ABSTRACT

Indonesia experiences an increase in cyber-attacks every year, especially on web applications that are at risk of causing operational disruption and data leakage. This research aims to evaluate the security of web applications through black box-based penetration testing using the ELEMENT framework. Testing is focused on identifying vulnerabilities based on the OWASP Top 10 2021, followed by an analysis of the results obtained. Based on the study, mitigation recommendations are made to reduce risks and improve the security of the tested web application. The test results showed that the target web application had several vulnerabilities, including an expired SSL Certificate, Cross-Site Scripting (Reflected), publicly displayed admin email information, inappropriate error handling, potential for clickjacking attacks, use of outdated Bootstrap and PHP versions, no lockout mechanism, and no verification of external file integrity. These vulnerabilities are relevant to several categories of OWASP Top 10 2021. This research successfully identified the relevant vulnerabilities, while demonstrating that a testing approach based on the OWASP Top 10 2021 using the ELEMENT framework effectively evaluates the security of web applications.

Keywords: *ELEMENT framework, owasp, pentest, vapt.*