{{image\_1}}

­­­

目录

[目录 2](#_Toc23519966)

[1 前言 5](#_Toc23519967)

[1.1 阅读报告说明 5](#_Toc23519968)

[1.2 目标参数 5](#_Toc23519969)

[1.3 网站资产情况 6](#_Toc23519970)

[1.3.1 网站资产信息 6](#_Toc23519971)

[1.3.2 网站端口信息 6](#_Toc23519972)

[2 专家建议指导 6](#_Toc23519973)

[2.1 安全服务建议 6](#_Toc23519974)

[2.1.1 安全评估 6](#_Toc23519975)

[2.1.2 渗透测试 6](#_Toc23519976)

[2.1.3 安全加固 7](#_Toc23519977)

[2.1.4 安全培训 7](#_Toc23519978)

[2.1.5 应急响应 7](#_Toc23519979)

[2.1.6 红蓝对抗 7](#_Toc23519980)

[2.1.7 漏洞扫描服务 8](#_Toc23519981)

[2.1.8 安全保障服务 8](#_Toc23519982)

[2.2 风险类型处理建议 8](#_Toc23519983)

[2.2.1 SQL注入类 8](#_Toc23519984)

[2.2.2 跨站脚本类 9](#_Toc23519985)

[2.2.3 密码泄露类 9](#_Toc23519986)

[2.2.4 其他类 9](#_Toc23519987)

[2.2.5 服务最小化 9](#_Toc23519988)

[2.2.6 配置权限 9](#_Toc23519989)

[2.2.7 配置日志 10](#_Toc23519990)

[2.3 Web安全监测依据 10](#_Toc23519991)

[2.4 安全级别说明 11](#_Toc23519992)

[3 测试概述 12](#_Toc23519993)

[3.1 综述 12](#_Toc23519994)

[3.2 风险分布 12](#_Toc23519995)

[3.2.1 存在问题测评项目数 12](#_Toc23519996)

[3.2.2 风险等级分布 12](#_Toc23519997)

[3.2.3 风险类型分布 13](#_Toc23519998)

[4 检测详情 13](#_Toc23519999)

[4.1 Web安全检测报告摘要 13](#_Toc23520000)

[4.2 总体结论 13](#_Toc23520001)

[4.3 Web安全监测报告详情 13](#_Toc23520002)

[5 报告生成时间 14](#_Toc23520003)

# 前言

## 阅读报告说明

本次安全检测报告从服务器网站应用安全、网站服务器中间件安全等方面对您的网站进行的安全检测。由于检测方法的不同，检测结果可能会有差异。

您的安全检测报告结论是基于您提供的网站域名或 IP 进行漏洞检测，对服务器网站应用及中间件应用进行检测，如果您服务器在扫描期间开启WAF，可能会导致相关检测结论有偏差。

由于检测项目本身的局限性，本次检测结果未发现风险并不代表没有风险，如您有更深层次的检测需求，可以和项目作者联系。

感谢您对我们的信任和支持。现将对您网站的漏洞检测报告呈上。

## 目标参数

|  |  |
| --- | --- |
| 地址/URL | {{target\_url}} |
| 问题数量 | {{number\_of\_vulnerabilities\_in\_the\_target\_website}} |

表1.1基本信息

# 专家建议指导

## 安全服务建议

### 安全评估

由专业的安全技术人员对系统进行全面的安全隐患排查，从技术角度分析出客户业务中存在的安全问题，并指导客户进行加固和修复的专业安全服务。

### 渗透测试

通过渗透测试可帮助企业全面发现主机安全问题、业务漏洞、网络风险、人员安全意识弱点，并提供专业修复解决方案来抵御外部攻击。

### 安全加固

在客户授权委托的情况下，远程登录得到客户的业务系统服务器上，对外网或内网主机进行全方位的基线加固和组件升级，提前修补系统潜在的各种高危漏洞和安全威胁，保障客户业务系统安全。

### 安全培训

根据企业具体情况与需求，定制个性化的安全培训课程计划，帮助企业了解并掌握相关安全知识。通过培训，帮助企业在研发和运维过程中尽量避免由于安全知识的匮乏而造成信息安全事故。

### 应急响应

在您的系统遭受黑客攻击时提供快速、专业、高效的应急处理，包括入侵行为排查、病毒木马查杀、入侵原因分析、入侵防护意见、入侵影响评估等；帮助客户正确应对黑客攻击，降低攻击带来的安全损失，本服务7\*24小时全天候。

