BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi berkembang pesat seiring dengan pertumbuhan penggunanya. Contoh dari perkembangan teknologi adalah penggunaan website untuk mendukung kegiatan pembelajaran. Website merupakan kumpulan halaman web yang dapat diakses secara publik. Website dapat terdiri dari teks, gambar, video, dan media suara lainnya. Namun dengan berkembangnya suatu teknologi, maka perkembangan kerentanan atau serangan terhadap teknologi tersebut juga bertambah. Berdasarkan laporan tahunan monitoring keamanan siber tahun 2021 oleh Badan Siber dan Sandi Negara (BSSN), terdapat lebih dari 1,6 miliar serangan siber yang telah terjadi di Indonesia.

Fakultas Rekayasa Industri sebagai salah satu fakultas dari Universitas Telkom telah menggunakan website yang bernama virtualfri untuk dapat membantu kegiatan administrasi fakultas seperti administrasi kerja praktek, rekruitasi asisten laboratorium, dan administrasi peminatan. Salah satu website yang ada pada virtualfri adalah website dashboard proposal tugas akhir untuk mahasiswa Fakultas Rekayasa Industri.

Dengan pentingnya keamanan data pada website dashboard tugas akhir tersebut, maka website dashboard tugas akhir tersebut perlu dijaga keamanannya dari kerentanan dan ancaman yang ada. Untuk menghadapi hal tersebut, pengelolaan keamanan informasi pada website dashboard tugas akhir perlu ditingkatkan. Salah satu cara untuk mendeteksi resiko kerentanan yang ada yaitu dengan melakukan *vulnerability assessment*. Mengidentifikasi ancaman yang ada sangat penting bagi seluruh jaringan komputer atau web untuk menggambarkan seberapa aman suatu perangkat dan web itu berdasarkan jumlah kerentanan yang diidentifikasi. (Jetty, 2018)

Pada tugas akhir ini akan dilakukan *vulnerability assessment* terhadap website dashboard tugas akhir yang dikelola oleh Fakultas Rekayasa Industri Universitas Telkom dengan menggunakan Acunetix karena dapat mendeteksi sampai 7000

kerentanan, serta dapat memindai semua halaman dan web apps. Penulis juga menggunakan tools nmap karena tools ini terdokumentasi secara baik serta di update secara berkala sehingga dapat mendeteksi kerentanan terbaru, selain itu tools ini memiliki banyak fitur yang dapat digunakan untuk mencari kerentanan pada suatu website dan telah mendapatkan banyak penghargaan yang salah satunya adalah Information Security Product of the Year dari Linux Journal.

I.2 Perumusan Masalah

Berdasarkan latar belakang yang telah disebutkan diatas, rumusan masalah pada penelitian ini adalah:

a. Bagaimana kerentanan yang ada pada website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri Telkom University?
b. Bagaimana solusi dari kerentanan yang ada pada website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri Telkom University?
c. Bagaimana hasil dan karakteristik dari tiap tools yang digunakan saat proses *vulnerability scanning*?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah, maka tujuan dari penelitian ini adalah:

a. Kerentanan yang ada pada website dashboard proposal tugas akhir Fakultas Rekayasa Industri Telkom University dari hasil *vulnerability scanning*
b. Solusi yang diperoleh dari hasil *vulnerability scanning* pada website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri Telkom University
c. Hasil dan karakteristik dari tiap *tools* yang digunakan saat proses vulnerability scanning

I.4 Batasan Penelitian

Adapun batasan masalah pada penelitian ini adalah:

a. Solusi yang direkomendasikan berdasarkan kerentanan yang ada
b. Penelitian tidak mencakup proses penetration testing

I.5 Manfaat Penelitian

Adapun manfaat penelitian ini adalah:

1. Secara teoritis, hasil penelitian ini dapat membantu Fakultas Rekayasa Industri mengetahui kerentanan yang terdapat pada website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri.
2. Memberikan analisis mengenai kerentanan yang ada pada website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri.