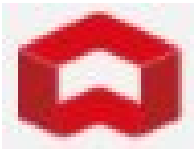

资源商城前台安全性审计测试报告

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 16:56:22

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 8/10 个部分中检测到问题：

部分	问题的数量
A1 - Injection	6
A2 - Broken authentication and session management	32
A3 - Cross site scripting (XSS)	23
A4 - Broken Access Control	114
A5 - Security Misconfiguration	74
A6 - Sensitive Data Exposure	45
A7 - Insufficient Attack Protection	0
A8 - Cross site request forgery (CSRF)	32
A9 - Using Components with Known Vulnerabilities	64
A10 - Underprotected APIs	0

部分违例（按问题）

在规则的 8/10 个部分中检测到 115 个唯一问题：

URL	实体	问题类型	部分
https://redirector.gvt1.com/edgedl/chrome/dict/en-us-7-1.bdic	redirector.gvt1.com	针对 SSL/TLS 的浏览器探索（又名 BEAST）	A2, A4, A8
https://redirector.gvt1.com/edgedl/chrome/dict/en-us-7-1.bdic	redirector.gvt1.com	检测到 SHA-1 密码套件	A2, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	sqlnet.log	Oracle 日志文件信息泄露	A4, A6
https://redirector.gvt1.com/robots.txt	redirector.gvt1.com	针对 SSL/TLS 的浏览器探索（又名 BEAST）	A2, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart	缺少“Content-Security-Policy”头	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart	缺少“X-Content-Type-Options”头	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart	缺少“X-XSS-Protection”头	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/getgoodsclasslisttomallshop	getgoodsclasslisttomallshop	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage	缺少“Content-Security-Policy”头	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/user/initLogin	initLogin	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://cms.mall.xt.weilian.cn/s/373cc681e1d9b286d55ec0c9ccb38f42	373cc681e1d9b286d55ec0c9ccb38f42	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage	缺少“X-Content-Type-Options”头	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage	缺少“X-XSS-Protection”头	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/resourceLevel/resourceLevelListH5	resourceLevelListH5	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://cms.mall.xt.weilian.cn/d/e5034f82d1b9bed050194b91024ef282	e5034f82d1b9bed050194b91024ef282	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://cms.mall.xt.weilian.cn/d/ccd6bcc2fd7b642f48bdc1a0ef937d45	ccd6bcc2fd7b642f48bdc1a0ef937d45	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://cms.mall.xt.weilian.cn/s/9afbaf88341562b5e60e2e3de2d9b380	9afbaf88341562b5e60e2e3de2d9b380	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://cms.mall.xt.weilian.cn/d/7b96c1cc3725c71d45c041b73cc3fdb6	7b96c1cc3725c71d45c041b73cc3fdb6	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/getUserWorth	getUserWorth	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://cms.mall.xt.weilian.cn/d/66990a4633a7282d5ce0e133ac0da3f8	66990a4633a7282d5ce0e133ac0da3f8	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/0	0	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/getOrgWorth	getOrgWorth	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://cms.mall.xt.weilian.cn/s/2290d054775005a2a1eddc3a12b13284	2290d054775005a2a1eddc3a12b13284	过度许可的 CORS 访问测试	A4, A5, A6, A9

