ABSTRACT

In this ever-evolving digital age, web application security is an important aspect that every company, including information technology service companies, must pay attention to. This study aims to identify, evaluate, and mitigate vulnerabilities on website X using the Vulnerability Assessment and Penetration Testing (VAPT) approach. The research process began with an information gathering phase using Nmap to obtain initial information regarding ports and running services. Subsequently, vulnerability scanning was conducted using OWASP ZAP and Acunetix to detect potential security flaws on the website. Based on the scanning results, 13 types of vulnerabilities with varying severity levels were identified, including SQL Injection, Cross-Site Scripting (XSS), unencrypted credential transmission, publicly readable .htaccess files, Slow HTTP DoS, and various security header configuration vulnerabilities.

After the scanning stage, exploitation testing was conducted using Burp Suite, slowhttptest, and other manual methods to validate whether the vulnerabilities could indeed be exploited. The test results showed that some vulnerabilities, such as readable .htaccess files, missing security headers (Content-Security-Policy, X-Frame-Options), and information leaks through headers, were successfully exploited. Meanwhile, the SQL Injection and XSS vulnerabilities detected turned out to be false positives after further testing.

The final stage of the research is mitigation, which involves applying middleware configurations on the Laravel framework, modifying the .htaccess file, and setting cookies to have security attributes. Some vulnerabilities were fully addressed, such as the readable .htaccess file, missing security headers, and X-Powered-By information leakage. However, other vulnerabilities, such as the use of HTTP for credential transmission, could not be fully resolved due to limitations in implementing the HTTPS protocol in the testing environment.

Keywords: *Vulnerability Assessment, Penetration Testing*, Keamanan *Web, OWASP ZAP, Acunetix*, *Laravel*, Mitigasi Kerentanan