# SAFS-Scanner AI 自动化渗透测试报告

生成时间: 2025-12-30 18:55:08

---

## 1. 风险统计概览

**探测总点位:** 152

**高危 (Critical):** 127

**疑似 (Suspicious):** 25

**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: 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: 82.3%

## 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)** | " 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)** | " || 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)** | /*9721*/" 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: 84.1%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | %24%7B7%2A7%7D -- |
| **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: 83.3%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | %2527 -- |
| **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: 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%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: 50.0%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | %26%20ping%20-c%201%20127.0.0.1 |
| **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: 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: 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: 81.8%

## 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: 83.7%

## 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: 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: 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: 83.0%

## 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: 83.3%

## 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: 79.7%

## 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: 75.9%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ' && (SELECT 1 FROM (SELECT COUNT(*),CONCAT(0x7e,DATABASE(),0x7e,FLO||(R&&(0)*2))x FROM INF||MATION_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: 82.8%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ' && 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: 83.0%

## 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: 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: 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)** | /*6922*/' 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: 83.8%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | /*6922*/' 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: 86.1%

## 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: 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: 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: 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: 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: 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: 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: 84.8%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | /*1487*/') 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: 80.2%

## 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)** | ../../../../../../../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: 84.1%

## 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: 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(0.00), 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)** | ..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5Cwindows%5Cwin.ini%20--%20 |
| **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: 81.6%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5Cwindows%5Cwin.ini%20--%20 -- |
| **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(0.99)

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: 85.9%

## 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: 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)** | /*6666*/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: 83.0%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | 1' AND 1 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: 83.5%

## 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** | 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)** | /*9120*/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: 83.0%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | 1' AND 1 like 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: 86.1%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | 1' && 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=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)** | /*1461*/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: 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: 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: 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: 84.1%

## 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: 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: 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=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: 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:confirm(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: 81.7%

## 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: 83.5%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | <img src=x onerror=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: 81.8%

## 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: {}

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)** | <img src=x onerror=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: 83.3%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | <img src=x on error=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: 82.4%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | <script>confirm(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: 82.4%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | <img src=x onerror=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: 83.7%

## 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: 81.8%

## 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: 84.9%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | <svg/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: 84.8%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | <svg/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)** | <svg/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: 50.0%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | C:\Windows\win.ini%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: 84.8%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | C:\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(0.00), 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)** | C:\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(0.00), 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)** | C:\Windows\win.ini%00%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: 85.2%

## 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: 81.8%

## 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: 85.1%

## 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)** | hello_world |
| **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: 82.8%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | hello_world #%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: 86.0%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | hello_world # |
| **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)** | hello_world%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: 84.1%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | hello_world%20--%20 |
| **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)** | hello_world -- -- |
| **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)** | hello_world%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: 84.1%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | javascript: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)** | javascript: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: 85.3%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ok -- |
| **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)** | javascript: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: 50.0%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ok |
| **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)** | ok # |
| **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: 83.2%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ok -- # |
| **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)** | ok%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: 81.8%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ok -- |
| **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)** | ok %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: 83.2%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ok -- %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: 85.3%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ok -- -- |
| **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: 83.2%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ok -- # |
| **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: 82.6%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | php://filter/convert.base64-encode/resource=index.php -- |
| **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)** | php://filter/convert.base64-encode/resource=index.php |
| **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: 50.0%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ready |
| **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: 83.2%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ready # # |
| **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)** | php://filter/convert.base64-encode/resource=index.php%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(0.01), 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: 81.8%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ready # |
| **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)** | ready -- |
| **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)** | ready -- %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: 85.9%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ready%2500 # |
| **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: 85.1%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ready%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: 85.9%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | ready%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)** | ready%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)** | ready%2500 -- |
| **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)** | ready%252500 |
| **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)** | test_safe_string |
| **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: 84.5%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | test_safe_string # |
| **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)** | test_safe_string -- |
| **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: 84.9%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | test_safe_string -- |
| **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: 83.8%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | test_safe_string -- -- |
| **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)** | test_safe_string%2500 |
| **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}} |
| **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: 83.3%

## 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: 50.0%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | %7B%7Bconfig%7D%7D |
| **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: 85.9%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | {{config}} # |
| **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: 85.1%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | {{config}} -- |
| **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)** | \| type C:\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(0.00), 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)** | \| type C:\Windows\win.ini%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: 83.8%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | \| whoami%00%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: 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: 81.8%

## 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: 85.1%

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

| | |
|---|---|
| **注入参数** | query |
| **攻击载荷 (Payload)** | \| whoami%00%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: 85.2%

## 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: 85.9%

## 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: 85.1%

## 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: 83.2%

## 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: {}