ABSTRAK

Situs web XYZ memiliki dua situs resmi yang berfungsi untuk mendukung aktivitas lembaga, yaitu situs A dan situs B. Situs web A digunakan sebagai sumber berita terkait kegiatan lembaga XYZ, sementara situs B berfungsi sebagai penyedia informasi lembaga. Situs B menyimpan data pribadi pengguna yang diunggah ke dalam sistem, seperti email, nomor telepon, alamat, hingga dokumen Kartu Tanda Penduduk (KTP). Oleh karena itu, kedua situs ini harus memiliki lapisan keamanan yang kuat untuk mencegah manipulasi informasi dan eksploitasi dari serangan siber yang dapat merusak kredibilitas lembaga. Salah satu metode untuk mengidentifikasi kerentanan pada sistem adalah melalui pengujian penetrasi. Penelitian ini menggunakan metode analisis keamanan berdasarkan panduan OWASP Top 10 2021. Tujuan dari penelitian ini adalah untuk mengevaluasi kerentanan keamanan yang mungkin terdapat pada kedua situs tersebut. Proses penelitian dilakukan melalui beberapa tahapan seperti *Planning*, *Information Gathering*, *Vulnerability Scanning*, *Attacking*, Validasi, Analisa Hasil, dan Reporting. Hasil penelitian menunjukkan terdapat 11 kerentanan pada situs A yang terdiri dari 1 kerentanan high, 6 kerentanan medium, dan 4 kerentanan kerentanan low. Di situs B terdapat 11 kerentanan yang diantaranya 2 kerentanan high, 4 kerentanan medium, dan 5 keentanan low. Dari kerentanan tersebut, diajukan rekomendasi perbaikan yang diharapkan dapat diterapkan pada situs A dan situs web B untuk mengurangi potensi serangan siber oleh pihak yang tidak bertanggung jawab serta menjaga nama baik lembaga.

Kata Kunci:. *Keamanan situs web, Evaluasi Kerentanan, Uji Penetrasi, OWASP Top 10, Lembaga XYZ.*