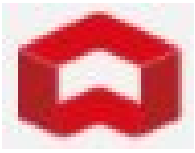

资源商城后台安全性审计测试报告

该报告包含有关 web 应用程序的重要安全信息。

OWASP Top 10 2017 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

条例

OWASP Top Ten 2017 – The Ten Most Critical Web Application Security Risks

Summary Description

The goal of the Top 10 project is to raise awareness about application security by identifying some of the most critical risks facing organizations. Development projects should address these potential risks in their requirements documents and design, build and test their applications to ensure that they have taken the necessary measures to reduce these risks to the minimum. Project managers should include time and budget for application security activities including developer training, application security policy development, security mechanism design and development, penetration testing, and security code review as part over the overall effort to address the risks.

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security risks. The Top 10 provides basic guidance on how to address against these risks and where to go to learn more on how to address them.

Although setout as an education piece, rather than a standard or a regulation, it is important to note that several prominent industry and government regulators are referencing the OWASP top ten. These bodies include among others VISA USA, MasterCard International and the American Federal Trade Commission (FTC).

However, according to the OWASP team the OWASP top ten first and foremost an education piece, not a standard. The OWASP team suggests that any organization about to adopt the Top Ten paper as a policy or standard to consult with the OWASP team first.

What Changed From 2013 to 2017?

The threat landscape for applications and APIs constantly changes. Key factors in this evolution are the rapid adoption of new technologies (including cloud, containers, and APIs), the acceleration and automation of software development processes like Agile and DevOps, the explosion of third-party libraries and frameworks, and advances made by attackers. These factors frequently make applications and APIs more difficult to analyze, and can significantly change the threat landscape. To keep pace, the OWASP organization periodically update the OWASP Top 10. In this 2017 release, following changes were made:

Merged 2013-A4: Insecure Direct Object References and 2013-A7: Missing Function Level Access Control back into 2017-A4: Broken Access Control.

Added 2017-A7: Insufficient Attack Protection.

Added 2017-A10: Underprotected APIs.

Dropped: 2013-A10: Unvalidated Redirects and Forwards.

Covered Entities

All companies and other entities that develop any kind of web application code are encouraged to address the top ten list as part of their over all security risk management. Adopting the OWASP Top Ten is an effective first step towards changing the software development culture within the organization into one that produces secure code.

For more information on OWASP Top Ten, please review the - OWASP Top Ten 2017 – The Ten Most Critical Web Application Security Risks, at http://www.owasp.org

For more information on securing web applications, please visit http://www-03.ibm.com/software/products/en/category/application-security

The information provided does not constitute legal advice. The results of a vulnerability assessment will demonstrate potential vulnerabilities in your application that should be corrected in order to reduce the likelihood that your information will be compromised. As legal advice must be tailored to the specific application of each law, and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent counsel. IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.

违例部分

在规则的 9/10 个部分中检测到问题：

部分	问题的数量
A1 - Injection	13
A2 - Broken authentication and session management	58
A3 - Cross site scripting (XSS)	24
A4 - Broken Access Control	142
A5 - Security Misconfiguration	87
A6 - Sensitive Data Exposure	90
A7 - Insufficient Attack Protection	1
A8 - Cross site request forgery (CSRF)	58
A9 - Using Components with Known Vulnerabilities	88
A10 - Underprotected APIs	0

部分违例（按问题）

在规则的 9/10 个部分中检测到 142 个唯一问题：

URL	实体	问题类型	部分
http://system-rest-enterprise.mall.xt.weilian.cn/		缺少“Content-Security-Policy”头	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/		自动填写未对密码字段禁用的 HTML 属性	A2, A4, A5, A8, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	2	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/		缺少“X-Content-Type-Options”头	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/		缺少“X-XSS-Protection”头	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/		过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/		使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html	缺少“Content-Security-Policy”头	A4, A5, A6, A9
http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	selectVipRoleList	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html	缺少“Content-Security-Policy”头	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getUserInfo	getUserInfo	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html	缺少“X-Content-Type-Options”头	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html	缺少“X-Content-Type-Options”头	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html	缺少“X-XSS-Protection”头	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList	getdetailList	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html	缺少“X-XSS-Protection”头	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodsgsbm/selectList	selectList	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	getGoodsStockList	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodslevel/selectList	selectList	过度许可的 CORS 访问测试	A4, A5, A6, A9

