BAB I

PENDAHULUAN

1.1. Latar Belakang

Website merupakan wadah untuk menginformasikan kepada masyarakat tentang perusahaan atau instansi-instansi pemerintah dimana tujuannya adalah agar masyarakat mengetahui perkembangan informasi yang ada pada saat ini. Selain sebagai media untuk menyebarkan informasi, *website* juga digunakan sebagai media transaksi berbasis online seperti transaksi pembelian, transaksi penjualan, transaksi pemesanan dll sehingga dapat membantu masyarakat untuk bertransaksi khususnya untuk masyarakat yang lokasi tempat tinggalnya jauh dari toko.

Website harus memiliki tampilan yang bagus dan mudah digunakan oleh masyarakat, selain itu *website* harus memiliki keamanan dari serangan *hacker* karena *website* tersebut memiliki sebuah *database* untuk menyimpan data-data penting pelanggan. Sebagai contoh data pribadi pelanggan, data transaksi, data keuangan dll. Oleh sebab itu penting adanya keamanan pada *website* dimana nanti bisa diketahui celah yang dapat masuk ke dalam *website* tersebut. Ada beberapa teknik untuk menguji keamanan *website*, salah satunya yaitu SQLI (*Structured Query Language Injection*) dan XSS (*Cross Site Scripting*).

SQLI dan XSS merupakan salah satu teknik *hacking* yang sering digunakan oleh seorang *hacker*. Teknik ini bisa mengetahui isi dari tabel-tabel pada *database*, *session*, *cookies*, *user*, tipe *database* dan versi *database* dengan mencantumkan *script* atau *payload* pada sebuah *website* (Kumar, et al. 2018). Teknik ini bisa menjadi sebuah ancaman jika sebuah *website* tidak memiliki keamanan yang dapat menangkal serangan tersebut. Biasanya *hacker* mencari celah dengan menggunakan teknik tersebut pada sebuah *menu login*, *searching*, *menu upload*, *menu input*, *gallery*, berita dan URL (*Uniform Resource Locator*) yang berakhiran dengan angka seperti www.target.com/photo?id=30, tetapi tidak semua *website* yang bisa diserang menggunakan teknik ini (Efendi, et al. 2016).

SQLI adalah sebuah kerentanan yang menyebabkan seorang penyerang memiliki kemampuan untuk mempengaruhi *query* SQL yang dikirimkan melalui aplikasi ke *database* (Yulianingsih, 2016). Secara teori SQLI merupakan serangan kepada *website* yang menggunakan *query* dari SQL yang ditambahkan dengan karakter-karakter selain huruf dan angka. Secara praktek SQLI biasanya menggunakan satu karakter (‘) atau (“) atau (#) pada akhir parameter angka untuk menguji apakah *website* tersebut *vuln* atau tidak (Wiguna, et al. 2020).

Hacker dengan kemampuan tinggi dapat melakukan *remote* setelah mendapat celah dengan melakukan serangan SQLI, dimana *hacker* dapat mengirimkan *script* dengan menggunakan *script* khusus ke *website* tertentu dengan cara melakukan teknik rekayasa sistem (Sahren, et al. 2019). SQLI dapat diartikan suatu kegiatan menipu atau memanipulasi *query* dari *database* dengan cara menyisipkan kode SQL tambahan sehingga seseorang dapat mengetahui dan mendapatkan informasi yang terdapat pada *database* dimana kode SQLI yang disisipkan ke dalam perintah SQL yang asli, maka yang akan dieksekusi adalah perintah SQLI (Efendi, et al. 2016).

XSS adalah sebuah teknik serangan yang menggantikan konteks data ke konteks kode dengan menggunakan karakter khusus (Nagpal, et al. 2017). XSS dilakukan dengan menggunakan kode yang memiliki karakter khusus dan biasanya kode diletakkan di belakang URL. Kode yang dimaksud adalah kode *javascript* yang disisipkan di menu pencarian (Dhivya, et al. 2018). Dampak dari serangan menggunakan XSS ini, seorang *hacker* bisa mengetahui database berserta tabel dan isinya dan ini pastinya sangat berbahaya jika itu terjadi (Aliero, et al. 2020).

XSS juga dapat diartikan sebagai kelemahan yang terjadi karena *web server* tidak dapat memvalidasi data masukan yang diberikan oleh pengguna (Setiawan dan Setiyadi, 2018). Dalam serangan XSS, kita akan menggunakan *payload* untuk mengaitkan situs *website* dengan *JavaScript* sehingga penyerang dapat mengakses mesin korban dari jarak jauh, dimana *script JavaScript* yang dikaitkan ke situs *website* seperti ‘<script src ="http://192.168.234.131:3000/hook.js"></script>’. Setelah terpancing, kami membuat pop di bawahnya yang akan membuat *browser* korban selalu *online*. Kemudian kami mengarahkan korban ke situs *web phishing* (Gunawan, et al. 2018). Dengan XSS maka halaman web ditampilkan, perintah sebenarnya tidak boleh ditampilkan. XSS merupakan salah satu kelemahan yang

sering dimanfaatkan oleh penyerang, namun banyak penyedia layanan yang tidak mengenali kelemahan tersebut.

