BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam pembuatan suatu produk, tentu banyak melalui berbagai prosedur atau proses agar menghasilkan produk yang baik serta sesuai yang direncanakan [1], sama halnya dengan produk teknologi informasi, yang biasa disebut aplikasi. Salah satu proses yang dilalui dalam pembuatan aplikasi yaitu *testing* atau pengujian [2], salah satu pengujian aplikasi dengan cara mencari kerentanan keamanannya, apakah aplikasi telah aman dari suatu ancaman atau serangan dari luar yang tidak bertanggung jawab sehingga dapat merugikan dan mengganggu ekosistem yang telah dibuat pada aplikasi tersebut [3]. Oleh karena itu penulis membuat penelitian ini sebagai referensi ketika membangun atau membentuk suatu aplikasi teknologi informasi yang bertujuan menganalisa kerentanan keamanannya menggunakan suatu kerangka pengujian penetrasi yaitu ISSAF (*Information Systems Security Assessment Framework*).

ISSAF adalah kerangka kerja yang terstruktur dengan mengkategorikan penilaian keamanan sistem informasi dalam berbagai domain serta rincian kriteria evaluasi atau pengujian khusus untuk masing-masing domainnya [4]. Penulis menggunakan ISSAF dikarenakan salah satu satu metode pengujian penetrasi yang bersifat *open source* dan salah satu pengujian penetrasi populer [5] yang memiliki keunggulan pada hubungan bagian teknis dan manajerial yang terpisah sehingga publik dapat memahami bagian manajemen dan bagian teknis. Pada bagian manajerial salah satunya untuk manajer dalam merencanakan dan memahami atau menghindari masalah (seperti masalah hukum) dan pada bagian teknis pun memiliki beberapa rincian seperti urutan *task* yang jelas, memberikan kerangka kerja yang disiplin dan hal teknis lainnya [6].

Semakin meningakatnya kecanggihan dalam kejahatan dunia maya dan peningkatan pengguna internet maka peretasan juga akan berkembang [7] dan terjadi pada berbagai industri seperti energi organisasi, keuangan & asuransi dan industri lainnya [8]; salah satu platform favorit untuk peretasan pada website [9]

maka perusahaan perlu melakukan pendekatan dalam pengujian kerentanan keamanan siber (*penetration testing*) pada aplikasi untuk memastikan bahwa aplikasi tersebut tetap mengikuti perkembangan teknologi serta mendapatkan keamanan yang kuat sehingga dapat mengurangi serangan yang merugikan bahkan untuk memperbaiki sistem pada aplikasi tersebut [10]. Dengan menerapkan kerangka pengujian penetrasi ISSAF diharapkan dapat mengatasi permasalahan tersebut sehingga penulis menyusun suatu penelitian dengan judul analisis kerentanan keamanan aplikasi manajemen asset berbasis web menggunakan metode ISSAF (*Information System Security Assestment Framework)* studi kasus PT.XYZ bertujuan untuk memberikan tolak ukur dalam menilai keamanan siber pada aplikasi terutama berbasis web yang diharapkan dapat mengurangi, meningkatkan keamanan dan melindungi sistem aplikasi dari peretas atau *attacker*.

1.2. Perumusan Masalah

Rumusan masalah penelitian ini adalah:

"Bagaimana melakukan analisis kerentanan keamanan aplikasi manajemen asset berbasis web menggunakan metode ISSAF (*Information System Security Assestment Framework*) studi kasus PT.XYZ?"

Untuk membantu pembahasan tersebut, maka akan diuraikan beberapa pokok pembahasan yang akan dikaji sebagai berikut:

1. Bagaimana cara melakukan analisis terhadap web manajemen asset PT.XYZ menggunakan metode ISSAF?
2. Apa saja kerentanan keamanan web manajemen asset PT.XYZ yang dapat ditemukan?

1.3. Tujuan dan Manfaat Penelitian

Tujuan penelitian ini adalah:

1. Melakukan analisis kerentanan keamanan web manajamen aset PT.XYZ dengan metode ISSAF.
2. Mendapatkan kerentanan keamanan pada aplikasi web manajemen asset PT.XYZ.

Adapun manfaat dari penelitian ini adalah:

1. Mengetahui kerentanan aplikasi manajemen asset berbasis web PT. XYZ dan memberikan solusi untuk pengamanan.
2. Dapat mengetahui serangan dan ancaman serta mengoptimalkan keamanan pada web manajeman aset PT.XYZ.

1.4. Batasan Masalah

Pada penelitian ini, penulis menentukan dan menetapkan beberapa hal serta aspek yang menjadi batasan masalah agar lebih efektif, berikut yang menjadi batasan masalah dalam penelitian ini:

1. Menggunakan Framework ISSAF draft 0.2.1B.
2. Pengujian kerentanan keamanan dengan jaringan lokal.
3. Pengujian kerentanan keamanan pada website yang sedang dalam pengembangan.
4. Aplikasi web manajemen asset PT.XYZ dengan framework laravel versi 8.
5. Menggunakan alat bantu/*tools* gratis dalam melakukan pentest.
6. Tidak memperbaiki kerentanan keamanan yang telah diperoleh.

1.5. Sistematika Penulisan

Untuk mempermudah dalam menyusun penelitian ini, penulis membuat ringkasan singkat mengenai beberapa bab yang telah dibuat. Ringkasan penulisan sebagai berikut:

BAB I PENDAHULUAN
Bab ini menjelaskan dari latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, serta sistematika penulisan.

BAB II KAJIAN LITERATUR
Bab ini menjelaskan teori dasar yang berkaitan dalam penelitian, dan terdapat referensi berkaitan dengan penelitian ini.

BAB III METODOLOGI PENELITIAN
Bab ini menjelaskan bagaimana penelitian ini akan dilaksanakan, meliputi metode – metode yang akan digunakan dalam penelitian ini.

BAB IV IMPLEMENTASI
Bab ini menjelaskan apa saja dan tahapan yang dilakukan ketika melakukan penelitian ini.

BAB V KESIMPULAN DAN SARAN
Bab ini menyimpulkan dan memberikan saran terhadap pengembangan penelitian ini serta menjawab pertanyaan pada rumusan masalah.