BAB I

PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi banyak diterapkan pada institusi pendidikan yang ada di Indonesia. Pemanfaatan teknologi informasi menjadi sebuah kebutuhan, bukan hanya sekadar *lifestyle* (Indrayani, 2011). Teknologi informasi diartikan sebagai teknologi yang mendukung kegiatan manusia dalam melakukan pengelolaan dan penyebaran informasi. Informasi yang dikelola dan disebarkan ke publik harus memiliki integritas atau dapat dipercaya, oleh sebab itu keamanan terhadap informasi juga menjadi hal yang penting, karena dapat mempengaruhi citra institusi pendidikan tersebut. Ancaman pada keamanan informasi dapat berupa serangan dari luar maupun dari dalam institusi, karena hal tersebut dapat mengancam keberlangsungan teknologi informasi dan dapat menyebabkan gangguan bahkan terjadi kegagalan proses bisnis. Penyerang dapat memanfaatkan celah keamanan untuk menyadap hak akses dan menggunakannya untuk mengambil data penting.

Institusi pendidikan XYZ menjadi salah satu institusi yang menerapkan teknologi informasi dalam kegiatan akademik. Namun, belum adanya dokumentasi tentang celah keamanan aset, menimbulkan kekhawatiran bagi pihak institusi tersebut, karena celah tersebut dapat dimanfaatkan oleh penyerang untuk mengambil informasi dari sebuah aset.

Salah satu aset penting milik institusi pendidikan XYZ yang belum memiliki dokumentasi tentang celah keamanan adalah web aplikasi repositori. Penentuan aset ini mengacu pada penelitian sebelumnya yang membahas tentang daftar urutan aset kritis milik institusi pendidikan XYZ. Repositori menempati urutan kedua dengan tingkat kerentanan High, dikarenakan web aplikasi tersebut menyimpan beberapa informasi yang bersifat rahasia yang dinilai berisiko jika tersebar ke publik. Web aplikasi ini juga dilaporkan sering terjadi percobaan serangan (Yuhaz, 2018).

Metode yang digunakan untuk mencari kerentanan dan dampak yang ditimbulkan dalam penelitian ini adalah metode VAPT (*Vulnerability Assessment and Penetration Testing*). *Tool* yang digunakan pada penelitian ini adalah Nessus. Nessus adalah aplikasi untuk mencari kerentanan dalam suatu web aplikasi. Hasil dari penelitian ini akan dibuat dalam bentuk laporan yang diserahkan kepada Institusi Pendidikan XYZ.

1.2. Rumusan Masalah

Belum adanya dokumentasi dan evaluasi keamanan terkait kerentanan pada aset web aplikasi repositori Institusi Pendidikan XYZ. Sehingga menghawatirkan jika sewaktu-waktu terjadi serangan dan pihak institusi pendidikan XYZ belum diketahui dampak yang dihasilkan.

1.3. Batasan Masalah

1. Penelitian ini menggunakan metode VAPT (*Vulnerability Assessment and Penetration Testing*).
2. Melakukan *vulnerability scanning* pada web aplikasi repositori Institusi Pendidikan XYZ menggunakan *tool* Nessus.

1.4. Tujuan Penelitian

Membuat laporan hasil *Security Assessment* pada web aplikasi repositori Institusi Pendidikan XYZ.

1.5. Manfaat Penelitian

Dengan adanya penelitian ini diharapkan dapat membantu pihak Institusi Pendidikan XYZ dalam hal mengetahui celah keamanan pada web aplikasi repositori Institusi Pendidikan XYZ.

1.6. Sistematika Penulisan

Sistematika penulisan tugas akhir dibagi menjadi lima bab. Berikut adalah penjelasan dari masing-masing bab.

BAB I PENDAHULUAN

Penjelasan mengenai latar belakang masalah, batasan masalah, tujuan penelitian, manfaat penelitian serta sistematika penulisan tugas akhir.

BAB II LANDASAN TEORI

Mengenai dasar teori yang mendukung masalah yang sedang dikaji, antara lain Penelitian Sebelumnya, *Information Technology Security Assessment*, metode VAPT, Nessus, Nmap, *Man In The Middle*, Arpspoof, SSLStrip, Metasploit, Brute Force, *Social Engineering*.

BAB III METODOLOGI PENELITIAN

Penjelasan tentang tahapan dalam kegiatan yang akan dilakukan dalam penelitian, berupa *Scope, Reconnaissance, Vulnerability Detection, Information Analysis and Planning, Penetration Testing, Privilege Escalation* dan *Reporting*.

BAB IV HASIL DAN PEMBAHASAN

Penjelasan tentang penerapan metode penelitian pencarian celah keamanan, berupa *Scope, Reconnaissance, Vulnerability Detection, Information Analysis and Planning, Penetration Testing, Privilege Escalation* dan *Reporting*.

BAB V KESIMPULAN DAN SARAN

Kesimpulan dari hasil penelitian dan saran yang diberikan untuk penelitian selanjutnya

DAFTAR PUSTAKA

Berisikan daftar jurnal, tesis, buku atau alamat website rujukan yang digunakan dalam penulisan