BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Pesatnya perkembangan *website* di Indonesia dikarenakan bertambahnya pengguna layanan internet yang semakin meningkat dari waktu ke waktu. Saat ini beberapa *website* yang banyak dikunjungi oleh pengguna seperti *social networking, e-commerce, forum, search engine, portal* berita dan lain lain. Namun dari berbagai kemudahan layanan yang tersedia saat ini pada setiap *website,* ternyata ada masalah pada celah keamanan diantaranya : *web defacement, information leakage, session management, authentication and authorization, SQL injection, cross-site scripting, CSRF* dan lain-lain. Di Indonesia sendiri, ada beberapa fenomena telah menunjukan bahwa rendahnya tingkat keamanan *digital* Indonesia. Pada tahun 2021, 5.940 kasus *web defacement* dan untuk kasus terbanyak terdapat di bulan Maret dengan 727 kasus yang terjadi di Indonesia. Dari data (laporan tahunan monitoring keamanan siber) menjelaskan bahwa ada 10 sektor yang menjadi sasaran dari serangan *web defacement*, dan terdapat bahwa sektor Akademik dalam hal ini adalah perguruan tinggi yang menjadi sektor dengan kasus terbanyak dengan 2.217 kasus. Disebutkan juga bahwa halaman yang paling banyak terdampak adalah halaman tersembunyi dengan 4.435 kasus sedangkan halaman muka dengan 1.505 kasus. Karena pada halaman tersembunyi akan lebih sulit terdeteksi oleh pengelola sistem (ID-SIRTII/CC, 2021).Untuk meningkatkan keamanan pada sebuah aplikasi berbasis *website* maka diperlukan analisis dan penilaian kerentanan terhadap *website* tersebut secara berkala. Hal ini penting dilakukan agar dapat memastikan *website* tersebut aman dalam waktu jangka panjang dan terhindar dari serangan *cracker* maupun *hacker* (Panji Muryandi T, 2018). Berdasarkan wawancara dengan pengelola situs web FTTI, bahwa pengujian kerentanan pada situs web FTTI belum pernah dilakukan pengujian kerentanan. Oleh karena itu penelitian ini dilakukan untuk menganalisis

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

kerentanan pada beberapa *website* FTTI di Universitas Jenderal Achmad Yani Yogyakarta.

Fakultas Teknik dan Teknologi Informasi (FTTI) merupakan perubahan bentuk dari Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Jenderal Achmad Yani Yogyakarta. Pada tahun 2018, STMIK dan STIKES Jenderal Achmad Yani dari yayasan Kartika Eka Paksi bergabung dan membentuk Universitas Jenderal Achmad Yani Yogyakarta. Pada saat itu STMIK Jenderal Achmad Yani berubah bentuk menjadi Fakultas Teknik dan Teknologi Informasi (Ftti.unjaya, 2018). Menurut data yang diperoleh dari ID-SIRTII sebagian besar kasus yang terdampak adalah sektor akademik yang mendominasi di perguruan tinggi. Maka dari itu peneliti melakukan *vulnerability assessment* dan pengujian kerentanan pada *website* di Universitas Jenderal Achmad Yani Yogyakarta. Dengan menggunakan *tool* Nmap, Nessus dan WPScan. Untuk mengetahui berbagai *port, host* yang aktif dan *output* yang diperoleh maka akan terlihat berbagai kerentanan dan solusi untuk *website* tersebut agar bisa melakukan penilaian dan meningkatkan keamanan sistem.

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta

1.2 PERUMUSAN MASALAH

Penelitian ini dilakukan untuk menilai dan menganalisis beberapa *website* yang ada pada Fakultas Teknik dan Teknologi Informasi (FTTI) di Universitas Jenderal Achmad Yani Yogyakarta. Menurut data dari ID-SIRTII yang menunjukan bahwa sektor terbanyak yang mengalami serangan *web defacement* adalah perguruan tinggi. Berdasarkan wawancara dengan pengelola situs web FTTI, pengujian keamanan belum pernah dilakukan sesuai standar pengujian. Maka dari itu peneliti melakukan penilaian beberapa *website* yang ada di FTTI.

1.3 PERTANYAAN PENELITIAN

Pertanyaan terkait masalah dalam penelitian ini, sebagai berikut:

1. Bagaimana mengetahui kerentanan pada *website* ?
2. Apa saja parameter yang diukur dalam mengetes kerentanan pada *website* ?

3. Apa saja bentuk kerentanan yang akan dijumpai pada *website* yang diuji?

1.4 TUJUAN PENELITIAN

Tujuan yang ingin dicapai dalam penelitian ini adalah dapat menganalisis dan mengetahui tingkat keamanan serta bentuk-bentuk kerentanan pada *website* FTTI di Universitas Jenderal Achmad Yani Yogyakarta yaitu ftti.unjaya.ac.id, elearning.ftti.unjaya.ac.id, dan app.ftti.unjaya.ac.id. Dengan hasil yang diperoleh dari analisis, peneliti harus melaporkan kepada Kepala Pusat Sistem Informasi (PUSI) FTTI.

.

1.5 MANFAAT HASIL PENELITIAN

Manfaat yang diharapkan dalam melakukan penelitian ini adalah sebagai berikut :

1. Bagi Peneliti:
   a. Dapat menerapkan ilmu pengetahuan yang telah didapatkan selama di perkuliahan.
   b. Mengimplementasikan dan menambah wawasan tentang keamanan jaringan *website*.
2. Bagi FTTI Unjaya:
   a. Dapat mengetahui seberapa rentannya *website-website* FTTI terhadap serangan orang yang tidak bertanggung jawab.
   b. Dengan mengetahui kerentanannya, sehingga dapat dilakukan penanggulangan sejak dini.

Perpustakaan Universitas Jenderal Achmad Yani Yogyakarta