BAB I
PENDAHULUAN

1.1. Latar Belakang

Aplikasi web adalah suatu aplikasi yang diakses menggunakan *browser* web melalui jaringan internet [1]. Jenis-jenis aplikasi web sangat beragam, seperti toko *online* dan *website* informasi yang dalam beberapa tahun terakhir menjadi target serangan *hacker* [2]. Berdasarkan data dari *The Open Web Application Security Project* (OWASP) pada tahun 2013, yang melakukan *survey* mengenai ancaman yang sering terjadi pada aplikasi web diantaranya merupakan ancaman *SQL Injection, Cross-Site Scripting* dan *Unrestricted File Upload* [3].

SQL (Structure Query Language) Injection adalah jenis ancaman yang mengizinkan *query SQL* dapat di-*inject* oleh *client* kemudian diteruskan oleh *server* untuk dieksekusi [4]. Ancaman ini terjadi pada *database* aplikasi web. *Cross-Site Scripting* atau sering dikenal dengan XSS adalah ancaman yang mengizinkan kode (*client side script*) dimasukan ke dalam suatu *website* yang dapat dijalankan pada sisi *client. Unrestricted File Upload* adalah jenis ancaman yang mengizinkan *user* untuk menyisipkan *file*, biasanya *file* yang di-*upload* telah disediakan oleh *attacker* dan digunakan untuk mengeksekusi kode jarak jauh (*Remote Code Execution*) [5].

Keamanan pada aplikasi web kurang mendapat perhatian dari *developer* sehingga menyebabkan serangan di internet dilakukan terhadap sebuah *web*, untuk itu diperlukan pengamanan khusus yakni dengan *Web Application Firewall* [6]. *Web Application Firewall* adalah Suatu metode untuk pengamanan pada aplikasi web, yang berupaya mencegah adanya ancaman dari *attacker* [7]. *Web Application Firewall* dapat bekerja dengan terlebih dahulu melakukan konfigurasi tambahan pada web *server* dan tidak perlu melakukan perubahan pada *script* pembangun aplikasi, sehingga dapat diterapkan pada aplikasi yang sudah berjalan.

Web Application Firewall (WAF) memiliki beberapa fungsi, mulai dari monitoring trafik, *secure directory*, pemfilteran *string* dan proteksi terhadap serangan seperti *SQL Injections*, *Cross-Site Scripting*, dan *Unrestricted File*

Upload. *Web Application Firewall* membentuk lapisan keamanan yang dapat mendeteksi dan mencegah serangan pada aplikasi web. Adapun tindakan yang dapat dilakukan seperti menghentikan *request* dengan status 403 *forbidden* dan juga dapat melakukan *virtual patching.* Dimana *virtual patching* merupakan suatu *rule* yang diterapkan untuk melakukan *patch* tanpa menyentuh aplikasi guna memblokir *request* yang berbahaya [8].

Berdasarkan uraian tersebut, pada pembangunan aplikasi web, segi keamanan kurang mendapat perhatian khusus dari *develeoper*. Dimana bentuk serangan yang sering terjadi berdasarkan data dari OWASP diantaranya *SQL Injection, Cross-Site Scripting,* dan *Unrestricted File Upload* masih menjadi suatu ancaman yang membahayakan pada aplikasi web. Salah satu metode pengamanan yang dapat diterapkan yaitu dengan menggunakan *Web Application Firewall.* Dimana metode tersebut akan diterapkan pada *website* penjualan dan untuk bentuk pengujian pertahanan, akan dicoba disimulasikan teknik serangan yang paling sering terjadi. Dengan sistem pertahanan ini, diharapkan dapat memberikan rekomendasi untuk meningkatkan segi keamanan, sehingga aplikasi web yang dibangun tidak hanya mempunyai desain yang baik namun juga terjaga integritas datanya. Penelitian yang mengambil topik *security* pada aplikasi web ini diberi judul "**SIMULASI KEAMANAN PADA APLIKASI WEB dengan *WEB APPLICATION FIREWALL*".**

1.2. Rumusan Masalah

Berdasarkan latar belakang tersebut, masalah dapat dirumuskan dalam pertanyaan sebagai berikut :

1. Bagaimana menanggulangi ancaman *SQL Injection, Cross-Site Scripting* dan *Unrestricted File Upload.*
2. Bagaimana membangun mekanisme keamanan pada aplikasi web dengan *Web Application Firewall.*

1.3. Maksud dan Tujuan

Maksud dari penulisan tugas akhir ini adalah untuk mensimulasikan sistem keamanan pada *website* penjualan dengan *Web Application Firewall.*

Sedangkan tujuan yang ingin dicapai dalam penelitian ini adalah :

1. Mensimulasikan *Web Application Firewall* pada ancaman *SQL Injection*, *Cross-Site Scripting* dan *Unrestricted File Upload.*
2. Melakukan pengujian terhadap *Web Application Firewall* serta menghasilkan rekomendasi keamanan yang baik pada aplikasi web.

