ABSTRAK

Kemajuan teknologi yang pesat telah mendorong peningkatan penggunaan internet, namun hal ini juga diiringi dengan meningkatnya risiko serangan siber. Ancaman siber dapat berupa pelanggaran hukum yang merusak dan mencuri data penting dari aplikasi web, sehingga membahayakan keamanan jaringan, basis data, dan sistem komputer. *Website* resmi Pemerintah Kabupaten Xyz yang dikelola oleh Dinas Komunikasi dan Informatika (Diskominfo) memiliki peran penting sebagai media komunikasi dan penyampaian informasi kepada masyarakat. Penelitian ini bertujuan untuk menganalisis tingkat keamanan dan kerentanan *website* tersebut menggunakan metode *penetration testing*. Metode ini melibatkan simulasi serangan siber untuk mengidentifikasi potensi celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Proses pengujian dilakukan melalui beberapa tahapan, mulai dari pengumpulan informasi, identifikasi celah, eksploitasi, hingga pelaporan hasil. Alat bantu seperti *SQLMap* dan *Xray* digunakan untuk mendeteksi kerentanan umum seperti *SQL Injection, Cross-Site Scripting (XSS),* dan kelemahan dalam konfigurasi server. Hasil penelitian menunjukkan adanya beberapa celah keamanan yang berpotensi dieksploitasi. Temuan ini dapat digunakan sebagai dasar dalam menyusun langkah mitigasi guna meningkatkan keamanan situs web Pemerintah Kabupaten Xyz sebelum dimanfaatkan oleh pihak yang tidak berwenang.

Kata Kunci: Keamanan Siber, *Penetration testing*, Situs Pemerintah, Sistem Keamanan, *Website*, Kerentanan