ABSTRACT

With rapid of information technology, the web-based applicationswere widely used in many fields, however, it increases the concerns of web application security. Aim of this research is to find and assess the security weakness in the XYZ's website by using a Vulnerability Assessment approach through using both OWASP ZAP and Nikto scanners. The selected approach was one of black-box testing, i.e., we only test publicly available endpoints without ever looking at the internal source code. Test results showed 29 vulnerabilities and 15 vulnerabilities were manually validated as valid. One critical vulnerability (missing HSTS Header) with a CVSS v3.1 score of 9.3 was identified, as well as many suboptimal security header configurations and cookies settings. After combining the scan results of these two tools, the precision and recall are both at 0.93 showing the capability of the combined methodology to detect vulnerabilities without producing a high number of false positives. This research also provides a set of actionable mitigation suggestions, categorized by risk level, to assist development and security teams to strengthen the security posture of the XYZ website.

Keywords: *vulnerability assessment, OWASP ZAP, Nikto, black-box testing, CVSS, website security.*