http://cms.mall.xt.weilian.cn/d/d01d456252207951dd77748824eb3738	d01d456252207951dd77748824eb3738	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://cms.mall.xt.weilian.cn/d/72717242bd947db4d1f51871a3946c5c	72717242bd947db4d1f51871a3946c5c	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/searchOrderPageList	searchOrderPageList	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://cms.mall.xt.weilian.cn/d/2e9ab77d6c184df8e6cafba8e897f666	2e9ab77d6c184df8e6cafba8e897f666	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	receive	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	queryGoodsList	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://cms.mall.xt.weilian.cn/d/de93adf99fe7a1ee6d16abf48e4ceb65	de93adf99fe7a1ee6d16abf48e4ceb65	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	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/1	1	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1631595097176654	1631595097176654	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://mall.xt.weilian.cn/web/static/js/app.b53433e86cc1ce27aa04.js	app.b53433e86cc1ce27aa04.js	发现电子邮件地址模式	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	sqlnet.log	Oracle 日志文件信息泄露	A4, A6
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1651607004806654	1651607004806654	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/3	3	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateApprovalRecover	updateApprovalRecover	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/4	4	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://mall.xt.weilian.cn/web/static/js/app.b53433e86cc1ce27aa04.js	app.b53433e86cc1ce27aa04.js	发现内部 IP 泄露模式	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	sqlnet.trc	Oracle 日志文件信息泄露	A4, A6
http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	updateShoppingCart	过度许可的 CORS 访问测试	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsNum"	跨站点脚本编制	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/resourceLevel/resourceLevelListH5	->"enterpriseId"	跨站点脚本编制	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsType"	跨站点脚本编制	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsChecked"	跨站点脚本编制	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"brandId"	跨站点脚本编制	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsId"	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	enterpriseid	跨站点脚本编制	A2, A3, A4, A8

http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	enterpriseid	链接注入（便于跨站请求伪造）	A2, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopId"	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	goodsid	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	goodscode	发现数据库错误模式	A1, A4
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	enterpriseid	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	goodsclasscode	发现数据库错误模式	A1, A4
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	storeid	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/queryGoodsList	goodsid	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/queryGoodsListForPage	storeid	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	storeid	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	start	JSON 中反映的未清理用户输入	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	enterpriseid	链接注入（便于跨站请求伪造）	A2, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	sqlnet.trc	Oracle 日志文件信息泄露	A4, A6
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	storeid	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/queryGoodsListForPage	length	JSON 中反映的未清理用户输入	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsNum"	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	pageNum	JSON 中反映的未清理用户输入	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsId"	跨站点脚本编制	A2, A3, A4, A8
http://mall.xt.weilian.cn/web/static/	static/	检测到隐藏目录	A4
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.zip	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shopId"	跨站点脚本编制	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"rid"	跨站点脚本编制	A2, A3, A4, A8
http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	goodsclasscode	JSON 中反映的未清理用户输入	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"serveId"	JSON 中反映的未清理用户输入	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsType"	跨站点脚本编制	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsChecked"	跨站点脚本编制	A2, A3, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/or	selectOrderList.gz	发现压缩目录	A4, A5,

der/selectOrderList/			A9
https://redirector.gvt1.com/robots.txt	redirector.gvt1.com	检测到 SHA-1 密码套件	A2, A4, A8
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.rar	发现压缩目录	A4, A5, A9
https://redirector.gvt1.com/robots.txt	robots.txt	未实施加密	A6
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.ace	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.lha	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.zip	发现压缩目录	A4, A5, A9
https://redirector.gvt1.com/robots.txt	robots.txt	发现电子邮件地址模式	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.lzh	发现压缩目录	A4, A5, A9
https://redirector.gvt1.com/robots.txt	robots.txt	缺少 HTTP Strict-Transport-Security 头	A4, A5, A6, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.tar	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.arj	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.arc	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.tar.gz	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.gz	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.rar	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.ace	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.lha	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.lzh	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.tar	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.arj	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.arc	发现压缩目录	A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.tar.gz	发现压缩目录	A4, A5, A9
https://redirector.gvt1.com/	robots.txt	Robots.txt 文件 Web 站点结构暴露	A4
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	owa_util.signature	Oracle Application Server PL/SQL 未授权的 SQL 查询执行	A1, A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	owa_util.listprint	Oracle Application Server PL/SQL 未授权的 SQL 查询执行	A1, A4, A5, A9

http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	owa_util.signature	Oracle Application Server PL/SQL 未授权的 SQL 查询执行	A1, A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	owa_util.listprint	Oracle Application Server PL/SQL 未授权的 SQL 查询执行	A1, A4, A5, A9
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/0	0	归档文件下载	A4, A5
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/0	0	临时文件下载	A4, A5
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/1	1	归档文件下载	A4, A5
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/1	1	临时文件下载	A4, A5
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/4	4	临时文件下载	A4, A5
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1631595097176654	1631595097176654	归档文件下载	A4, A5
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/4	4	归档文件下载	A4, A5
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1631595097176654	1631595097176654	临时文件下载	A4, A5
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/3	3	归档文件下载	A4, A5
http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/3	3	临时文件下载	A4, A5

