BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dinas Komunikasi dan Informatika Jawa Barat (Diskominfo Jabar) adalah sebuah instansi yang bertanggung jawab atas pengolahan informasi dalam lingkungan Pemerintahan Jawa Barat. Tentunya web menjadi kebutuhan yang sangat penting di instansi pemerintah khususnya Dinas Komunikasi dan Informatika Jawa Barat. Dengan adanya *web*, informasi, komunikasi, transaksi antara masyarakat dan pemerintah dilakukan via internet. Beberapa manfaat *web* yang banyak digunakan di bidang pemerintahan diantaranya: menjadi media penyampaian informasi resmi, memudahkan penyampaian aspirasi masyarakat, mempermudah masyarakat mendapatkan akses pelayanan publik, memudahkan sistem administrasi, menjadi media promosi, mendukung keterbukaan informasi, dan sebagainya. Dibalik itu dalam penyampaian informasi, *web* memiliki kerentanan yang bervarian. Kerentanan ini cukup berbahaya berhubung informasi dan data yang dimiliki suatu instansi pemerintah khususnya Dinas Komunikasi dan Informasi Jawa Barat tidak semuanya bersifat terbuka.

Berdasarkan hasil kuisioner didukung dengan hasil wawancara pada tanggal 11 Februari 2016 terhadap salah satu petugas Dinas Komunikasi dan Informatika Jawa Barat, terdapat kurang lebih 170 *web* memiliki keterkaitan dengan Dinas Komunikasi dan Informatika. Dipaparkan bahwa terdapat kerentanan dan rekaman aktivitas pada sistem yang menimbulkan resiko serius terkait keamanan aplikasi/sistem di Dinas Komunikasi dan Informatika Jawa Barat (terlampir). Selain itu belum ada standar yang dijadikan sebagai panduan dalam pengelolaan resiko yang mungkin terjadi di Dinas Komunikasi dan Informatika Jawa Barat.

Penanganan awal yang dilakukan oleh Dinas Komunikasi dan Informatika adalah menginformasikan kepada tim CSIRT yang bertanggung jawab terhadap

monitoring, menganalisa suatu serangan, memberikan kesadaran terhadap pentingnya keamanan informasi jika terjadi insiden di wilayah Jawa Barat.

Dari fenomena tersebut, perlu dilakukannya analisis kerentanan terhadap setiap *web* yang berhubungan dengan Dinas Komunikasi dan Informatika Jawa Barat. Adanya panduan atau standarisasi keamanan dalam pengembangan *web* sangat penting guna meminimalisir hal-hal yang tidak diinginkan. *Open Web Application Security Project (OWASP)* adalah jenis organisasi baru yang memberikan informasi standar internasional terkait keamanan aplikasi yang tidak bias, praktis, dan efektif biaya. Hasil yang dilakukan dari pengujian *OWASP* ini akan dipetakan menggunakan parameter penilaian *Risk Rating*. *Risk Rating* adalah parameter penilaian yang digunakan untuk mengukur tingkat suatu resiko. Pada metodologi ini resiko (*risk*) adalah hasil kali kemungkinan (*Likelihood*) dengan dampak (*impact*). Hasil dari pengujian tersebut akan dijadikan parameter penilaian seberapa tinggi tingkat keamanan suatu *web*.

Berdasarkan masalah yang terjadi di Dinas Komunikasi dan Informatika Jawa Barat maka penelitian yang diambil adalah Analisis *Vulnerability assessment* Terhadap *Web* Diskominfo Jabar Menggunakan Standarisasi *OWASP* dan Parameter Penilaian *Risk Rating*. Hasil keluaran ini berupa saran/rekomendasi yang akan menjadi evaluasi terhadap sistem di Dinas Komunikasi dan Informatika Jawa Barat.

1.2 Identifikasi Masalah

Berdasar latar belakang yang terjadi, dapat diidentifikasikan beberapa masalah sebagai berikut:

1. Adanya kerentanan pada sistem yang dapat menimbulkan resiko yang serius terkait keamanan aplikasi/sistem di Dinas Komunikasi dan Informatika Jawa Barat (terlampir).
2. Belum ada standar yang dijadikan sebagai panduan dalam pengelolaan resiko yang mungkin terjadi di Dinas Komunikasi dan Informatika Jawa Barat.

1.3 Maksud dan Tujuan

Maksud dari penelitian ini adalah menganalisis *Vulnerability assessment* Terhadap *Web* Diskominfo Jabar Menggunakan Standarisasi *OWASP* dan Parameter Penilaian *Risk Rating*.

Adapun tujuan yang ingin dicapai pada penelitian yang akan dilakukan adalah sebagai berikut:

1. Melakukan *assessment* terhadap web yang terkait di Dinas Komunikasi dan Informatika Jawa Barat.
2. Memberikan saran/rekomendasi sebagai standar yang dijadikan panduan dalam pengelolaan resiko yang mungkin terjadi di Dinas Komunikasi dan Informatika Jawa Barat.

