密 级：aa

文档编号：

{{name}}

信息安全风险评估报告

**C:\Users\admin\Desktop\getqqicon.jpggetqqicon**

Xxxxx限公司

检查结束时间： {{time}}

**一、评估目标**

为了了解{{name}}的安全现状，在许可和可控制的范围内，对其进行安全评估；以期了解该系统在开发过程中是否存在安全隐患，并通过评估结果进行相关开发代码及系统相关配置的整改，为生产环境的应用安全提供保障。

**二、评估范围、地点及周期**

此次风险评估的范围为：{{name}}本身，包括操作系统、数据库、中间件及其他第三方应用软件的安全评估。

评估对象为：{{name}}

评估域名/ip：{{url}}

评估时间： {{time}}

**三、评估方法**

此次评估的主要策略是首先对测评对象进行资产识别，包括评估软体资产存在的弱点、面临的威胁，进而得出评估对象的等级和风险值。

**可能会采用以下工作方式完成评估目标**：

* 信息收集：通过客户访谈，从应用特性、开发技术本身等角度了解客户信息资产相关的安全要素，为进一步挖掘系统存在的安全隐患提供基本数据；
* 漏洞发现：通过国际标准漏洞验证方式，高效率地从技术角度发现信息资产存在的安全弱点，并进行威胁和风险分析；
* 自动化渗透：通过黑盒测试手段进行尝试性渗透，进而得出可视化的客观的信息资产安全现状；
* 报告分析：通过一系列检查手段，通过资深工程师的综合评判，得出评估对象的安全现状，并赋值得出结论。

在本次安全评估中，我们会对目标的安全状况按照层次进行分别评述，并给出最后的评价，评价共分为五级，分别为极度风险，严重风险，严重隐患，一般隐患，暂时安全。

1. **评价等级依据:**

极度风险:评估对象存在1个及以上的严重漏洞或3个及以上的高危漏洞，可能被获取webshell权限、数据库管理权限以及主机系统权限;

严重风险:评估对象存在2个及以内的高危漏洞或5个及以上中危漏洞，可能被篡改页面内容、获取webshell权限、数据库用户权限等;

严重隐患:评估对象存在2个及以上5个以内中危漏洞，并未被获取webshell、数据库、主机等权限，但存在旁注问题，或存在入侵迹象，存在持久性攻击风险，易存在被获取本站webshell权限的风险;

一般隐患:评估对象只存在1个及以内中危漏洞或5个及以内低危漏洞，不存在管理后台、webshell、数据库用户权限、主机权限等被获取的风险;

暂时安全:评估对象不存在漏洞，在一定时间段内不存在被入侵的风险。

**四、评估结论**

此次{{name}}信息安全评估，评估结论为{{**risk\_level**}}**。**

描述：

此次信息安全评估共发现风险点{{common}}个，其中严重风险点{{serious}}个，高危风险点{{high}}个，中危风险点{{medium}}个，低危风险点{{low}}个。

**五、评估过程概述**

站点基本漏洞信息：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **系统名称** | **漏洞名称** | **风险等级** |

{%p for z in hostlist %}

|  |  |  |  |
| --- | --- | --- | --- |
| {{z.id}} | {{name}} | {{z.name}} | {% if z.bugLevel == 5 %}严重{%elif z.bugLevel == 4 %}高危{%elif z.bugLevel == 3 %}中危{%elif z.bugLevel == 2 %}低危{%elif z.bugLevel == 1 %}无危害{% endif %} |

{%p endfor %}

**重要风险细节描述**

{%p for z in alerts %}

{%p for i in z.path %}

## 风险点 {{i.id}}、{{i.name}}

漏洞风险等级：{% if z.bugLevel == 5 %}严重{%elif z.bugLevel == 4 %}高危{%elif z.bugLevel == 3 %}中危{%elif z.bugLevel == 2 %}低危{%elif z.bugLevel == 1 %}无危害{% endif %}  
 漏洞地址：{{i.url}}  
 漏洞详细描述：