详细的安全性问题（按部分）

高 A1 - Injection 6

Oracle Application Server PL/SQL 未授权的 SQL 查询执行

风险：	可能会查看、修改或删除数据库条目和表
原因：	Web 应用程序编程或配置不安全
固定值：	阻止对 PL/SQL 过程和应用程序进行未认证的 PUBLIC 访问

严重性	URL	实体
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	owa_util.signature
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	owa_util.listprint
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	owa_util.signature
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	owa_util.listprint

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/queryGoodsList	goodscode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	goodsclasscode

高 A2 - Broken authentication and session management 32

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://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsNum"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/resourceLevel/resourceLevelListH5	->"enterpriseId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsType"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsChecked"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"brandId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsId"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	enterpriseid
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopId"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	goodsid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	enterpriseid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	storeid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	storeid
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsNum"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shopId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"rid"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsType"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsChecked"

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/queryGoodsList	enterpriseid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	storeid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	goodsid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	enterpriseid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	storeid

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/queryGoodsListForPage	start
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	length
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	pageNum
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	goodsclasscode
参考	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"serveId"

检测到 SHA-1 密码套件

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：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	更改服务器的受支持密码套件

严重性	URL	实体
参考	https://redirector.gvt1.com/edgedl/chrome/dict/en-us-7-1.bdic	redirector.gvt1.com
参考	https://redirector.gvt1.com/robots.txt	redirector.gvt1.com

针对 SSL/TLS 的浏览器探索（又名 BEAST）

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：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	更改服务器的受支持密码套件

严重性	URL	实体
参考	https://redirector.gvt1.com/edgedl/chrome/dict/en-us-7-1.bdic	redirector.gvt1.com
参考	https://redirector.gvt1.com/robots.txt	redirector.gvt1.com

高 A3 - Cross site scripting (XSS) 23

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://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsNum"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/resourceLevel/resourceLevelListH5	->"enterpriseId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsType"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsChecked"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"brandId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsId"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	enterpriseid
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopId"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	goodsid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	enterpriseid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	storeid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	storeid
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsNum"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shopId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"rid"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsType"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsChecked"

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/queryGoodsListForPage	start
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	length
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	pageNum
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	goodsclasscode
参考	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"serveId"

高 A4 - Broken Access Control 114

Oracle Application Server PL/SQL 未授权的 SQL 查询执行

风险：	可能会查看、修改或删除数据库条目和表
原因：	Web 应用程序编程或配置不安全
固定值：	阻止对 PL/SQL 过程和应用程序进行未认证的 PUBLIC 访问

严重性	URL	实体
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	owa_util.signature
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	owa_util.listprint
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	owa_util.signature
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	owa_util.listprint

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://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsNum"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/resourceLevel/resourceLevelListH5	->"enterpriseId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsType"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsChecked"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"brandId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsId"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	enterpriseid
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopId"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	goodsid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	enterpriseid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	storeid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	storeid
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsNum"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shopId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"rid"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsType"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsChecked"

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/queryGoodsList	enterpriseid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	storeid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	goodsid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	enterpriseid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	storeid

Oracle 日志文件信息泄露

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：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	关闭跟踪，限制对日志文件的访问，或者将其除去

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	sqlnet.log
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	sqlnet.log
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	sqlnet.trc
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	sqlnet.trc

Robots.txt 文件 Web 站点结构暴露

风险：	可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	将敏感内容移至隔离位置，以避免 Web 机器人搜索到此内容

