ABSTRAK

Dalam era digital yang terus berkembang, keamanan aplikasi web menjadi aspek penting yang harus diperhatikan oleh setiap perusahaan, termasuk perusahaan layanan teknologi informasi. Penelitian ini bertujuan untuk mengidentifikasi, mengevaluasi, dan memitigasi kerentanan pada website X menggunakan pendekatan Vulnerability Assessment dan Penetration Testing (VAPT). Proses penelitian diawali dengan tahap *information gathering* menggunakan Nmap untuk memperoleh informasi awal terkait port dan layanan yang berjalan. Selanjutnya, dilakukan *vulnerability scanning* menggunakan OWASP ZAP dan Acunetix untuk mendeteksi potensi celah keamanan pada website. Berdasarkan hasil pemindaian, ditemukan sebanyak 13 jenis kerentanan dengan tingkat keparahan berbeda, di antaranya SQL Injection, Cross-Site Scripting (XSS), pengiriman kredensial tanpa enkripsi, file .htaccess dapat dibaca publik, Slow HTTP DoS, serta berbagai kerentanan konfigurasi header keamanan.

Setelah tahap scanning, dilakukan pengujian eksploitasi (exploit) menggunakan Burp Suite, slowhttptest, dan metode manual lainnya untuk memvalidasi apakah kerentanan benar-benar dapat dimanfaatkan. Hasil pengujian menunjukkan bahwa beberapa kerentanan seperti file .htaccess terbaca, hilangnya header keamanan (Content-Security-Policy, X-Frame-Options), serta kebocoran informasi melalui header berhasil dieksploitasi. Sementara itu, kerentanan SQL Injection dan XSS yang terdeteksi ternyata merupakan false positive setelah diuji lebih lanjut.

Tahap akhir penelitian adalah mitigasi, yaitu dengan menerapkan konfigurasi middleware pada framework Laravel, modifikasi file .htaccess, dan pengaturan cookie agar memiliki atribut keamanan. Beberapa kerentanan berhasil ditutup sepenuhnya, seperti .htaccess readable, header keamanan yang hilang, dan kebocoran X-Powered-By. Namun, beberapa kerentanan lain seperti penggunaan HTTP pada pengiriman kredensial tidak dapat sepenuhnya ditangani karena keterbatasan penerapan protokol HTTPS di lingkungan pengujian.

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