BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

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 di balik 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. Aspek ini juga kurang mendapat perhatian dari para perancang dan pengelola aplikasi web serta berada di urutan setelah tampilan, atau bahkan berada di urutan terakhir dari daftar yang dianggap penting, sehingga menyebabkan banyak ancaman yang terjadi. Berdasarkan data dari *Web Hacking Incidents Database* (WHID)[13] pada tahun 2010, dari 75 jenis ancaman terhadap aplikasi web, sebanyak 21% merupakan ancaman *SQL Injection* dan 9% adalah ancaman *Cross Site Scripting*. Ancaman *SQL Injection* merupakan ancaman yang terjadi pada database aplikasi web. Database digunakan sebagai media penyimpanan data yang berisi informasi berkaitan dengan aplikasi. Dalam penanganan ancaman *SQL Injection*, metode yang digunakan adalah *Base64_Encode*, namun metode ini masih rentan terhadap manipulasi *string*. Ancaman kedua adalah *Cross Site Scripting* yang terjadi pada tampilan aplikasi web. Salah satu penyebab ancaman ini adalah kurangnya metode *Input Encoding* dalam proses penyaringan karakter sehingga mengizinkan

karakter tertentu dieksekusi. Kedua ancaman di atas menyulitkan para perancang aplikasi web untuk mengetahui mekanisme ancaman yang terjadi.

Untuk mengurangi ancaman ini, dibutuhkan mekanisme pertahanan yang baik sehingga sistem yang telah dibangun tidak hanya mempunyai desain yang bagus namun mempunyai jaminan terhadap integritas data yang ada. Metode yang digunakan dalam penelitian ini adalah *Validating Input. Validating Input* adalah proses pengujian masukan yang diterima oleh aplikasi terhadap standar yang telah didefinisikan. Metode ini digunakan karena sesuai dengan bentuk ancaman yang disimulasikan.

Melalui penelitian ini diharapkan bisa mendapatkan solusi terhadap ancaman yang terjadi dan dapat membangun aplikasi web dengan memperhatikan alasan keamanan sehingga tampilan dan integritas data dapat terjamin. Penelitian ini diberi judul **"SIMULASI ANCAMAN KEAMANAN PADA APLIKASI BERBASIS WEB"**.

1.2 Identifikasi Masalah

Identifikasi masalah dapat dirumuskan dalam pertanyaan sebagai berikut:

1. Sulitnya mengetahui ancaman yang terjadi pada aplikasi web.
2. Lemahnya metode *Input Encoding* dalam menghadapi ancaman *Cross Site Scripting*.
3. Lemahnya metode *Base64_Encode* dalam menghadapi ancaman *SQL Injection*.
4. Bagaimana membangun mekanisme pertahanan yang baik pada aplikasi web menggunakan metode *Validating Input*.

1.3 Maksud dan Tujuan

Maksud dari penulisan tugas akhir ini adalah untuk mensimulasikan ancaman keamanan jaringan komputer pada aplikasi berbasis web.

Sedangkan tujuan yang akan dicapai dalam penelitian ini adalah :

1. Mengetahui bagaimana mekanisme ancaman yang terjadi pada aplikasi web.
2. Mengimplementasikan metode *Validating Input* sebagai pengganti metode *Input Encoding* pada ancaman *Cross Site Scripting.*
3. Mengimplementasikan metode *Validating Input* sebagai pengganti metode *Base64_Encode* pada ancaman *SQL Injection.*
4. Menghasilkan rekomendasi pertahanan yang baik pada aplikasi web.

1.4 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Metode ancaman yang dilakukan pada aplikasi web di sisi database adalah *SQL Injection* dan di sisi tampilan adalah *Cross Site Scripting*.
2. Simulasi ancaman dan pertahanan dilakukan di Internet dengan bentuk *target* simulasi adalah sebuah website portal informasi.
3. Struktur URL *target* dalam metode *SQL Injection* berbentuk **id** yang me-*lookup* ke database, seperti struktur berikut ini :
   a. /mod.php?kategori=lounge&**id=4**
   b. /mod.php?kategori=sains&**id=2**
   c. /mod.php?kategori=teknologi&**id=3**
   d. /mod.php?kategori=kesehatan&**id=2**

e. /mod.php?kategori=tahukah_kamu&**id=2**

f. /mod.php?kategori=unik&**id=1**

4. Bentuk *form* dalam metode *Cross Site Scripting* adalah *form* buku tamu dan *form* pencarian.
5. Metode yang digunakan untuk mengamankan sistem adalah *Validating Input*.
6. Model sistem dibangun dengan bahasa pemrograman PHP dan DBMS MySQL versi 5.
7. Server menggunakan *Virtual Private Server* (VPS) yang telah terhubung dengan DNS server dan internet, sebagai perangkat untuk menjalankan web.
8. Sistem Operasi server yaitu CentOS 5 32bit-kloxo.