严重性	URL	实体
低	https://redirector.gvt1.com/	robots.txt

临时文件下载

风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/0	0
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/1	1
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/4	4
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1631595097176654	1631595097176654
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/3	3

发现压缩目录

风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.zip
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.gz
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.rar
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.ace
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.lha
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.zip
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.lzh
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.tar
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.arj
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.arc
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.tar.gz
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.gz
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.rar
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.ace
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.lha
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.lzh
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.tar
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.arj
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.arc

低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.tar.gz

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/queryGoodsList	goodscode
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	goodsclasscode

归档文件下载

风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/0	0
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/1	1
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1631595097176654	1631595097176654
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/4	4
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/3	3

检测到隐藏目录

风险：	可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去

严重性	URL	实体
低	http://mall.xt.weilian.cn/web/static/	static/

缺少 HTTP Strict-Transport-Security 头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	实施 HTTP Strict-Transport-Security 策略

严重性	URL	实体
低	https://redirector.gvt1.com/robots.txt	robots.txt

缺少“Content-Security-Policy”头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为使用“Content-Security-Policy”头

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage

缺少“X-Content-Type-Options”头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为使用“X-Content-Type-Options”头

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage

缺少“X-XSS-Protection”头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为使用“X-XSS-Protection”头

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage

过度许可的 CORS 访问测试

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	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/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/getgoodsclasslisttomallshop	getgoodsclasslisttomallshop
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/user/initLogin	initLogin
低	http://cms.mall.xt.weilian.cn/s/373cc681e1d9b286d55ec0c9ccb38f42	373cc681e1d9b286d55ec0c9ccb38f42
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/resourceLevel/resourceLevelListH5	resourceLevelListH5
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage
低	http://cms.mall.xt.weilian.cn/d/e5034f82d1b9bed050194b91024ef282	e5034f82d1b9bed050194b91024ef282
低	http://cms.mall.xt.weilian.cn/d/ccd6bcc2fd7b642f48bdc1a0ef937d45	ccd6bcc2fd7b642f48bdc1a0ef937d45
低	http://cms.mall.xt.weilian.cn/s/9afbaf88341562b5e60e2e3de2d9b380	9afbaf88341562b5e60e2e3de2d9b380
低	http://cms.mall.xt.weilian.cn/d/7b96c1cc3725c71d45c041b73cc3fdb6	7b96c1cc3725c71d45c041b73cc3fdb6
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/getUserWorth	getUserWorth
低	http://cms.mall.xt.weilian.cn/d/66990a4633a7282d5ce0e133ac0da3f8	66990a4633a7282d5ce0e133ac0da3f8
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/0	0
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/getOrgWorth	getOrgWorth
低	http://cms.mall.xt.weilian.cn/s/2290d054775005a2a1eddc3a12b13284	2290d054775005a2a1eddc3a12b13284
低	http://cms.mall.xt.weilian.cn/d/d01d456252207951dd77748824eb3738	d01d456252207951dd77748824eb3738
低	http://cms.mall.xt.weilian.cn/d/72717242bd947db4d1f51871a3946c5c	72717242bd947db4d1f51871a3946c5c
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/searchOrderPageList	searchOrderPageList

	http://cms.mall.xt.weilian.cn/d/2e9ab77d6c184df8e6cafba8e897f666	2e9ab77d6c184df8e6cafba8e897f666
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	receive
	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	queryGoodsList
	http://cms.mall.xt.weilian.cn/d/de93adf99fe7a1ee6d16abf48e4ceb65	de93adf99fe7a1ee6d16abf48e4ceb65
	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/1	1
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1631595097176654	1631595097176654
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1651607004806654	1651607004806654
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/3	3
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateApprovalRecover	updateApprovalRecover
	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/4	4
	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	updateShoppingCart

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/queryGoodsListForPage	start
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	length
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	pageNum
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	goodsclasscode
参考	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"serveId"

