武汉宝龙达信息技术有限公司漏洞检测报告

1. 概要信息

1.1. 检测概要

本报告由天融信云安全服务中心制作，采用漏扫安全检查后结合人工复现得出的检测报告，属于内部资料，请进行妥善管理。

本报告共检测 1 个网站，共发现漏洞 2 个，其中 0 个紧急，0 个高危，0 个中危，3 个低危。

1.2. 检测对象

单位名称	武汉宝龙达信息技术有限公司
设备 IP	
域名	www.bitland.com.cn
主办单位名称	武汉宝龙达信息技术有限公司
主办单位性质	企业
ICP 备案号	

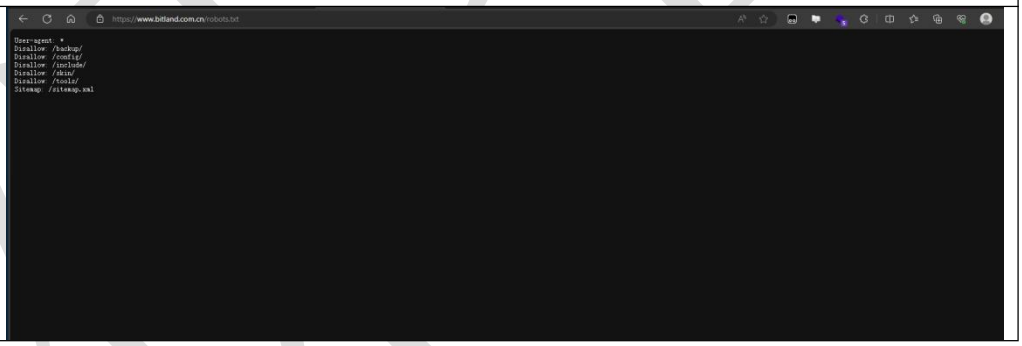
1.3. 网站风险分布

各漏洞风险等级个数

紧急	高危	中危	低危	总数
0	0	0	3	3

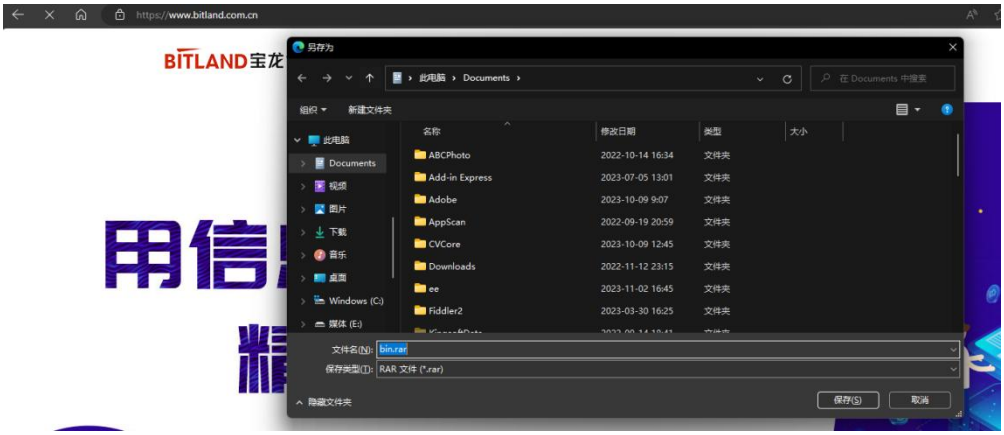
2. 漏洞详情

2.1. robots 信息泄露

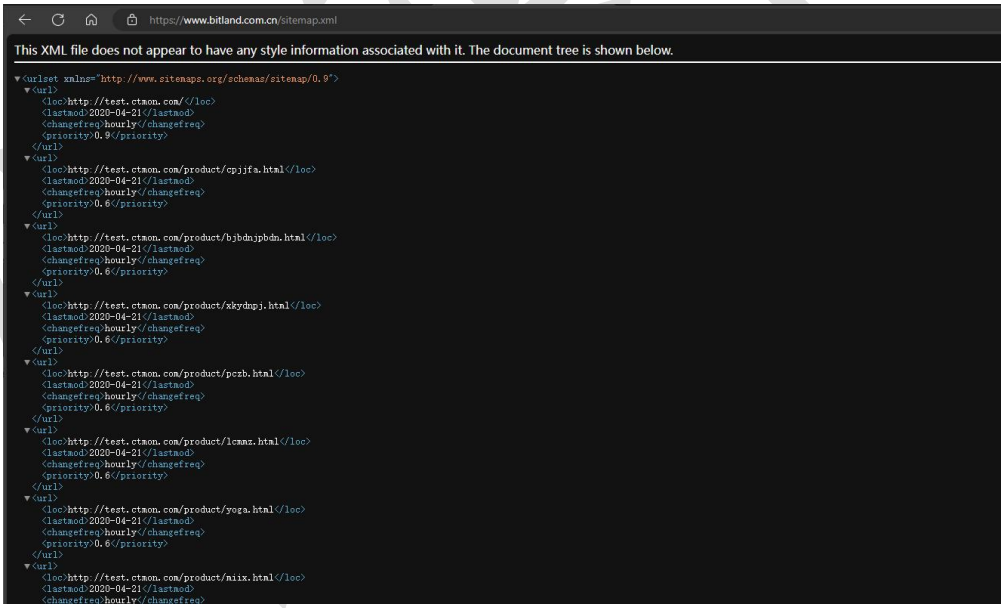
漏洞等级	低危
漏洞 IP	http://www.bitland.com.cn
漏洞 POC	http://www.bitland.com.cn/robots.txt
漏洞取证	

2.2. bin.rar 文件泄露

漏洞等级	低危
漏洞 IP	http://www.bitland.com.cn
漏洞 POC	http://www.bitland.com.cn/bin.rar

漏洞取证	

2.3. sitemap.xml 文件泄露漏洞

漏洞等级	低危
漏洞 IP	http://www.bitland.com.cn
漏洞 POC	http://www.bitland.com.cn/sitemap.xml
漏洞取证	

3. 修复建议

漏洞类型	漏洞描述	修复建议
robots 信息泄露	搜索引擎可以通过 robots 文件可以获知哪些页面可以爬取，哪些页面不可以爬取。robots.txt 文件可能会泄露网站的敏感目录或者文件，比如网站后台路径，从而得知其使用的系统类型，从而有针对性地进行利用。	不使用 robots 文件保护或隐藏信息；使用模糊规则实现 robots；适度提升网站内容命名复杂度。
bin.rar 文件泄露	攻击者可以通过分析 bin.rar 文件获取敏感信息	限制对 bin.rar 文件的访问
sitemap.xml 文件泄露漏洞	攻击者可以通过分析 Sitemap.xml 文件获取敏感信息，如网站结构、重要页面、目录结构等。这种信息泄露可能为更深层次的攻击提供了有利条件。	考虑生成随机的文件名代替固定的 "Sitemap.xml"，以增加攻击者猜测的难度。这可以通过定期更改文件名或使用动态生成的文件名来实现,确保网站开发遵循安全最佳实践，以减少可能导致泄露漏洞的程序错误。对网站代码进行安全审查，并确保没有不安全的文件处理或访问控制问题。

天融信云安全服务中心结合天融信设备、人员、服务的优势，提升检测、分析、处置能力的同时，快速解决客户安全问题。对天融信安全服务产品体系需求进行统一规划，点对点的派遣专项专职的安全技术人员，并提供标准化、专业化的设备支持，统一调度、规划、部署，实现全方位、高质量的服务云端安全服务。