1.5 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini adalah metode deskriptif dengan tahapan sebagai berikut:

a. Literatur

   Pengumpulan data dengan cara mengumpulkan literatur, jurnal, paper dan bacaan-bacaan yang ada kaitannya dengan judul penelitian.

b. Perumusan Masalah

   Perumusan masalah merupakan suatu rumusan yang mempertanyakan suatu fenomena, baik dalam kedudukannya sebagai fenomena mandiri, maupun dalam kedudukannya sebagai fenomena yang saling terkait di antara fenomena yang satu dengan yang lainnya, baik sebagai penyebab maupun sebagai akibat.

c. Pemodelan Simulasi

   Pemodelan simulasi merupakan suatu teknik meniru operasi-operasi atau proses- proses yang terjadi dalam suatu sistem dengan bantuan perangkat komputer dan dilandasi oleh beberapa asumsi tertentu sehingga sistem tersebut bisa dipelajari secara ilmiah (Law and Kelton, 1991).

d. Pengujian

   Pengujian simulasi dilakukan dengan dua metode yaitu *SQL Injection* dan *Cross Site Scripting*. Adapun parameter yang diujikan pada *SQL Injection* adalah :

   1) Pengujian Celah Keamanan
   2) Pengujian Jumlah Kolom pada Tabel

3) Pengujian Informasi Database

4) Pengujian Tabel

5) Pengujian Kolom

6) Pengujian Record

Adapun parameter yang diujikan pada *Cross Site Scripting* adalah:

1) Eksekusi Kode HTML

2) Eksekusi Kode untuk menampilkan Cookie

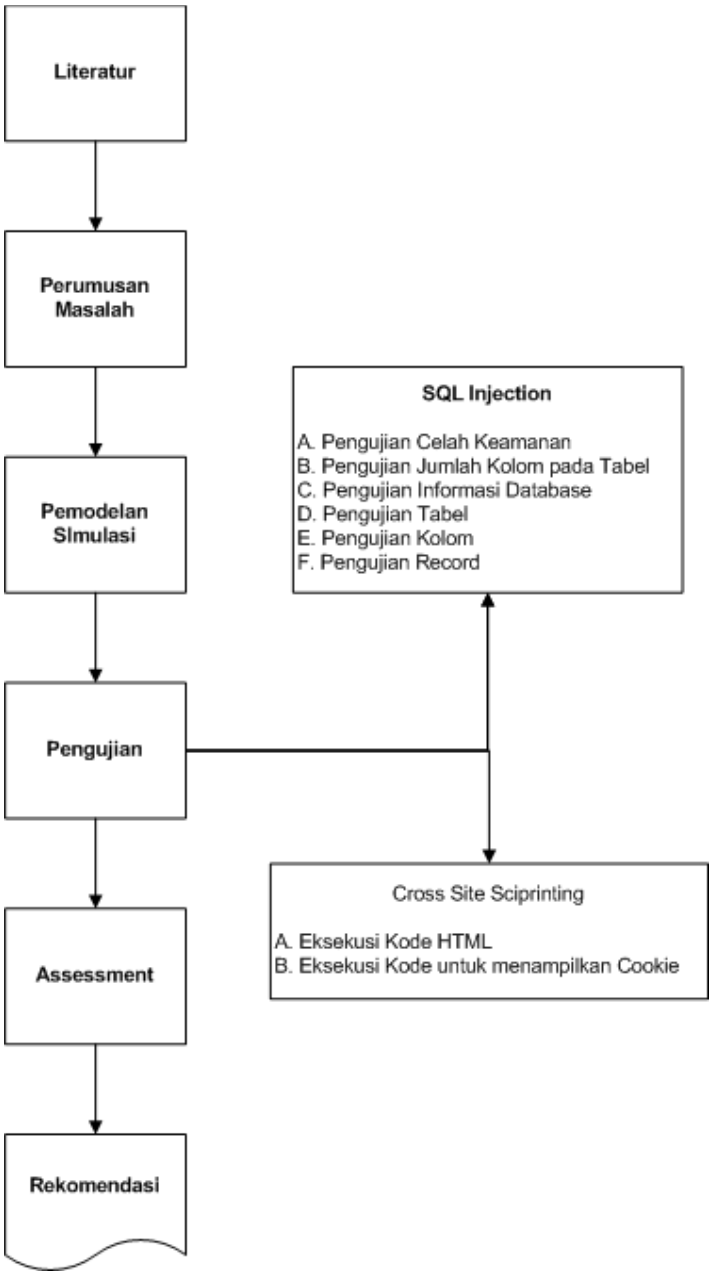
e. Assessment

Pada bagian *assessment*, *attacker* yang terkoneksi dengan internet akan mengakses layanan pada server yaitu sebuah portal informasi, kemudian attacker menginjeksikan kode tertentu pada aplikasi web menggunakan metode *SQL Injection* dan *Cross Site Scripting*.

f. Rekomendasi

Merekomendasikan metode yang dapat mencegah ancaman *SQL Injection* dan *Cross Site Scripting*.

Gambar 1.1 berikut ini merupakan tahapan-tahapan yang dilakukan.



Gambar 1.1 *Tahapan Penelitian*

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang, identifikasi masalah, maksud dan tujuan, batasan masalah, metodologi penelitian dan sistematika penelitian.

BAB II. LANDASAN TEORI

Bab ini berisi teori-teori pendukung yang berhubungan dengan sistem yang akan disimulasikan, seperti Arsitektur Jaringan Komputer, HTTP Respon, Keamanan Komputer, Basis Data, Bahasa Pemrograman, dan Metode yang digunakan.

BAB III. ANALISIS MASALAH

Bab ini berisi deskripsi sistem, analisis kebutuhan dalam pembangunan sistem serta perancangan sistem yang dikembangkan.

BAB IV. PERANCANGAN DAN IMPLEMENTASI

Bab ini berisi implementasi sistem yang dibangun, ujicoba dan hasil pengujian sistem

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang diperoleh dari hasil pengujian sistem, serta saran pengembangan sistem ke depan.