BAB I
PENDAHULUAN

I.1 Latar Belakang

Pada era perkembangan teknologi saat ini penggunaan tekonologi informasi dalam melakukan pertukaran informasi digital telah sangat berkembang. Seiring dengan perkembangan infotmasi digital ini juga disertai oleh pertambahan jumlah kejahatan dan menimbulkan ancaman terhadap keamanan jaringan. Kegiatan yang dapat mengancam yang dikenal dengan *cyber crime* atau kejahatan siber seperti melakukan *hacking*, menyebarkan virus kepada target, *spyware*, *trojan* dan lain terus bertambah dalam dunia *cyber crime*. Informasi merupakan suatu aset penting bagi suatu perusahaan karena hal tersebut merupakan salah satu sumber daya yang dapat digunakan dalam perncangan strategi perusahaan dalam meningkatkan *value* usaha serta dalam upaya peningkatan kepercayaan publik sehingga publik dapat mengakses informasi suatu perusahaan tersebut dengan memanfaatkan *website* dari perusahaan tertentu agar dapat diakses secara umum dan bersifat general. Selain itu pemanfaatan *website* saat ini sangat membantu aktifitas dan melakukan visualisasi data pada bidang sektor perusahaan luar dan dalam negeri, pemerintahan, dan kesehatan, hal ini dapat memicu jumlah serangan siber terhadap aset-aset organisasi dan perusahaan yang bisa saja terjadinya pencurian data karena adanya celah pada suatu website, selain itu pemanfaatan media sosial yang terus meningkat serta penetrasi internet yang terus berkembang dapat menjadi kejatahan siber terus berkembang.

Perlindungan manajemen keamanan informasi pada suatu organisasi dan perusahaan perlu ditingkatkan dari segi pengelolaan keamanan informasi, dapat dilakukan dengan melakukan *vulnerability scanning*. Berdasarkan hasil laporan di Indonesia, menurut Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat 88.414.296 serangan siber telah terjadi sejak 1 Januari hingga 12 April 2020. Pada bulan Januari telah terjadi 25.224.811 serangan dan kemudian pada bulan Februari terekam 29.188.645 serangan lalu kemudian pada bulan Maret terjadi 26.423.989 serangan dan sampai dengan 12 April 2020 telah tercatat 7.576.851 serangan. Serangan yang terjadi

umunya merupakan serangan berjenis *Malicious* phising dari website yang memiliki sistem keamanan yang lemah dan rentan untuk terkena serangan siber. (BSSN, 2020). Ancaman serangan tersebut dengan berbagai jenis serangan diantaranya *Trojan HawkEye Reborn, Blackwater malware, BlackNET RAT, DanaBot Banking Trojan, Spynote RAT, ransomware Netwalker, Cerberus Banking Trojan, malware Ursnif, Adobot Spyware, Trojan Downloader Metasploit, Projectspy Spyware, Anubis Banking Trojan, Adware, Hidden Ad (Android), AhMyth Spyware, Metasploit, Xerxes Bot, dan Covid19 Tracker Apps* (BSSN, 2020).

Kejahatan siber juga terjadi secara hampir diseluruh dunia, dengan demikian hal tersebut tetap menjadi perhatian penting bagi setiap negara didunia agar konsisten dan memperketat keamanan internet diberbagai aspek tata kelola teknologi informasi. Berdsasarkan laporan *Cybersecurity Ventures* (Lembaga penelitian dan penerbit terkemuka dunia yang meliput ekonomi siber global dan sumber terpercaya untuk fakta, angka, dan statistik keamanan siber) memperkirakan bahwa biaya kejahatan dunia maya secara global akan tumbuh sebesar 15 persen per tahun selama lima tahun ke depan, selain itu diprediksi pada tahun 2025 mencapai $10,5 triliun USD, naik dari $3 triliun USD pada tahun 2015. Hal tersebut merupakan transfer kekayaan ekonomi terbesar dalam sejarah (Morgan, 2020).

