BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Website adalah sekumpulan halaman informasi yang disediakan melalui jalur internet sehingga dapat diakses seluruh dunia selama terkoneksi dengan jaringan internet tanpa terbatas ruang dan waktu [1]. Keamanan sistem informasi pada website merupakan salah satu isu utama dalam perkembangan teknologi dan komunikasi saat ini. Masalah tersebut penting karena jika informasi pada website diakses oleh orang yang tidak bertanggung jawab maka keakuratan informasi tersebut akan diragukan bahkan bisa menjadi informasi yang menyesatkan [2].

Website sering kali mendapatkan serangan dari pihak yang tidak bertanggung jawab yang seringkali di sebut *Hacker* atau peretas. Berbagai macam alasan *hacker* mencari celah pada website bertujuan untuk mendapatkan infromasi pada sebuah organisasi atau perusahaan untuk kepentingan-kepentingan yang membuat kerugian pada pihak lain. Salah satu metode untuk menguji keamanan website adalah Metode *Penetration Testing*, Pengertian dari *penetration testing* sendiri adalah sebuah metode pengujian keamanan sistem dengan cara mensimulasikan serangan-serangan yang mungkin bisa dilakukan pada suatu sistem agar mengetahui celah keamanan pada website [3]. Adapun tools yang dipakai untuk menguji keamanan website adalah *OWAPS ZAP* merupakan organisasi *non-profit* amal di *Amerika Serikat* yang didrikan pada tanggal 21 April 2004 yang berdedikasi untuk membuat *framework* pengujian keamanan yang bebas digunakan oleh siapa saja [4].

Mengetahui celah keamanan sendiri tidak akan membantu manajemen untuk meningkatkan keamanan pada website. Melakukan analisis celah keamanan website dengan mencari kelemahan yang ada pada website dengan memberikan penjelasan solusi yang lebih untuk mengamanankan website lebih baik lagi.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang diatas maka dapat diambil suatu perumusan masalah adalah analisis celah keamanan website menggunkan metode *penetration testing* untuk menemukan celah keamanan yang ada pada website dan memberikan saran atau solusi untuk mengantisipasi terjadinya serangan dari pihak-pihak tertentu yang tidak bertanggung jawab.

1.3 Batasan Masalah

Dalam pembuatan skripsi ini, penulis membatasi masalah yang akan dianalisis yaitu:

1. Penggunaan aplikasi *Owaps Zap* untuk menganalisis celah keamanan website.
2. Penulis memberikan saran dan solusi untuk mengantisipasi terjadinya serangan dari pihak-pihak tertentu yang tidak bertanggung jawab

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam pembuatan tugas akhir ini adalah untuk menganalisis celah keamanan website menggunakan metode *penetration testing* dan memberikan saran atau solusi untuk mengantisipasi terjadinya serangan dari pihak-pihak tertentu yang tidak bertanggung jawab.

1.5 Sistematika Penulisan

Sistematika penulisan merupakan bagian yang menjelaskan isi dari setiap bab, dimana penjelasan ini dapat memberikan gambaran langsung mengenai isi setiap bab yang ada dalam penulisan ini, secara singkat dapat diuraikan sebagai berikut:

1. BAB 1 PENDAHULUAN

   Bab 1 membahas mengenai latar belakang masalah, rumusan masalah, maksud dan tujuan penelitian dan sistematika penulisan untuk Analisis Celah Keamanan Webiste Menggunakan Metode Penetration Testing
2. BAB II LANDASAN TEORI

Bab II membahas mengenai landasan teori yang digunakan sebagai referensi dalam pembuatan tugas penelitian Analisis Celah Keamanan Webiste Menggunakan Metode Penetration Testing. Landasan teori berupa defenisi atau model yang langsung berkaitan dengan ilmu atau masalah yang diteliti.

3. BAB III METODOLOGI

   Bab III membahas mengenai metodologi penetration testing dalam pembuatan tugas penelitian Analisis Celah Keamanan Website Menggunkan Metode Penetration Testing.

4. BAB IV HASIL DAN PEMBAHASAN

   Bab IV membahas mengenai hasil pengujian website dan masalah dari jenis-jenis peringtan yang di dapat dan solusi pencegahan nya.

5. BAB V PENUTUP

   Bab V membahas mengenai kesimpulan dan saran dari seluruh pembahasan.