ABSTRACT

Cybersecurity has become a critical issue in the digital era, especially for government institutions that are responsible for delivering public information in a transparent and secure manner. The District Court of Purwokerto, as a judicial body, manages its official website as a medium for public communication and legal information dissemination. However, institutional websites are often targeted by cyberattacks due to misconfigurations, outdated systems, or security vulnerabilities within web applications. This study aims to analyze the security vulnerabilities of the District Court of Purwokerto's website and develop mitigation strategies based on the OWASP Top Ten framework. Vulnerability detection was carried out using tools such as OWASP ZAP and Burp Suite, along with the Kali Linux distribution, to test security flaws according to OWASP Top 10 categories. The methodology used is penetration testing with the support of tools like OWASP ZAP, Burp Suite, Xray, and Sqlmap within a controlled testing environment. The testing revealed several significant vulnerabilities, including Broken Access Control, Cryptographic Failures, Injection, Vulnerable and Outdated Components, and Identification and Authentication Failures through authentication testing. These findings indicate that the website still contains weaknesses in access control, encryption, input validation, and system updates. Based on these results, technical and procedural mitigation recommendations were developed to enhance the website's resilience against potential cyberattacks. This study is expected to provide an accurate overview of the security condition of the District Court of Purwokerto's website and serve as a reference for other government institutions in strengthening their web system security.

Keywords: Cybersecurity, OWASP Top Ten, Vulnerability Analysis, District Court of Purwokerto, Web Application Vulnerabilities.