{%p for b in i.verification%}

{{b}}

{%p endfor %}

解决方案：  
 {{i.suggestions}}

{%p endfor %}

{%p endfor %}

**六、安全性总结**

根据此次渗透性测试安全评估，{{name}}的评估结论为{{**risk\_level**}}**。**

**附录：评估技术点与评分依据**

“xx”平台通过核心引擎分析目标类型及目标体量，制定检测策略并调用各功能模块对目标系统的主机系统、数据库、中间件、WEB应用、应用框架等进行全方位自动化风险点识别、检测、验证、利用；在检测完成后进行结论数据整合及自动化出具风险评估报告。以下部分为“xx”平台的评估技术点与相关评分依据。

|  |  |  |  |
| --- | --- | --- | --- |
| 操作系统 | | | |
| 编号 | 弱点类型 | 描述 | 等级 |
| 1 | 远程溢出 | 包括CVE、CNVD确认的可以进行远程溢出攻击的系统漏洞； | 严重 |
| 2 | 本地溢出 | 包括CVE、CNVD确认的可以进行本地溢出攻击的系统漏洞； | 高危 |
| 3 | 拒绝服务 | 包括CVE、CNVD确认的可以进行拒绝服务攻击的系统漏洞； | 严重 |
| 4 | 弱口令 | 包括TOP 1000弱口令验证； | 严重 |
| 5 | 后门程序 | 包括常见Rootkit、远程控制等后门的识别； | 严重 |
| 中间件 | | | |
| 1 | 弱口令 | 包括TOP 1000弱口令验证； | 高危 |
| 2 | 命令执行 | 包括TOMCAT、AIX2等中间件的命令执行漏洞识别； | 高危 |
| 3 | 解析漏洞 | 包括IIS、Apache、Nginx等中间件的解析漏洞； | 高危 |
| 4 | 目录遍历 | 包括IIS、Apache、TOMCAT、Nginx等中间件的目录遍历漏洞； | 中、高危 |
| 数据库 | | | |
| 1 | 弱口令 | 包括TOP 1000弱口令验证； | 高危 |
| 2 | 远程溢出 | 包括CVE、CNVD确认的可以进行远程溢出攻击的数据库漏洞； | 严重 |
| 3 | 拒绝服务 | 包括CVE、CNVD确认的可以进行拒绝服务攻击的数据库漏洞； | 严重 |
| WEB | | | |
| 1 | 注入 | 包括GET、POST、COOKIE、盲注、HTTP头请求等注入方式 | 高危、严重 |
| 2 | 跨站脚本漏洞 | 包括存储型、反射性、DOM型等跨站攻击方式 | 中、高危 |
| 3 | 跨站请求伪造 | 包括GET、POST等跨站请求伪造漏洞 | 中、高危 |
| 4 | 文件上传 | 包括本地验证、MINE类型检测、目录路径检测、文件内容检测等绕过进行文件上传 | 高危 |
| 5 | 文件包含 | 包括本地文件包含、远程文件包含漏洞检测 | 高危 |
| 6 | 命令执行 | 包括代码执行、系统命令执行等命令执行漏洞 | 高危、严重 |
| 7 | 弱口令 | 包括TOP50用户名、TOP1000密码验证 | 高危 |
| 8 | 越权访问 | 包括身份验证绕过、JS禁用绕过、权限越级等越权漏洞 | 中、高危 |
| 9 | 信息泄露 | 包括路径信息泄露、SVN信息泄露、phpinfo、异常信息泄露等 | 低危 |
| 10 | 敏感信息 | 包括数据库备份、网站源码备份等敏感信息泄露文件 | 中、高危 |
| 11 | 文件遍历 | 包括任意文件读取、下载、删除等文件遍历操作漏洞 | 中危 |
| 12 | 拒绝服务 | 包括脚本程序处理过程中导致网站无法访问的漏洞 | 高危 |
| 13 | 设计缺陷 | 包括程序设计缺陷、逻辑错误等此类漏洞 | 中、高危 |
| 14 | 其他 | 未验证的重定向和转发等，新爆发出的漏洞不在以上分类的漏洞 | 根据漏洞危害判定 |