安全评估报告

目标：test.example.com

生成时间：2026-02-08 05:33:51

评估工具：HexStrike AI (Nmap + Nuclei)

扫描统计摘要

项目	数量
严重漏洞	0
高危漏洞	1
中危漏洞	1
低危漏洞	0
开放端口	4

漏洞扫描结果

高危 (1)

漏洞名称	SQL Injection
标签	sqli, mysql
描述	Potential SQL injection vulnerability detected....

中危 (1)

漏洞名称	SSH Weak Algorithms
标签	ssh, crypto
描述	SSH server supports weak encryption algorithms....

信息 (1)

漏洞名称	Apache HTTP Server Version Disclosure
标签	misconfig, exposure, apache, http
描述	Apache HTTP Server version disclosure detected....

端口扫描结果

端口/协议	服务	版本	风险等级
22/tcp	ssh	OpenSSH 8.2	严重
80/tcp	http	Apache 2.4.41	中危
443/tcp	https	nginx 1.18.0	中危
3306/tcp	mysql	MySQL 8.0.27	低危

安全建议

SSH 安全加固

- 禁用密码登录，只允许密钥认证
- 修改默认端口（22）
- 配置 fail2ban 防暴力破解
- 限制访问来源 IP（防火墙）

漏洞修复优先级

- 立即修复严重和高危漏洞
- 隔离受影响的系统
- 检查是否存在已遭受攻击的迹象
- 应用最新的安全补丁

报告说明

本报告由 HexStrike AI 自动生成

建议：定期进行安全评估，及时修复发现的漏洞

生成时间：2026-02-08 05:33:51