http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List	缺少“Content-Security-Policy”头	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List	缺少“X-Content-Type-Options”头	A4, A5, A6, A9
http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List	缺少“X-XSS-Protection”头	A4, A5, A6, A9
http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://cms.mall.xt.weilian.cn/upload	upload	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pictrue/getGoodsPictrueList	getGoodsPictrueList	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsList	goodsList	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html	saleOrderList.html	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/initTreeNode	initTreeNode	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	jquery-1.7.2.min.js	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubApprovalType/selectList	selectList	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	jquery-1.7.2.min.js	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/checkGoodscodeIsNotOne	checkGoodscodeIsNotOne	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js	layui.js	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js	layui.js	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js	form.js	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js	laypage.js	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js	form.js	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsLi	getGoodsListToBrand	过度许可的 CORS 访问测试	A4, A5, A6, A9

stToBrand			
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete	goodsbatchDelete	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js	laypage.js	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsAddToSave	goodsAddToSave	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js	table.js	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js	laytpl.js	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js	table.js	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js	laytpl.js	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/batchImportGood	batchImportGood	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	exportGoodsInfo	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList	goodsclassList	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js	element.js	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	goodsclassAdd	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateSendGoods	updateSendGoods	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js	element.js	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	0	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://cms.mall.xt.weilian.cn/upload	upload	IBM WebSphere "WASPostParam" Cookie 反序列化拒绝服务	A1, A4, A7, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	updateGoodsOnOff	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	goodsclassAddToSave	过度许可的 CORS 访问测试	A4, A5, A6, A9

http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	updateGoodsStock	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	pageNum	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	pageNum	链接注入（便于跨站请求伪造）	A2, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	start	链接注入（便于跨站请求伪造）	A2, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	length	链接注入（便于跨站请求伪造）	A2, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageSize	链接注入（便于跨站请求伪造）	A2, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	searchValue	发现数据库错误模式	A1, A4
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageNum	链接注入（便于跨站请求伪造）	A2, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	start	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodscode	发现数据库错误模式	A1, A4
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	length	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	searchValue	JSON 中反映的未清理用户输入	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageNum	跨站点脚本编制	A2, A3, A4, A8
http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	goodslevelid	链接注入（便于跨站请求伪造）	A2, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodsids	发现数据库错误模式	A1, A4
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand	keyword	发现数据库错误模式	A1, A4
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageSize	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsLi	keyword	SQL 注入	A1, A4

stToBrand			
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodsname	发现数据库错误模式	A1, A4
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodslevelid	链接注入（便于跨站请求伪造）	A2, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	opcode	发现数据库错误模式	A1, A4
http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	goodslevelid	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	gsbmid	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	gsbmid	链接注入（便于跨站请求伪造）	A2, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodslevelid	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	approvaltypeid	链接注入（便于跨站请求伪造）	A2, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	approvaltypeid	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete	->"goodsInfos"[0]->"goodsid"	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	->"enterpriseid"	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList	classcode	发现数据库错误模式	A1, A4
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList	searchValue	发现数据库错误模式	A1, A4
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageSize	链接注入（便于跨站请求伪造）	A2, A4, A8
http://system-rest-enterprise.mall.xt.weilian.cn/login	login	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/	jQuery, Bootstrap.js, jQuery plugins and Custom JS code	HTML 注释敏感信息泄露	A4, A6
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	->"classid"	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	classcode	发现数据库错误模式	A1, A4
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAd	classcode	JSON 中反映的未清理用户输入	A2, A3, A4, A8

