Evaluation of the final project (Unit 11) vs. the design proposal (Unit 6)

We evaluated various tools to carry out the work, namely NMAP, Burp Suite, Metasploit, Nessus Essentials, SQLMap, Wapiti, Nikto, OWASP ZAP, Dimitry, Knockpy, Hydra, and Skipfish. We prioritised these tools considering manual or automated testing.

These tools provided valuable and expected findings:

1. OWASP ZAP
2. Nmap
3. Burp Suite
4. Nikto
5. Hydra

In the Part 1 Design Document, we provided assumptions for potential vulnerabilities. Due to no access, some were not detected, such as unsecured websites / unsecured transactions. However, detected assumptions were found using Burp Suite and ZAP tool where passwords and logins are submitted in cleartext. Some of the browsers are able to redirect the website HTTP to HTTPS with TLS 1.3 (Appendix 6.4) for communication certificates.

Further omissions were discovered that DNS record does not contain Anti Spam/ Phishing policy, DOS/ DDOS attacks are excluded in the test due to the 'house rules'. The website was hosted by a genuine company using WAF (Appendix 6.5) and used four subdomains in two different locations; this guaranteed protection and availability of service. The tools did not detect unrestricted access and weak authentication vulnerabilities. We could not access the login to the website by using the default user with a common password list to bypass the login and crack the website credentials.