BAB I
PENDAHULUAN

1.1 Latar Belakang

Semenjak Covid-19 menjadi pandemi diawal tahun 2020, semua kegiatan yang dilakukan bertatap muka atau pertemuan secara langsung dapat dilakukan dengan cara *online* seperti berbelanja, rapat kerja, kegiatan belajar mengajar, dan lain lain. Kegitan *online* dapat terjadi yaitu dengan menggunakan internet pada *smartphone* atau komputer pengguna sehingga pengguna dapat berinteraksi dengan pengguna lain secara *online* melalui internet. Dengan hadirnya internet, kegiatan secara *online* dengan mudah menjangkau seluruh lapisan masyarakat untuk dapat menggunakannya dengan bermodalkan jaringan seluler atau berlangganan ISP (*Internet Service Provider*).

Dari laman situs kompas.com (Riyanto, 2021), diawal tahun 2021 pengguna internet Indonesia mencapai 202,6 juta. Dalam hal ini penggunaan internet di Indonesia mengalami peningkatan 15,5 persen dibandingkan di bulan Januari 2020. Selain dari penambahan jumlah internet, pengguna di Indonesia menghabiskan waktu berinternet rata-rata 8 jam 52 menit.

Dengan hadirnya internet dan terjadinya pandemi Covid-19 kegiatan perkantoran saat ini dapat dilakukan di rumah atau bisa disebut dengan *Work From Home* (WFH). Kegiatan WFH yaitu bekerja di rumah dengan menggunakan perangkat pribadi. Dalam melakukan WFH, pekerja atau masyarakat menggunakan *software* yang terinstall pada perangkatnya, namun saat ini masih banyak pengguna menggunakan *software* bajakan. Padahal menggunakan *software* bajakan membuka celah keamanan pada perangkat pribadi. Selain menggunakan *software* bajakan secara pribadi, banyak juga perusahaan yang masih menggunakan *software* bajakan. Hal ini akan berdampak pada keamanan data yang dimiliki perusahaan.

Dilansir dari detikInet (tim, 2020), mayoritas pada perusahaan yang berada di Indonesia memakai *software* bajakan. Tingkat pemakaian *software* bajakan mencapai 83%, persentase ini merupakan nilai tertinggi dibandingkan dengan persentase rata-rata di Asia Pasifik dengan persentase 57%. Persentase yang hampir

dominan pada perusahaan yang menggunakan *software* bajakan di Indonesia, dapat terancamnya data pribadi warga yang tersimpan di komputer perusahaan pengguna *software* bajakan.

Perusahaan Kazar merupakan perusahaan swasta yang bergerak dibidang teknologi informasi. Perusahaan ini menyediakan jasa seperti perbaikan komputer atau laptop, penghapusan virus dan *spyware*, pemulihan dan pencadangan data, topologi jaringan, dan penjualan *hardware* dan *software*. Perusahaan ini sudah memiliki beberapa klien yang menggunakan jasanya sehingga klien tersebut menggunakan *software original* dan pelayanan yang disediakan oleh perusahaan Kazar. Perusahaan ini melakukan promosinya melalui *social media*, dan juga memiliki *website* perusahaan untuk lebih mengenal layanan yang disediakan oleh perusahaan tersebut.

Website merupakan aplikasi yang menggunakan protokol HTTP (*hypertext transfer protocol*) yang berisikan konten multimedia dan dalam pengaksesan website, menggunakan *software* yaitu *browser* (Hasugian, 2018, hlm.83). Dengan penggunaan *browser*, *website* dapat diakses dengan mudah melalui *smartphone*, *personal computer*, dan *android television* sehingga saat ini pengguna tidak lepas dari penggunaan *website*.

Informasi dari katadata.co.id (Burhan, 2021). Kejadian kebocoran data pada BPJS Kesehatan disebut membuat negara mengalami kerugian mencapai 600 triliun. Kerugian tersebut dihitung berdasarkan dampak peretasan nomor telepon dan akun media sosial secara masif, dan angka kerugian juga memperhitungkan dampak terhadap program pemerintah. Data kependudukan yang bocor juga dapat digunakan untuk kejahatan siber seperti penggunaan pinjaman online, membuka rekening bank yang menampung hasil kejahatan, dan membobol nomor ponsel.

Berdasarkan kasus tersebut dapat dibuktikan bahwa data pengguna sangat penting dan sensitif, apabila dilakukan penyerang oleh orang yang tidak bertanggungjawab maka data sensitif dapat disalahgunakan. Pengunaan *website* saat ini selain berisikan konten multimedia juga dapat melakukan input data-data penting pengguna sesuai kebutuhan adminstrasi dalam penggunaan *website* tertentu. Karena *website* saat ini dapat menyimpan data sensitif, maka penulis

melakukan penelitian yaitu analisis keamanan *website* untuk mengetahui dan menguji tingkat keamanan *website* perusahaan Kazar. Analisis *web* dilakukan terhadap *website* Kazar karena pada *website* tersebut dapat melakukan pengiriman pesan dari klien ke perusahaan dan menjamin pengirim pesan tersebut merupakan klien dan penerima pesan tersebut merupakan perusahaan Kazar. Metode analisis keamanan yang digunakan oleh penulis yaitu metode *Vulnerability Assessment and Penetration Testing* (VAPT).

