ABSTRAK

Keamanan sistem informasi menjadi tantangan serius dalam pengembangan dan pengoperasian website, terutama bagi platform yang menyajikan informasi publik. Situs berita PT XYZ sebagai salah satu portal berita yang banyak diakses oleh masyarakat Indonesia. Saat ini, PT XYZ memiliki kunjungan bulanan yang hampir menyentuh angka 300 ribu, menunjukkan tingginya jumlah pengunjung yang mengakses dan berinteraksi dengan situs setiap bulan. Dengan tingginya volume lalu lintas pengguna, risiko eksploitasi celah keamanan semakin meningkat, sehingga penguatan sistem keamanan menjadi hal yang krusial. Pada tahun sebelumnya, PT XYZ mengalami insiden keamanan yang menyebabkan seluruh database situs terhapus akibat serangan siber. Meskipun data dapat dipulihkan dari cadangan, kejadian ini menunjukkan adanya celah keamanan yang dapat dieksploitasi oleh pihak tidak bertanggung jawab. Serangan tersebut tidak hanya berdampak pada hilangnya data, tetapi juga berpotensi menurunkan kepercayaan pengguna terhadap keamanan informasi yang dikelola oleh situs. Dengan jumlah pengunjung yang besar, keberlanjutan operasional situs sangat bergantung pada ketahanan sistem terhadap serangan siber. Oleh karena itu, diperlukan langkah proaktif berupa *penetration testing* untuk mengidentifikasi dan menutup potensi kerentanan guna mencegah insiden serupa di masa mendatang. Penelitian ini akan melakukan *vulnerability testing* dan *penetration testing* dengan menggunakan framework OWASP (*Open Web Application Security Project*). Pengujian akan mengacu pada standar *OWASP Top 10 2021* serta menggunakan OWASP ZAP sebagai alat utama. Hasil pengujian menunjukkan bahwa tingkat keamanan website Situs XYZ, XYZ Jurnalis, dan XYZ Editor masih tergolong rentan. Hasil uji penetrasi menunjukkan Terdapat 20 kerentanan, 4 bersifat tinggi, 10 bersifat sedang, dan 6 bersifat rendah. Prioritas perbaikan difokuskan pada *SQL Injection Potential*, header keamanan yang hilang, komponen usang, dan perlindungan *bruteforce*. Rekomendasi perbaikan mencakup penerapan HTTPS, *header* keamanan seperti CSP dan HSTS, pembaruan komponen, validasi input, serta mekanisme anti-bot. Langkah-langkah ini bertujuan untuk meningkatkan ketahanan situs terhadap serangan siber dan menjaga kepercayaan pengguna.

Kata Kunci: Keamanan Sistem Informasi, OWASP, Vulnerability Test, Penetration Test