Unit 6 vs Unit 11 Evaluation

In unit 6 we prepared a design document to perform penetration and network tests against an e-commerce website in order to check how secure it is and if it complies with the GDPR and PCI-DSS regulations.

In our design document, we stated two steps that we would perform: the information gathering, the documentation and the investigation of gathered data.

During the information gathering, we stated that we would consult the Open Web Application Security Project (OWASP) and use tools such as Fingerprinting, DNS scans, IP scans and penetration tools such as the OWASP ZAP Proxy.

During the documentation and investigation of gathered data, we stated that we would first consider the probability and severity of any vulnerabilities found to calculate the risk and then classify the ratings in three categories: low, medium, and high risk.

Finally, we asserted the testing limitations expected, such as limitation of time to perform further penetration tests, limitation in the access level and limitation of the methods we can use to penetrate the web application.

In Unit 11, after we performed all scans mentioned above, we prepared an executive summary, written in an easy-to-understand non-technical manner stating all vulnerabilities and risks found. The risks were presented in a table divided into low, medium, and high risk, followed by further explanation of each vulnerability and probable future troubles either in the security of the website, or troubles complying with the required regulations.

Overall, the final assignment in Unit 11 was solely based on our first assignment, and no notable deviations between the two assignments occurred.