d			
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"goodsid"	跨站点脚本编制	A2, A3, A4, A8
http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	Scroll to top link, initialized in js/app.js - scrollToTop()	HTML 注释敏感信息泄露	A4, A6
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"status"	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"stockqty"	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"departmentid"	发现数据库错误模式	A1, A4
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"enterpriseid"	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"departmentid"	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"goodsid"	跨站点脚本编制	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageNum	链接注入（便于跨站请求伪造）	A2, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageSize	跨站点脚本编制	A2, A3, A4, A8
http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	<script src="http://cdn.bootcss.com/require.js/2.3.3/require.min.js"></script>	HTML 注释敏感信息泄露	A4, A6
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageNum	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList	searchValue	JSON 中反映的未清理用户输入	A2, A3, A4, A8
http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify	userModify	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserRealMenuList	getUserRealMenuList	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login-password	已解密的登录请求	A2, A4, A6, A8
http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	style.js	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix	getModularPrefix	发现内部 IP 泄露模式	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix	getModularPrefix	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.	personal_settings.html	过度许可的 CORS 访问	A4, A5,

weilian.cn/static/component_pages/personal_settings.html		测试	A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	getCommonConfig.js	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	dashboard.html	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	index.html	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserInfo	getUserInfo	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	dashboard.html	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	style.js	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	index.html	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	getCommonConfig.js	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html	自动填写未对密码字段禁用的 HTML 属性	A2, A4, A5, A8, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html	自动填写未对密码字段禁用的 HTML 属性	A2, A4, A5, A8, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	commons.js	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	commons.js	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	dictionaryInit.js	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	dictionaryInit.js	使用 HTTP 动词篡改的认证旁路	A2, A4, A5, A6, A8, A9
http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html	自动填写未对密码字段禁用的 HTML 属性	A2, A4, A5, A8, A9
http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html	查询中接受的主体参数	A4, A5, A6, A9
http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify	->"userId"	跨站点脚本编制	A2, A3, A4, A8
http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/custom.js" type="text/ja	HTML 注释敏感信息泄露	A4, A6

	vascript" charset=...		
http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	<script src="http://sunui.scn.weilian.cn:12809/sys/getCommonConfig.js" type="text/javascript" charse...	HTML 注释敏感信息泄露	A4, A6
http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html		HTML 注释敏感信息泄露	A4, A6
http://system-rest-enterprise.mall.xt.weilian.cn/login	username	发现数据库错误模式	A1, A4

详细的安全性问题（按部分）

高 A1 - Injection 13

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

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

严重性	URL	实体
高	http://cms.mall.xt.weilian.cn/upload	upload

SQL 注入

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

严重性	URL	实体
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand	keyword

发现数据库错误模式

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

严重性	URL	实体
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	searchValue
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodscode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodsids
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand	keyword
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodsname
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	opcode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList	classcode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList	searchValue
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	classcode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"departmentid"
低	http://system-rest-enterprise.mall.xt.weilian.cn/login	username

高 A2 - Broken authentication and session management 58

已解密的登录请求

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。

严重性	URL	实体
高	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login-password

跨站点脚本编制

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

严重性	URL	实体
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	pageNum
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	start
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	length
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageNum
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageSize
高	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	goodslevelid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	gsbmid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodslevelid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	approvaltypeid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete	->"goodsInfos"[0]->"goodsid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	->"enterpriseid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	->"classid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"goodsid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"status"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"stockqty"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"enterpriseid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"departmentid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"goodsid"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageSize

高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageNum
高	http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify	->"userId"

使用 HTTP 动词篡改的认证旁路

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

严重性	URL	实体
中	http://system-rest-enterprise.mall.xt.weilian.cn/	
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	jquery-1.7.2.min.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js	layui.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js	form.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js	laypage.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js	table.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js	laytpl.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js	element.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	dashboard.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	style.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	index.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	getCommonConfig.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	commons.js