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://mall.xt.weilian.cn/web/static/js/app.b53433e86cc1ce27aa04.js	app.b53433e86cc1ce27aa04.js

发现电子邮件地址模式

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 站点中的电子邮件地址

严重性	URL	实体
参考	http://mall.xt.weilian.cn/web/static/js/app.b53433e86cc1ce27aa04.js	app.b53433e86cc1ce27aa04.js
参考	https://redirector.gvt1.com/robots.txt	robots.txt

检测到 SHA-1 密码套件

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：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	更改服务器的受支持密码套件

严重性	URL	实体
参考	https://redirector.gvt1.com/edgedl/chrome/dict/en-us-7-1.bdic	redirector.gvt1.com
参考	https://redirector.gvt1.com/robots.txt	redirector.gvt1.com

针对 SSL/TLS 的浏览器探索（又名 BEAST）

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：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	更改服务器的受支持密码套件

严重性	URL	实体
参考	https://redirector.gvt1.com/edgedl/chrome/dict/en-us-7-1.bdic	redirector.gvt1.com
参考	https://redirector.gvt1.com/robots.txt	redirector.gvt1.com

高 A5 - Security Misconfiguration 74

Oracle Application Server PL/SQL 未授权的 SQL 查询执行

风险：	可能会查看、修改或删除数据库条目和表
原因：	Web 应用程序编程或配置不安全
固定值：	阻止对 PL/SQL 过程和应用程序进行未认证的 PUBLIC 访问

严重性	URL	实体
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	owa_util.signature
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	owa_util.listprint
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	owa_util.signature
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	owa_util.listprint

临时文件下载

风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/0	0
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/1	1
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/4	4
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1631595097176654	1631595097176654
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/3	3

发现压缩目录

风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.zip
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.gz
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.rar
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.ace
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.lha
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.zip
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.lzh
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.tar
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.arj
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.arc
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.tar.gz
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.gz
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.rar
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.ace
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.lha
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.lzh
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.tar
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.arj
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.arc

低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.tar.gz

归档文件下载

风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/0	0
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/1	1
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1631595097176654	1631595097176654
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/4	4
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/3	3

缺少 HTTP Strict-Transport-Security 头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	实施 HTTP Strict-Transport-Security 策略

严重性	URL	实体
低	https://redirector.gvt1.com/robots.txt	robots.txt

缺少“Content-Security-Policy”头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为使用“Content-Security-Policy”头

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage

缺少“X-Content-Type-Options”头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为使用“X-Content-Type-Options”头

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage

缺少“X-XSS-Protection”头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为使用“X-XSS-Protection”头

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage

过度许可的 CORS 访问测试

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	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/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/getgoodsclasslisttomallshop	getgoodsclasslisttomallshop
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/user/initLogin	initLogin
低	http://cms.mall.xt.weilian.cn/s/373cc681e1d9b286d55ec0c9ccb38f42	373cc681e1d9b286d55ec0c9ccb38f42
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/resourceLevel/resourceLevelListH5	resourceLevelListH5
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage
低	http://cms.mall.xt.weilian.cn/d/e5034f82d1b9bed050194b91024ef282	e5034f82d1b9bed050194b91024ef282
低	http://cms.mall.xt.weilian.cn/d/ccd6bcc2fd7b642f48bdc1a0ef937d45	ccd6bcc2fd7b642f48bdc1a0ef937d45
低	http://cms.mall.xt.weilian.cn/s/9afbaf88341562b5e60e2e3de2d9b380	9afbaf88341562b5e60e2e3de2d9b380
低	http://cms.mall.xt.weilian.cn/d/7b96c1cc3725c71d45c041b73cc3fdb6	7b96c1cc3725c71d45c041b73cc3fdb6
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/getUserWorth	getUserWorth
低	http://cms.mall.xt.weilian.cn/d/66990a4633a7282d5ce0e133ac0da3f8	66990a4633a7282d5ce0e133ac0da3f8
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/0	0
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/getOrgWorth	getOrgWorth
低	http://cms.mall.xt.weilian.cn/s/2290d054775005a2a1eddc3a12b13284	2290d054775005a2a1eddc3a12b13284
低	http://cms.mall.xt.weilian.cn/d/d01d456252207951dd77748824eb3738	d01d456252207951dd77748824eb3738
低	http://cms.mall.xt.weilian.cn/d/72717242bd947db4d1f51871a3946c5c	72717242bd947db4d1f51871a3946c5c
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/searchOrderPageList	searchOrderPageList

