ABSTRAK

Website DipoVerify merupakan sistem verifikasi surat sakit digital berbasis fullstack web yang dikembangkan untuk mendukung proses penerbitan dan validasi surat keterangan sakit mahasiswa secara digital. Dalam arsitektur sistem informasi kesehatan digital, aspek keamanan basis data pada lapisan backend sangat krusial untuk melindungi integritas data rekam medis. Penelitian ini bertujuan untuk menganalisis batas ambang ketahanan serta mengevaluasi efektivitas metode pengamanan basis data relasional MySQL pada backend REST API Express.js platform DipoVerify terhadap ancaman serangan SQL Injection (SQLi) dan Cross-Site Scripting (XSS). Evaluasi keamanan siber ini dilakukan melalui metode eksperimen laboratorium dengan pendekatan pengujian penetrasi (penetration testing) berbasis Black-Box Testing. Pengujian dilakukan pada tiga target utama, yaitu Endpoint Autentikasi Pengguna (Login API), Endpoint Modul Penerbitan Surat Sakit Digital, dan Endpoint Modul Verifikasi Keaslian Dokumen secara manual menggunakan alat uji Postman untuk eksploitasi parameter dan manipulasi payload serangan siber. Skenario pengujian membandingkan dua kondisi arsitektur kode kueri, yaitu kondisi aplikasi rentan (pre-patching) dan kondisi aplikasi defensif (post-patching) setelah diterapkan metode kueri berparameter (parameterized queries) serta sanitasi input (input sanitization). Variasi kategori payload yang disimulasikan meliputi In-band SQLi (Error-based & Union-based), Inferential/Blind SQLi (Boolean-based & Time-based), Bypass Authentication, dan Stored XSS. Hasil pengujian penetrasi awal pada kondisi aplikasi rentan menunjukkan bahwa seluruh objek endpoint berhasil dieksploitasi, dibuktikan dengan jebolnya hak akses login tanpa kredensial valid, kebocoran struktur tabel database, terjadinya kebocoran data (data leakage) rekam medis dengan respon sukses HTTP 200 OK, serta tereksekusinya skrip JavaScript berbahaya pada browser. Namun, setelah diimplementasikan mekanisme pertahanan menggunakan parameterized queries dan pustaka sanitasi XSS, tingkat ketahanan sistem meningkat secara signifikan. Seluruh variasi payload serangan siber yang disuntikkan berhasil ditangkal sepenuhnya, ditunjukkan melalui respon status kode HTTP 400 Bad Request atau HTTP 500 Internal Server Error yang aman tanpa membocorkan arsitektur basis data, serta konversi payload XSS menjadi entitas HTML pasif. Kesimpulan dari penelitian ini menegaskan bahwa penerapan kueri berparameter dan sanitasi input pada framework Express.js mampu memitigasi celah keamanan manipulasi instruksi SQL dan injeksi skrip secara absolut, sekaligus memberikan perlindungan yang tangguh bagi integritas dokumen kesehatan digital DipoVerify.

Kata kunci: *Backend, Express.js, MySQL, SQL Injection, Cross-Site Scripting, Parameterized Queries, Penetration Testing, DipoVerify.*