ABSTRAK

Keamanan sistem pembayaran elektronik melalui payment gateway menjadi krusial dalam mendukung integritas dan kepercayaan dalam transaksi finansial online. Dalam era digital saat ini, website top-up games telah menjadi komponen penting dalam industri game, memberikan platform bagi pengguna untuk melakukan transaksi finansial. Namun, platform ini sering menjadi target serangan oleh pihak yang tidak bertanggung jawab, terutama melalui teknik serangan SQL Injection. Oleh karena itu, penelitian ini bertujuan untuk menganalisis dan mendeteksi potensi kerentanan terhadap serangan SQL Injection pada sistem pembayaran elektronik.

Metodologi penelitian ini melibatkan pengujian penetrasi menggunakan payload SQL Injection dengan pernyataan Data Manipulation Language (DML) dan Data Definition Language (DDL). Tujuannya adalah untuk memahami bagaimana aplikasi merespons terhadap serangan yang mencoba memanipulasi data di dalam database dan apakah aplikasi memiliki lapisan keamanan yang memadai untuk melindungi struktur database.

Hasil pengujian menunjukkan bahwa sistem memiliki mekanisme keamanan yang cukup efektif dalam mendeteksi dan mencegah serangan SQL Injection. Meskipun ada beberapa serangan yang berhasil, yang mengindikasikan adanya celah keamanan, sebagian besar serangan gagal berkat mekanisme keamanan yang ada. Hasil ini memberikan wawasan yang mendalam tentang kerentanan keamanan dan langkah-langkah mitigasi yang diperlukan untuk memperkuat keamanan sistem.

Kata kunci: Data, Database, Injeksi SQL, Keamanan Siber.