BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan Teknologi Informasi dan Komunikasi membawa kemudahan bagi kehidupan manusia. Salah satu yang berkembang cukup pesat adalah website. Website merupakan sekumpulan halaman informasi yang tersedia melalui internet sehingga dapat diakses kapan saja selama terkoneksi dengan jaringan internet tanpa terbatas waktu dan ruang[1]. website menjadi pilihan karena dapat berjalan di berbagai platform. Perkembangan website menjadi tantangan sendiri bagi para pengembang aplikasi berbasis website dalam mengembangkan aspek keamanan pada aplikasi tersebut. Kerentanan atau kelemahan pada website sangat beragam. Karena aplikasi berbasis web terdiri dari banyak komponen, sehingga aplikasi berbasis web mempunyai banyak sisi untuk diserang. *Vulnerability* merupakan suatu kelemahan atau kerentanan yang rentan terhadap serangan [2].

Maka perlu Melakukan *vulnerability Assessment* akan mampu membantu proses identifikasi kelemahan dalam sistem sebelum serangan dapat terjadi serta dapat menjadi langkah pencegahan dalam meningkatkan keamanan terhadap sebuah sistem[3]. *Vulnerability Assessment* dapat memanfaatkan tools pengujian seperti Acunetix web vulnerability[4], Nessus[5] dan Owasp ZAP[6]. Menggunakan *vulnerability Assessment* memungkinkan untuk pendeteksian dini dan sekaligus dapat dilakukan penanganan yang sudah diketahui kerentanannya serta mudah untuk mengidentifikasi kerentanan yang ada pada sistem.

Hasil dari *vulnerability Assessment* dapat menghasilkan laporan yang berisi jumlah kerentanan, tingkat keparahan, detail dari setiap temuan dan rekomendasi untuk memperbaiki kerentanan [7]. Kerentanan yang ditemukan untuk melihat level resiko, Sehingga penelitian ini dapat digunakan untuk memberikan evaluasi keamanan terhadap website.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, dapat dirumuskan sebuah permasalahan yaitu:

1. Celah keamanan apa yang ditemukan dalam sebuah website.

1.3 Batasan Masalah

Untuk mempersempit pembahasan pada skripsi ini, maka dibuat batasan-batasan sebagai berikut:

a. Menggunakan Acunetix, Owasp ZAP dan Nessus sebagai alat bantu pencarian kerentanan.
b. Penggunaan sistem operasi Windows sebagai wadah instalasi software Acunetix, Owasp ZAP dan Nessus.
c. *Website* yang diuji adalah login page yang secara online dari administrator *website*.

1.4 Tujuan Penelitian

Tujuan yang ingin diraih dalam pembuatan laporan skripsi ini adalah Memberikan informasi tentang celah keamanan yang ditemukan sehingga keamanan pada website tersebut dapat ditingkatkan.

1.5 Manfaat Penelitian

Melalui hasil analisis kerentanan menggunakan Acunetix, Nessus dan Owasp ZAP dapat mengetahui resiko kerentanan dan sebagai pencegahan terhadap kerentanan yang berpotensi untuk dieksploitasi serta memberikan rekomendasi untuk memperbaiki kerentanan tersebut.

1.6 Sistematika Penulisan

Sistematika Penulisan Skripsi analisis celah keamana website menggunakan metode *Vulnerability Assessment* sebagai berikut:

Bab I PENDAHULUAN, Pada bab ini menjelaskan tentang latar belakang masalah, batasan masalah dalam pengujian sistem, tujuan penelitian, metode penelitian yang dilakukan dalam pengujian sistem dan sistematika penulisan.

Bab II TINJAUAN PUSTAKA, Pada bab ini akan menjelaskan berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan.

Bab III METODE PENELITIAN, Bab ini berisi tentang skenario analisis vulnerability assessment serta kebutuhan perangkat keras dan perangkat lunak yang digunakan untuk membantu penyelesaian tugas akhir.

BAB IV HASIL DAN PEMBAHASAN, Bab ini merupakan tahap implementasi dan pembahasan hasil kerentanan yang didapat dari *vulnerability Scanning*.

BAB V PENUTUP, bab ini berisi mengenai kesimpulan yang dapat diambil dari semua yang telah dikerjakan.