BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan Internet dalam teknologi informasi berkembang dengan pesat seiring dengan pertumbuhan penggunanya. Demikian pula, tingkat kejahatan dalam teknologi informasi sangat berbahaya baik bagi pengguna individu maupun organisasi. Keamanan teknologi informasi dibutuhkan dalam meningkatkan efektivitas dan efisiensi keamanan *cybercrime*, pemeliharaan, analisis ancaman, dan insiden dalam keamanan teknologi informasi.

Berdasarkan data dari Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri menerima 2.259 laporan kasus kejahatan siber sepanjang Januari hingga September 2020. Tercatat, laporan soal penyebaran konten provokatif merupakan yang paling banyak dilaporkan yakni sebanyak 1.048 kasus. Selain itu, masyarakat juga melaporkan kejahatan siber lainnya sepert penipuan online, pornografi, akses ilegal, manipulasi data, pencurian data/identitas, dan sebagainya. Melalui situs patrolisiber.id, hingga saat ini terdapat total 7.535 aduan masyarakat terkait kejahatan siber. Ribuan kasus ini diprediksi telah menimbulkan kerugian sebesar Rp 27,19 miliar (Annur, 2020).

Serangan siber menjadi tantangan untuk Indonesia mengingat pada bulan Mei tahun 2017 terjadi serangan *Ransomware Wannacry* yang berdampak pada sektro perusahaan dan rumah sakit lebih dari 150 negara termasuk dengan Indonesia. Dengan jumlah serangan siber terus meningkat pada asset perusahaan dan organisasi, maka sangat perlu diperhatikan dalam pengelolaan keamanan sistem informasi khsusnya pada suatu *website* peruasahaan atau organisasi. Salah satu upaya peningkatan keamanan *website* yaitu dengan melakukan *Vulnerability Assesment Scanning.* Hasil dari *vulnerability scanning* akan menghasilkan rekomendasi yang dapat membantu perusahaan atau organisasi dalam mengelola keamanan siber dengan tujuan melindungi suatu sistem dalam mengantisapasi celah ataupun serangan siber.

PT. XYZ adalah perusahaan yang bergerak pada bidang *food and bevarage* dan salah satu produsen es krim terkenal di Indonesia. Proses penjualan dan promosi

yang diterapkan pada PT. XYZ ini dilakukan secara *online* dengan memanfaatkan aplikasi berbasis *website. Website* PT. XYZ dikembangkan pada tahun 2012 dan *versi* selanjutnya di kembangkan pada tahun 2018 hingga saat ini. *Website* akan terus berkembang mengikuti tren yang ada pada saat ini ataupun penambahan fitur yang memang dibutuhkan oleh *user*. Tentu saja hal tersebut bukanlah sesuatu yang mudah bagi perusahaan untuk bisa menjamin dan menjaga keamanan *user* dan informasi perusahaan yang di sebabkan oleh banyaknya jumlah ancaman serangan siber yang semakin meningkat. Berdasarkan hasil wawancara dengan narasumber menyatakan bahwa *Website* PT. XYZ pernah mengalami beberapa kali peretasan diikuti dengan akun spam yang dapat menggangu kestabilan *website,* berdasarkan pernyataan tersebut hal itu dapat mempengarusih asset IT yang ada. Maka dari itu diperlukan perhatian dalam mengelola keamanan sistem informasi dan pengelolaan sumber daya agar bisa mengurangi dampak yang dapat merugikan perusahaan. *Management Resource* merupakan bagian dari perusahaan untuk memastikan perusahaan dapat mengoptimalkan dan mengalokasikan sumber daya ke kebutuhan yang tepat, kebutuhan yang selaras dengan strategi perusahaan dan memberikan nilai maksimal. *Resource Priority* adalah sesuatu yang bisa mendukung perusahaan bekerja baik dari sisi *human* atau dari sisi energi atau dari sisi yang lainnya yang dibutuhkan oleh perusahaan. Perusahaan membagi menjadi beberapa tipe sumber daya yang diprioritaskan, sumber daya dapat dilihat dari sesuatu yang terlihat (*Tangible*) atau sesuatu yang tidak terlihat (*Intangible*).

