安全扫描报告

扫描信息

目标URL	https://127.0.0.1:5001
扫描时间	2025-03-31 11:25:28
漏洞总数	5

漏洞摘要

按严重程度划分

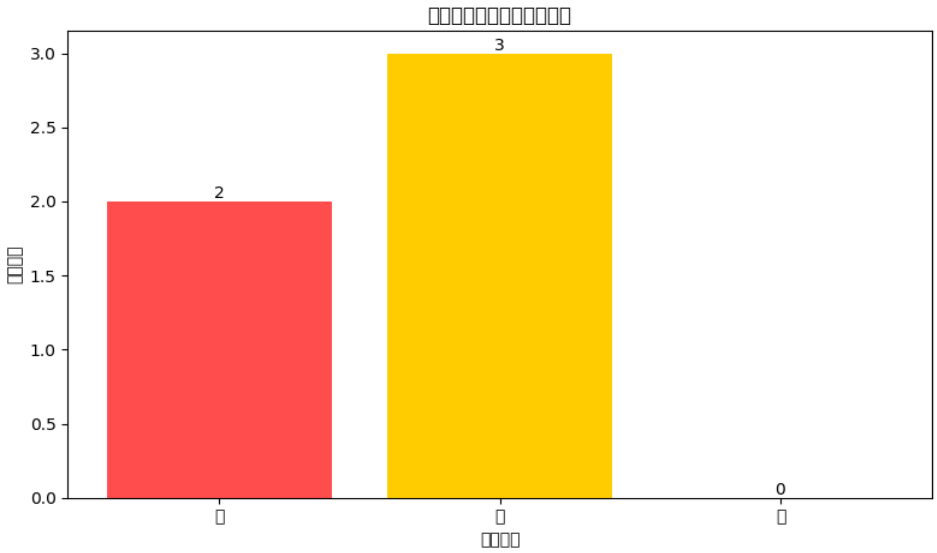
严重程度	数量
高	2
中	3
低	0

按漏洞类型划分

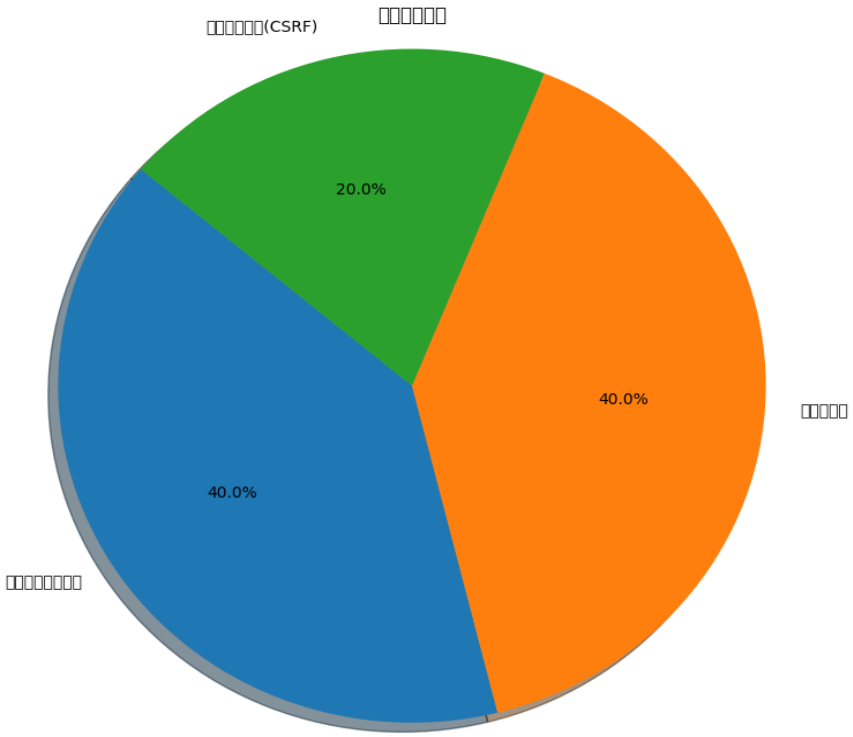
漏洞类型	数量
缺少暴力破解防护	2
弱密码策略	2
跨站请求伪造(CSRF)	1

图表与统计

漏洞严重程度分布



漏洞类型分布



漏洞详细信息

漏洞 #1: 缺少暴力破解防护

严重程度	高
描述	系统未实施暴力破解防护机制
受影响端点	/api/authenticate

详情:
- 问题: 多次失败登录后仍可继续尝试
- 风险: 容易遭受密码暴力破解攻击

建议修复方案:
- 实施账户锁定机制
- 在连续失败登录后增加延迟
- 实施验证码或其他人机验证
- 考虑使用双因素认证

漏洞 #2: 缺少暴力破解防护

严重程度	高
描述	系统未实施暴力破解防护机制
受影响端点	/auth/token

详情:
- 问题: 多次失败登录后仍可继续尝试
- 风险: 容易遭受密码暴力破解攻击

建议修复方案:
- 实施账户锁定机制
- 在连续失败登录后增加延迟
- 实施验证码或其他人机验证
- 考虑使用双因素认证

漏洞 #3: 弱密码策略

严重程度	中
描述	系统接受弱密码
受影响端点	/api/authenticate

详情:
- 问题: 接受简单密码如'password123'
- 风险: 容易被字典攻击或暴力破解

建议修复方案:
- 实施强密码策略
- 要求密码包含大小写字母、数字和特殊字符
- 实施密码定期更换机制
- 使用密码强度检查器

漏洞 #4: 弱密码策略

严重程度	中
描述	系统接受弱密码
受影响端点	/auth/token

详情:
- 问题: 接受简单密码如'password123'
- 风险: 容易被字典攻击或暴力破解

建议修复方案:
- 实施强密码策略
- 要求密码包含大小写字母、数字和特殊字符
- 实施密码定期更换机制
- 使用密码强度检查器

漏洞 #5: 跨站请求伪造(CSRF)

严重程度	中
描述	缺少CSRF保护
受影响端点	/api/update_profile

详情:
- 问题: 表单提交未包含CSRF令牌验证
- 风险: 攻击者可以诱导用户执行未授权的操作

建议修复方案:
- 实现CSRF令牌验证
- 验证请求来源(Origin/Referer)
- 使用SameSite Cookie属性