ABSTRACT

The XYZ website has two official sites that support the institution's activities: Site A and Site B. Site A serves as a news source related to the institution's activities, while Site B functions as an information provider for the organization. Site B stores users' personal data uploaded into the system, including email addresses, phone numbers, home addresses, and identity card (KTP) documents. Therefore, both websites must have strong security layers to prevent information manipulation and cyber exploitation that could harm the institution's credibility. One method to identify system vulnerabilities is through penetration testing. This study employs a security analysis method based on the OWASP Top 10 2021 guidelines. The objective of this research is to evaluate potential security vulnerabilities in both websites. The research process follows several stages, including Planning, Information Gathering, Vulnerability Scanning, Attacking, Validation, Result Analysis, and Reporting. The findings indicate 11 vulnerabilities in Site A, consisting of 1 high-risk vulnerability, 6 medium-risk vulnerabilities, and 4 low-risk vulnerabilities. Similarly, Site B has 11 vulnerabilities, including 2 high-risk, 4 medium-risk, and 5 low-risk vulnerabilities. Based on these vulnerabilities, recommendations for improvement have been proposed, which are expected to be implemented on both Site A and Site B to mitigate potential cyber threats from malicious actors and uphold the institution's reputation.

Keywords: *Website Security, Vulnerability Assessment, OWASP Top 10, XYZ Institution.*