**Vulnerability Analysis – Literature Review Activity**

The National Cyber Security Centre (NCSC) in the UK requires to raise a request to check the national vulnerabilities database and will review and store the information provided to ensure the organisational eligibility for using this service (NCSC, 2021). Thus, other sources that are freely and more easily accessible were explored. The Open Web Application Security Project’s (OWASP) list of vulnerability scanning tools (OWASP, 2022) was reviewed; as a result, the website ‘HostedScan’ was identified and leveraged to conduct a vulnerability assessment on the chosen website (<https://ehr-online.co.uk>).

The OWASP Zed Attack Proxy (ZAP) web penetration testing was performed via the ‘HostedScan’ tool. The OWASP ZAP (Makino & Klyuev, 2015) generates a proxy between the website and the client, trying the website’s features and recording the actions performed. Thereafter, it attacks the website via known methods (Sudhodanan *et al*., 2016).

Two medium-, four low-, and one informational-level alerts were identified as per the attached pdf report. The two medium-level alerts were the absence of anti-cross-site request forgery (CSRF) tokens and the use of the jquery library with version 1.4.3 having a security vulnerability; upgrading the jquery library to the latest version would resolve the latter medium-level issue. The four low-level alerts were: 1) a cookie is set with no HttpOnly flag, i.e., the cookie could be accessed by JavaScript and transmitted to another site if a malicious script were run on the webpage; 2) a cookie is set without a secure flag, i.e., the cookie can be accessed via unencrypted connections; 3) a cookie is set without the SameSite attribute, i.e., the cookie can be sent further to a ‘cross-site’ request; 4) the server leaks information via one or more “X-Powered-By” HTTP response header fields, i.e., such details may enable attackers to identify other components the web application relies on and their associated vulnerabilities.

The informational-level alert identified was pertaining to re-examining cache-control directives to ensure that the cache-control header is set properly, thus allowing the browser and proxies to cache the content on the webpage; nevertheless, the resources should be checked to ensure that no sensitive information is cached. Further information is provided in the attached pdf report, including evidence of the attacks performed during penetration testing and suggested solutions to mitigate the issues identified.

Not to impact the comprehensiveness of the assessment required for the final report, further sources were researched, identified, and used to provide a more thorough analysis of the chosen website. These sources and related findings will be collated and presented in the final report itself.

**References**

Makino, Y., & Klyuev, V. (2015) Evaluation of web vulnerability scanners. In *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Vol. 1, pp. 399-402). IEEE.

NCSC (2021) Web Check. Retrieved from <https://www.ncsc.gov.uk/information/web-check>.

OWASP (2022) Vulnerability Scanning Tools. Retrieved from <https://owasp.org/www-community/Vulnerability_Scanning_Tools>.

Sudhodanan, A., Armando, A., Carbone, R., & Compagna, L. (2016) Attack Patterns for Black-Box Security Testing of Multi-Party Web Applications. In *NDSS*.