FSI LEI 2025/2026

Practical Exercises #7

Goals

Auditing security using OWASP ZAP and WSTG top 10

Use Kali Linux to remotely explore security of a system

Installing and configuring OWASP ZAP

1. Download and install OWASP *ZAP* [1]

Running an automated scan

2. Run an automated scan against the Altoro Mutual web site. [2]
3. Explore alerts and OWASP Top 10.
4. Analyze solutions proposed by ZAP.

Running an active attack

5. Configure your browser to proxy requests through ZAP (manually or launch via ZAP for manual exploration).
6. Attack the login form via SQL-injection. Use break points in ZAP to intercept and modity the request. [3]

Information gathering using Kali Linux

7. Run a network scan via *nmap* (open ports and HTTP headers).
8. Remotely audit the Altoro Mutual web site using tools available in Kali Linux (e.g. whatweb, nikto, dirb).

References

- OWASP ZAP
- OWASP ZAP docs
- OWASP Top 10: 2025
- Kali Linux
- Altoro Mutual web site
- Altoro Mutual website GitHub

[1] Can be used locally in your system or with Kali Linux
[2] Altoro Mutual (testfire.net) is a deliberately vulnerable website maintained by IBM for educational purposes. Applying any technique described here to systems without express authorization is illegal.
[3] Suggestion: use the expression ' OR TRUE --' as the user id in the attack