring(0,imgSrc.indexOf(".png"))+"_hover.png";           }else{
imgObj.src=imgSrc.substring(0,imgSrc.indexOf("_hover.png"))+".png";           }         }         function
clickView(xzqhdm,xmdm){           //parent.window.location.href="xmjg-project-info!projectInfo.action?
```

```
id="+id;// var name ="${name}";          var djzt="";          var pageNo="25";          //获取搜索框的数据值
var searchXmdm = window.parent.document.getElementById("xmdm").value;          var searchXmmc =
window.parent.document.getElementById("xmmc").value;          var searchSpjdSearch =
window.parent.document.getElementById("spjdSearch").value;          var searchWhetherBinglian =
window.parent.document.getElementById("whether_binglian").value;          /*          var url=ctx+"/xmjg-
project-info!projectInfo.action?
xzqhdm="+xzqhdm+"&xmdm="+xmdm+"&currentPageNo="+pageNo+"&currentCityName="+currentCityName+"&name="+name+"&dj
zt="+djzt+
"&searchXmdm="+searchXmdm+"&searchXmmc="+searchXmmc+"&searchSpjdSearch="+searchSpjdSearch+"&searchWhetherBing
lian="+searchWhetherBinglian+"&startDate="+oldStartDate+"&endDate="+oldEndDate+"&intoWay=1";//intoWay:进入到流
程展示页面的方式：1表示从一个系统中进入，2表示从综合查询页面进入          */          var basePath = ctx;          var
url="mid-xmjg-project-info!projectInfo.action?
xzqhdm="+xzqhdm+"&xmdm="+xmdm+"&currentPageNo="+pageNo+"&currentCityName="+currentCityName+"&name="+name+"&dj
zt="+djzt+
"&searchXmdm="+searchXmdm+"&searchXmmc="+searchXmmc+"&searchSpjdSearch="+searchSpjdSearch+"&searchWhetherBing
lian="+searchWhetherBinglian+"&startDate="+oldStartDate+"&endDate="+oldEndDate+"&intoWay=1";
commonWindow.toWindowForReturn(basePath+url);          /*          parent.window.open(url);*/
//commonWindow.toWindowForReturn(url);          //parent.window.location.href=url;  //currentPageNo 当前的页数
currentCityName 当前选择的审批流程类型          //parent.window.location.href="xmjg-project-
info!projectInfo.action?
id="+id+"&currentPageNo="+${currentPageNo}+"&currentCityName="+currentCityName+"&name="+name;//currentPageNo
当前的页数 currentCityName 当前选择的审批流程类型        }        function locationmap(xmdm){//
$(window.parent.document.getElementById("Map")).css('display','block');$(window.parent.document.getElementByI
d("rightTjDiv")).css('display','none');
$(window.parent.document.getElementById("changetomap")).click();          setTimeout(function(){          var
win = window.parent.document.getElementById("dtzs_content_frame").contentWindow;          var data =
{type:1,value:{xmdm:xmdm}};          win.postMessage(JSON.stringify(data),"*");          }, 1000);        }
function toClearForm(){          //clearForm();          $("#xmdm").val("");          $("#xmmc").val("");
search();        }        //排序方法        function orderByTitle(orderByName,th){          parent.orderNameId
= $(th).attr("id");          if(parent.orderClickName == orderByName){          parent.orderClickCount ++;
}else{          parent.orderClickCount = 1;          }          parent.orderClickName = orderByName;
var cur_xmlx = parent.xmlx;          var cur_djzt = parent.djzt;          var cur_splcmc = parent.sub_splcmc;
var cur_splcbm = parent.sub_splcbm;          if(parent.orderClickCount % 2 == 1){          orderByName +=
"DESC";          }          var spjdUrl;          if($("#dateEnd",parent.document).val() == parent.dateStr){
spjdUrl=ctx+"projectInfo/qbMdxmList.do?
name="+parent.name+"&orderByName="+orderByName+"&djzt="+cur_djzt+"&splclx="+cur_xmlx+"&xzqhdm="+parent.xzqhdm
+"&splcmc="+cur_splcmc+"&splcbm="+cur_splcbm+"&currentPageNo=1&currentCityName="+cur_splcmc+"&startDate="+$("
#dateStart",parent.document).val().substring(0,4)+"-"+$("#dateStart",parent.document).val().substring(5,7)+"-
01"+"&endDate="+parent.defaultEnd;          }else{    ...
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
agcloudJumpPage(1)
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
agcloudJumpPage(24)
```

http://127.0.0.1:8000/xmjg/projectInfo/qbMdxmList.do

```
agcloudJumpPage(0)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
          var ctx='/xmjg/';var bigScreenFolder="";var xzqhdms="";var tjkssj="2020-01-01";var tjjssj="2020-12-
29";var orderByFlag="";var dataType="15";var sfzb="";var sfbyxz="";var sfjgqqxt="";var spjd="1";var
blqk="3";var splclx="";var splcmc="";var sfyq="";var tjTypeVal="";var qtTypeVal = "";var splcbm="";var
dateEnd = "2020-12-29";var provinceCode="";var dataType="15";  //1:各阶段平均用时（审批用时）; 2:各阶段跨度用时; 3:
```

```
各阶段最长用时; 4:各阶段平均受理次数;var stageType="1"; //0: 总数, 1: 立项用地规划许可; 2: 工程建设许可; 3: 施工许可; 4: 竣
工验收           var oldStartDate = "2020-01-01";           var oldEndDate = "2020-12-29";           var
flag="2";           var xzqhdm="660300"; //跳转带过来的行政区划代码 用于钻取标题显示           var name="三师图木舒克
市";//跳转带过来的城市名称 用于钻取标题显示var sfType = "";//算法类型
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
jumpPage(24)
```

http://127.0.0.1:8000/xmjg/city-page/getCityProjectList.do

```
jumpPage(25)
```

cookie 3

TOC

名称	首先设置	域	安全
值	请求的 URL		到期
JSESSIONID	http://127.0.0.1:8090/opus-front-sso/authentication/require	127.0.0.1	False
BE7491190EC980E7ACE00310E82D7BB9	http://127.0.0.1:8090/opus-front-sso/authentication/require		
JSESSIONID	http://127.0.0.1:8000/xmjg/opus/front/blue/index.html	127.0.0.1	False
88EC0811EF33C028F8A8929B13B6A33A	http://127.0.0.1:8000/xmjg/login		
username			False
admin	http://127.0.0.1:8090/opus-front-sso/authentication/form		