### 红蓝对抗

有区别于传统意义上的仅关注资产，基于漏洞库和扫描器等方式的安全评估方式。  
针对分析资损风险、逻辑漏洞、业务风险、数据风险、应用风险、员工风险、第三方关联风险等基于人工分析和漏洞相结合的手段，以攻击者视角对目标进行全面深入的分析判断，从而全面细节的评估企业风险。

### 漏洞扫描服务

通过伏特分布式漏洞扫描平台对指定的远程或者本地计算机系统进行安全脆弱性检测，提供专业漏洞扫描报告，漏洞扫描报告结果可读性强，也提供专家解读或指导服务。

### 安全保障服务

针对企业重要IT系统资产、包括主机、网络、应用等系统运行维护，保障企业开展大型活动或会议时业务的安全性。

## 风险类型处理建议

### SQL注入类

没有被授权的恶意攻击者可以在有该漏洞的系统上任意执行 SQL 命令，这将威胁到数据库的安全，并且会泄漏敏感信息。 针对 SQL 注入，目前的解决办法是：

1. 在程序中限制用户提交数据的长度。

2、对用户输入的数据进行合法性检查，只允许合法字符通过检测。对于非 字符串类型的，强制检查类型；字符串类型的，过滤单引号。

3、WEB 程序调动低权限的 sql 用户连接，勿用类似于 dbo 高权限的 sql 账 号。细化 Sql 用户权限，限定用户仅对自身数据库的访问控制权限。

4、使用具备拦截 SQL 注入攻击能力（专门算法）的 IPS（入侵防御设备） 来保护网站系统。

### 跨站脚本类

1、在程序中限制用户提交数据的长度。

2、对用户输入的数据进行合法性检查，只允许合法字符通过检测。

3、使用具备拦截跨站脚本攻击能力（专门算法）的 IPS（入侵防御设备） 来保护网站系统。

### 密码泄露类

采用 HTTPS 协议，保护登录页面。 并对用户名密码参数采用密文传输。

### 其他类

如上传漏洞修改程序过滤恶意文件；证书错误修改证书；链接错误修改错误链接，开放不安全端口等。

### 服务最小化

对系统主机的服务进行确认关闭一些无用的服务或端口，确保主机安全。 对数据库的一些端

口建议对端口进行做防火墙连接限制，保证不能让外界主机 对数据库进行管理。

### 配置权限

将网站的各个目录（包括子目录）尽量减小权限，需要用什么权限开什么权限，其他的权限全部删除。

### 配置日志

对访问网站的 URL 动作进行记录全部日志，以便日后的审计和检查。

## Web安全监测依据

|  |
| --- |
| WEB 安全检测依据 |
| 《OWASP TOP 10 2019》 |
| 《中华人民共和国网络安全法》 |
| 《中华人民共和国计算机信息系统安全保护条例》 |
| 《信息安全等级保护管理办法》 |
| 《计算机信息系统安全保护等级划分准则》 |
| 《信息系统安全等级保护定级指南》 |
| 《信息系统安全等级保护基本要求》 |
| 《信息系统安全等级保护测评准则》 |
| 《信息安全技术 公共及商用服务信息系统个人信息保护指南》 |
| 《GB/T 20270-2006 信息安全技术 网络基础安全技术要求》 |
| 《GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求》 |
| 《GB/T 20272-2006 信息安全技术 操作系统安全技术要求》 |
| 《GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求》 |
| 《GB/T 20984-2007 信息安全技术 信息安全风险评估规范》 |
| 《GB/Z 20985-2007 信息安全技术 信息安全事件管理指南》 |

表 2.2 WEB 安全检测依据

# 检测详情

## Web安全监测报告详情

|  |  |
| --- | --- |
|  | {%tr for i in vulnerability %} |
| 漏洞名称 | {{i.vulnerability\_name}} |
| 漏洞地址 | {{i.vulnerability\_address}} |
| 漏洞级别 | {{i.vulnerability\_level}} |
| 发现时间 | {{i.find\_the\_time}} |
| 漏洞描述 | {{i.vulnerability\_description}} |
| 漏洞危害 | {{i.vulnerability}} |
| 漏洞细节 | {{i.vulnerability\_details}} |
| 修复建议 | {{i.repair\_suggestions}} |

表4.0 存在 HTML Form found in redirect page [high severity] 漏洞

|  |  |
| --- | --- |
|  | {%tr endfor %} |

5.报告生成时间

报告生成时间：2019-12-20 11:11:23~2019-12-20 11:21:49

报告导出时间：2020-05-26 16:57:08