低	http://cms.mall.xt.weilian.cn/d/2e9ab77d6c184df8e6cafba8e897f666	2e9ab77d6c184df8e6cafba8e897f666
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	receive
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	queryGoodsList
低	http://cms.mall.xt.weilian.cn/d/de93adf99fe7a1ee6d16abf48e4ceb65	de93adf99fe7a1ee6d16abf48e4ceb65
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/1	1
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1631595097176654	1631595097176654
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1651607004806654	1651607004806654
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/3	3
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateApprovalRecover	updateApprovalRecover
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/4	4
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	updateShoppingCart

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://mall.xt.weilian.cn/web/static/js/app.b53433e86cc1ce27aa04.js	app.b53433e86cc1ce27aa04.js

发现电子邮件地址模式

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 站点中的电子邮件地址

严重性	URL	实体
参考	http://mall.xt.weilian.cn/web/static/js/app.b53433e86cc1ce27aa04.js	app.b53433e86cc1ce27aa04.js
参考	https://redirector.gvt1.com/robots.txt	robots.txt

低 A6 - Sensitive Data Exposure 45

Oracle 日志文件信息泄露

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：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	关闭跟踪，限制对日志文件的访问，或者将其除去

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	sqlnet.log
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	sqlnet.log
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	sqlnet.trc
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	sqlnet.trc

未实施加密

风险：	可能会窃取诸如信用卡号和社会保险号等未经加密即发送了的敏感数据
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，强制使用 HTTPS

严重性	URL	实体
低	https://redirector.gvt1.com/robots.txt	robots.txt

缺少 HTTP Strict-Transport-Security 头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	实施 HTTP Strict-Transport-Security 策略

严重性	URL	实体
低	https://redirector.gvt1.com/robots.txt	robots.txt

缺少“Content-Security-Policy”头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为使用“Content-Security-Policy”头

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage

缺少“X-Content-Type-Options”头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为使用“X-Content-Type-Options”头

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage

缺少“X-XSS-Protection”头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为使用“X-XSS-Protection”头

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage

过度许可的 CORS 访问测试

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	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/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/getgoodsclasslisttomallshop	getgoodsclasslisttomallshop
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/user/initLogin	initLogin
低	http://cms.mall.xt.weilian.cn/s/373cc681e1d9b286d55ec0c9ccb38f42	373cc681e1d9b286d55ec0c9ccb38f42
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/resourceLevel/resourceLevelListH5	resourceLevelListH5
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage
低	http://cms.mall.xt.weilian.cn/d/e5034f82d1b9bed050194b91024ef282	e5034f82d1b9bed050194b91024ef282
低	http://cms.mall.xt.weilian.cn/d/ccd6bcc2fd7b642f48bdc1a0ef937d45	ccd6bcc2fd7b642f48bdc1a0ef937d45
低	http://cms.mall.xt.weilian.cn/s/9afbaf88341562b5e60e2e3de2d9b380	9afbaf88341562b5e60e2e3de2d9b380
低	http://cms.mall.xt.weilian.cn/d/7b96c1cc3725c71d45c041b73cc3fdb6	7b96c1cc3725c71d45c041b73cc3fdb6
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/getUserWorth	getUserWorth
低	http://cms.mall.xt.weilian.cn/d/66990a4633a7282d5ce0e133ac0da3f8	66990a4633a7282d5ce0e133ac0da3f8
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/0	0
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/getOrgWorth	getOrgWorth
低	http://cms.mall.xt.weilian.cn/s/2290d054775005a2a1eddc3a12b13284	2290d054775005a2a1eddc3a12b13284
低	http://cms.mall.xt.weilian.cn/d/d01d456252207951dd77748824eb3738	d01d456252207951dd77748824eb3738
低	http://cms.mall.xt.weilian.cn/d/72717242bd947db4d1f51871a3946c5c	72717242bd947db4d1f51871a3946c5c
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/searchOrderPageList	searchOrderPageList

