BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada masa sekarang ini *Internet* bukan lagi menjadi hal yang asing dan aneh terutama bagi orang-orang yang berkecimpung di dunia komputer dan teknologi informasi bahkan bagi orang yang awam sekalipun. *World wide web* (*www*) yang merupakan bagian dari *internet* telah menjadi bagian dari kehidupan manusia, dimana *web* menjadi sumber informasi yang sangat dibutuhkan dikarenakan *web* dapat menyajikan informasi yang diinginkan secara mudah, cepat, dan murah. *Internet* diterapkan kedalam berbagai bidang kehidupan manusia, termasuk bidang pemerintahan dengan adanya *e-Government*.

E-government di pemerintahan pada umumnya membangun *website* berdasarkan instruksi Presiden No. 3 Tahun 2003. Isinya tentang pemanfaatan teknologi informasi dalam menunjang aktivitas pemerintahnya, baik pemerintahan pusat maupun pemerintahan daerah menuju terwujudnya *e-Government* di Indonesia dan juga berdasasrkan Keputusan Menteri Negara Komunikasi dan informasi nomor:12/SK/MENEG/KI/2002 tanggal 1 maret 2002 tentang pembentukan satuan tugas pengembangan *e-Government* di setiap lembaga pemerintah Republik Indonesia.

Pada perkembangannya, *web* telah meluas fungsinya dengan adanya aplikasi-aplikasi yang dibangun di atas *platform* berbasis *web* yang lazim dikenal

sebagai *web based application* (aplikasi berbasis *web*). Di era sebelumnya penyajian informasi bersifat statis, setelah berkembangnya teknologi aplikasi berbasis *web* penyajian informasi menjadi bersifat lebih dinamis. Aplikasi berbasis *web* memungkinkan sebuah proses dinamisasi dengan cara mengambil informasi dari *database* untuk kemudian ditampilkan ke dalam halaman *web*. Ketika informasi yang dimiliki relatif kecil, proses pencarian informasi dapat berjalan relatif mudah, akan tetapi ketika jumlah informasi yang disajikan semakin banyak, maka proses pencarian dan penampilan informasi tersebut ke dalam halaman *web* juga akan menjadi kendala tersendiri dan aplikasi harus dapat merespon akan hal ini. Untuk itu diperlukan sebuah cara dan mekanisme tertentu agar proses *information retrieval* dapat berjalan dengan cepat, karena kecepatan merupakan faktor yang sangat penting dalam proses *information retrieval* atau perolehan informasi.

Isi *website* yang dinamis akan dapat menampilkan hasil yang berbeda disetiap pengguna sesuai dengan konfigurasi dan kebutuhan yang diinginkan. Teknologi ini membawa perubahan yang signifikan dalam proses pembangunan sistem penyedia layanan dalam jaringan *internet*. Teknologi ini memampukan penyedia layanan untuk memberikan layanan yang lebih inovatif. Efek yang diharapkan tentu saja peningkatan dari segi ekonomi. Namun dibalik keuntungan itu semua, teknologi ini memiliki permasalahan dari segi keamanan. Salah satu ancaman yang paling umum selain virus, trojan, backdoor dan spam adalah pemanfaatan *scripts* untuk memperoleh akses kedalam sistem dan salah satu

penyerangan oleh hacker yaitu teknik *Cross Site Scripting* (XSS) dan juga *SQL Injection*.

Seringkali masalah keamanan sistem aplikasi terabaikan justru setelah semua peralatan dan infrastruktur pengaman telah terpasang. Bahkan pentingnya pengamanan baru disadari setelah terjadi bencana. Kerugian sebuah institusi/organisasi yang diakibatkan dari sebuah serangan terhadap sistem aplikasi sangatlah besar, tetapi hal ini sangat sukar dideteksi, karena secara umum tidak akan diakui dengan berbagai alasan. Tanpa pengamanan sistem aplikasi yang baik, penerapan teknologi sehebat apapun akan sangat membahayakan institusi/organisasi itu sendiri.

Nilai informasi yang begitu penting dan strategis mengakibatkan serangan dan ancaman terhadap sistem aplikasi dan arus informasi semakin meningkat. Kebutuhan keamanan sistem aplikasi timbul dari kebutuhan untuk melindungi data. Pertama, dari kehilangan dan kerusakan data. Kedua, adanya pihak yang tidak diijinkan hendak mengakses atau mengubah data

Vulnerability atau celah keamanan adalah suatu kelemahan yang mengancam nilai *integrity*, *confidentiality* dan *availability* dari suatu asset. *Vulnerability* tidak hanya berupa *software bugs* atau *kelemahan security* jaringan. Namun kelemahan seperti pegawai yang tidak ditraining, dokumentasi yang tidak tersedia maupun prosedur yang tidak dijalankan dengan benar. *Vulnerability* bisa dikategorikan ke dalam tiga bagian, yaitu kelemahan pada sistem itu sendiri, jalur akses menuju kelemahan *system*, serta kemampuan dari seorang *hacker* untuk melakukan *attacking*. *Acunetix Website Application Scanner* merupakan

perangkat lunak yang dikembangkan untuk melakukan *scanning vulnerabilities* pada suatu *website*. Kelebihan dari *tools* ini adalah kemampuannya untuk memberikan solusi dari kelemahan yang ditemukan dan mengelola *traceability* dari setiap *vulnerabilities* tersebut.