1.4. Batasan Masalah

Adapun batasan masalah yang diterapkan pada penelitian ini adalah sebagai berikut :

1. Jenis ancaman yang disimulasikan pada aplikasi web adalah *SQL Injection*, *Cross-Site Scripting* dan *Unrestricted File Upload.*
2. Simulasi pertahanan dan ancaman dilakukan pada aplikasi berbasis web dengan target sebuah *website e-commerce*.
3. Bentuk *form* dalam metode *SQL Injection* adalah *form login*.
4. Bentuk *form* dalam metode *Cross Site Scripting* adalah *form* hubungi kami.
5. Bentuk *form* dalam metode *Unrestricted File Upload* adalah *form upload*.
6. Aplikasi web yang dibangun menggunakan bahasa pemrograman *PHP* dan DBMS *MySQL* versi 5.
7. Pengamanan aplikasi web dengan metode *Web Application Firewall* menggunakan *ModSecurity 2.7.5 Apache* dan *ModSecurity*-CRS 2.2.5.
8. *Server* menggunakan *Virtual Private Server* (VPS) yang telah terhubung dengan DNS *server* dan internet, sebagai perangkat untuk menjalankan web.
9. Sistem operasi *server* yaitu *Ubuntu 12.04.*

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 memperdalam dan mencermati suatu kasus, baik dalam kedudukannya sebagai kasus individu atau berdiri sendiri, maupun kasus yang saling berhubungan dengan kasus lainnya, baik sebagai penyebab atau sebagai akibat.

c. Pemodelan Simulasi

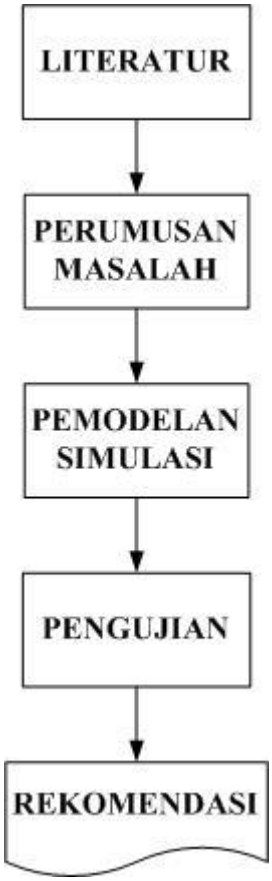
   Pemodelan simulasi merupakan suatu teknik meniru operasi-operasi atau proses-proses yang terjadi dalam suatu sistem dengan bantuan perangkat komputer dan dilandasi oleh beberapa asumsi tertentu sehingga sistem tersebut bisa dipelajari secara ilmiah (Law and Kelton, 1991).

d. Pengujian

   Pada bagian ini, *attacker* akan mengakses layanan pada *server* yaitu sebuah *web*site penjualan (*e-commerce*). *Attacker* akan menginjeksikan kode tertentu pada aplikasi web yang menggunakan *Web Application Firewall* dengan metode ancaman yang sering terjadi yaitu *SQL Injection, Cross-Site Scripting* dan *Unrestricted File Upload* sebagai tolak ukur yang menentukan apakah *Web Application Firewall* dapat meminimalisir ancaman yang sering terjadi pada aplikasi web.

e. Rekomendasi

   Berdasarkan pengujian yang dilakukan disimpulkan bahwa metode *Web Application Firewall* dapat direkomendasikan sebagai metode keamanan terhadap ancaman *SQL Injection, Cross Site Scripting* dan *Unrestricted File Upload.*Gambar 1.1 menunjukan tahap penelitian.



Gambar 1.1 Tahap Penelitian

1.6. Sistematika Penulisan

Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan 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 Jaringan Komputer, Arsitektur Jaringan Komputer, Internet, Situs, HTTP Respon, Keamanan Komputer, Basis Data, Bahasa Pemrograman, dan Metode yang digunakan.

BAB III. ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi deskripsi sistem, analisis kebutuhan dalam pembangunan sistem serta perancangan sistem yang dikembangkan, seperti Analisis Kebutuhan

Perangkat Keras, Analisis Kebutuhan Perangkat Lunak, Analisis Metode Ancaman, dan Analisis Metode Keamanan.

BAB IV. IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini berisi implementasi sistem yang dibangun, ujicoba sistem keamanan pada aplikasi web dengan metode ancaman diantaranya *SQL Injection, Cross Site Scripting,* dan *Unrestricted File Upload* serta hasil dari pengujian sistem.

BAB V. KESIMPULAN DAN SARAN

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