Berdasarkan latar belakang di atas, maka penulis mengambil judul tesis yaitu "Optimalisasi dalam Penetrasi Testing Keamanan Website Menggunakan Teknik SQL Injection dan XSS" dengan studi kasus sebuah *website* rental mobil CV. Merdeka Auto Rental yang berlokasi di Kota Padang. Penelitian ini bertujuan untuk membantu pemilik usaha agar *website* yang digunakan bisa terhindar dari serangan SQLI dan XSS dengan menggunakan *script* khusus yang dapat menahan serangan SQLI dan XSS.

1.2. Perumusan Masalah

Berdasarkan permasalahan yang ada, supaya tesis ini sesuai dengan tujuan yang ingin dicapai, maka penulis merumuskan beberapa permasalahan sebagai berikut :

1. Bagaimana cara melindungi *website* rental mobil agar terhindar dari serangan SQLI?
2. Bagaimana cara melindungi *website* rental mobil agar terhindar dari serangan XSS?
3. Bagaimana cara mengoptimalkan keamanan *website* rental mobil dari serangan SQLI dan XSS?

1.3. Batasan Masalah

Agar pembahahasan pada penelitian ini tidak menyimpang maka penulis membatasi ruang lingkup objek penelitian. Adapun ruang lingkup penelitian antara lain:

1. Pengujian keamanan *website* rental mobil hanya menggunakan teknik serangan SQLI.
2. Pengujian keamanan *website* rental mobil hanya menggunakan teknik serangan XSS.

3. Pengujian keamanan *website* rental mobil menggunakan *script* khusus yang dapat menahan serangan SQLI dan XSS.

1.4. Tujuan Penelitian

Tujuan yang ingin diperoleh dari penelitian ini agar lebih bermanfaat kedepannya adalah:

1. Memperbaiki keamanan *website* rental mobil agar terhindar dari serangan SQLI.
2. Memperbaiki keamanan *website* rental mobil agar terhindar dari serangan XSS.
3. Mengoptimalkan keamanan *website* rental mobil dari serangan SQLI dan XSS.

1.5. Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat kedepannya, yang beberapa diantaranya adalah:

1. Bagi Pemilik Usaha Rental Mobil

   Diharapkan keamanan pada *website* rental mobil CV. Merdeka Auto Rental lebih optimal dalam menangkis serangan SQLI dan XSS.

2. Bagi Masyarakat

   Diharapkan dengan dilakukannya pengujian keamanan *website* rental mobil di CV. Merdeka Auto Rental agar dapat mengedukasi masyarakat yang mempunyai *website* bisnis usaha untuk lebih berhati-hati dalam serangan *hacker* khususnya serangan dengan teknik SQLI dan XSS yang dapat mencuri data-data yang ada di *website* tersebut dan masyarakat menjadi sadar betapa pentingnya keamanan pada sebuah *website* agar terhindar dari serangan *hacker* jahat.

1.6. Sistematika Penulisan

Sistematika yang digunakan dalam penyusunan tesis ini adalah sebagai berikut:

Bab I PENDAHULUAN

Berisi Latar Belakang, Perumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, dan Sistematika Penelitian.

Bab II LANDASAN TEORI

Pada bab ini dijelaskan teori tentang SQLI dan XSS serta menggunakan *script* seperti *htmlspecialchar*, *mysqli_real_escape_string*, *htmlentities* dan *strip_tags* untuk menangkal dari serangan tersebut.

Bab III METODE PENELITIAN

Bab ini membahas tentang metode yang digunakan untuk melakukan pengujian keamanan *website* ini adalah dengan teknik SQLI dan XSS.

Bab IV ANALISA DAN PERANCANGAN

Bab ini membahas analisa celah SQLI dan XSS serta membuat perancangan pencegahan berupa melakukan perbaikan pada *source code website*.

Bab V PENGUJIAN DAN HASIL

Bab ini membahas implementasi dari perancangan yang telah dibuat serta melakukan pengujian kembali terhadap *website* rental mobil

Bab VI KESIMPULAN DAN SARAN

Bab ini membuat kesimpulan dan hasil penelitian yaitu keunggulan jika sebuah website menggunakan *htmlspecialchar, mysqli_real_escape_string, htmlentities, strip_tags* dan script function PHP pada *coding* programnya.