**Instructions**

Carry out a literature search/audit on software sites and the national vulnerabilities database to create a baseline audit on potential vulnerabilities with websites.

Possible vulnerabilities

1. SQL Injection
2. Cross-Site Scripting (XSS)
3. Cross-site Request Forgery (CSRF)
4. Broken authentication & session
5. Bad bots and Distributed Denial of Service (DDoS)
6. OWASP A3:2017-Sensitive Data Exposure
7. Insecure direct object references (IDOR)
8. OWASP M3: Insufficient Transport Layer Protection
9. Online payment fraud
10. Unvalidated redirects and forwards

Reflect on this activity by answering the following questions:

* Did you have any issues or challenges with the literature search/audit on software sites and the national vulnerabilities database?
* How did you overcome them?
* How will they affect your final report?

A lot of research was needed to be done to be able to conduct this assignment. Overall this helped a lot in finding out what to look for in terms of vulnerabilities

References:

Owasp Web Security Testing Guide (no date) OWASP Web Security Testing Guide | OWASP Foundation. Available at: https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP\_Testing\_Guide\_v4.pdf (Accessed: February 20, 2023).

Content security policy (CSP) - http: MDN (no date) HTTP | MDN. Available at: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP (Accessed: February 20, 2023).

Strict-transport-security - http: MDN (no date) HTTP | MDN. Available at: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security (Accessed: February 20, 2023).

Cross site scripting (XSS) (no date) Cross Site Scripting (XSS) | OWASP Foundation. Available at: https://owasp.org/www-community/attacks/xss/ (Accessed: February 20, 2023).

Brute Force attack (no date) Brute Force Attack | OWASP Foundation. Available at: https://owasp.org/www-community/attacks/Brute\_force\_attack (Accessed: February 20, 2023).