BAB I

PENDAHULUAN

1.1. Latar Belakang

Internet sebagai jaringan komunikasi global dapat dijadikan sebagai media dan sumber informasi terkini, seperti ilmu pengetahuan, teknologi, hiburan, bisnis dan sumber informasi lainnya. Kemudahan serta kenyamanan seperti ini menyebabkan internet selalu digunakan. Namun dibalik kemudahan dan kenyamanan internet, ternyata ada satu aspek yang saat ini masih kurang diperhatikan oleh pengguna internet, yaitu keamanan yang merupakan salah satu aspek penting pada aplikasi web. Sampai saat ini tidak ada website yang dapat dikatakan benar-benar aman.

SQL Injection adalah kerentanan yang terjadi ketika penyerang memiliki kemampuan untuk mempengaruhi *Structured Query Language* (SQL) *Query* yang melewati suatu aplikasi ke database back-end.dengan mampu mempengaruhi apa yang akan diteruskan ke database, penyerang dapat memanfaatkan sintaks dan kemampuan dari SQL, serta kekuatan dan fleksibilitas untuk mendukung operasi dan fungsionalitas sistem yang tersedia ke database. Injeksi SQL bukan merupakan kerentanan yang eksklusif mempengaruhi aplikasi web, kode yang menerima masukan dari sumber yang tidak dipercaya dan kemudian menggunakan input yang membentuk SQL dinamis bisa rentan. Kasus SQL Injection terjadi ketika penyerang dapat memasukan serangkaian pernyataan SQL ke query dengan memanipulasi data input ke aplikasi.

Berdasarkan penjelasan diatas dapat dikatakan bahwa serangan SQL Injection sangat berbahaya karena penyerangan yang telah berhasil memasuki database sistem dapat melakukan manipulasi data yang ada pada database sistem. Proses manipulasi data yang tidak semestinya oleh penyerang dapat menimbulkan kerugian bagi pemilik website yang terinjeksi kebocoran data dan informasi merupakan hal yang fatal. Data-data tersebut dapat disalahgunakan oleh pihak yang tidak bertanggung jawab.

Keamanan data dan informasi menjadi aspek penting dalam menjaga ketahanan website. Oleh karena itu penulis mencoba membuat simulasi pencegahan dilakukan untuk menguji sebuah website. Berdasarkan latar belakang diatas penulis berniat untuk mengambil tema tentang keamanan website yang berjudul "ANALISIS KEAMANAN MENGGUNAKAN WEB APLIKASI BWAPP TERHADAP SERANGAN XSS DAN SQL INJECTION".

1.2. Rumusan Masalah

Berdasarkan pada latar belakang yang dijelaskan sebelumnya maka rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana Simulasi serangan XSS (Cross Site Scripting)
2. Bagaimana simulasi serangan SQL Injection berjalan
3. Pengujian simulasi serangan XSS dan SQL Injection
4. Pencegahan terhadap serangan XSS dan SQL Injection

1.3. Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Metode serangan yang dipakai pada serangan XSS adalah reflected GET
2. Metode serangan yang dipakai pada serangan SQL Injection adalah SQL Injection Get/Search
3. Simulasi disini menggunakan web aplikasi bwapp

1.4. Tujuan

Tujuan yang ingin dicapai penulis adalah

1. Mengetahui bagaimana mekanisme simulasi serangan yang terjadi pada aplikasi web.
2. Menganalisa web yang terserang XSS dan SQL Injection
3. Bagaimana mencegah web yang terserang SQL Injection
4. Bagaimana mencegah web yang terserang XSS (Cross Site Scripting)

1.5. Manfaat

Manfaat yang didapat dari penelitian ini adalah

1. Dapat mengetahui mekanisme serangan SQL injection
2. Dapat mengetahui mekanisme serangan XSS (Cross Site Scripting)
3. Dapat mengetahui langkah atau tindakan pencegahan berdasarkan analisa keamanan suatu website