ABSTRAK

Keamanan sistem informasi telah muncul sebagai perhatian kritis bagi organisasi di era digital, terutama mengingat ancaman siber yang semakin canggih. Penelitian ini berfokus pada mengidentifikasi dan menangani kerentanan keamanan di sebuah situs web dengan menerapkan metode Penilaian Kerentanan. Objek penelitian adalah situs kloning cselu-clone.web.id, yang berbasis pada sistem manajemen konten WordPress. Penelitian ini mengadopsi metodologi Riset Ilmu Desain (DSR) dengan strategi pengujian kotak abu-abu, tanpa melakukan eksploitasi penuh atau pengujian penetrasi.

Proses pengumpulan data terstruktur menjadi tiga fase kunci: fase awal (yang mencakup identifikasi masalah dan tinjauan literatur), fase pengujian (yang terdiri dari pengumpulan informasi, deteksi kerentanan, dan validasi), dan fase akhir (yang terdiri dari dokumentasi dan rekomendasi mitigasi). Berbagai alat digunakan, termasuk Nmap untuk pengintaian, Nessus untuk kerentanan umum. Berbagai alat digunakan, termasuk Nmap untuk pengintaian, Nessus untuk pemindaian kerentanan umum, WPScan untuk mengidentifikasi masalah terkait WordPress, OWASP ZAP untuk menganalisis aplikasi web, dan Burp Suite untuk verifikasi manual.

Sebanyak 11 kerentanan ditemukan, dikategorikan berdasarkan tingkat keparahan: 2 masalah dengan tingkat keparahan tinggi (DNS Server Spoofed Request Amplification DDoS dan ThemeMakers Themes Information Disclosure), 6 masalah dengan tingkat keparahan sedang (seperti DNS Recursive Query Poisoning, tidak adanya HSTS, XSS di plugin Elementor, HTML Injection di Tutor LMS, tidak adanya header CSP, dan tidak adanya header anti-clickjacking), dan 3 masalah dengan tingkat keparahan rendah (termasuk pengungkapan informasi server, eksposur timestamp Unix, dan tidak adanya header X-Content-Type-Options).

Kata Kunci— Keamanan Sistem Informasi, Penilaian Kerentanan, Pengujian Kotak Abu-abu, Keamanan WordPress, Kerentanan Aplikasi Web