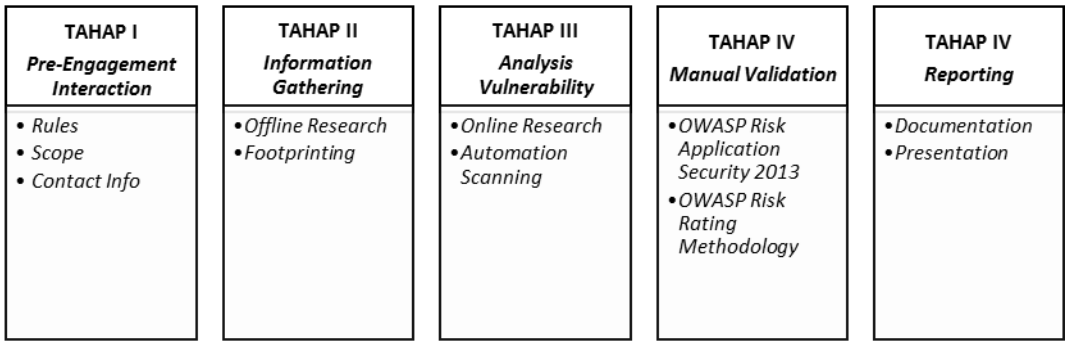
1.4 Batasan Masalah

Pada penelitian ini terdapat batasan masalah yang dibuat oleh penulis untuk membantu proses penelitian menjadi lebih terarah sesuai dengan tujuan yang diharapkan, yaitu:

1. *Website* yang diuji berjumlah 20 domain dari daftar domain yang diberikan oleh petugas diskominfo jabar.
2. *Website* yang diuji adalah *website* yang tersedia/*available* secara *online*.
3. Pengujian sistem dilakukan secara *Black Box Testing.*
4. Pengelompkan Resiko Aplikasi mengacu pada *OWASP Top 10 Application Security Risk 2013.*
5. Penilaian *assessment* menggunakan *OWASP Risk Rating* methodology.
6. *Scanning* yang dilakukan pada tahap *footprinting* menggunakan aplikasi nmap, whatweb, dan whois.
7. Teknik pencarian pada tahap *online research* menggunakan mesin pencari *Google.*
8. Informasi *Engine, Programming, Database Website Vulnerability* mengacu pada website *CVE Details* dengan alamat https://www.cvedetails.com/.

9. *Scanning* yang dilakukan pada tahap *automation scanning* menggunakan aplikasi *Acunetix.*
10. Pengujian tidak bersifat destruktif seperti misalnya melakukan serangan *DoS (Denial of Service)* pada sistem.

1.5 Alur Penelitian



Gambar 1. 1 Alur Penelitian *(Blackbox Penetration Testing)*

1. Pre-Engagement Interaction

Pada tahap ini, peneliti bekerja sama dengan pihak diskominfo untuk memperoleh ijin penelitian terhadap sistem nantinya dijadikan sebagai target dalam pengujian, menentukan metode pengujian serta menetapkan aturan keterlibatan peneliti dengan pihak diskominfo dan ruang lingkup penelitian yang dilakukan.

2. Information Gathering

Peneliti *mengumpulkan* informasi mengenai alamat *website* yang menjadi target dalam penelitian, dimana pada tahap ini, peneliti akan mencoba mengumpulkan data/informasi dan mengidentifikasi target yang akan diuji. Tahap *information gathering* meliputi *offline research*, dan *footprinting*.

3. Analysis Vulnerability

Dalam tahap ini peneliti akan melakukan *assessment vulnerability* (kerentanan) yang ada terdapat pada *website*. Pemeriksaan mengenai *vulnerability* dilakukan dengan menggunakan aplikasi atau *tools* yang disesuaikan. Tahap ini meliputi *online research* dan *automation scanning*.

4. Manual Validation

Tahap ini bertujuan untuk memvalidasi hasil *scanning* yang didapat dari *tools* yang digunakan. Agar pengelompokan *vulnerability* lebih terstruktur maka peneliti mengelompokan jenis serangan dan resiko sesuai *OWASP Risk Application Security 2013.* Selanjutnya adalah memetakan penilaian dari *vulnerability* yang terdapat pada sistem menggunakan *OWASP Risk Rating Methodology.*

5. Reporting

Reporting adalah hasil *assessment* dari penelitian yang telah dilakukan. Tahap ini meliputi *documentation* dan *presentation*. Pada tahap ini peneliti membuat laporan ini berupa temuan dan saran/rekomendasi yang akan diberikan kepada pemilik/pengurus sistem. Laporan ditulis dengan baik dan informatif, sehingga laporan mudah dipahami dan harus menyoroti semua risiko yang ditemukan selama tahap penilaian. Setelah itu laporan siap dipresentasikan kepada pemilik/pengurus sistem.

1.6 Sistematika Penulisan

Uraian singkat mengenai struktur dan penulisan isi pada masing-masing bab adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini akan diuraikan latar belakang masalah mengapa sistem harus diuji, kemudian identifikasi masalah terhadap sistem yang digunakan, maksud dan tujuan diujinya sistem, batasan masalah dalam pengujian sistem lunak, metode penelitian yang dilakukan dalam pengujian sistem dan sistematika penulisan laporan pembuatan perangkat lunak.

BAB II LANDASAN TEORI

Pada bab ini akan diuraikan berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian-penelitian serupa yang telah pernah dilakukan sebelumnya termasuk sintesisnya.

BAB III ANALISIS MASALAH

Bab ini berisi tentang analisis masalah dan skenario analisis *vulnerability assessment* yang meliputi analisis masalah yang terjadi dan *blackbox penetration testing* dalam menentukan *vulnerability* yang terdapat pada sistem.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini merupakan tahap implementasi dan pembahasan hasil yang didapat dari analisis berdasarkan metode yang digunakan. serta pembahasan resiko dan rekomendasi/saran yang akan dijadikan sebagai panduan dalam pengelolaan resiko yang mungkin terjadi.

BAB V KESIMPULAN DAN SARAN

Dalam bab ini berisi mengenai kesimpulan yang dapat diambil dari semua yang telah dikerjakan serta saran yang dapat diberikan untuk proses pengujian berikutnya agar sistem menjadi lebih baik.