中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	dictionaryInit.js

链接注入（便于跨站请求伪造）

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

严重性	URL	实体
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	pageNum
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	start
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	length
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageSize
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageNum
中	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	goodslevelid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodslevelid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	gsbmid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	approvaltypeid
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageSize
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageNum

自动填写未对密码字段禁用的 HTML 属性

风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

JSON 中反映的未清理用户输入

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

严重性	URL	实体
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	searchValue
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	classcode
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList	searchValue

高 A3 - Cross site scripting (XSS) 24

跨站点脚本编制

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

严重性	URL	实体
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	pageNum
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	start
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	length
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageNum
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageSize
高	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	goodslevelid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	gsbmid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodslevelid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	approvaltypeid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete	->"goodsInfos"[0]->"goodsid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	->"enterpriseid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	->"classid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"goodsid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"status"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"stockqty"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"enterpriseid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"departmentid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"goodsid"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageSize

高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageNum
高	http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify	->"userId"

JSON 中反映的未清理用户输入

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

严重性	URL	实体
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	searchValue
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	classcode
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList	searchValue

高 A4 - Broken Access Control 142

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

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

严重性	URL	实体
高	http://cms.mall.xt.weilian.cn/upload	upload

SQL 注入

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

严重性	URL	实体
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand	keyword

已解密的登录请求

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。

严重性	URL	实体
高	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login-password

跨站点脚本编制

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

严重性	URL	实体
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	pageNum
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	start
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	length
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageNum
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageSize
高	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	goodslevelid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	gsbmid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodslevelid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	approvaltypeid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete	->"goodsInfos"[0]->"goodsid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	->"enterpriseid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	->"classid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"goodsid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"status"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"stockqty"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"enterpriseid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"departmentid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"goodsid"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageSize

高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageNum
高	http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify	->"userId"

使用 HTTP 动词篡改的认证旁路

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

严重性	URL	实体
中	http://system-rest-enterprise.mall.xt.weilian.cn/	
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	jquery-1.7.2.min.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js	layui.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js	form.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js	laypage.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js	table.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js	laytpl.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js	element.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	dashboard.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	style.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	index.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	getCommonConfig.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	commons.js

中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	dictionaryInit.js

链接注入（便于跨站请求伪造）

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

严重性	URL	实体
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	pageNum
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	start
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	length
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageSize
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageNum
中	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	goodslevelid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodslevelid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	gsbmid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	approvaltypeid
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageSize
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageNum

发现数据库错误模式

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

严重性	URL	实体
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	searchValue
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodscode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodsids
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand	keyword
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodsname
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	opcode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList	classcode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList	searchValue
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	classcode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"departmentid"
低	http://system-rest-enterprise.mall.xt.weilian.cn/login	username

查询中接受的主体参数

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

缺少“Content-Security-Policy”头

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List

缺少“X-Content-Type-Options”头

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List

缺少“X-XSS-Protection”头

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List

自动填写未对密码字段禁用的 HTML 属性

风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

过度许可的 CORS 访问测试

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

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	2
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	selectVipRoleList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getUserInfo	getUserInfo
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList	getdetailList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodsgsbm/selectList	selectList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	getGoodsStockList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodslevel/selectList	selectList
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List
低	http://cms.mall.xt.weilian.cn/upload	upload
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pictrue/getGoodsPictrueList	getGoodsPictrueList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsList	goodsList
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html	saleOrderList.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/initTreeNode	initTreeNode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubApprovalType/selectList	selectList
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	jquery-1.7.2.min.js
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/checkGoodscodeIsNotOne	checkGoodscodeIsNotOne

	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js	layui.js
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js	form.js
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js	laypage.js
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand	getGoodsListToBrand
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete	goodsbatchDelete
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsAddToSave	goodsAddToSave
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js	table.js
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js	laytpl.js
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/batchImportGood	batchImportGood
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	exportGoodsInfo
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList	goodsclassList
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js	element.js
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	goodsclassAdd
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateSendGoods	updateSendGoods
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	0
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	updateGoodsOnOff
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	goodsclassAddToSave
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	updateGoodsStock
	http://system-rest-enterprise.mall.xt.weilian.cn/login	login
	http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify	userModify
	http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserRealMenuList	getUserRealMenuList
	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html

