BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi, Internet sudah menjadi kebutuhan bagi setiap pengguna *digital hardware* saat ini. Hampir semua aktivitas yang dilakukan sehari-hari membutuhkan internet sebagai penunjang keperluannya. seperti halnya komunikasi, mencari informasi, transaksi digital, dan bahkan hiburan pun saat ini marak dengan penggunaan internet. semakin maraknya penggunaan internet dikalangan masyarakat luas, semakin bertambahnya peluang kejahatan siber. seperti halnya kebocoran data yang berisikan informasi dari suatu website oleh oknum tak bertanggung jawab yang dapat merugikan banyak pihak. Kebocoran data atau perusakan dapat mengancam setiap saat seiring dengan meningkatnya sumber daya manusia. Berdasarkan Pasal 26 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang mengatur bahwa penggunaan data pribadi harus dilakukan dengan sepersetujuan orang yang bersangkutan, dan bahwa setiap orang yang dilanggar haknya dapat mengajukan gugatan. Perlu dilakukannya pengujian celah atau biasa disebut uji penetrasi keamanan terhadap *website* guna meminimalisir penjahat siber dapat menembus sistem keamanan yang sudah ada. Dengan adanya pengujian celah keamanan tersebut dapat menjadi sebuah solusi yang digunakan sebagai tolak ukur untuk memperbaiki sistem keamanan *website* selanjutnya.

Ada beberapa metode yang dapat digunakan untuk menjadi landasan uji penetrasi. Salah satu nya adalah *Open Web Application Security Project* (OWASP). *Open Web Application Security Project* (OWASP) adalah komunitas terbuka yang bertujuan untuk memungkinkan organisasi mengembangkan, membeli, dan memelihara aplikasi tepercaya. OWASP adalah jenis organisasi baru. OWASP mendukung penggunaan komersial teknologi keamanan, tetapi tidak berafiliasi dengan perusahaan teknologi. (OWASP, 2010) OWASP secara konsisten melindungi data terpenting yang dikumpulkan hingga saat ini terhadap standar keamanan aplikasi. (OWASP, 2010). Tujuan utama OWASP TOP 10 adalah untuk mendidik pengembang, desainer, arsitek, manajer, dan organisasi tentang konsekuensi kesalahan keamanan di

aplikasi web yang paling umum dan penting. OWASP TOP 10 memberikan teknik dasar untuk melindungi dari area masalah berisiko tinggi ini dan memberikan saran tentang cara melanjutkan dari sana. (OWASP, 2017).

Studi Kasus yang akan menjadi objek penelitian ini yaitu *Website* Sistem Informasi Manajemen (SIM) xxx. SIM merupakan sistem yang digunakan sebagai pemantauan suatu sistem lainnya, yang dimana pemantauan tersebut difungsikan untuk melihat sebuah kegiatan yang bersifat keamanan. Sebuah *server* tidak dapat memantau dirinya sendiri sehingga diperlukan suatu sistem yang dapat memonitoring kegiatan yang ada pada *server*. *Server management and monitoring* diperlukan agar *admin* dapat memantau dengan mudah apa saja yang terjadi pada *server*. Untuk itu SIM dapat dipertimbangkan sebagai suatu sistem informasi yang cukup penting untuk dilakukannya pengamanan yang kuat, guna meminimalisir hal-hal yang tidak diinginkan seperti pencurian data, penyalaah gunaan data, dan bahkan pengambil alihan sistem oleh pihak attacker. Untuk mencari tahu kekurangan apa saja yang dimiliki website SIM xxx tersebut, pada penelitian ini akan dilakukan uji penetrasi berdasarkan standar keamanan yang ada pada OWASP TOP 10.

Hasil dari penelitian ini adalah untuk menemukan celah keamanan yang terdapat pada *website* Sistem Informasi Manajemen (SIM) xxx yang akan digunakan sebagai landasan atau rujukan untuk perbaikan sistem keamanan guna meminimalisir celah untuk masuk ke *website* SIM xxx selanjutnya.

