1. Pendahuluan

Latar Belakang

Seiring dengan kemajuan jaman, teknologi seperti internet merupakan hal yang sangat penting. Terutama teknologi internet seperti website. Menurut data dari kominfo menyebutkan bahwa berdasarkan penelitian yang dilakukan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pengguna internet di Indonesia telah mencapai 143,26 juta jiwa atau 54,68 persen dari penduduk Indonesia meningkat 10,56 juta jiwa dari hasil survei tahun 2016 (Kominfo, 2018). Pertumbuhan pengguna internet ini sejalan dengan pertumbuhan jumlah website yang semakin berkembang. Hal ini membuktikan bahwa sudah banyak orang yang tersadar bahwa website adalah suatu teknologi yang penting untuk menyebarkan informasi ke khalayak ramai. Selain pembuatannya yang relatif mudah, penyebaran informasi pada website terbilang cukup efektif.

Perkembangan teknologi tidak diseimbangi oleh keamanan dari teknologi itu sendiri. Tindakan kriminal di dunia maya setiap tahun selalu berkembang semakin besar dan semakin banyak jenisnya berdasarkan data OWASP Top 10, serangan paling banyak dalam dua survey terakhir yang telah dilakukan organisasi tersebut adalah serangan berbasis injection seperti SQL, NoSQL, OS dan LDAP (OWASP, 10AD). Data yang bersumber dari WhiteHat Security menyebutkan bahwa setidaknya terdapat 83% website yang memiliki minimal satu celah kritis didalamnya (Grossman, 2011). Sistem yang tidak dibangun dengan keamanan maka akan berdampak fatal jika terkena serangan. Tidak sedikit pembobol sistem yang mengambil keuntungan dari sistem yang dirusaknya seperti meminta tebusan terhadap data yang diambilnya atau merusak hanya demi kesenangan semata. Penyebab utama dari buruknya keamanan website adalah pengembang yang tidak menerapkan keamanan yang efektif dan memprogram sistem dengan kode yang lebih aman (Acar et al., 2017).

Metode yang digunakan untuk melakukan penetrasi pada website adalah Blind SQL Injection. Penggunaan metode Blind SQL Injection berdasarkan pada kerumitannya ketika harus memasukkan sintaksnya satu persatu untuk mencari celah yang ada. Dengan penelitian yang dilakukan, proses injeksi sintaks tersebut akan dibuat otomatis. Mempenetrasi website melalui halaman login menggunakan Blind SQL Injection dapat memberikan hasil optimal karena metode ini memberikan pertanyaan-pertanyaan yang menghasilkan jawaban benar atau salah saja sehingga proses injeksi menghasilkan jawaban yang pasti. Kemudian algoritma yang digunakan adalah linear search, binary search dan interpolation search.

Topik dan Batasannya

Permasalahan yang dikerjakan pada tugas akhir ini adalah otomatisasi injeksi SQL yang jarang sehingga PenTester membutuhkan waktu yang lama untuk melakukan serangan serta tidak mengetahui tentang algoritma tes terbaik. Penetration testing sendiri memiliki tiga tahap yang harus dilalui yaitu Information Gathering, Attack Generation dan Response Analysis (Halfond, Choudhary, & Orso, 2009). Fase Information Gathering adalah proses untuk menganalisa target yang bertujuan untuk mengidentifkasi informasi yang berguna untuk menentukan celah serangan yang tepat. Pada penelitian ini fase Information Gathering sudah dilakukan karena menggunakan website localhost yang telah dibuat oleh penulis serta sudah diketahui posisi untuk menginjeksi serangan. Sehingga fokus penelitian ini pada tahap Attack Generation.

Terdapat tiga jenis algoritma yang digunakan dijelaskan pada tabel 1 sebagai berikut:

Tabel 1. Jenis Algoritma

No.	Jenis	Keterangan
1.	Linear Search (Brute Force)	Hasil dicari secara urut berdasarkan urutan data yang dibuat.
2.	Binary Search	Data akan dibagi menjadi dua kemudian dibandingkan apakah hasil tersebut berada dibagian atas atau bawah dari pembagian yang sudah dilakukan sebelumnya lalu akan terus membaginya sampai data yang dicari sama dengan hasilnya.
3	Interpolation Search	Mencari data dengan memperkirakan letak datanya menggunakan nilai kunci (key values).

Sintaks kueri SQL yang berjenis Blind akan diterapkan pada ketiga algoritma tersebut sehingga apabila hasil kueri tersebut benar maka akan memberikan output berupa huruf yang nantinya disusun menjadi sebuah kata yang mengindikasikan bahwa database dari website tersebut telah berhasil ditembus. Output yang ada ditampilkan pada

aplikasi yang dibangun dan tidak memberikan efek tampilan apapun pada halaman website yang di injeksi. Hal ini bertujuan untuk mempermudah pengguna dalam membaca hasilnya.

Sistem yang dibangun fokus pada skema injeksi berdasarkan Blind SQL. Sistem ini dijalankan menggunakan website localhost yang dibangun oleh penulis sehingga tidak melanggar Undang-Undang Internet dan Transaksi Elektronik (UU ITE) yang ada. Ketiga algoritma pada tabel 1 dipilih karena masing-masing memiliki skema pencarian yang berbeda-beda sehingga dapat dijadikan acuan untuk mengukur performansi waktu dari setiap algoritma yang menerapkan skema otomatisasi injeksi SQL.

Tujuan

Tujuan dari tugas akhir ini adalah:

1. Merancang dan mengimplementasikan otomatisasi injeksi Blind SQL menggunakan algoritma linear, binary dan interpolation search.
2. Menganalisis dari segi performansi waktu untuk setiap algoritma yang di implementasikan.

Organisasi Tulisan

Pada tugas akhir ini akan membahas sebanyak lima bab yaitu:

1. Membahas pendahuluan yang berisi pengenalan mengenai penelitian yang dilakukan.
2. Membahas studi terkait penelitian yang sudah ada sebelumnya akan dijadikan referensi pada tugas akhir ini.
3. Membahas bagaimana sistem yang dibangun mencakup rancangannya.
4. Evaluasi yang berisi hasil dari pengujian dan analisisnya.
5. Kesimpulan akhir dari penelitian yang telah dilakukan pada tugas akhir ini.