低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	style.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix	getModularPrefix
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	getCommonConfig.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	dashboard.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	index.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserInfo	getUserInfo
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	commons.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	dictionaryInit.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

HTML 注释敏感信息泄露

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

严重性	URL	实体
参考	http://system-rest-enterprise.mall.xt.weilian.cn/	jQuery, Bootstrap.js, jQuery plugins and Custom JS code
参考	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	Scroll to top link, initialized in js/app.js - scrollToTop()
参考	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	<script src="http://cdn.bootcss.com/require.js/2.3.3/require.min.js"></script>
参考	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/custom.js" type="text/javascript" charset=...
参考	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	<script src="http://sunui.scn.weilian.cn:12809/sys/getCommonConfig.js" type="text/javascript" charse...
参考	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	

JSON 中反映的未清理用户输入

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

严重性	URL	实体
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	searchValue
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	classcode
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList	searchValue

发现内部 IP 泄露模式

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

严重性	URL	实体
参考	http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix	getModularPrefix

中 A5 - Security Misconfiguration 87

使用 HTTP 动词篡改的认证旁路

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

严重性	URL	实体
中	http://system-rest-enterprise.mall.xt.weilian.cn/	
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	jquery-1.7.2.min.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js	layui.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js	form.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js	laypage.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js	table.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js	laytpl.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js	element.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	dashboard.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	style.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	index.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	getCommonConfig.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	commons.js

中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	dictionaryInit.js

查询中接受的主体参数

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

缺少“Content-Security-Policy”头

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List

缺少“X-Content-Type-Options”头

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List

缺少“X-XSS-Protection”头

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List

自动填写未对密码字段禁用的 HTML 属性

风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

过度许可的 CORS 访问测试

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

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	2
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	selectVipRoleList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getUserInfo	getUserInfo
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList	getdetailList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodsgsbm/selectList	selectList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	getGoodsStockList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodslevel/selectList	selectList
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List
低	http://cms.mall.xt.weilian.cn/upload	upload
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pictrue/getGoodsPictrueList	getGoodsPictrueList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsList	goodsList
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html	saleOrderList.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/initTreeNode	initTreeNode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubApprovalType/selectList	selectList
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	jquery-1.7.2.min.js
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/checkGoodscodeIsNotOne	checkGoodscodeIsNotOne

	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js	layui.js
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js	form.js
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js	laypage.js
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand	getGoodsListToBrand
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete	goodsbatchDelete
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsAddToSave	goodsAddToSave
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js	table.js
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js	laytpl.js
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/batchImportGood	batchImportGood
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	exportGoodsInfo
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList	goodsclassList
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js	element.js
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	goodsclassAdd
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateSendGoods	updateSendGoods
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	0
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	updateGoodsOnOff
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	goodsclassAddToSave
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	updateGoodsStock
	http://system-rest-enterprise.mall.xt.weilian.cn/login	login
	http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify	userModify
	http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserRealMenuList	getUserRealMenuList
	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html

低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	style.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix	getModularPrefix
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	getCommonConfig.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	dashboard.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	index.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserInfo	getUserInfo
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	commons.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	dictionaryInit.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

发现内部 IP 泄露模式

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

严重性	URL	实体
参考	http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix	getModularPrefix

高 A6 - Sensitive Data Exposure 90

已解密的登录请求

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。

严重性	URL	实体
高	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login-password

使用 HTTP 动词篡改的认证旁路

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

严重性	URL	实体
中	http://system-rest-enterprise.mall.xt.weilian.cn/	
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	jquery-1.7.2.min.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js	layui.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js	form.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js	laypage.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js	table.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js	laytpl.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js	element.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	dashboard.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	style.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	index.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	getCommonConfig.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	commons.js

