ABSTRACT

The security of information systems has emerged as a critical concern for organizations in the digital age, especially in light of increasingly sophisticated cyber threats. This study focuses on identifying and addressing security vulnerabilities on a website by applying the Vulnerability Assessment method. The research object is the cloned site cselu-clone.web.id, which is based on the WordPress content management system. The study adopts the Design Science Research (DSR) methodology with a grey-box testing strategy, without performing full exploitation or penetration testing.

The data collection process is structured into three key phases: the initial phase (which includes problem identification and literature review), the testing phase (comprising information gathering, vulnerability detection, and validation), and the final phase (consisting of documentation and mitigation recommendations). Various tools were employed, including Nmap for reconnaissance, Nessus for general vulnerability scanning, WPScan for identifying WordPress-related issues, OWASP ZAP for analyzing web applications, and Burp Suite for manual verification.

A total of 11 vulnerabilities were discovered, categorized by severity: 2 high-severity issues (DNS Server Spoofed Request Amplification DDoS and ThemeMakers Themes Information Disclosure), 6 medium-severity issues (such as DNS Recursive Query Poisoning, absence of HSTS, XSS in the Elementor plugin, HTML Injection in Tutor LMS, missing CSP header, and missing anti-clickjacking header), and 3 low-severity issues (including disclosure of server information, Unix timestamp exposure, and the absence of the X-Content-Type-Options header).

Keywords— Information System Security, Vulnerability Assessment, Grey-box Testing, WordPress Security, Web Application Vulnerabilities