BAB 1
PENDAHULUAN

1.1 Latar Belakang

Layanan internet memudahkan bagi pengguna untuk berbagi layanan bersama dan saling bertemu melalui aplikasi web yang sudah ada pada saat ini. Semua informasi dengan mudah didapatkan dari aplikasi web yang ada. Dengan adanya teknologi informasi saat ini aplikasi web dijadikan sebagai incaran *hacker*. Beberapa ancaman yang sering terjadi pada aplikasi web diantaranya *SQL Injection*, *Cross-Site Scripting* dan *Command Execution*.

SQL (Structure Query Language) Injection adalah teknik yang memanfaatkan kode yang terdapat di dalam program sebuah situs yang lemah tanpa perlindungan yang kuat dari sebuah admin situs tersebut. *Cross-Site Scripting* atau sering dikenal dengan XSS adalah ancaman yang mengizinkan kode (*client side script*) dimasukkan ke dalam suatu *website* yang dapat dijalankan pada sisi *user*. *Command Execution* adalah *bug* yang memungkinkan *attacker* untuk menjalankan perintah – perintah secara *remote* melalui *url*.

Keamanan pada aplikasi *web* kurang mendapatkan perhatian dari *developer* dan akibatnya banyak serangan terhadap *web* melalui internet, maka dari itu dibuat pengamanan khusus yakni *Web Application Firewall* dengan *tools shadow daemon*.

Shadow daemon merupakan sekumpulan *tools* untuk mendeteksi, merekam dan mencegah dari serangan pada aplikasi web. *Application Firewall* bekerja dengan menambahkan konfigurasi pada web server dan tidak melakukan perubahan pada aplikasi web, sehingga dapat berjalan jika sudah diterapkan pada aplikasi.

Web Application Firewall (WAF) berfungsi, mulai dari monitoring trafik, *secure directory*, pemfilteran *string* dan proteksi terhadap serangan pada *SQL Injections*, *Cross-Site Scripting*, dan *Command Execution*. Dengan adanya sistem ini, diharapkan dapat memberikan solusi untuk meningkatkan segi keamanan pada aplikasi web.

Penelitian yang mengambil topik *security* pada aplikasi web ini diberi judul "**IMPLEMENTASI KEAMANAN PADA APLIKASI WEB dengan WEB APPLICATION FIREWALL SHADOW DAEMON**".

1.2 Rumusan Masalah

Banyak sekali yang melakukan serangan informasi seperti ancaman *SQL Injection, Cross-Site Scripting* dan *Commannd Injection*. Maka dari itu dibutuhkan pengamanan pada aplikasi *web application firewall* dengan *tools shadow daemon*.

1.3 Tujuan

Adapun berdasarkan uraian latar belakang dan perumusan masalah diatas, maka adapun tujuan dari proyek akhir ini adalah yaitu:

1. Mengimplementasikan mekanisme keamanan pada aplikasi web *firewall* dengan *tools shadow daemon*.
2. Membangun sistem untuk mencegah *SQL Injection, Cross – Site Scripting,* dan *Command Injection* sesuai kode parameter yang diberikan dalam suatu request.

1.4 Batasan Masalah

Adapun batasan – batasan masalah dalam pengerjaan proyek akhir ini adalah sebagai berikut:

1. Pengamanan aplikasi web dengan *application firewall* menggunakan *shadow daemon.*
2. Penyerang menggunakan virtual sistem operasi ubuntu.
3. Jenis ancaman yang di implementasikan pada aplikasi web adalah *SQL Injection, Cross – Site Scripting* dan *Command Injection*.
4. Menggunakan layanan web pada virtual sistem operasi Ubuntu.