中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	dictionaryInit.js

查询中接受的主体参数

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

缺少“Content-Security-Policy”头

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List

缺少“X-Content-Type-Options”头

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List

缺少“X-XSS-Protection”头

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List

过度许可的 CORS 访问测试

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

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	2
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	selectVipRoleList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getUserInfo	getUserInfo
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList	getdetailList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodsgsbm/selectList	selectList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	getGoodsStockList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodslevel/selectList	selectList
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List
低	http://cms.mall.xt.weilian.cn/upload	upload
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pictrue/getGoodsPictrueList	getGoodsPictrueList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsList	goodsList
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html	saleOrderList.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/initTreeNode	initTreeNode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubApprovalType/selectList	selectList
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	jquery-1.7.2.min.js
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/checkGoodscodeIsNotOne	checkGoodscodeIsNotOne

	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js	layui.js
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js	form.js
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js	laypage.js
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand	getGoodsListToBrand
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete	goodsbatchDelete
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsAddToSave	goodsAddToSave
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js	table.js
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js	laytpl.js
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/batchImportGood	batchImportGood
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	exportGoodsInfo
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList	goodsclassList
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js	element.js
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	goodsclassAdd
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateSendGoods	updateSendGoods
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	0
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	updateGoodsOnOff
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	goodsclassAddToSave
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	updateGoodsStock
	http://system-rest-enterprise.mall.xt.weilian.cn/login	login
	http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify	userModify
	http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserRealMenuList	getUserRealMenuList
	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html

低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	style.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix	getModularPrefix
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	getCommonConfig.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	dashboard.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	index.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserInfo	getUserInfo
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	commons.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	dictionaryInit.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

HTML 注释敏感信息泄露

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

严重性	URL	实体
参考	http://system-rest-enterprise.mall.xt.weilian.cn/	jQuery, Bootstrap.js, jQuery plugins and Custom JS code
参考	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	Scroll to top link, initialized in js/app.js - scrollToTop()
参考	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	<script src="http://cdn.bootcss.com/require.js/2.3.3/require.min.js"></script>
参考	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	<script src="http://sunui.scn.weilian.cn:12809/se/demo/js/custom.js" type="text/javascript" charset=...
参考	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	<script src="http://sunui.scn.weilian.cn:12809/sys/getCommonConfig.js" type="text/javascript" charse...
参考	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	

发现内部 IP 泄露模式

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

严重性	URL	实体
参考	http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix	getModularPrefix

高 A7 - Insufficient Attack Protection 1

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

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

严重性	URL	实体
高	http://cms.mall.xt.weilian.cn/upload	upload

高 A8 - Cross site request forgery (CSRF) 58

已解密的登录请求

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。

严重性	URL	实体
高	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login-password

跨站点脚本编制

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

严重性	URL	实体
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	pageNum
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	start
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	length
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageNum
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageSize
高	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	goodslevelid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	gsbmid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodslevelid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	approvaltypeid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete	->"goodsInfos"[0]->"goodsid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	->"enterpriseid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	->"classid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"goodsid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"status"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"stockqty"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"enterpriseid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	->"departmentid"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	->"goodsonoff"[0]->"goodsid"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageSize

高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageNum
高	http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify	->"userId"

使用 HTTP 动词篡改的认证旁路

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

严重性	URL	实体
中	http://system-rest-enterprise.mall.xt.weilian.cn/	
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	jquery-1.7.2.min.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js	layui.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js	form.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js	laypage.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js	table.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js	laytpl.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js	element.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	dashboard.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	style.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	index.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	getCommonConfig.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	commons.js

中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	dictionaryInit.js

链接注入（便于跨站请求伪造）

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

严重性	URL	实体
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	pageNum
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	start
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	length
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageSize
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	pageNum
中	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	goodslevelid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	goodslevelid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	gsbmid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	approvaltypeid
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageSize
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	pageNum

