

SAFS-Scanner AI 自动化渗透测试报告

生成时间: 2025-12-30 19:10:17

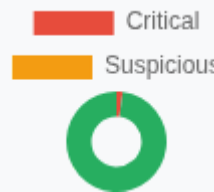
1. 风险统计概览

探测总点位: 101

高危 (Critical): 2

疑似 (Suspicious): 0

安全 (Safe): 99



特征解释表:

特征	含义
Length Diff	响应长度变化比例; 大幅减少可能意味着异常重定向或错误页。
Status Change	HTTP 状态码发生变化, 可能触发 WAF 或异常处理。
Time Delay	响应耗时增加; 在 SQL 盲注/时间延迟探测中常见。
Err Score	页面中出现数据库或错误关键字的得分。
DOM Sim	与基线页面的 DOM 相似度; 低值代表页面结构差异大。
Reflect	Payload 在页面中的反射比例; 低值可能是后端处理但仍存在风险。

Exploitation Result (全局利用成果)


无成功利用证据


2. 详细发现清单

AI 置信度: 65.8%

目标 URL: http://testaspnet.vulnweb.com/search.aspx?query=test

注入参数	query
攻击载荷 (Payload)	"
风险等级	CRITICAL

 **AI 判定依据:** Payload 存在高比例反射 (疑似 XSS)

 **修复建议:** 检测到反射型风险 (可能 XSS/报错注入)。请对输出进行严格的 HTML 实体编码，过滤危险标签/事件，并最小化错误回显；启用 CSP 限制内联脚本。

AI 特征指纹: 长度差异(0.00), 报错匹配(0.0), DOM相似度(1.00)


核心发现与证据

[MSFCONSOLE] 成功拿到证据: {}

AI 置信度: 84.8%

目标 URL: http://testaspnet.vulnweb.com/search.aspx?query=test

注入参数	query
攻击载荷 (Payload)	'
风险等级	CRITICAL

 **AI 判定依据:** Payload 存在高比例反射 (疑似 XSS)

 **修复建议:** 检测到反射型风险 (可能 XSS/报错注入)。请对输出进行严格的 HTML 实体编码，过滤危险标签/事件，并最小化错误回显；启用 CSP 限制内联脚本。

AI 特征指纹: 长度差异(0.00), 报错匹配(0.0), DOM相似度(1.00)

核心发现与证据

[MSFCONSOLE] 成功拿到证据: {}