

SAFS-Scanner AI 自动化渗透测试报告

生成时间: 2025-12-30 19:06:21

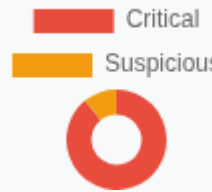
1. 风险统计概览

探测总点位: 74

高危 (Critical): 66

疑似 (Suspicious): 8

安全 (Safe): 0



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

尝试利用 (未成功)


- sqlmap · URL: http://demo.testfire.net/search.jsp?query=bank · Param: query · 原因: 执行超时, 可能需要更长等待或降低防护 · 日志: [timeout] sqlmap execution exceeded timeout


2. 详细发现清单

AI 置信度: 86.1%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	" OR 1=1 --
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: 84.1%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

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: 83.7%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

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: 84.1%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	/*9904*/" OR 1=1 --
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: 86.1%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	" + OR + 1 = 1 + --
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: 50.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	\${7*7}
风险等级	SUSPICIOUS



AI 判定依据: Payload 存在高比例反射 (疑似 XSS)

反射提示: 仅回显, 需验证是否可执行

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

AI 判定理由: Payload 存在高比例反射 (疑似 XSS)

AI 置信度: 83.5%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	/*9904*/*/**/OR/**/1=1/**/--
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: 83.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	\${7*7} #
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: 85.9%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	\${7*7} --
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: 83.7%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	& ping -c 1 127.0.0.1 --
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: 82.4%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	& ping -c 1 127.0.0.1 # --
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: 85.9%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	%26%20whoami
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: 85.2%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	& whoami%00
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: 50.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	& ping -c 1 127.0.0.1
风险等级	SUSPICIOUS

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

 **反射提示:** 仅回显, 需验证是否可执行

 **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

AI 判定理由: Payload 存在高比例反射 (疑似 XSS)

AI 置信度: 83.7%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

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: 84.1%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

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: 66.5%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	& ping -c 1 127.0.0.1 #
风险等级	CRITICAL

 **AI 判定依据:** 响应显著延迟 (疑似时间盲注, 3.27s) | Payload 存在高比例反射 (疑似 XSS)

 时间盲注迹象：需复核

 **修复建议:** 检测到 SQL 注入风险/利用成功。请使用参数化查询 (Prepared Statements) 或存储过程，避免拼接 SQL；关闭数据库错误回显，并最小化数据库账户权限。

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: 81.8%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

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: 81.8%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	' %00
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: 81.8%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

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: 86.1%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

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: 83.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

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: 75.2%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	' AND (SELECT 1 FROM (SELECT COUNT(*),CONCAT(0x7e,DATABASE(),0x7e,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) --
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(0.02), 报错匹配(0.0), DOM相似度(0.99)

核心发现与证据

[MSFCONSOLE] 成功拿到证据: {}

AI 置信度: 75.2%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	'+AND+(SELECT+1+FROM+(SELECT+COUNT(*),CONCAT(0x7e,DATABASE(),0x7e,FLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.PLUGINS+GROUP+BY+x)a)++
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(0.02), 报错匹配(0.0), DOM相似度(0.99)

核心发现与证据

[MSFCONSOLE] 成功拿到证据: {}

AI 置信度: 75.1%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	" AND (SELECT 1 FROM (SELECT COUNT(*),CONCAT(0x7e,DATABASE(),0x7e,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) --
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(0.02), 报错匹配(0.0), DOM相似度(0.99)

核心发现与证据

[MSFCONSOLE] 成功拿到证据: {}

AI 置信度: 75.5%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	' aND (SelEcT 1 fROM (SElecT cOunT(*),cONCAT(0X7E,DaTAbASE(),0X7E,Floor(raND(0)*2))X FRoM iNFORmation_SchemA.plUgins GRoUP by x)a) --
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(0.02), 报错匹配(0.0), DOM相似度(0.99)

