BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi world wide web (www) pada era sekarang ini sudah sangat berkembang dengan pesat, sehingga memunculkan media baru diberbagai aspek dalam penyebaran informasi dan peningkatan komunikasi dimasyarakat seluruh dunia. Berbagai aktivitas yang sebelumnya dinilai tidak mungkin dapat dilaksanakan sekarang telah menjadi bagian dari masyarakat teknologi terkini. Tukar menukar surat elektronik (email) dan juga keberadaan dari halaman web adalah bentuk komunikasi yang membawa perubahan besar pada kehidupan manusia. Dengan adanya teknologi web, sepertinya dunia menjadi tanpa batas dengan potensi pengembangan yang tidak ada batasannya. (Krisna, 2012).

Fungsi-fungsi web secara umum adalah sebagai berikut (Sarwosri, 2009) :

1. Fungsi Komunikasi
2. Fungsi Informasi
3. Fungsi Hiburan

4. Fungsi Transaksi

Dari penjelasan fungsi-fungsi web diatas maka keamanan web harus dijaga dengan benar untuk memperlancar komunikasi, menjaga keamanan dan kerahasiaan informasi serta kenyamanan dan keamanan dalam bertransaksi melalui media website. Sehingga dengan begitu akan tercapai fungsi-fungsi dari sebuah website.

Kejahatan di dunia teknologi dan informasi terutama pada aplikasi web semakin marak terjadi. Salah satu faktor yang menyebabkan kurangnya tingkat keamanan pada aplikasi web adalah kesalahan penulisan kode program. Kesalahan penulisan kode program dalam pembuatan aplikasi web adalah hal yang sering dimanfaatkan oleh para penyerang, hal ini mengakibatkan rata-rata aplikasi web bisa diserang dengan memanfaatkan kesalahan ini. Kelemahan-kelemahan yang sering dimanfaatkan oleh para penyerang diantaranya adalah kelemahan terhadap SQL Injection, XSS, Remote File Inclusion, dan Username Enumeration. (Chandrika,dkk. 2012).

Programmer juga merupakan manusia yang tidak akan luput dari salah, sehingga seperti pemaparan diatas bahwa salah

satu faktor penyebab kurangnya tingkat keamanan web adalah kesalahan dalam penulisan kode program. Dari situ penulis berkeinginan untuk membantu meningkatakan keamanan web dengan cara membuat sebuah aplikasi yang berfungsi untuk mengamankan web terhadap serangan-serangan dari pihak-pihak yang tidak bertanggung jawab.

1.2 Rumusan Masalah

Berdasarakan latar belakang seperti yang telah diuraikan diatas, maka dapat dirumuskan suatu permasalahan yaitu bagaimana membuat modul yang dapat mengamankan web aplikasi dari serangan-serangan yang dapat membahayakan web tersebut.

1.3 Ruang Lingkup

Dalam pembuatan modul ini, terdapat beberapa batasan masalah yang digunakan, sebagi berikut :

1. Modul dibuat menggunakan *PHP* dan hanya bisa diterapkan pada web yang berbasis *PHP* dan menggunakan database *MySQL*.
2. Modul dapat mengfilter serangan *SQL Injection, Cross Site Scripting, Comman Execution, Upload File* dan *File Inclution.*

3. Modul dapat menghindari serangan *Brute Forcing*.
4. Pengamanan dilakukan dengan cara *encoding*, pengenalan *string* dan juga pengenalan pola serangan.
5. Data string pengenal atau sample bersifat dinamik, dimana data bisa ditambah maupun dikurangi sesuai kebutuhan.
6. Modul dapat membuat *log history* serangan-serangan yang telah terjadi.
7. Dari yang log yang telah ada akan dibuat *chart history* serangan.

1.4 Tujuan

Tujuan penelitian ini adalah untuk membuat modul pegaman web dari serangan *brute forcing, SQL Injection, Cross Site Scritping, Command Execution, File Inclution, dan Arbitrary File Upload*.