XXXX产品安全检测报告

XXX安全有限公司

20XX年XX月XX日

**文档信息**

|  |  |  |  |
| --- | --- | --- | --- |
| **项目名称** | XXXXX安全检测项目 | | |
| **文档名称** | XXXXX安全检测项目渗透测试报告 | | |
| **文档编号** |  | | |
| **文件类型** | 项目文档 | **密级** | 商业秘密 |
| **创 建 人** |  | **版本** |  |
| **审 核 人** |  | **审核日期** |  |
| **批 准 人** |  | **批准日期** |  |
| **接 收 方** | XXXXX | **接收日期** |  |
| **保密申明** | 本文件包含来自XXX安全有限公司的可靠权威的信息，以及被检测单位信息系统的敏感信息，接受这份文件表示同意对其内容保密并且未经北京京XXX安全有限公司面请求和书面认可，不得复制，泄露或散布这份文件。如果你不是有意接受者，请注意对这份文件内容的任何形式的泄露、复制或散布都是被禁止的。 | | |
| **版权说明** | 本文件中出现的全部内容，除另有特别注明，版权均属XXX安全有限公司所有。任何个人、机构未经**XXX安全公司**书面授权许可，不得以任何方式复制或引用文件的任何片断。 | | |

目录

[1. 服务摘要 4](#_Toc20488158)

[2. 服务概述 7](#_Toc20488159)

[2.1测试范围 7](#_Toc20488160)

[2.2测试流程 7](#_Toc20488161)

[2.3测试人员 8](#_Toc20488162)

[2.4测试风险管理 8](#_Toc20488163)

[2.4.1测试时间管理 8](#_Toc20488164)

[2.4.2技术手段和流程管理 8](#_Toc20488165)

[2.4.3测试工具管理 8](#_Toc20488166)

[2.5测试依据 9](#_Toc20488167)

[3. 安全漏洞详情 10](#_Toc20488168)

[3.1 XXXXX站点存在SQL注入 10](#_Toc20488169)

[4. 其他测试详情 11](#_Toc20488170)

[4.1 XXXXX主站XXXX业务测试 11](#_Toc20488171)

[5. 安全风险总结 12](#_Toc20488172)

[6. 安全建议汇总 12](#_Toc20488173)

[7. 致谢 13](#_Toc20488174)

# 服务摘要

经XXXXX公司授权，安全有限公司安全服务团队于20xx年xx月xx日至20xx年xx月xx日(非业务高峰时段)，对XXXXX进行了安全测试。

本次测试项目负责任人：XXXX，联系方式：130XXXXXXX

通过安全服务团队测试后发多处安全漏洞，其结果如下所示：

**严重漏洞**：X 个

**高危漏洞**：X 个

中危漏洞：X 个

低危漏洞：X 个

安全风险汇总如下:

|  |  |
| --- | --- |
| **威胁级别** | **安全漏洞名称** |
| **严重漏洞** | SQL注入 |
| 任意SQL语句执行 |
| 密码弱口令 |
| 敏感信息读取 |
| **高危漏洞** | 文件上传漏洞 |
| 敏感信息泄露 |
| **中危漏洞** | CSRF跨站伪造请求 |
| **低危漏洞** |  |
|  |  |

