BAB 1
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi, internet menjadi bagian dari kebutuhan dalam setiap aktivitas yang dilakukan oleh masyarakat secara umum, seperti komunikasi, mencari informasi, transaksi, berwirausaha dan banyak hal yang tidak bisa disebutkan satu persatu. Dalam penggunaan internet sudah banyak teknologi yang mendukung untuk bisa mengakses internet, contohnya seperti *wireless* yang saat ini sering di temukan di berbagai tempat. Dengan adanya *wireless* di berbagai tempat, tentunya memerlukan pengamanan yang kuat agar jaringan *wireless* tersebut tidak di salah gunakan. Salah satu pengamanan dalam infrastruktur jaringan *wireless* yaitu dengan menerapkan *captive portal*. Penerapan *captive portal* dilakukan untuk menahan agar tidak adanya trafik sehingga *user* harus melakukan registrasi terlebih dahulu untuk menggunakan jaringan *wireless* tersebut. *Captive portal* akan memaksa *user* yang belum terdaftar atau terautentikasi untuk masuk ke dalam *authentication* web dan akan langsung menampilkan halaman *login* (Zam, 2014).

Keamanan sistem informasi menjadi suatu hal yang sangat penting. Salah satu indikator yang dapat terlihat adalah banyaknya serangan yang terjadi. Badan Siber dan Sandi Negara (BSSN) yang bekerja sama dengan *Indonesian Honeynet Project* (IHP) mencatat terdapat 12.895.554 jumlah total serangan siber dan 513.863 jumlah total serangan *malware* dengan sumber serangan tertinggi berasal dari Rusia, Tiongkok dan Amerika Serikat yang diambil rentang waktu Januari 2018 sampai dengan Desember 2018 yang dideteksi menggunakan 22 sensor aktif tersebar di 6 sampai 9 provinsi di Indonesia (BSSN, 2019). Contoh serangan siber paling umum adalah *malicious Codes, viruses, worms* dan *trojans, malware, malicious insiders, stolen devices, phishing*, *social engineering* dan serangan berbasis web (Bendovschi, 2015). Adapun contoh serangan berbasis web secara umum yang paling sering dilancarkan, seperti *Structured Query Langueage (SQL) Injection, Distributed Denial of Service (DDoS), Cross Site Scripting (XSS),*

Defacement, Account Hijacking, dan *Malware* (Kaur dan Kaur, 2016).

Dengan mengetahui jenis dan jumlah serangan yang terjadi, maka keamanan sistem informasi perlu menjadi perhatian berbagai pihak. Adapun pihak yang sering terkena serangan siber yaitu pemerintahan, lembaga keuangan, berita, edukasi, *software* dan *video games*, kesehatan, *e-commerce*, jejaring sosial, perjalanan tur dan hiburan daring. (Kaur dan Kaur, 2016). Meskipun pihak penyerang lebih sering melakukan penyerang terhadap lembaga tertentu seperti lembaga keuangan, lembaga pemerintahan, lembaga berita, tidak menutup kemungkinan penyerang juga terjadi pada lembaga lain mungkin dari segi kepentingan akan sangat jauh berbeda dari lembaga di atas. Hal ini dilakukan guna mendapatkan informasi untuk kepentingan pribadi maupun organisasi penyerang sistem web tadi.

Selain itu faktor lain yang mempengaruhi tingkat kerentanan suatu *website* terhadap ancaman penyerang adalah kegagalan pihak developer *website* sendiri yang menyebabkan banyak ditemukan *bug* dan juga celah yang dapat digunakan oleh penyerang untuk bisa mengetahui informasi maupun mengakuisisi suatu sistem *website*.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka dapat ditarik rumusan masalah penelitian sebagai berikut:

1. Bagaimana cara untuk mengetahui informasi penting yang dibutuhkan dalam *penetration testing website* suhu.co.id dan itda.ac.id?
2. Apa saja celah dan tingkat kerentanan yang merupakan kegagalan dalam membangun *website* suhu.co.id dan itda.ac.id sehingga dapat memberikan ancaman bagi *website* suhu.co.id dan itda.ac.id dan apakah butuh untuk segera diperbaiki?
3. Apa saja teknik *penetration testing* yang digunakan dalam proses *exploitation website* suhu.co.id dan itda.ac.id?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah disebutkan, maka didapatkan Batasan Masalah sebagai berikut:

1. Aplikasi berbasis web yang akan diuji adalah suhu.co.id dan itda.ac.id
2. Penelitian ini menggunakan standar keamanan *Open Web Application Security Project* (OWASP) dan *tools* pengujian yang mendukung standar keamanan OWASP.
3. Penelitian ini melakukan pengujian kerentanan dengan teknik *black box penetration* dan menarik kesimpulan kerentanan menggunakan *Common Vulnerability Scoring System* (CVSS) versi 3.0.
4. Penerapan rekomendasi akan diserahkan sepenuhnya pada kewenangan instansi terkait yaitu PT. Kata Suhu Kita dan Institut Teknologi Dirgantara Adisutjipto.

1.4 Tujuan Penelitian

Penelitian dengan judul ini mempunyai tujuan antara lain:

1. Melakukan pengujian dan analisis untuk mengetahui kondisi serta melakukan pengukuran tingkat kerentanan sistem informasi pada *website* suhu.co.id dan itda.ac.id.
2. Menjabarkan celah serta mengukur tingkat kerentanan yang perlu untuk segera diperbaiki sehingga dapat membantu untuk memperbaiki kegagalan dalam mempertahankan keamanan sistem informasi pada *website* suhu.co.id dan itda.ac.id.

1.5 Manfaat Penelitian

Adapun manfaat yang diperoleh dari analisis *penetration testing* penelitian ini adalah sebagai berikut:

1. Mengetahui celah dan tingkat kerentanan *website* yang dimiliki oleh perusahaan.

2. Membantu memberikan evaluasi terhadap perusahaan sehingga dapat melakukan perbaikan terhadap celah keamanan *website* perusahaan.
3. Meningkatkan keamanan sistem informasi.
4. Mencegah terjadinya serangan terhadap sistem informasi *website* perusahaan.