Untuk mengantisipasi ancaman yang mungkin terjadi, para pengembang *website* melakukan *Vulnerability Assessment*. *Vulnerability Assessment* adalah proses mengidentifikasi, menilai, dan mengklasifikasikan tingkat kerentanan keamanan di jaringan komputer, sistem, aplikasi, atau bagian lain dari sistem IT berdasarkan prioritas yang dibutuhkan oleh perusahaan. Vulnerability Assessment pada *website* PT. XYZ. bertindak sebagai pelengkap dan menguji kinerja serangan pada target sehingga para pengembang dapat melihat kelemahan dan kerentanan yang dapat mengancam *website* PT. XYZ. Adapun *tools* yang digunakan penyusun untuk melakukan vulnerability assessment yaitu Burp Suite.

I.2 Rumusan Masalah

Berdasarkan latar belakang, adapun perumusan masalah yang terdapat pada penelitian ini, yaitu:

1. Bagaimana mengidentifikasi potensi terjadinya celah kerentanan pada *website* PT. XYZ dalam melakukan unit bisnis penjualan, pemesanan, serta pengiriman produk menggunakan *tools* Burp Suite?
2. Bagaimana menentukan hasil *priority score* sebagai rujukan untuk menentukan *resource priority* pada PT. XYZ?
3. Bagaimana menentukan kerentanan yang harus diprioritaskan berdasarkan analisis *vulnerability* pada *website* PT. XYZ dengan aspek *environment* pada PT. XYZ berdasarkan *Domain Security*?

I.3 Tujuan Penelitian

Berdasarkan perumusan masalah, maka tujuan dari penelitian ini adalah:

1. Mengidentifikasi potensi terjadinya celah kerentanan *website* PT. XYZ dengan teknik *vulnerability scanning* menggunakan *tools* Burp Suite.
2. Melakukan penentuan aspek *environment* pada lingkungan PT. XYZ yang mungkin berdampak pada aspek Teknologi Informasi, kemudian menentukan *resource priority* dengan melakukan perhitungan menggunakan *priority score*
3. Melakukan analisa *mapping* berdasarkan *Domain Security* dan melakukan identifikasi *vulnerability* berdasarkan kerentanan yang ditemukan, untuk menentukan aspek mana yang berpengaruh pada sumber daya pada PT. XYZ

I.4 Batasan Penelitian

Adapun Batasan masalah pada tugas akhir ini adalah:

1. Hasil *vulnerability scanning* digunakan untuk menentukan kerentanan mana yang harus di prioritaskan berdasarkan *resource* yang dimiliki perusahaan
2. Pada penelitian ini hanya menganalisis *vulnerability scanning* dan tidak mencakup *Penetration Testing* untuk mengidentifikasi kerentanan yang ada pada *website* PT. XYZ.
3. Pada penelitian ini hasil *Score* CVSS digunakan untuk *Value* pada *priority table*

4. Penentuan *priority resource* berdasarkan formula perhitungan *priority score*
5. Pada penelitian ini menggunakan *framework* VAPT sebagai rujukan

I.5 Manfaat Penelitian

Adapun manfaat penelitian ini adalah:

1. Membantu memberikan informasi terkait keretanan suatu *website* dengan menggunakan *framework* VAPT sehingga pihak perusahaan atau organisasi dapat lebih waspada dalam melakukan proses bisnisnya.
2. Hasil penelitian ini dapat membantu organisasi dalam menentukan kerentanan apa yang ada pada *website* dan perlu di prioritaskan, berdasarkan *framework* VAPT dan *Security Domain*
3. Hasil penelitian ini dapat membantu organisasi dalam menghitung *priority score* dan menentukan *resource* apa yang perlu di prioritaskan berdasarkan formula yang digunakan pada penelitian ini