Metode VAPT dipilih oleh penulis karena memiliki alur tahapan yang teratur, dan metode ini mudah dipahami karena dalam pengujiannya menggunakan tahapan penetrasi yang sering digunakan. Keunggulan dari metode ini yaitu diawali dengan melakukan pemindaian mengenai celah keamanan yang ada pada aplikasi yang diteliti setelah itu memberikan rekomendasi yang tepat untuk memperbaiki celah yang ditemukan. Tahapan metode VAPT yaitu *scope*, *reconnaissance, vulnerability detection, information analysis and planning, penetration testing, privilege escalation, result analysis, reporting, clean-up*.

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka didapatkan rumusan masalah sebagai berikut:

1. Apa saja jenis kerentanan pada sistem *website* perusahaan CV. Kazar Teknologi Indonesia?
2. Bagaimana cara menguji kerentanan *website* perusahaan CV. Kazar Teknologi Indonesia menggunakan metode VAPT?
3. Apa saja rekomendasi untuk celah keamanan yang ditemukan dalam perbaikan keamanan pada *website* perusahaan CV. Kazar Teknologi Indonesia?

1.3 Ruang Lingkup

Ruang lingkup pada penelitian ini:

1. Menggunakan *OS Windows 10 Home* dan *Kali Linux*.
2. Pengujian keamanan *website* pada domain kazar.xxx.xxx menggunakan metode VAPT.

3. *Vulnerability assessment website* menggunakan *Nessus*, *OpenVAS*, *OWASP ZAP*, dan *WPScan*.
4. *Scope* yang digunakan dalam penelitian ini yaitu *blackbox testing*.

1.4 Tujuan Penelitian

Berdasarkan latar belakang, dan rumusan masalah. Tujuan penelitian yaitu:

1. Menjadikan sistem cukup aman dalam waktu yang tidak dapat ditentukan dari serangan *hacker* pada *website* CV. Kazar Teknologi Indonesia.
2. Menemukan kerentanan atau celah keamanan yang terdapat pada *website* CV. Kazar Teknologi Indonesia.
3. Memberikan solusi dari celah keamanan untuk menutupi atau memperbaiki dari celah keamanan yang ditemukan pada *website* CV. Kazar Teknologi Indonesia.

1.5 Manfaat

Berdasarkan latar belakang, rumusan masalah, dan tujuan penelitian yang sudah dijelaskan. Maka, penelitian ini memberikan manfaat:

1. Meningkatkan keamanan *website* perusahaan *website* CV. Kazar Teknologi Indonesia serta merekomendasikan bagaimana cara untuk memperbaiki celah keamanan yang ditemukan oleh peneliti.
2. Diharapkan dapat menjadikan referensi untuk penelitian yang terkait pada tulisan ini.

1.6 Luaran yang Diharapkan

Luaran yang diharapkan dari penelitian ini adalah mengetahui tingkat keamanan serta celah keamanan pada *website* perusahaan Kazar serta hasil dari penelitian ini adalah laporan atau *report* mengenai celah keamanan yang dimiliki oleh *website* perusahaan Kazar yang akan dilaporkan kepada perusahaan terkait.

1.7 Sistematika Penulisan

Pada penelitian ini, penulis menggunakan sistematika penulisan yang terdiri dari bagian utama sebagai berikut:

BAB 1 Pendahuluan

Pada bab ini membahas mengenai latar belakang, rumusan masalah, ruang lingkup, tujuan penelitian, manfaat penelitian, luaran yang diharapkan, dan sistematika penulisan pada penelitian ini.

BAB 2 Landasan Teori

Pada bab ini membahas tentang teori-teori untuk memperkuat dan menjadikan referensi untuk mendasari pembahasan pada penelitian ini.

BAB 3 Metodologi Penelitian

Pada bab ini membahas metode, kerangka berpikir, dan jadwal kegiatan yang dilakukan dalam penelitian ini.

BAB 4 Hasil dan Pembahasan

Pada bab ini menjelaskan bagaimana proses serta pembahasan dan hasil yang didapat dalam penerapan metode *VAPT* pada *website* CV. Kazar Teknologi Indonesia.

BAB 5 Penutup

Pada bab ini memberikan kesimpulan dari hasil seluruh penelitian yang dilakukan serta memberikan saran sebagai acuan untuk penelitian selanjutnya.

Daftar Pustaka

Riwayat Hidup

Lampiran