

ABSTRAK

Teknologi berkembang pesat seiring berkembangnya zaman, salah satu contoh dari perkembangan teknologi yaitu dengan berkembangnya penggunaan website pada kegiatan sehari-hari. Banyak institusi dan entitas yang telah memanfaatkan penggunaan website untuk mendukung proses bisnis yang dijalankan. Fakultas Rekayasa Industri sebagai salah satu fakultas dari Universitas Telkom telah menggunakan website yang bernama virtualfri untuk dapat membantu kegiatan administrasi. Salah satu website dari Fakultas Rekayasa Industri adalah website dashboard proposal tugas akhir yang berisi plottingan pembimbing tugas akhir serta judul tugas akhir. 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. Oleh karena itu, perlu dilakukannya metode *vulnerability assessment* untuk dapat mengetahui kerentanan yang terdapat pada suatu website dan juga solusi yang dapat diterapkan untuk mengatasi kerentanan tersebut. Pada penelitian ini akan dilakukan *vulnerability assessment* pada website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri dengan menggunakan tools Nmap dan Acunetix. Hasil yang didapat setelah dilakukannya proses *vulnerability assessment* yaitu terdapat 12 kerentanan yang ada pada website dashboard proposal tugas akhir mahasiswa Fakultas Rekayasa Industri dengan Nmap mendeteksi 3 kerentanan beresiko menengah dan 1 kerentanan beresiko rendah sedangkan Acunetix berhasil mendeteksi 2 kerentanan beresiko menengah dan 6 kerentanan beresiko rendah.

Kata kunci : Kerentanan, Website, Vulnerability Assessment, Acunetix, Nmap.