BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini, situs *web* telah menjadi sumber informasi yang sangat penting bagi berbagai bidang dan beragam kalangan. Sebagai sumber informasi terbuka, situs *web* dapat diakses dengan mudah oleh banyak orang. Oleh karena itu, kemajuan dan ketersediaan informasi ini harus diimbangi dengan tingkat keamanan yang tinggi. Meskipun situs *web* dapat diakses oleh banyak orang, namun terdapat informasi penting di dalamnya yang harus dijaga dengan baik, seperti data pengguna, informasi pribadi, dan sebagainya.

Jika keamanan situs *web* tidak diprioritaskan, kelemahan atau kerentanan tersebut dapat dieksploitasi oleh pihak yang tidak bertanggung jawab untuk kepentingan mereka sendiri. Kerentanan merupakan titik lemah di mana suatu sistem menjadi rentan terhadap serangan. Ada beberapa jenis kerentanan yang mungkin terjadi, oleh karena itu, penting untuk melakukan pencarian kerentanan dengan melakukan *penetration testing*.

Penetration testing merupakan proses di mana aplikasi menjalankan pemindaian keamanan dan mengevaluasi kerentanan Proses pemindaian kerentanan menggunakan berbagai alat pengujian yang tersedia seperti *Acunetix web vulnerability, Nessus, Vega, openVAS*, alat-alat daring, dan alat lainnya. Namun, perlu dicatat bahwa tidak semua informasi tersebut bersifat publik dan bebas diakses oleh masyarakat umum.

Meskipun demikian, kita harus menyadari bahwa tidak hanya pihak yang memiliki otorisasi yang dapat mengakses informasi tersebut, ada kemungkinan pihak lain yang tidak bertanggung jawab dapat memperoleh akses dan menyalahgunakan informasi tersebut. Ada tiga prinsip dasar yang menjadi landasan dalam menentukan keamanan suatu jaringan, yaitu Kerahasiaan (*Confidentiality*) yang melibatkan menjaga kerahasiaan informasi dari pihak yang tidak berhak, Integritas (*Integrity*) yang melibatkan menjaga agar informasi tidak diubah oleh pihak yang tidak berhak, dan Ketersediaan (*Availability*) yang menjamin agar

informasi selalu tersedia untuk diakses. Prinsip-prinsip ini sering disingkat sebagai CIA TRIAD.

Jika tiga faktor dasar keamanan jaringan tersebut tidak terpenuhi, maka jaringan tersebut dapat dianggap tidak aman dan rentan terhadap penyusupan oleh pihak yang tidak berhak. Dalam menangani masalah ini, salah satu langkah yang dapat diambil adalah dengan menganalisis sistem dan jaringan yang ada pada sistem x dari perspektif luar atau jaringan publik. Penelitian ini bertujuan untuk mengumpulkan informasi dan menguji sistem yang ada dengan menggunakan metode *penetration testing* (pentest) berdasarkan pada metode *Open Web Application Security Project* (OWASP10).

1.2 Rumusan Masalah

Berdasarkan dari latar belakang yang telah di jelaskan di atas, maka rumusan masalah pada penelitian ini sebagai berikut:

1. Bagaimana menemukan celah kerentanan dan kelemahan?
2. Bagaimana melakukan pengujian kerentanan yang ditemukan?
3. Bagaimana menganalisis hasil pengujian kerentanan?
4. Bagaimana mengetahui solusi dari kelemahan yang ditemukan?

1.3 Batasan Masalah

Agar penelitian tetap terarah dan tidak menyimpang, maka diperlukan sebuah batasan-batasan agar bisa terfokus dengan masalah yang ada oleh sebab itu batasan masalah dalam kasus ini sebagai berikut:

1. Penelitian ini hanya untuk mengetahui celah keamanan pada sistem X.
2. Pengujian celah dilakukan hanya pada celah yang berada pada tingkat ancaman High dan Medium.
3. Pada penelitian ini diberikan rekomendasi dari celah yang ditemukan tetapi tidak dilakukan perbaikan.
4. Penelitian dilakukan dengan mengacu pada metodologi OWASP (Open Web Application Security Project).
5. Hasil penelitian berupa laporan tertulis.
6. Ruang lingkup penelitian ini hanya terbatas pada sistem yang vulnerability

terhadap metodologi OWASP.

1.4 Tujuan Penelitian

Adapun tujuan yang diharapakan tercapai dalam melakukan penelitian ini adalah:

1. Melakukan pengujian dan analisis untuk mengetahui kondisi serta melakukan pengukuran tingkat kerentanan pada sistem X.
2. Melakukan pengujian keamanan pada sistem X terhadap serangan dari luar oleh orang yang tidak bertanggung jawab.
3. Membuat sebuah hasil pentest ke dalam sebuah laporan.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini sebagai berikut:

1.5.1 Bagi Peneliti

1. Sebagai salah satu syarat bagi peneliti untuk memenuhi syarat dalam mendapatkan gelar Sarjana Komputer (S.kom).
2. Peneliti dapat memiliki ilmu dan pengalaman baru tentang menganalisa sebuah kerentanan pada sistem X.
3. Dapat mengimplementasikan ilmu pengetahuan yang selama ini diperoleh di perkuliahan.
4. Mendapatkan pembelajaran baru tentang metode OWASP.

1.5.2 Bagi Universitas

1. Sebagai tambahan referensi terhadap penelitian keamanan sistem selanjutnya.
2. Sebagai kontribusi karya ilmiah dalam disiplin ilmu di bidang Teknik Informatika.

1.5.3 Bagi Pembaca

1. Pembaca mendapatkan wawasan baru mengenai kerentanan terhadap sebuah sistem x, sebagai bagian dari ilmu pengetahuan tambahan tentunya dibidang Teknik Informatika.
2. Sebagai bahan referensi untuk penelitian selanjutnya dalam bidang Teknik Infromatika pada topik yg berkaitan.

1.6 Sistematika Penulisan

Untuk memberikan gambaran secara menyeluruh mengenai masalah yang akan dibahas dalam penulisan penelitian ini, maka sistematika laporan ini dibagi menjadi 5 bab. Adapun penjabarannya sebagai berikut:

BAB I PENDAHULUAN

Bab pendahuluan berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan laporan penetration testing pada sistem x menggunakan metode OWASP10.

BAB II TINJAUAN PUSTAKA

Bab ini membahas tentang gambaran umum tentang teori yang diterapkan dalam pengujian penetration testing, menggunakan OWASP 10. Selain itu dalam bab ini juga terdapat penjelasan tentang metode dan tools yang digunakan untuk melakukan penetration testing.

BAB III METODE PENELITIAN

Bab ini membahas tentang metode yang dilakukan dalam penelitian. Metode tersebut adalah pengumpulan data, analisis kebutuhan serta perancangan pembanguan sistem dan termasuk didalamnya perancangan pengujian yang dilakukan secara sistematis.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang langkah-langkah proses pengujian yang dilakukan dan hasil yang didapatkan dari proses pengujian yang dilakukan terhadap beberapa target yang ditentukan.

BAB V PENUTUP

Bab ini berisi penutup yang meliputi kesimpulan-kesimpulan dari hasil pengujian yang telah dilakukan sebelumnya yang berupa hasil analisis pengujian yang telah dilakukan dan terdapat saran-saran dari hasil pengujian.