

BAB I

PENDAHULUAN

1.1 Latar Belakang

Website top-up games telah menjadi komponen integral dalam industri game, menyediakan platform bagi pengguna untuk melakukan pembelian dalam permainan, mengakses konten premium, dan melaksanakan transaksi finansial. Keberhasilan dan kepercayaan pengguna terhadap platform ini sangat terkait dengan keamanan sistem yang diterapkan. Dalam beberapa tahun terakhir, terjadi peningkatan diversifikasi game yang tersedia di platform top-up, mencakup game PC, konsol, dan mobile, yang semakin meluaskan pangsa pasar top-up games [1].

Perusahaan top-up games semakin memprioritaskan keamanan transaksi dan perbaikan layanan pelanggan, menyadari pentingnya membangun kepercayaan pengguna di dalam platform mereka. Terlebih lagi, munculnya dompet digital beberapa tahun terakhir mempermudah pengguna untuk melakukan pembayaran digital, yang meningkatkan kecepatan transaksi di ekosistem digital secara eksponensial [2].

Namun, platform seperti situs web dan aplikasi mobile sering kali menjadi sasaran bagi pihak yang tidak bertanggung jawab, terutama melihat celah atau kerentanan dalam sistem. Salah satu teknik serangan yang paling umum namun memiliki dampak kerugian yang signifikan jika berhasil digunakan adalah SQL Injection. Teknik ini digunakan untuk mengekstrak data-data krusial seperti informasi transaksi, Token atau Signature key, data pribadi konsumen, atau struktur data tabel yang digunakan untuk melaksanakan transaksi.

Dalam konteks keamanan transaksi digital, deteksi dan pencegahan terhadap serangan SQL Injection memiliki urgensi yang besar. Ini penting karena transaksi digital melibatkan data sensitif, seperti informasi finansial dan data pribadi pengguna. Kebocoran data atau transaksi yang terganggu bisa mengakibatkan kerugian finansial yang signifikan bagi perusahaan dan pengguna. Di samping itu, terdapat regulasi hukum terkait perlindungan data yang, jika dilanggar, bisa mengakibatkan denda besar dan dampak hukum lainnya.

Melalui penelitian ini, diharapkan dapat meningkatkan kualitas keamanan platform-platform transaksi digital seperti top up games. Selain itu penelitian ini dapat membantu mendeteksi potensi-potensi serangan yang terjadi sehingga kerugian akibat serangan tersebut dapat dihindari.

Dari permasalahan yang sudah dipaparkan diatas oleh karena itu penulis membuat penelitian yang berjudul “**ANALISIS DAN DETEKSI SERANGAN SQL INJECTION PADA JARINGAN KEAMANAN PAYMENT GATEWAY**” agar para pengembang aplikasi ataupun website dapat meminimalisir serangan yang merugikan Perusahaan ataupun Konsumen dalam sebuah transaksi digital.

1.2 Rumusan Masalah

Bedasarkan latar belakang yang sudah dibahas, maka dapat dibuat beberapa rumusan masalah pada penelitian kali ini, yaitu:

1. Bagaimana cara mendeteksi aktivitas yang berpotensi terjadinya SQL injection dalam sebuah sistem?
2. Bagaimana cara mencegah SQL injection terjadi disebuah sistem transaksi digital?
3. Bagaimana cara mengamankan sebuah data agar ketika SQL injection terjadi, Data tersebut tidak diterima ataupun diterima secara acak oleh penyerang?

1.3 Tujuan dan Manfaat

Adapun tujuan dari penelitian ini dibuat adalah untuk mendeteksi, mencegah, dan mengamankan terjadinya sebuah kebocoran data transaksi digital yang menyebabkan kerugian bagi Perusahaan ataupun konsumen. Manfaat yang diharapkan dari penelitian ini, sebagai berikut:

1. Peningkatan keamanan sebuah transaksi digital.
2. Pencegahan terjadinya penyerangan kedalam sebuah sistem ataupun data vital.
3. Peningkatan kontrol dan monitoring terhadap proses keamaan jaringan.

1.4 Batasan Masalah

Adapun batasan masalah yang penulis gunakan agar penelitian ini berjalan dengan efektif :

1. Penelitian ini akan berfokus pada analisa dan deteksi sebuah sistem transaksi digital top up games.
2. Data yang digunakan untuk melakukan testing adalah data dummy sehingga tidak ada pihak yang di rugikan ketika melakukan uji coba.

1.5 Metode Penelitian

Dalam melakukan metode penelitian pada pembuatan tugas akhir ini penulis menggunakan metode *System Engineering Process* sebagai berikut:

1. Studi Literatur
Melakukan studi literatur terkait topik penelitian, konsep-konsep dasar, dan teknologi yang digunakan.
2. Analisis Kebutuhan
Mengidentifikasi dan menganalisis kebutuhan pengguna dan fungsionalitas sistem yang akan dikembangkan.
3. Perancangan Sistem
Merancang arsitektur, antarmuka, dan algoritma sistem berdasarkan hasil analisis kebutuhan.
4. Integrasi Komponen
Mengintegrasikan komponen-komponen sistem yang telah dirancang, seperti modul, database, dan API.
5. Pengembangan Perangkat Lunak
Mengimplementasikan kode program sistem sesuai dengan rancangan yang telah dibuat.
6. Uji coba dan Evaluasi
Melakukan uji coba dan evaluasi terhadap sistem yang telah dikembangkan, baik secara fungsional maupun non-fungsional.
7. Analisis Data

Menganalisis data yang diperoleh dari hasil uji coba dan evaluasi, serta membandingkannya dengan studi literatur yang relevan.

8. Kesimpulan

Menyimpulkan hasil penelitian yang sudah dilakukan berdasarkan hasil Analisis data.

1.6 Jadwal Pelaksanaan

Dalam menyelesaikan penelitian ini peneliti telah menyiapkan timeline kegiatan penulisan projek akhir. Hal ini berfungsi agar semua kegiatan penulisan sesuai dengan rencana penelitian.

Tabel 1.1 *Timeline* Pengerjaan Projek Akhir

| No. | Deskripsi Tahapan | Durasi | Tanggal Selesai | Milestone |
|-----|------------------------------|----------|-----------------|-----------------------------|
| 1 | Studi Literatur | 2 minggu | 17 April 2024 | <i>Research</i> |
| 2 | Analisis Kebutuhan | 2 minggu | 1 Mei 2024 | <i>Wireframe</i> |
| 3 | Perancangan Sistem | 3 Minggu | 15 Mei 2024 | <i>Project planning</i> |
| 4 | Integrasi Komponen | 3 minggu | 5 Juni 2024 | <i>Prototype and coding</i> |
| 5 | Pengembangan Perangkat Lunak | 6 minggu | 17 Juli 2024 | <i>Sytem development</i> |
| 6 | Uji coba dan evaluasi | 2 minggu | 31 Juli 2024 | <i>Testing</i> |
| 7 | Analisis Data | 2 minggu | 13 Agustus 2024 | <i>Analysis Sample</i> |
| 8 | Kesimpulan | 3 Hari | 16 Agustus 2024 | <i>Summary Report</i> |