密级 ★ 内部

网站渗透检测报告

Website Security Vulnerability Detection Report

系统名称：数据资产扫描工具

版 本 号：V 1.0

委托单位：信息安全所-数据安全团队

检测时间：二〇二〇年七月六日

目录

一、 检测目的

中国电信研究院信息安全所，于2020年7月3日至2020年7月6日对数据资产扫描工具开展渗透检测，根据被测系统当前的安全现状，给出检测结果并提出整改建议。

二、 检测依据

- OWASP Top 10 Web Application Security Risks

三、 参考依据

- OWASP Top 10 Web Application Security Risks
- CVSS 3.1 Calculator

四、 用户文档

无

五、 检测范围及对象

本次渗透检测在测试环境中进行，安全测试范围主要包括网站安全和业务逻辑安全两个方面。检测对象包括：

- 数据资产扫描工具（Web 端）

5.1 系统概述

数据资产扫描工具集成了数据资产的管理功能，提供给各省公司进行数据资产管理工作。

5.2 检测工具

工具类型	名称	版本号
抓包工具	Telerik Fiddler Web Debugger	4.6
	Burp Suite Community Edition	-
渗透工具	Kali Linux	2020.1

六、 检测结果

6.1 漏洞等级分布统计

风险名称	数量	危险等级
数据库名称字段溢出	1	中危
登录验证码暴力猜解	1	中危
服务器信息泄露	1	低危
Web 应用服务不稳定	1	建议项
总计	4	

七、 漏洞详情

7.1 数据库名称字段溢出

- 漏洞等级

  CVSS 评分：中危（6.8）

- 漏洞描述

  数据库名称前后端都未校验长度，可通过构造超长的字符串导致服务崩溃，见下图：

- 修复建议

  前后端对数据库名称字段长度进行校验，避免 Fuzz 攻击导致服务崩溃。

7.2 登录验证码暴力猜解

- 漏洞等级

  CVSS 评分：中危（6.3）

- 漏洞描述

  登录验证码采用个位数的“+”或“*”，输入次数无上限，可对

验证码进行两位数字的暴力猜解，见下图：

- 修复建议

建议采用登录界面采用增加图形验证码的复杂度，避免暴力猜解。

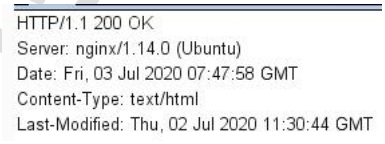
7.3 服务器信息泄露

- 漏洞等级

CVSS 评分：低危（3.5）

- 漏洞描述

登录接口的返回值中包含服务器版本信息，见下图：



- 修复建议

建议在服务的接口返回信息中隐藏相关的服务器版本信息。

7.4 Web 应用服务不稳定（建议项）

- 漏洞等级

CVSS 评分：无

- 漏洞描述

Web 应用服务经常出现验证码无法加载，接口请求无返回值等情况，见下图：

- 修复建议

建议上线前对 Web 应用服务的稳定性进行测试，并根据用户的体量进行压力测试。

八、 检测结论

“数据资产扫描工具”在本次检测过程发现中危风险 2 处，建议根据整改建议进行修复。

九、 检测结果签字确认

姓名	部门	签字
何昆	信息安全所	
吴吞	信息安全所	
姚腾东	信息安全所	
黄玉娈	信息安全所	
张尚华	信息安全所	
审核人： 批准人：		

注意事项：

- 报告无检测、审核、批准人签字无效。
- 报告改动无效。
- 未经信息安全所书面批准，不得复制报告，否则无效。
- 本报告检测结果只针对送检来样负责。
- 对本报告若有异议，请于收到报告之日起十五日内提出，逾期不予受理。

地址：上海市浦东新区秀沿西路 189 号中国电信信息园区 B23 号楼

邮政编码：201315

联系电话：021-50881612