表1 安全漏洞汇总

漏洞类型测试结果如下：

|  |  |  |
| --- | --- | --- |
| **测试分类** | **漏洞类型** | **测试结果** |
| 应用层 | SQL注入攻击 | 存在 |
| 跨站脚本攻击 | 通过 |
| 代码执行 | 通过 |
| 命令执行 | 通过 |
| 文件上传 | 通过 |
| 文件读取 | 通过 |
| 文件包含 | 通过 |
| 跨站点请求伪造(CSRF) | 通过 |
| 服务端请求伪造(SSRF) | 通过 |
| URL重定向 | 通过 |
| 点击劫持 | 通过 |
| XML外部实体注入攻击 | 通过 |
| LDAP注入攻击 | 通过 |
| CRLF注入攻击 | 通过 |
| 跨域资源共享攻击(CORS) | 通过 |
| 反序列化攻击 | 通过 |
| 加密算法使用不当 | 通过 |
| XPATH注入攻击 | 通过 |
| 服务端 | 敏感信息泄露 | 通过 |
| 弱点端口检测 | 通过 |
| 弱点服务检测 | 通过 |
| 运维不当 | 通过 |
| 目录遍历 | 通过 |
| Git/SVN文件泄露 | 通过 |
| 不安全的HTTP请求方法 | 通过 |
| 默认凭证 | 通过 |
| 栈异常跟踪 | 通过 |
| 弱密码规则测试 | 通过 |
| 缓冲区溢出 | 通过 |
| Host绑定不安全因素 | 通过 |
| DNS域传送 | 通过 |
| Squid不安全代理 | 通过 |
| 第三方组件安全 | 通过 |
| CI安全检测 | 通过 |
| Web应用上线Debug未关闭 | 通过 |
| 中间件 | 中间件弱口令测试 | 通过 |
| 中间件文件解析漏洞 | 通过 |
| Java中间件已知安全漏洞 | 通过 |
| 中间件配置不当 | 通过 |
| 中间件默认管理页面泄露 | 通过 |
| 中间件示例页面泄露 | 通过 |
| 业务逻辑 | 用户身份体系 | 通过 |
| 垂直权限测试 | 通过 |
| 水平权限测试 | 通过 |
| 授权绕过 | 通过 |
| 暴力破解 | 通过 |
| 在线支付逻辑测试 | 通过 |
| OAuth授权测试 | 通过 |
| 验证码复用 | 通过 |
| 密码重置测试 | 通过 |
| 手机SMS接口安全问题 | 通过 |
| 人员安全意识 | 员工弱口令 | 通过 |
| Github敏感信息泄露 | 通过 |
| 社会工程学攻击 | 通过 |
| 云环境 | 云网络环境安全测试 | 通过 |
| 云服务器安全测试 | 通过 |
| 容器服务安全测试 | 通过 |
| 云数据库安全测试 | 通过 |
| 大数据处理套件安全测试 | 通过 |
| 云函数安全测试 | 通过 |
| AI服务安全测试 | 通过 |
| 计费系统安全测试 | 通过 |
| 云对象存储系统安全测试 | 通过 |

表2 安全测试项汇总

# 服务概述

## 2.1测试范围

根据XXXXXX有限公司与XXXX安全有限公司签订的合同所述，本次网站或应用程序安全测试范围以及环境如下表所示：

|  |  |
| --- | --- |
| 网站范围 | XXXX有限公司所有网络资产 |
| IP 范围 | 本次测试甲方（XXXX有限公司）未提供 IP 范围。由乙方（XXXX安全有限公司）安全服务团队术人员通过技术手段获得。 |
| 服务器环境 | http://\*.xxxx.com XXXX有限公司所有线上服务器 |
| 测试账号 | 本次测试甲方（XXXX有限公司） 未提供测试帐号。由乙方（XXXX安全有限公司）安全服务组技术人员通过技术手段获得。 |
| 其他 | 无 |

表3测试范围与环境说明

## 2.2测试流程

XXXX安全有限公司渗透测试服务流程定义如下：

清除测试数据

输出报告

成果收集

缺陷利用

弱点分析

信息收集

图1 测试流程图

1. 信息收集：安全服务团队通过技术手段将对测试目标进行必要的信息收集，如IP地址、网站域名、软件版本信息、开发技术栈、以及各大网站与测试目标相关的公开信息。
2. 弱点分析：在信息收集的基础之上，安全服务团队对信息进行分析寻找出测试目标的中存在的攻击面，通过安全测试的方法寻找其中存在的薄弱点。
3. 缺陷利用：在不影响业务的前提下，安全服务团队针对弱点进行进一步的利用，挖掘出潜在的危害。
4. 成果收集：安全服务团队对前期收集的各类弱点、漏洞等问题进行分类，集中展示。
5. 输出报告：安全服务团队将发现的安全问题进行全面分析后编写直观的服务报告，并提供漏洞修复建议。
6. 清除测试数据：安全服务团队在完成测试之后，清除测试中遗留的数据，避免对后续业务产生影响。

## 2.3测试人员

|  |  |  |  |
| --- | --- | --- | --- |
| 姓名 | 联系方式 | 出口IP地址 | 备注 |
| 王佳宁 | jianing.wang@boudaryx.com | X.X.X.X | Web测试 |
| 王洪超 | hongchaowang@boudaryx.com | X.X.X.X | Web测试 |
| 陈佩文 | pwchen@boudaryx.com | X.X.X.X | Web测试 |
|  |  |  |  |

表4 测试人员信息

## 2.4测试风险管理

XXXX安全有限公司安全服务团队在信息搜集和整理的环节会优先审查受测网站或程序的基本参数，以便在安全检测过程中尽可能减少对受测网站或程序的压力，保证其安全、稳定的运转。除此之外，还通过以下方式方法对测试风险进行合理管控。

