XXXX公司

渗透测试报告

2020.06.10

 XX 安全公司

目录

1 项目概述 3

1.1 渗透测试目的 3

1.2 渗透测试范围 3

1.3 渗透测试工具 3

1.4 渗透测试组织 3

1.5 渗透测试原则 3

2 渗透测试方法 4

2.1 工具自动分析 4

2.2 人工手动分析 4

2.3 风险评估 4

3 网站漏洞详情 6

４ 总结 7

４.1 网站目前安全现状 7

４.2 存在问题和整改建议 7

# 1 项目概述

## 1.1 渗透测试目的

 测试人员以攻击者的角度,对客户网站的业务、网络、信息系统进行安全评估及渗透测试,并给出相应的漏洞详情和修复建议,加固系统安全.

## 1.2 渗透测试范围

XXXX公司(xxxx.com).

## 1.3 渗透测试工具

 BurpSuite 渗透测试套件

 Sqlmap SQL注入测试工具

wyDomain 子域名枚举工具

Xsstrike XSS漏洞测试工具

......

## 1.4 渗透测试组织

 XX 安全公司

## 1.5 渗透测试原则

 在不影响客户网站业务的正常运行下,对其网站业务、信息系统进行渗透测试.

# 2 渗透测试方法

## 2.1 工具自动分析

 由于Web程序漏洞主要体现在程序对输入的处理上,而Ｗeb应用扫描器则根据这个特点,发送精心构造的请求,并且对服务器返回的响应来判断是否存在指定的Web应用漏洞.所以,Ｗeb应用扫描器通常情况下能够发现SQL注入,XSS和CSRF等常见的Web漏洞.

注: 我们使用BurpSuite套件对网站进行渗透测试,在保证不对网站业务造成影响的情况下分析漏洞.

## 2.2 人工手动分析

 我们的渗透测试人员将通过手工的方式对Web应用扫描器检测到的漏洞依次进行复现, 从而排除扫描器误报的漏洞并且针对复现成功的漏洞进行风险评估,给出相应的漏洞修复方案.

## 2.3 风险评估

 我们使用Microsoft (微软)的DREAD模型进行风险评估.

 高危: 12-15分, 中危: 8-11分, 低危: 0-7分.

|  |  |  |  |
| --- | --- | --- | --- |
| 等级 | 高(3) | 中(2) | 低(1) |
| Damage Potential | 获取完全验证权限; 执行管理员操作; 非法上传文件 | 泄露敏感信息 | 泄露其他信息 |
| Reproducibility | 攻击者可以随意再次攻击 | 攻击者可以重复攻击, 但有时间限制 | 攻击者很难重复攻击 |
| Exploitability | 初学者在短期内能掌握攻击方法 | 熟练的攻击者才能完成这次攻击 | 漏洞利用条件非常苛刻 |
| Affected users | 所有用户, 默认配置, 关键用户 | 部分用户, 非默认配置 | 极少数用户, 匿名用户 |
| Discoverability | 漏洞很明显, 攻击条件很容易获得 | 在私有区域, 部分人能看到, 需要深入挖掘漏洞 | 发现该漏洞极其困难 |

# 3 网站漏洞详情

#### 3.1、XX漏洞

##### 3.1.1 漏洞等级

##### 3.1.2 测试过程

##### 3.1.3 相关截图

##### 3.1.3 修复建议

# ４ 总结

## ４.1 网站目前安全现状

## ４.2 存在问题和整改建议