BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era saat ini, *internet* sudah menjadi suatu kebutuhan yang harus terpenuhi untuk mencari atau memperoleh informasi. Segala kemudahan bisa tercapai dengan adanya *internet* pada saat ini. Berdasarkan data dari Kementerian Komunikasi dan Informatika (Kemenkominfo) pengguna *internet* diindonesia pada tahun 2015 adalah 150 juta orang, atau sekitar 61% dari populasi indonesia, ditambah dengan perkembangnya aplikasi *web* yang terhubung dengan basis data seperti *toko online*, *social networks, website sistem informasi penting* dan sebagainya. Hal ini berakibat kuaitas dan implikasi dari serangan dari internet yang beberapa tahun terakhir menjadi target serangan *hacker*. 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 *Cross-Site Scripting (XSS), SQL Injection, Local File Inclusion(LFI),* dan *Remote File Inclusion (RFI).*

Oleh karena itu dengan berkembangnya teknologi *web*, faktor keamanan informasi tentunya menjadi suatu perhatian yang penting seperti dengan memasang *firewall.*Terkait celah keamaman pada aplikasi *web*, biasanya celah tersebut muncul karena adanya *bug* atau kesalahan pemrograman yang lupa untuk diatasi oleh pemrogram. Misalkan lupa untuk mem-*filter* suatu masukan, sehingga jika memasukkan karakter-karakter berbahaya seperti tanda petik(‘) akan mengakibatkan kesalahan dan munculnya sebuah *error* pada halaman *web* dan biasanya hal tersebut dimanfaatkan oleh peretas untuk mencoba mendapatkan informasi dari *error*. Untuk itu diperlukan pengamanan dan pendeteksian dari segala bentuk usaha percobaan serangan terhadap aplikasi berbasis *web* dengan cara melakukan pencocokan terhadap *rule* atau polapola serangan. *Rule* atau pola-pola serangan tersebut dicocokkan dengan data *request HTTP*.

Berdasarkan kasus tersebut maka akan dilakukan pengamanan dan pendeteksian pada aplikasi *web* dengan Metode pengamanan yang akan di terapkan yaitu menggunakan *Web Application Firewall* dan *Modsecurity*. *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 *Remote File Inclusion. Web Application Firewall Modsecurity* nantinya akan berjalan pada sebuah sistem operasi

linux ubuntu 12.04, sistem operasi tersebut akan disimolasikan pada mesin vritual yaitu virtualbox. Sedangan *Modsecurity* seperti *firewall* pada umumnya memiliki tugas untuk melakukan pemfilteran pada data yang masuk maupun keluar, dan melakukan blocking traffic yang dianggap berbahaya sesuai dengan rule yang ditetapkan. Setelah itu segala bentuk serangan yang telah terdeteksi akan disimpan pada suatu database.

Aplikasi *web* yang akan diuji yaitu sampel data dari *website* pentesterlab.com nantinya akan diuji tingkat keamanan terhadap serangan seperti *SQL Injections*, *Cross-Site Scripting*, dan *Remote File Inclusion* pada apliasi *web* tersebut, dengan menggunakan metode pengamanan dan pendeteksian serangan dengan metode *Web Application Firewall* dan *Modsecurity*. Dengan adanya kedua pengamanan tersebut makan dapat dilakukan analisa tingkat dan keakuratan keamanan aplikasi *web*d engan menggunakan dua metode tesebut khususnya serangan-serangan *SQL Injections, Cross-Site Scripting* dan *Remote File Inclusion.*

Berkaitan dengan hal tersebut, melalui penelitian ini Hasil yang diharapkan nantinya adalah serangan-serangan seperti *SQLInjection, Cross Site Scripting (XSS), Local File Inclusion(LFI)* dan *Remote File Inclusion (RFI)* yang dapat membahayakan kerahasiaan, integritas dan ketersediaan yang diberikan oleh *web* tersebut dapat sedikit lebih aman.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang yang diuraikan diatas, maka merumuskan beberapa masalah yang akan dibahas sebagai berikut:

1. Bagaimana membangun mekanisme pengamanan pada aplikasi *web* dengan metode *Web Application Firewall* dan Modsecurity?
2. Bagaiaman menguji aplikasi web dengan serangan *SQL Injections*, *Cross-Site Scripting* dan *Remote File Inclusion*?
3. Bagaiman menganalisa mekanisme metode pengamanan *Web Application Firewall* dan Modsecurity?

1.3 Batasan Masalah

Agar tidak menyimpang jauh dari permasalahan, maka penelitian ini mempunyai batasan masalah sebagai berikut:

1. Uji coba serangan pada Aplikasi *web* menggunakan:
    a. Cross-Site Scripting

b. *SQL Injections*
c. *Remote File Inclusion*

2. Metode pengamanan menggunakan *Web Application Firewall* dan *Modsecurity* untuk mendeteksi serangan serangan tersebut
3. Pengecekan hanya dibatasi pada *request,* tidak sampai pada pengecekan konten dari suatu berkas.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah:

1. Membangun mekanisme pengamanan pada aplikasi *web* dengan metode *WebApplication Firewall* dan Modsecurity
2. Menguji aplikasi web dengan deteksi serangan *SQL Injections, Cross-SiteScripting* dan *Remote File Inclusion*
3. Menganalisa mekanisme metode pengamanan *Web Application Firewall* dan Modsecurity

1.4 Manfaat Penelitian

Manfaat yang diharapkan dari hasil penelitian ini adalah mengamankan aplikasi *web* dari serangan-serangan yang tidak bertanggung jawab sehingga kerahasiaan, integritas dan ketersediaan data dan layanan *web* tetap terjaga dan menutupi celah keamanan pada aplikasi *web*. Selain itu juga dapat memudahkan *admin* dalam melakukan pemantauan terhadap serangan dengan adanya *web monitoring* serangan terhadap aplikasi aplikasi *web.*