### 2.4.1测试时间管理

从测试时间安排上，XXXX安全有限公司安全服务团队会在安全测试之前与对方项目负责人充分沟通，要求测试人员将将尽量避免在数据高峰时进行测试，以此来减小测试工作对被测试系统带来的压力。另外，测试人员在每次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

### 2.4.2技术手段和流程管理

为了防止测试过程中出现意外，安全服务团队会在每一项测试前预估多种可能后果，对于可能产生不良后果的测试（如：任意命令执行等）将被记录并跳过，在与对方项目负责人沟通协商后决定是否进行此项测试，以及测试方法。

此外，安全服务组会在测试过程中随时关注受测网站或程序的负荷信息，以确保在异常状况发生时，及时停止测试并与相关负责人联络。

### 2.4.3测试工具管理

为了保证检测的完整性，安全服务团队的部分安全检测可能使用自动扫描工具，当使用自动扫描工具扫描时，会通过对线程、插件数量等参数的设置，尽可能减小对受测目标的系统压力；此外，类似远程溢出攻击类、拒绝服务攻击类等有可能对受测网站或系统产生不良影响的也会排除。

## 2.5测试依据

为了保证此次渗透测试的先进性、完备性、规范性，XXXX安全有限公司安全服务团队将参考下列有关标准进行工作。

* ISO/IEC 27001:2005信息技术-安全技术-信息系统规范与使用指南
* ISO/IEC 13335-1: 2004 信息技术-安全技术-信息技术安全管理指南
* ISO/IEC TR 15443-1: 2005 信息技术安全保障框架
* ISO/IEC PDTR 19791: 2004 信息技术 安全技术 运行系统安全评估
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 19715.1-2005 信息技术-信息技术安全管理指南
* GB/T 19716-2005 信息技术-信息安全管理实用规则
* GB/T 18336-2001 信息技术-安全技术-信息技术安全性评估准则
* GB/T17859-1999 计算机信息系统安全保护等级划分准则
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 20988-2007信息系统灾难恢复规范
* GB/Z 20986-2007信息安全事件分类分级指南
* 渗透测试最佳实践
* OWASP OWASP\_Top\_10\_2017\_RC1\_V1.0
* OWASP OWASP\_Testing\_Guide\_v3
* OWASP Risk Rating Methodology

# 安全漏洞详情

## 3.1 XXXXX站点存在SQL注入

**测试点**

|  |  |
| --- | --- |
| 漏洞URL | http://www.xxxx.com |
| 漏洞参数 | id |
| 漏洞等级 | 严重 |

**测试结果**

通过专业的安全测试发现该业务中存在XXXX漏洞

**漏洞详情**

测试过程、测试方法、利用结果

数据包为

|  |
| --- |
| POST /XXXXX |

代码为

|  |
| --- |
| Xxx  Xxxx  xxxx |

**漏洞危害**

* 通过专业的安全评估判断，若被恶意攻击将造成XXXXXX。

**漏洞修复建议**

Xxxxx

# 其他测试详情

## 4.1 XXXXX主站XXXX业务测试

**测试点**

|  |  |
| --- | --- |
| 测试URL | http://www.xxxx.com |
| 测试参数 | id |
| 安全状况 | 优 |

**测试结果**

Xxxxxx

**安全状况评估**

Xxxxxx

# 安全风险总结

XXXX安全有限公司安全服务团队对XXXXXXX有限公司XXXX项目进行专业的安全深度测试，发现XXXXX项目网络环境存在危害度极高的安全问题，这些安全问题可能导致结果评估如下：

* 通过专业的安全评估判断，如果被恶意攻击，可以造成敏感信息和机密数据泄露。
* 通过专业的安全评估判断，如果被恶意攻击，可以导致加密传输被破解或劫持。
* 通过专业的安全评估判断，如果被恶意攻击，可以导致内部某些敏感接口泄漏。
* 通过专业的安全评估判断，如果被恶意攻击，可以导致用户端受到恶意控制，或被窃取身份信息。

# 安全建议汇总

本次安全检测由XXXX安全有限公司安全服务组独立完成，测试中发现XXXXX有限公司安全测试项目中存在严重的安全隐患，测试详情和安全建议请参看报告内容。

鉴于测试结果的严重性，为保护用户数据、公司敏感信息，以及项目的安全运行，XXXX安全有限公司安全服务组建议尽快修复安全问题，并做好安全管理工作，定期进行安全巡检，最大程度地避免安全问题。

# 致谢

在贵公司的大力配合下，本次安全深度检测得以顺利完成。XXXX安全有限公司向XXXXXXX有限公司所有参与并提供支持的部门及个人表示深深的感谢。