PT. XYZ merupakan sebuah perusahaan yang bergerak pada pusat perbelanjaan *online*. Proses promosi serta penjualan produk saat ini dengan memanfaatkan *website* sebagai wadah dalam melakukan proses bisnisnya secara online. Hal tersebut tentunya menjadi sebuah tantangan perusahaan dalam menjaga informasi perusahaan serta data pengguna *website e-commerce* PT XYZ dikarenakan menurut berdasarkan hasil wawancara kerap terjadi percobaan peretasan terhadap elemen atau fungsionalitas yang penting pada *website e-commerce* PT XYZ, berdasarkan pernyataan tersebut maka sangat perlu diperhatikan dalam pengelolaan keamanan sistem informasi dan perlu untuk melakukan manajemen resiko terkait permasalahan yang terjadi yang mana manajamen resiko ini memiliki peran penting dalam menghindari risiko yang terjadi pada perusahaan. Manajemen resiko merupakan teori yang penting untuk diterapkan dalam pembangunan bisnis atau pada perusahaan, karena tanpa adanya manajemen yang baik, pihak perusahaan tidak dapat mendeteksi hal-hal buruk yang dapat

mengganggu proses bisnis dari sebuah perusahaan, khsusnya pada suatu website peruasahaan atau organisasi. Salah satu upaya peningkatan keamanan website yaitu dengan melakukan *Vulnerability Assesment Scanning* dengan menambahkan sudut pandang dari analisa risiko. Hasil dari *vulnerability scanning* akan menghasilkan identifikasi kerentanan yang terjadi pada *website* tersebut sehingga dapat membantu perusahaan atau organisasi dalam mengelola keamanan siber dengan tujuan melindungi suatu sistem dalam mengantisapasi celah ataupun serangan siber selain itu terdapat sebuah *mapping* pada aspek lingkungan pada perusahaan PT. XYZ yang dapat mendukung keamanan perusahaan sehingga kerentanan yang terjadi tidak terulang kembali dan menjadi bahan evaluasi perusahaan.

I.2 Perumusan Masalah

Berdasarkan latar belakang, terdapat rumusan masalah yang mendasari penelitian ini adalah:

1. Bagaimana melakukan identifikasi potensi terjadinya celah kerentanan pada *website e-commerce* PT XYZ.
2. Bagaimana menentukan hasil *risk score* berdasarkan simulasi celah kerentanan menggunakan OWASP ZAP dalam metodologi yang digunakan.
3. Bagaimana identifikasi *risk assessment* menggunakan *framewok* VAPT.

I.3 Tujuan Penelitian

Tujuan yang ingin dicapai pada penelitian Tugas Akhir ini dengan mengacu rumusan masalah adalah:

1. Melakukan *vulnerability scanning* menggunakan *scanning tools* OWASP ZAP sehingga dapat melakukan identifikasi potensi terjadinya celah kerentanan pada *website e-commerce* PT XYZ.
2. Melakukan perhitungan *risk score* menggunakan metode indikator standar nilai kerentanan Teknologi Informasi *Common Vulnerability Scanning System* (CVSS) berdasarkan hasil *vulnerability scanning*.
3. Melakukan analisa *mapping* berdasarkan empat domain aspek lingkungan serta melakukan *hazard identification* berdasarkan kerentanan pada *website e-commerce* PT XYZ.

I.4 Batasan Penelitian

Batasan masalah pada Tugas Akhir ini adalah sebagai berikut.

1. Proses *mapping* pada domain keamanan lingkungan hanya melakukan identifikasi bahwa domain aspek keamanan lingkungan tersebut tersedia pada perusahaan.
2. Proses identifikasi pada elemen *website* berfokus pada fungsionalitas penting yang dijadikan sebagai aset perusahaan, hal tersebut menjadi langkah awal dalam melakukan analisa risiko.
3. Kerangka kerja penelitian menggunakan *framework* VAPT yang dapat acuan dalam melakukan penelitian ini.
4. Proses penialaian *risk score* menggunakan metode CVSS *Common Vulnerability Scoring System.*
5. Metode penilaian CVSS tidak melakukan perhitungan akumulasi, melainkan dengan menggunakan metode *assigning.*
6. Penelitian ini tidak melakukan *penetration testing* hanya melakukan *vulnerability assessment* terhadap hasil kerentanan yang terjadi.

I.5 Manfaat Penelitian

Manfaat pada Tugas Akhir penelitian ini:

1. Secara teoritis, manfaat dari hasil penelitian ini dapat mengetahui bagaimana cara *framework* VAPT dalam melakukan proses *vulnerability assessment* dengan dimulai penentuan *scope and goal* hingga proses *risk* pada *framework* VAPT, sehingga memberikan dokumentasi serta membantu menentukan estimasi risiko yang terjadi mengenai keretanan suatu *website*.
2. Secara praktis, dokumentasi penelitian ini dapat digunakan sebagai bahan referensi dalam melakukan proses *vulnerability assessment* dengan objek penelitian *website* dengan menambahkan sudut pandang pada analisis risiko.