



Automated Web Testing

Problems with web application security

-




Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack:

 Select...


Use traditional spider:


☒

Use ajax spider:

☐ with

Firefox Headless






 Attack

 Stop

Progress:

Attack complete - see the Alerts tab for details of any issues found

▼ Alerts (5)


- ▶  Cross Site Scripting (Reflected)
- ▶  X-Frame-Options Header Not Set (46)
- ▶  Absence of Anti-CSRF Tokens (6)
- ▶  Web Browser XSS Protection Not Enabled (48)
- ▶  X-Content-Type-Options Header Missing (48)

Software Vulnerability Tools

- ZAP
- Selenium
-

Cross Site Scripting (Reflected)

URL: `http://10.118.2.64/xss/example1.php?name=%3C%2Fhtml%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Chtml%3E`

Risk:  High

Confidence: Medium

Parameter: name

Attack: `</html><script>alert(1);</script><html>`

Evidence: `</html><script>alert(1);</script><html>`

CWE ID: 79

WASC ID: 8

Source: Active (40012 - Cross Site Scripting (Reflected))



By Stefan Zetko

