BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring semakin berkembangnya teknologi sistem informasi dikalangan masyarakat, berkembang pula sistem informasi yang dapat memudahkan masyarakat untuk mengakses dan mencari informasi melalui *internet.* Saat ini, banyak bermunculan aplikasi-aplikasi baik dalam bentuk *web* ataupun *mobile* yang memudahkan untuk kehidupan sehari-hari, untuk itu banyak pengembang aplikasi membuat berbagai macam aplikasi. Namun sistem informasi harus lah terjaga dengan aman supaya dapat terlindungi dari serangan atau kebocoran informasi yang sensitif seperti biodata pengguna/masyarakat yang menggunakan aplikasi dalam kehidupan sehari harinya.

Direktorat Keamanan Informasi dan Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika pada tahun 2011 telah mengeluarkan panduan tentang keamanan *web server* yang bertujuan merekomendasikan aspek keamanan untuk perancangan, implementasi, dan pengoperasian *web server* yang dapat diakses secara publik. Pedoman ini direkomendasikan bagi departemen dan lembaga pemerintah, namun dapat juga digunakan di sektor swasta dan organisasi dalam meningkatkan keamanan sistem *web server* untuk mengurangi jumlah dan frekuensi insiden keamanan yang terkait dengan *web*.

Ditambah dengan adanya peraturan-peraturan baru dari pemerintah yang mewajibkan setiap aplikasi untuk dilakukan uji *penetrasi* sebagai bentuk dari

perlindungan terhadap pengguna. hal ini membuat *developer* atau pengembang aplikasi untuk memasukkan aspek *security* menjadi satu hal yang penting sebelum aplikasi dipergunakan oleh publik.

Penetrasi testing adalah salah satu langkah baik untuk melakukan uji keamanan terhadap sistem informasi di suatu instansi/lembaga yang menyimpan suatu informasi di bidangnya. Seperti lembaga XYZ, merupakan organisasi yang bergerak di bidang pendidikan dan menggunakan *website* sebagai portal untuk melakukan pendaftaran *online* untuk penerimaan siswa baru. Dimana didalam *website* tersebut adalah sebuah sistem informasi lembaga XYZ itu sendiri yang berisikan *database user*/siswa, *administrator*, serta informasi lainya. Dalam pengelolaanya *website* tersebut hanya menggunakan fitur *default* yang kemungkinan masih terdapat celah keamanan.

Oleh sebab itu, penulis melakukan pengujian kepada *website* XYZ *yang* merupakan situs terbuka yang dapat diakses oleh siapa saja untuk mengetahui kemungkinan adanya celah keamanan agar terhindar dari *cyber attacker* dikemudian hari. Berdasarkan permasalahan di atas untuk menjaga keamanan *website* XYZ, jika menemukan celah keamanan pada *website* dapat melaporkannya kepada pihak admin *website* tersebut untuk dilakukan perbaikan.

Berdasarkan uraian latar belakang diatas maka penulis bermaksud untuk melakukan penelitian dengan judul " **PENETRATION TESTING WEBSITE MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP)**".

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan, maka dapat diidentifikasi beberapa masalah untuk pengujian *penetration testing* pada *website* XYZ adalah sebagai berikut.

1. Belum adanya upaya pengujian untuk mengetahui kerentanan pada *website* untuk meningkatkan keamanan sistem.
2. Belum adanya *web server* yang dapat membangun suatu *website* dengan sistem keamanan yang *secure* terhadap serangan *attacker*.
3. Belum adanya *file report* apabila ditemukan celah keamanan sehingga tidak ada catatan perbaikan yang sudah dilakukan sebelumnya.

1.3 Rumusan Masalah

Berdasarkan identifikasi masalah di atas dapat dirumuskan suatu masalah yang relevan adalah.

1. Bagaimana cara menganalisa kerentanan keamanan pada *website* XYZ ?
2. Bagaimana cara menemukan kelemahan pada *web server* sehingga dapat meningkatkan keamanan dan kenyamanan pada layanan *website* XYZ ?
3. Bagaimana cara memberikan rekomendasi perbaikan pada *website* XYZ ?

1.4 Batasan Masalah

1. Melakukan pengujian *penetration testing* pada *website* XYZ sebagai studi kasus menggunakan *tools owasp* sebagai alat uji dalam melakukan *security assessment*
2. Mengetahui struktur sistem informasi yang berada di *web server website* XYZ
3. Menginformasikan dan menampilkan hasil uji *penetration* dalam bentuk *file report* yang berisi catatan rekomendasi perbaikan

1.5 Tujuan dan manfaat

1.5.1 Tujuan penelitian

1. Meningkatkan sistem keamanan *internal* dan *external* pada *website* XYZ untuk mengurangi tingkat resiko ancaman serangan *attacker*.
2. Meningkatkan keamanan yang lebih *secure* pada *web server* dengan pengujian *penetration testing*.
3. Memberikan *file report* hasil *penetration testing* ke *administrator* untuk memperbaiki *website* dari celah keamanan.

1.5.2 Manfaat penelitian

1. Meningkatkan keamanan *web server* pada *website* XYZ.
2. Dapat mengetahui celah keamanan, sehingga dapat segera memperbaiki celah keamanan tersebut.

1.6 Metode Penelitian

Dalam penulisan tugas akhir yang berjudul *"* **Penetration Testing Website Menggunakan Open Web Application Security Project (OWASP)**" ini, penulis menggunakan metode *Blackbox,* dengan tahapan sebagai berikut :

1. Studi Pustaka, dilakukan dengan mengambil beberapa jurnal penelitian yang memiliki tema serupa untuk mendapatkan landasan informasi sebagai bahan acuan dalam melakukan perencanaan, percobaan, pembuatan dan penyusunan tugas akhir
2. Pengujian yang dilakukan dengan mengumpulkan informasi terkait sistem operasi, layanan, jaringan, dll yang dipergunakan oleh *website*, mengidentifikasi kelemahan pada *website*, melakukan eksploitasi terhadap *website*, membuat *report* hasil *penetration testing* sehingga dapat melakukan perbaikan terhadap *website*.
3. Analisis, melakukan identifikasi *vulnerability* menggunakan *tools* untuk memperoleh data dari perangkat lunak yang berkerja pada sistem sehingga dapat diketahui informasi sesuai yang diinginkan. Selain itu analisis digunakan untuk mengetahui tingkat keamanan pada *website* XYZ.

1.7 Sistematika Penulisan

Penyusunan laporan skripsi ini, dilaksanakan dengan beberapa metode dan format susunan yang terbagi ke dalam beberapa bab, yang terdiri dari:

BAB I PENDAHULUAN

Bab ini berisikan tentang penguraian mengenai perkembangan teknologi serta latar belakang, maksud dan tujuan, mafaaat, identifikasi masalah, batasan masalah, rumusan masalah, metodologi penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisikan tentang teori–teori yang terkait dengan topik penelitian, meliputi hal-hal yang berhubungan dengan sistem, informasi, dan sistem informasi, komponen-komponen desain informasi, manajemen *database* serta peralatan pendukung (*tools system*).

BAB III METODE PENELITIAN

Bab ini berisikan mengenai identifikasi dan analisa kebutuhan terhadap data dan aplikasi, metode penelitian dan pengembangan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisikan langkah langkah proses pengujian yang dilakukan dan hasil yang diperoleh dari proses pengujian yang dilakukan pada beberapa target yang sudah ditentukan.

BAB V PENUTUP

Di akhir bab ini berisi mengenai kesimpulan penelitian serta saran yang berhubungan dengan penyusunan skripsi.