自动填写未对密码字段禁用的 HTML 属性

风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

JSON 中反映的未清理用户输入

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

严重性	URL	实体
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	searchValue
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	classcode
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList	searchValue

高 A9 - Using Components with Known Vulnerabilities 88

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

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

严重性	URL	实体
高	http://cms.mall.xt.weilian.cn/upload	upload

使用 HTTP 动词篡改的认证旁路

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

严重性	URL	实体
中	http://system-rest-enterprise.mall.xt.weilian.cn/	
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	jquery-1.7.2.min.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js	layui.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js	form.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js	laypage.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js	table.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js	laytpl.js
中	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js	element.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	dashboard.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	style.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	index.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	getCommonConfig.js
中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	commons.js

中	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	dictionaryInit.js

查询中接受的主体参数

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

缺少“Content-Security-Policy”头

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List

缺少“X-Content-Type-Options”头

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List

缺少“X-XSS-Protection”头

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

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List

自动填写未对密码字段禁用的 HTML 属性

风险：	可能会绕开 Web 应用程序的认证机制
原因：	Web 应用程序编程或配置不安全
固定值：	将“autocomplete”属性正确设置为“off”

严重性	URL	实体
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

过度许可的 CORS 访问测试

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

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/2	2
低	http://system-rest-enterprise.mall.xt.weilian.cn/	
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/pubRole/selectVipRoleList	selectVipRoleList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getUserInfo	getUserInfo
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodscontrolList.html	goodscontrolList.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/getdetailList	getdetailList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodsgsbm/selectList	selectList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/static/goodstree.html	goodstree.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsStockList	getGoodsStockList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubGoodslevel/selectList	selectList
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List
低	http://cms.mall.xt.weilian.cn/upload	upload
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pictrue/getGoodsPictrueList	getGoodsPictrueList
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsList	goodsList
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/saleOrderList.html	saleOrderList.html
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/initTreeNode	initTreeNode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/pubApprovalType/selectList	selectList
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/jquery-1.7.2.min.js	jquery-1.7.2.min.js
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/checkGoodscodeIsNotOne	checkGoodscodeIsNotOne

	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/layui.js	layui.js
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/form.js	form.js
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laypage.js	laypage.js
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/getGoodsListToBrand	getGoodsListToBrand
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsbatchDelete	goodsbatchDelete
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/goodsAddToSave	goodsAddToSave
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/table.js	table.js
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/laytpl.js	laytpl.js
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/batchImportGood	batchImportGood
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/exportGoodsInfo	exportGoodsInfo
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassList	goodsclassList
	http://h5config-rest-enterprise.mall.xt.weilian.cn/static/orderpage/lay/modules/element.js	element.js
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAdd	goodsclassAdd
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateSendGoods	updateSendGoods
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectCmsOrderList/0	0
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsonoffdetail/updateGoodsOnOff	updateGoodsOnOff
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/goodsclassAddToSave	goodsclassAddToSave
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/updateGoodsStock	updateGoodsStock
	http://system-rest-enterprise.mall.xt.weilian.cn/login	login
	http://system-rest-enterprise.mall.xt.weilian.cn/user/userModify	userModify
	http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserRealMenuList	getUserRealMenuList
	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/modify_password.html	modify_password.html

低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/style.js	style.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix	getModularPrefix
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/personal_settings.html	personal_settings.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/getCommonConfig.js	getCommonConfig.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/component_pages/dashboard.html	dashboard.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/index.html	index.html
低	http://system-rest-enterprise.mall.xt.weilian.cn/user/getUserInfo	getUserInfo
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/commons.js	commons.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/static/js/dictionaryInit.js	dictionaryInit.js
低	http://system-rest-enterprise.mall.xt.weilian.cn/login.html	login.html

发现内部 IP 泄露模式

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

严重性	URL	实体
参考	http://system-rest-enterprise.mall.xt.weilian.cn/user/getModularPrefix	getModularPrefix

A10 - Underprotected APIs 0