Web Penetration Testing

Web application Vulnerabilities

- SQL Injection
- Cross site scripting
- Broken Authentication
- Sensitive Data Exposure
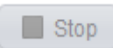- Broken Access Control

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 been given permission to test.

URL to attack:	http://10.118.2.64/xss/example1.php?name=hack ▼ 🌐 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
- Manual Testing

Zetksm1@student.op.ac.nz   by Stefan Zetko