Permasalahan dari penelitian ini yaitu untuk mengetahui *bugs* atau kelemahan pada Portal Pemerintahan Kota Palembang menggunakan *tools acunetix vulnerability*. Hasil dari penelitian ini mengetahui informasi *error* pada Portal Pemerintahan Kota Palembang dan memberikan saran dari *error* tersebut sebagai masukan dalam proses pengembangan portal kedepan.

Berdasarkan uraian-uraian di atas maka permasalahan tersebut diangkat sebagai bahan penelitian untuk proposal. Adapun judul yang dipilih yaitu **"Analisis *Web Vulnerability* pada Portal Pemerintahan Kota Palembang Menggunakan *Acunetix Vulnerability*".**

1.2 Perumusan Masalah

Berdasarkan uraian diatas, merumuskan yang ada untuk dijadikan titik tolak pada pembahasan proposal ini adalah "Bagaimana menganalisis *web vulnerability* Portal Pemerintahan Kota Palembang menggunakan *acunetix vulnerability* ?".

1.3 Batasan Masalah

Pelaksanaan penelitian ini menganalisis *web* pada Portal Pemerintahan Kota Palembang menggunakan *acunetix vulnerability* untuk mengetahui informasi

error dan memberikan saran untuk masukan dalam proses pengembangan portal kedepan.

1.4 Tujuan dan Manfaat Penelitian

1.4.1. Tujuan Penelitian

Adapun tujuan penelitian ini adalah untuk menganalisis *web vulnerability* Portal Pemerintahan Kota Palembang menggunakan *acunetix vulnerability*.

1.4.2. Manfaat Penelitian

Adapun manfaat penelitian ini adalah :

1. Dapat mengetahui informasi terhadap kelemahan-kelemahan keamanan sistem yang meliputi keamanan *web* server pada situs *web* Pemerintahan Kota Palembang.
2. Bagi penulis sendiri dapat mengembangkan ilmu komputer yang telah ditempuh selama penelitian.

1.5 Metodologi Penelitian

1.5.1 Waktu Penelitian

Penelitian analisis *web* pada portal pemerintahan Kota Palembang menggunakan *acunetix vulnerability* akan dilakukan mulai bulan Maret 2013 sampai dengan Agustus 2013.

1.5.2 Alat dan Bahan Penelitian

Adapun alat – alat yang digunakan dalam penelitian ini adalah :

1. ***Handware* :**

   a. *Processor Intel Core 2 Duo*

   b. *RAM 1 GB*

   c. *Hardisk 80 GB*

   d. *Monitor SVGA Color*

   e. *CDRW Room 52 x*

   f. *Printer*

   g. *Mouse*

   h. *Keyboard*

2. ***Software* :**

   a. *Microsoft Windows XP* atau sesuai dengan kebutuhan.

   b. *Microsoft Word XP*

   c. *Acunetix Web Vulnerability Scanner Versi 8*

1.5.3 Metode Pengumpulan Data

Dalam melakukan penelitian untuk mendapatkan data dan informasi, maka metode yang digunakan dalam proses pengumpulan data dilakukan sebagai berikut :

1. Metode Observasi

Dalam hal observasi ini yang akan di observasi adalah mempelajari permasalahan analisis keamanan sistem *web* menggunakan aplikasi *acunatix web vulnerability* study kasus situs *web* Pemerintahan Kota Palembang.

2. Metode Studi Pustaka

Metode yang dilakukan adalah dengan cara mancari bahan yang mendukung dalam pendefinisian masalah melalui buku-buku, *internet*, yang erat kaitannya dengan objek permasalahan.

1.5.4 Metode Pengujian Keamanan Aplikasi

Menurut Sutanta (2008:11), Metode kualitatif dengan menggunakan beberapa *tools* berupa perangkat lunak dan cara-cara tertentu yang lazim digunakan untuk menguji keamanan aplikasi. Tahap-tahap yang dilakukan adalah sebagai berikut:

1. Tahap Inisiasi, pada tahap ini dilakukan penelusuran dan pengkajian *literatur-literatur* yang berhubungan dengan keamanan aplikasi.
2. Tahap Investigasi, pada tahap ini dilakukan penyelidikan terhadap *web server*, program aplikasi yang digunakan.
3. Tahap Pengujian, pada tahap ini dilakukan pengujian terhadap keamanan aplikasi dengan menggunakan *tools*, yaitu *Acunetix web vurnerability scanner* dengan metode yang lazim digunakan dalam pengujian keamanan aplikasi dan sistem.
4. Tahap Verifikasi, pada tahap ini dilakukan verifikasi terhadap keamanan aplikasi untuk pemberitahuan kepada admin untuk dilakukan perbaikan-perbaikan atas dasar hasil investigasi dan pengujian pada aspek pemrograman.