核心发现与证据

[MSFCONSOLE] 成功拿到证据: {}

AI 置信度: 84.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	'+AND+sleep(5)+--
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: 82.4%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	/*1698*/' AND sleep(5) --
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: 84.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	' AND sleep(5) --
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: 81.8%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	'/**/AND/**/sleep(5)/**/--
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://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	"/**/ /**/1=1/**/--
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: 86.1%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	' 1=1 --
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: 86.1%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	' OR 1=1 --
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: 86.2%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	" 1=1 --
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: 83.5%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	' UNION SELECT 1,2,3,4,5 --
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: 82.4%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	' UNiOn SELEct 1,2,3,4,5 --
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: 83.5%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	" UNION SELECT 1,2,3,4,5 --
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: 82.5%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	""/><script/>alert(1)</script/>
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: 83.3%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	""><script>prompt(1)</script>
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: 81.3%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	'/**/UNION/**/SELECT/**/1,2,3,4,5/**/--
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: 81.8%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	""><script>alert(1)</script>
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: 86.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	') OR ('1'=1
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: 83.5%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	') OR ('1' like '1
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: 86.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	') ('1'='1
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: 86.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	')+OR+('1'=1
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: 50.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	../../../../../../../../etc/passwd
风险等级	SUSPICIOUS

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

 **反射提示:** 仅回显, 需验证是否可执行

 **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

AI 判定理由: Payload 存在高比例反射 (疑似 XSS)

AI 置信度: 82.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	../../../../../../../../etc/passwd --
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: 50.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	../../../../../../../../windows/win.ini
风险等级	SUSPICIOUS



AI 判定依据: Payload 存在高比例反射 (疑似 XSS)

反射提示: 仅回显, 需验证是否可执行

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(0.01), 报错匹配(0.0), DOM相似度(1.00)

核心发现与证据

AI 判定理由: Payload 存在高比例反射 (疑似 XSS)

AI 置信度: 81.9%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	../../../../../../../../windows/win.ini #
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(0.01), 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: 81.9%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	../../../../../../../../windows/win.ini --
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(0.01), 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: 50.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	/etc/passwd
风险等级	SUSPICIOUS

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

 反射提示：仅回显，需验证是否可执行

 **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


AI 判定理由: Payload 存在高比例反射 (疑似 XSS)


AI 置信度: 50.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	/etc/passwd%00
风险等级	SUSPICIOUS

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

 反射提示：仅回显，需验证是否可执行

 **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

AI 判定理由: Payload 存在高比例反射 (疑似 XSS)

AI 置信度: 85.1%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	/etc/passwd --
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://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	1'/**/AND/**/1=1/**/#
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: 82.4%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	1'/**/AND/**/1/**/like/**/1/**/#
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: 86.2%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	1' AND 1=1 #
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: 86.2%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	1'+AND+1=2+#
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: 82.4%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	1'/**/AND/**/1 like 1'/**/#
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: 86.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	1" AND 1=2 #
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://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	1'/**/AND/**/1=2/**/#
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: 86.2%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	1' AND 1=2 #
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://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	; cat /etc/passwd #
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://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	; cat /etc/passwd --
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://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	; cat /etc/passwd
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: 85.9%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	; whoami
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: 85.3%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	; whoami #
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: 50.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	%3C%25%3D%207%2A7%20%25%3E
风险等级	SUSPICIOUS

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

 反射提示：仅回显，需验证是否可执行

 **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

AI 判定理由: Payload 存在高比例反射 (疑似 XSS)


AI 置信度: 50.0%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	<%= 7*7 %>%00
风险等级	SUSPICIOUS

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

 反射提示：仅回显，需验证是否可执行

 **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


AI 判定理由: Payload 存在高比例反射 (疑似 XSS)

AI 置信度: 84.3%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	<body onload=alert(1)>
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://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	<body onload=prompt(1)>
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: 83.9%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	<body onload=confirm(1)>
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: 81.7%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	<iframe src=javascript:alert(1)></iframe>
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(0.01), 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: 82.1%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	<iframe src=javascript:alert(1)//></iframe//>
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(0.01), 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: 81.8%

目标 URL: http://demo.testfire.net/search.jsp?query=bank

注入参数	query
攻击载荷 (Payload)	<iframe src=javascript:prompt(1)></iframe>
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(0.01), 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: {}