ABSTRAK

Jumlah kebocoran data global pada kuartal ketiga 2022 mencapai 72,45 juta akun, dengan Indonesia berada di peringkat ketiga. Salah satu penyebab utamanya adalah lemahnya keamanan situs web, termasuk situs pemerintah. Situs web Pengadilan Negeri X menjadi objek penelitian untuk mengidentifikasi kerentanan dan meningkatkan keamanannya menggunakan metode *Penetration Testing Execution Standard* (PTES). Topik ini penting karena banyak situs pemerintah yang rawan terhadap serangan siber, seperti *Distributed Denial of Service* (DDoS) dan *Clickjacking*. Kondisi saat ini menunjukkan bahwa meskipun beberapa situs telah dilindungi *firewall*, banyak kerentanan lain seperti *header* keamanan yang tidak diatur atau tema CMS yang rentan terhadap eksploitasi. Solusi yang diterapkan meliputi enam tahapan PTES: pengumpulan data, pemodelan ancaman, analisis kerentanan, eksploitasi, *post-eksploitasi*, dan pelaporan. Penelitian dilakukan menggunakan alat seperti *OWASP ZAP, WPScan*, dan *SQL Map*. Hasil utama menunjukkan bahwa hanya serangan *Clickjacking* yang berhasil dieksploitasi, sementara empat serangan lainnya *XSS*, *SQL Injection, Brute Force,* dan DDoS belum berhasil mengeksploitasi situs web tersebut karena adanya perlindungan *firewall*. Kontribusi penelitian ini adalah mengetahui sistem keamanan dari website dan memberikan rekomendasi perbaikan, seperti penambahan *header X-Frame-Options* dan metode *Traffic Filtering*, untuk meningkatkan keamanan situs pemerintahan.

Kata Kunci : Keamanan sistem, *Penetration Testing*, *PTES*, *Website*