

# 安全扫描报告-2025-05-08

报告生成时间：2025-05-08 06:08:36

报告描述：无描述

报告类型：综合报告

## 安全概述

### 资产统计：

- 总资产数：12个

### 信息收集统计：

- 网络信息：3条
- 操作系统信息：1条
- 组件与服务信息：4条
- 总计：8条

### 漏洞扫描统计：

- 高危漏洞：17个
- 中危漏洞：0个
- 低危漏洞：0个
- SQL注入：2个
- XSS跨站脚本：1个
- 文件包含：4个
- 命令注入：10个
- SSRF：0个
- 总计：17个

## 信息收集详细结果

ID	资产	模块	描述	扫描时间
231	pikachu	组件与服务信息	路径探测	2025-05-07 12:41:11
229	www.gstatic.com	网络信息	端口扫描	2025-05-06 08:36:24
228	fonts.gstatic.com	网络信息	端口扫描	2025-05-05 12:58:33
227	pikachu	组件与服务信息	PHP	2025-05-05 12:58:23
226	pikachu	组件与服务信息	1	2025-05-05 12:58:23
225	pikachu	网络信息	端口扫描	2025-05-05 12:58:23
224	pikachu	组件与服务信息	Apache服务	2025-05-05 12:58:23
223	pikachu	操作系统信息	windows服务器	2025-05-05 12:58:23

漏洞扫描详细结果

ID	资产	漏洞名称	类型	严重程度	URL
228	pikachu	远程文件包含漏洞	文件包含	高	http://pikachu/vul/ssrf/ssrf_c...
226	pikachu	远程文件包含漏洞	文件包含	高	http://pikachu/vul/xss/xss_ref...
225	pikachu	URL参数 message 中的XSS漏洞	XSS跨站脚本	高	http://pikachu/vul/xss/xss_ref...
224	pikachu	URL参数 submit 中的命令执行漏洞	命令注入	高	http://pikachu/vul/fileinclude...
223	pikachu	URL参数 filename 中的命令执行漏洞	命令注入	高	http://pikachu/vul/fileinclude...
220	pikachu	URL参数 filename 中的命令执行漏洞	命令注入	高	http://pikachu/vul/fileinclude...
217	pikachu	远程文件包含漏洞	文件包含	高	http://pikachu/vul/fileinclude...
215	pikachu	URL参数 filename 中的命令执行漏洞	命令注入	高	http://pikachu/vul/fileinclude...
212	pikachu	URL参数 filename 中的命令执行漏洞	命令注入	高	http://pikachu/vul/fileinclude...
209	pikachu	URL参数 filename 中的命令执行漏洞	命令注入	高	http://pikachu/vul/fileinclude...
155	pikachu	URL参数 filename 中的命令执行漏洞	命令注入	高	http://pikachu/vul/fileinclude...
150	pikachu	URL参数 filename 中的命令执行漏洞	命令注入	高	http://pikachu/vul/fileinclude...
145	pikachu	URL参数 message 中的命令执行漏洞	命令注入	高	http://pikachu/vul/xss/xss_ref...
102	pikachu	URL参数 name 中的SQL注入漏洞	SQL注入	高	http://pikachu/vul/sqli/sqli_s...
101	pikachu	POST参数 id 中的SQL注入漏洞	SQL注入	高	http://pikachu/vul/sqli/sqli_i...
93	pikachu	URL参数 filename 中的命令执行漏洞	命令注入	高	http://pikachu/vul/fileinclude...
92	pikachu	本地文件包含漏洞	文件包含	高	http://pikachu/vul/fileinclude...

安全建议

- 定期更新系统和应用程序，以修复已知的安全漏洞
- 实施最小权限原则，限制用户和进程的权限
- 加强网络访问控制，使用防火墙和入侵检测系统
- 实施安全编码实践，预防常见的安全漏洞
- 定期进行安全培训，提高安全意识
- 建立安全事件响应计划，及时应对安全事件