低	http://cms.mall.xt.weilian.cn/d/2e9ab77d6c184df8e6cafba8e897f666	2e9ab77d6c184df8e6cafba8e897f666
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	receive
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	queryGoodsList
低	http://cms.mall.xt.weilian.cn/d/de93adf99fe7a1ee6d16abf48e4ceb65	de93adf99fe7a1ee6d16abf48e4ceb65
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/1	1
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1631595097176654	1631595097176654
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1651607004806654	1651607004806654
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/3	3
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateApprovalRecover	updateApprovalRecover
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/4	4
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	updateShoppingCart

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://mall.xt.weilian.cn/web/static/js/app.b53433e86cc1ce27aa04.js	app.b53433e86cc1ce27aa04.js

发现电子邮件地址模式

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 站点中的电子邮件地址

严重性	URL	实体
参考	http://mall.xt.weilian.cn/web/static/js/app.b53433e86cc1ce27aa04.js	app.b53433e86cc1ce27aa04.js
参考	https://redirector.gvt1.com/robots.txt	robots.txt

A7 - Insufficient Attack Protection 0

高 A8 - Cross site request forgery (CSRF) 32

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://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsNum"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/resourceLevel/resourceLevelListH5	->"enterpriseId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsType"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsChecked"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"brandId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopOrderDtos"[0]->"goodsId"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	enterpriseid
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	->"shopId"
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	goodsid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	enterpriseid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	storeid
高	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	storeid
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsNum"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shopId"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"rid"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsType"
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"goodsChecked"

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/queryGoodsList	enterpriseid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	storeid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	goodsid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	enterpriseid
中	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	storeid

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/queryGoodsListForPage	start
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	length
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	pageNum
参考	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	goodsclasscode
参考	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	->"shoppingCartList"[0]->"serveId"

检测到 SHA-1 密码套件

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：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	更改服务器的受支持密码套件

严重性	URL	实体
参考	https://redirector.gvt1.com/edgedl/chrome/dict/en-us-7-1.bdic	redirector.gvt1.com
参考	https://redirector.gvt1.com/robots.txt	redirector.gvt1.com

针对 SSL/TLS 的浏览器探索（又名 BEAST）

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：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	更改服务器的受支持密码套件

严重性	URL	实体
参考	https://redirector.gvt1.com/edgedl/chrome/dict/en-us-7-1.bdic	redirector.gvt1.com
参考	https://redirector.gvt1.com/robots.txt	redirector.gvt1.com

高 A9 - Using Components with Known Vulnerabilities 64

Oracle Application Server PL/SQL 未授权的 SQL 查询执行

风险：	可能会查看、修改或删除数据库条目和表
原因：	Web 应用程序编程或配置不安全
固定值：	阻止对 PL/SQL 过程和应用程序进行未认证的 PUBLIC 访问

严重性	URL	实体
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	owa_util.signature
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	owa_util.listprint
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	owa_util.signature
高	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	owa_util.listprint

发现压缩目录

风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.zip
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.gz
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.rar
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.ace
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.lha
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.zip
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.lzh
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.tar
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.arj
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.arc
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/	selectOrderList.tar.gz
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.gz
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.rar
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.ace
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.lha
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.lzh
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.tar
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.arj
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.arc

低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/	selectOrderDetailYN.tar.gz

缺少 HTTP Strict-Transport-Security 头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	实施 HTTP Strict-Transport-Security 策略

