BAB 1

PENDAHULUAN

1.1. Latar Belakang

Keamanan web merupakan proses mengamankan aplikasi web dari kerentanan yang memungkinkan pihak yang tidak berwenang dapat mengakses dan memodifikasi data-data dari *website* yang tersimpan secara *online*. Adanya kerentanan dalam *website* dapat meningkatkan ancaman tersendiri, hal ini memungkinkan penyerang dapat melakukan eksploitasi terhadap sistem.

Tujuan keamanan aplikasi adalah kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan informasi (*availability*). Ketiga konsep ini membentuk apa yang sering disebut sebagai *Triad CIA*. Ketiga konsep tersebut mewujudkan tujuan keamanan mendasar baik untuk data maupun informasi dan layanan komputasi (William Stallings, 2011). Berdasarkan data laporan kerentanan aplikasi web dari Acunetix tahun 2016, dari 55% aplikasi web setidaknya memiliki 1 kerentanan tingkat tinggi, 84% memiliki 1 kerentanan tingkat sedang dan dalam 12 bulan kerentanan tingkat tinggi naik 9% dari 46% di tahun 2015.

Gamatechno Web Application Framework merupakan *framework* PHP yang dikembangkan oleh PT Gamatechno Indonesia. Sudah banyak klien yang menggunakan aplikasi GTFW dari bidang akademik, pemerintahan maupun korporasi.

Solusi yang baik untuk menghindari eksploitasi *website* berbasis GTFW yaitu melakukan analisa celah keamanan dan melakukan pengujian dengan *OWASP Testing*, yang bertujuan untuk menemukan kerentanan aplikasi web berbasis GTFW dan mencari solusi yang tepat untuk menutup kerentanan tersebut.

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas, maka dalam pengerjaan skripsi ini dirumuskan rumusan masalah tentang bagaimana menerapkan kewanaman OWASP untuk pengujian aplikasi berbasis GTFW.

1.3. Ruang Lingkup

Berdasarkan identifikasi masalah yang ada maka dibuat ruang lingkup sebagai berikut.

1. *Web server* yang digunakan Apache HTTP Server.
2. Menggunakan GTFW (*Gamatechno Web Application Framework*) v3.7.
3. Pengujian kerentanan pada *Session Management* dan *Input Validation*.
4. Pengujian *Input Validation* meliputi *HTTP Verb Tampering*, *OS Command Injection*, *Stored Cross Site Scripting*.
5. Standar OWASP versi 4.
6. Pengujian sistem menggunakan metode *Grey Box*.

1.4. Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari skripsi adalah menguji dan mengamankan aplikasi berbasis GTFW dari kerentanan *Session Management* dan *Input Validation* berdasarkan OWASP.

1.5. Manfaat Penelitian

Penelitian diharapkan dapat menjadi bahan referensi untuk meningkatkan keamanan aplikasi berbasis GTFW.

1.6. Sistematika Penulisan

Secara garis besar sistematika penulisan pada skripsi yang dibuat adalah sebagai berikut.

1. Bagian awal skripsi terdiri dari halaman judul, halaman pengesahan, halaman moto, halaman persembahan, intisari, kata pengantar, daftar isi, daftar gambar, daftar tabel dan daftar lampiran.
2. Bagian isi skripsi terdiri dari lima bab yaitu.

BAB I : Pendahuluan, menguraikan tentang latar belakang, permasalahan, tujuan, manfaat penelitian, penegasan istilah dan sistematika skripsi.

BAB II : Landasan teori yaitu bab yang menguraikan tentang kajian pustaka baik dari buku-buku ilmiah, maupun sumber-sumber lain yang mendukung penelitian ini.

BAB III : Metodologi penelitian yaitu bab yang menguraikan tentang objek penelitian, metode penelitian, kebutuhan *input*, kebutuhan *output*, rancangan *server*, rancangan aplikasi..

BAB IV : Implementasi dan pembahasan yaitu bab yang menguraikan tentang pengujian kerentanan, analisa dan pencegahannya.

BAB V : Kesimpulan dan saran yaitu bab yang berisi kesimpulan dan serta hasil penelitian.

3. Bagian akhir skripsi : Terdiri dari daftar pustaka dan lampiran.