

ABSTRAK

Perkembangan teknologi dan IT saat ini sudah sangat pesat, salah satunya adalah dengan adanya penggunaan *website* sebagai penunjang berbagai aktivitas manusia yang awalnya bersifat manual menjadi terotomatisasi dengan sistem, selain itu dengan *website* segala informasi dapat diakses tanpa adanya batasan tempat dan waktu. Berdasarkan kemudahan tersebut hampir seluruh perusahaan, industri, pemerintahan, hingga institusi pendidikan memiliki *website* untuk menunjang proses bisnis beserta aktivitas yang ada didalamnya. Fakultas Rekayasa Industri (FRI) sebagai fakultas yang mengedepankan teknologi juga memanfaatkan teknologi *website* agar kegiatan dan proses administratif menjadi lebih terorganisir, efektif, dan efisien. Salah satu kegiatan administratif di Fakultas Rekayasa Industri (FRI) yang memanfaatkan teknologi *website* adalah proses rekrutasi asisten praktikum dan laboratorium Fakultas Rekayasa Industri (FRI). Namun dari semua kemudahan dan dampak positif dari adanya teknologi *website*, terdapat juga ancaman terhadap keamanan *website* itu sendiri. Oleh karena itu, untuk mengamankan *website* diperlukan metode *vulnerability assessment* untuk mengetahui celah kerentanan yang ada agar dapat diperbaiki sebelum terjadi penyerangan atau eksploitasi oleh pihak yang tidak bertanggung jawab. Dalam penelitian ini akan dilakukan *vulnerability assessment* menggunakan dua *tools* utama yaitu Nikto dan Nessus. Hasil yang didapat setelah proses *vulnerability scan* dan *vulnerability assessment* menunjukkan jenis kerentanan dan tingkat risiko yang berbeda. Hasil *tool* Nikto menunjukkan 13 celah kerentanan pada sistem. *Tool* Nessus menunjukkan 136 celah kerentanan yang terdiri dari 6 level *critical*, 3 level *high*, 12 level *medium*, 8 level *low*, dan 107 level *informational*.

Kata Kunci: *Vulnerability Assessment, Vulnerability Scan, Vulnerability Analysis, Nikto, Nessus.*