严重性	URL	实体
低	https://redirector.gvt1.com/robots.txt	robots.txt

缺少“Content-Security-Policy”头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为使用“Content-Security-Policy”头

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage

缺少“X-Content-Type-Options”头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为使用“X-Content-Type-Options”头

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage

缺少“X-XSS-Protection”头

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	将您的服务器配置为使用“X-XSS-Protection”头

严重性	URL	实体
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage

过度许可的 CORS 访问测试

风险：	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息 可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	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/shoppingCart/queryShoppingCart	queryShoppingCart
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsclass/getgoodsclasslisttomallshop	getgoodsclasslisttomallshop
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/user/initLogin	initLogin
低	http://cms.mall.xt.weilian.cn/s/373cc681e1d9b286d55ec0c9ccb38f42	373cc681e1d9b286d55ec0c9ccb38f42
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/resourceLevel/resourceLevelListH5	resourceLevelListH5
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsListForPage	queryGoodsListForPage
低	http://cms.mall.xt.weilian.cn/d/e5034f82d1b9bed050194b91024ef282	e5034f82d1b9bed050194b91024ef282
低	http://cms.mall.xt.weilian.cn/d/ccd6bcc2fd7b642f48bdc1a0ef937d45	ccd6bcc2fd7b642f48bdc1a0ef937d45
低	http://cms.mall.xt.weilian.cn/s/9afbaf88341562b5e60e2e3de2d9b380	9afbaf88341562b5e60e2e3de2d9b380
低	http://cms.mall.xt.weilian.cn/d/7b96c1cc3725c71d45c041b73cc3fdb6	7b96c1cc3725c71d45c041b73cc3fdb6
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/getUserWorth	getUserWorth
低	http://cms.mall.xt.weilian.cn/d/66990a4633a7282d5ce0e133ac0da3f8	66990a4633a7282d5ce0e133ac0da3f8
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/0	0
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/getOrgWorth	getOrgWorth
低	http://cms.mall.xt.weilian.cn/s/2290d054775005a2a1eddc3a12b13284	2290d054775005a2a1eddc3a12b13284
低	http://cms.mall.xt.weilian.cn/d/d01d456252207951dd77748824eb3738	d01d456252207951dd77748824eb3738
低	http://cms.mall.xt.weilian.cn/d/72717242bd947db4d1f51871a3946c5c	72717242bd947db4d1f51871a3946c5c
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/searchOrderPageList	searchOrderPageList

低	http://cms.mall.xt.weilian.cn/d/2e9ab77d6c184df8e6cafba8e897f666	2e9ab77d6c184df8e6cafba8e897f666
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/receive	receive
低	http://vr-goods-rest-enterprise.mall.xt.weilian.cn/goodsRestApi/queryGoodsList	queryGoodsList
低	http://cms.mall.xt.weilian.cn/d/de93adf99fe7a1ee6d16abf48e4ceb65	de93adf99fe7a1ee6d16abf48e4ceb65
低	http://vr-base-rest-enterprise.mall.xt.weilian.cn/ditionary/List	List
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/1	1
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1631595097176654	1631595097176654
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderDetailYN/1651607004806654	1651607004806654
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/3	3
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/updateApprovalRecover	updateApprovalRecover
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/order/selectOrderList/4	4
低	http://h5config-rest-enterprise.mall.xt.weilian.cn/shoppingCart/updateShoppingCart	updateShoppingCart

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://mall.xt.weilian.cn/web/static/js/app.b53433e86cc1ce27aa04.js	app.b53433e86cc1ce27aa04.js

发现电子邮件地址模式

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 站点中的电子邮件地址

严重性	URL	实体
参考	http://mall.xt.weilian.cn/web/static/js/app.b53433e86cc1ce27aa04.js	app.b53433e86cc1ce27aa04.js
参考	https://redirector.gvt1.com/robots.txt	robots.txt

A10 - Underprotected APIs 0