1.2 Rumusan Masalah

Berdasarkan penjabaran pada latar belakang, permasalahan yang akan dibahas adalah:

1. Apakah *website* Sistem Informasi Manajemen (SIM) xxx memiliki celah keamanan?
2. Bagaimana cara menguji keamanan aplikasi Sistem Informasi Manajemen (SIM) dengan teknik *Penetration Testing* Dan Metode OWASP ?
3. Jenis *Vulnerability* apa saja yang ada pada Sistem Informasi Manajemen (SIM) xxx berdasarkan metode OWASP TOP 10?

1.3 Tujuan dan Manfaat

Adanya penelitian ini bertujuan untuk mengetahui apakah Sistem Informasi Manajemen (SIM) xxx telah menerapkan standar keamanan dan apakah terdapat celah keamanan pada suatu *website* yang berisikan data pengguna yang bersifat rahasia

1.4 Manfaat Penelitian

Manfaat yang dapat diambil dari penelitian ini, sebagai berikut:

a. Untuk Pihak Instansi pemilik *website*
   Membantu menemukan celah keamanan pada *website* Sistem Informasi Manajemen (SIM) xxx.
b. Untuk Penulis
   Meningkatkan kemampuan dan wawasan dalam bidang Hacking terutama mengenai uji penetrasi menggunakan metode OWASP *TOP* 10 2017.
c. Untuk masyarakat umum
   Mengetahui standar keamanan (standar keamanan sistem informasi) pada aplikasi web

1.5 Batasan Masalah

a. Pada objek penelitian ini peneliti menggunakan *website* Sistem Informasi Manajemen (SIM) xxx. Dikarenakan mencegah terjadinya kebocoran informasi celah keamanan *website*. Pada saat publikasi tugas akhir dalam bentuk jurnal, nama *website* objek penelitian ini akan diganti menjadi *website* SIM xxx.

b. Penelitian yang dilakukan menggunakan metode Grey-Box dikarenakan meskipun mendapatkan izin akses terhadap website SIM dari pihak TIM IT, penguji tidak diberikan hak akses langsung terhadap website SIM tersebut .

b. Pada penelitian ini peneliti hanya menjelaskan hasil temuan uji celah keamanan *website* dalam bentuk laporan. Tidak adanya pembenaran keamanan pada *website* yang dijadikan objek penelitian tersebut.

1.6 Luaran yang Diharapkan

Luaran yang diharapkan adalah untuk melakukan Penerapan Standar Keamanan dari Sistem Informasi, dan mengetahui beberapa celah keamanan pada aplikasi SIM xxx.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan pada penelitian ini disusun dalam lima bab yang dibagi menjadi beberapa sub-bab di dalamnya, dan daftar pustaka yang disusun sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini berisi Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Ruang Lingkup, Luaran yang Diharapkan, dan Sistematika Penulisan pada penelitian ini.

BAB 2 LANDASAN TEORI

Bab ini menjelaskan logika yang digunakan dalam investigasi, termasuk keamanan informasi, keamanan web, kerentanan keamanan, mengidentifikasi jenis serangan aplikasi web, metode pengujian penetrasi, dan investigasi. Dalam tugas akhir ini, saya menggunakan penelitian sebelumnya sebagai referensi

BAB 3 METODOLOGI PENELITIAN

Bab ini membahas metode penelitian beserta urutan tahapan yang dilakukan dalam proses penelitian ini.

BAB 4 HASIL DAN PEMBAHASAN

Bab ini menjelaskan bagaimana hasil penerapan metode OWASP *TOP* 10 2017 teknik *penetration testing* pada *website* Sistem Informasi Manajemen (SIM) xxx .

BAB 5 PENUTUP

Bab ini berisi kesimpulan dan saran dari hasil penelitian sebagai acuan pada penelitian berikutnya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN