BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan merupakan bagian yang paling utama bagi kalangan developers untuk meningkatkan data dalam internet. Setiap perusahaan maupun organisasi harus selalu melindungi kerahasiaan, integritas, ketersedian data pada suatu *web server* yang mengacu pada standar keamanan nasional. Hal ini karena system jaringan telah mengalami perkembangan, sehingga membutuhkan peningkatan keamanan secara keseluruhan. Potensi adanya hackers atau attackers untuk mengganggu fungsi *system* dan hilangnya data akan semakin meningkat dengan kemungkinan kelemahan system. Berdasarkan data yang telah diperoleh untuk kerusakan *system* di setiap negara menjadi acuan agar waspada pada kelemahan *system* tersebut [1]. Serangan yang dilakukan biasanya menargetkan bagian sintaks dari aplikasi web [15].

Beberapa peneliti yang telah menerapkan pengujian keamanan *web server* menggunakan metode OWASP serta juga menggunakan tools Nessus. Tools Nessus digunakan selain dalam proses pentest juga untuk melihat kerentanan dalam jaringan. Selain itu juga terdapat metode lain seperti menggunakan metode penetration testing [2]. Dalam penelitian penulis menggunakan tools Nessus sebagai pengecekan kerentanan secara menyeluruh dan untuk OWASP Top 10 sebagai acuan panduan untuk meningkatkan keamanan dalam suatu perangkat yang dimana terdapat 10 celah keamanan paling berbahaya. Nmap, whois, dig, dan nslookup adalah tools lain yang penulis gunakan dalam penelitiannya yaitu Acunetic dan Nessus [2].

Penelitian telah dilakukan tentang penggunaan OWASP untuk menilai keamanan system, dan berbagai penelitian telah memaparkan bahwa metode dan alat memiliki dampak yang sangat besar terhadap hasil pengujian yang telah dijalankan [11]. OWASP adalah kerangka kerja terstruktur yang menyediakan langkah-langkah untuk mengelompokkan informasi dalam rencana uji keamanan, penilaian, serta pembuatan laporan domain yang telah diverifikasi dan dianalisis [7]. Sistem informasi akademik ini dirancang sebagaimana bertujuan memberikan

askses terhadap mahasiswa, dosen dan karyawan. *Hacking system*, perubahan file index, deface web dari file yang disisipkan dari backdoor di sistem, penyalahgunaan data sehingga seseorang dapat dengan mudah menyerang situs web secara terus menerus, memperlambat sistem akademik saat digunakan, hanyalah beberapa masalah yang sering muncul di server web. Namun, sistem informasi akademik di perguruan tinggi memiliki kelemahan keamanan yang bisa disalahgunakan oleh pihak tidak bertanggung jawab untuk melakukan tindakan peretasan [16]. Oleh sebab itu sangat perlu untuk mempertimbangkan bagaimana agar keamanan sistem infomasi akademik dan seluruh data dan infomasi yang termasuk didalamnya tetap terjaga.

Cara terbaik untuk menentukan tingkat keamanan informasi organisasi dan bagaimana mempertahankannya dari serangan adalah dengan menggunakan teknik pengujian penetresi, yang memungkinkan untuk menganalisis keamanan secara lebih efektif dan menemukan kerentanan baru, seperti yang telah dilakukan dalam penelitian, melindungi server web dari serangan oleh orang yang ceroboh [3].

Penetration testing adalah langkah utama dalam mengembangkan sistem pertahanan komputer berbasis server yang aman dari hacker atau peretas. Ini adalah tindakan hukum yang diambil yang membedakan penguji penetrasi dari penyerang [4]. Dalam *Penetration testing* digunakan untuk evaluasi keamanan terhadap sistem komputer atau server jaringan dengan mengidentifikasi kerentanan yang ada [3]. Pengujian penetrasi atau pentesting untuk menilai pertahanan jaringan komputer atau server web untuk mengeksekusi semua serangan dan kerentanan yang ada [3].

Berdasarkan penelitian sebelumnya sudah banyak melakukan metode yang berhubungan dengan pengujian penetrasi. Penelitian ini menghasilkan model kerentanan sebagai hasil penilaian yang dapat digunakan untuk meningkatkan keamanan akses website yang mempengaruhi kinerja layanan [12]. Tujuan dari penelitian ini adalah menggunakan metode penetration testing untuk menemukan kelemahan web akademik kampus untuk kemudian dijadikan bahan evaluasi oleh pihak terkait [6].

1.2 Rumusan Masalah

Berdasarkan pembahasan dari latar belakang yang diterangkan sebelumnya, perumusan masalah yang diperoleh adalah sebagai berikut :

a). Bagaiamana melakukan sebuah analisis pada website Simanta dengan menggunakan standart OWASP Top 10 ?

b). Bagaimana menganalisa hasil report dari metode Penetration Testing dengan memberikan informasi kepada developer untuk meningkatkan segi keamanan website ?

1.3 Tujuan Penelitian

Berdasarkan terhadap masalah yang sudah dijabarkan dalam rumusan permasalahan diatas, maka penelitian ini mempunyai tujuan sebagai berikut :

a). Memberikan informasi terhadap pihak institusi terkait web akademik agar lebih meningkatkan segi keamanan agar tidak terjadinya kebocoran data.

b). Diharapkan dapat menambah pengetahuan mahasiswa tentang pengujian web akademik.

1.4 Batasan Masalah

Batasan masalah harus ditetapkan supaya penelitian yang sedang berjalan tidak keluar dari topik pembahasan, maka cakupan masalah atau batasan masalah penelitian ini ialah sebagai berikut :

a). OWASP Top 10 dipilih berdasarkan 10 tingkatan keamanan tertinggi dalam menguji web akademik.

b). Penelitian ini hanya melakukan sebuah evaluasi celah keamanan yang dimana tertuju pada web simanta menggunakan metode penetration testing.

c). Website yang diujikan antara lain menggunakan website simanta umm.