ABSTRAK

Aplikasi web semakin menjadi target utama serangan siber seiring dengan meningkatnya ketergantungan bisnis dan organisasi terhadap layanan daring dalam era digital. Kerentanan pada aplikasi web seperti injeksi SQL, *cross-site scripting* (XSS), dan kelemahan autentikasi dapat dimanfaatkan oleh penyerang untuk mendapatkan akses tidak sah dan merusak integritas data. Aplikasi web yang dimiliki Sekolah X mengalami serangan siber yang berdampak pada layanan sekolah, oleh karena itu pengujian penetrasi pada website Sekolah X dilakukan. Pengujian ini bertujuan untuk mengidentifikasi dan memahami kerentanan yang ditemukan pada aplikasi web Sekolah X dengan metode *black-box.* Pengujian dilakukan berdasarkan prinsip-prinsip keamanan Open Web Application Security Project (OWASP) 2021 sebagai dasar pengujian dan mitigasi. Pengujian ini juga dilakukan dengan metode yang tidak mengganggu operasional situs web secara keseluruhan, sehingga pengguna tetap dapat mengakses layanan tanpa gangguan. Selain itu, kerahasiaan data sekolah dan informasi sensitif lainnya harus tetap terjaga sepanjang proses pengujian. Berdasarkan hasil pengujian, ditemukan sejumlah kerentanan dalam aplikasi web berupa penggunaan library JavaScript yang usang, absennya header keamanan seperti Content-Security-Policy dan X-Frame-Options, berpotensi terkena serangan brute force akibat ketiadaan mekanisme pembatasan login, serta paparan informasi sensitif seperti alamat email administrator yang ditampilkan secara terbuka yang dapat diatasi dengan langkah mitigasi sesuai rekomendasi OWASP.

Kata Kunci: pengujian penetrasi, aplikasi web, mitigasi, OWASP.