BAB I PENDAHULUAN

I.1 Latar Belakang

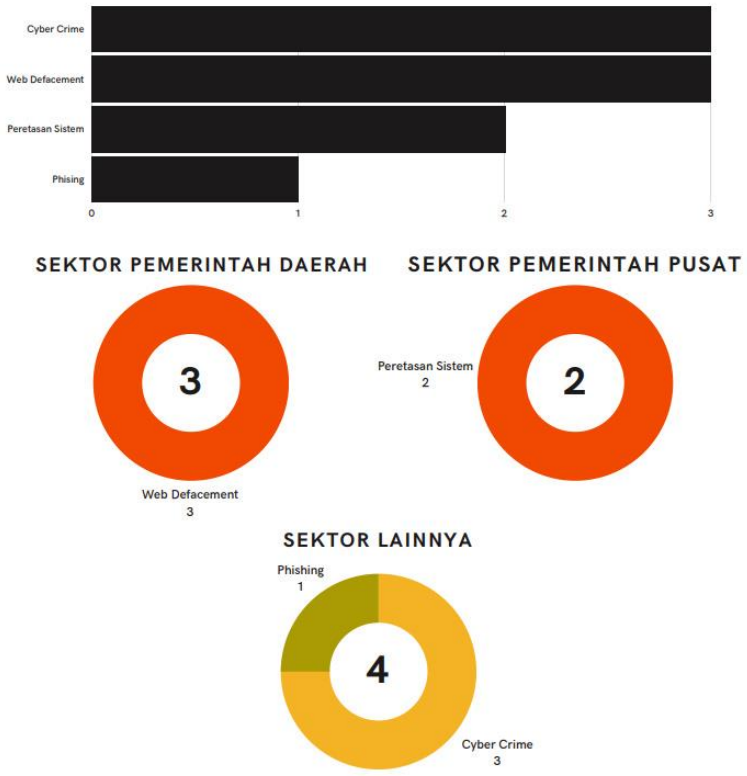
Teknologi mengalami perkembangan yang sangat pesat, salah satunya yaitu penggunaan *website*. Manfaat dari penggunaan *website* yaitu dapat membantu kegiatan yang semula bersifat manual menjadi terotomatisasi dengan sistem dan kemudahan dalam mengakses informasi dimana saja dan kapan saja selama terhubung dengan internet. Dengan manfaat tersebut, banyak perusahaan maupun organisasi mulai menggunakan *website* dalam menjalankan proses bisnis dan memberikan layanan kepada pelanggan. Tetapi dalam penggunaannya, sering ditemukan adanya kekurangan yang muncul dari *website* itu sendiri. Kekurangan ini bisa memunculkan celah kerentanan yang bisa berakibat fatal bagi *website*.

Vulnerability merupakan kerentanan dari suatu sistem atau jaringan yang memungkinan adanya akses tanpa izin oleh orang yang tidak bertanggung jawab. Kerentanan ini bisa muncul dari pengelolaan keamanan yang kurang dari pihak pengembang *website* maupun terdapat *bug* yang tidak diketahui dan belum diperbaiki. Jika kerentanan pada *website* tidak diperbaiki, maka dapat memunculkan peluang terkena serangan siber dan menimbulkan kerugian bagi perusahaan atau organisasi.

Berdasarkan hasil monitoring keamanan siber dari Badan Siber dan Sandi Negara (BSSN) pada bulan Desember 2022 (Id-SIRTII, 2022) menjelaskan mengenai kasus peretasan *website* yang ada di Indonesia.

Gambar I. 1 Data monitoring keamanan siber

Berdasarkan gambar I.1 terdapat 89 kasus yang terjadi pada bulan Desember 2022 dan 121 kasus yang didominasi di sektor pendidikan yang terjadi sepanjang tahun 2022. Upaya peretasan yang terjadi didominasi dengan menyerang halaman tersembunyi dari *website*. Selain data diatas, terdapat laporan dari aduan publik mengenai serangan siber yang terjadi pada *website* (Id-SIRTII, 2022)



Gambar I. 2 Data Aduan Publik

Berdasarkan gambar I.2 terdapat 9 aduan yang dilaporkan dengan penyebaran kasus terjadi pada sektor pemerintah daerah, pemerintah pusat, dan lainnya. Dari data aduan ini terdapat 3 aduan mengenai *Web Defacement* yang merupakan serangan yang berupaya mengubah tampilan dari *website*, baik dari halaman utama maupun halaman lain yang masih didalam satu *URL website* (Wibowo et al., 2023). Selain itu terdapat juga aduan mengenai peretasan sistem, *cyber crime*, dan *phising*.

Vulnerability Assessment and Penetration Testing (VAPT) merupakan metode yang digunakan dalam memberikan penilaian terhadap keamanan sistem dengan melakukan identifikasi dan analisa celah keamanan yang ditemukan kemudian melakukan pengujian terhadap celah keamanan dan dilakukan mitigasi kepada sistem. Terdapat beberapa tahapan dalam melakukan *Vulnerability Assessment and Penetration Testing (VAPT)* yaitu menetukan *scope,* mengumpulkan informasi dari *website,* melakukan *vulnerability detection*, analisis celah keamanan, melakukan pengujian dengan *penetration testing*, dan melakukan *reporting* (Umrao et al., 2012) Hasil dari pengujian ini dapat membantu dalam memperkuat keamanan dari *website* dan mencegah terjadinya upaya serangan siber (Goel & Mehtre, 2015).

Universitas XYZ adalah perusahaan yang bergerak di bidang pendidikan dan memiliki beberapa fakultas yang dimiliki. Universitas XYZ menggunakan *website* dalam menjalankan proses bisnis dan pengelolaan data, seperti pengelolaan keuangan dan layanan akademik. Dalam *website* layanan akademik terdapat informasi yang bersifat rahasia, seperti data Nomor Induk Mahasiswa (NIM) , Nomor Induk Pegawai (NIP), tempat tanggal lahir pengguna, alamat pengguna, dan lainnya. Pentingnya dalam menjaga informasi yang dimiliki oleh *website* sehingga perlu adanya penerapan aspek dari keamanan informasi yang terdiri dari *Confidentiality, Integrity,* dan *Availibility* (Andress, 2014).

Penerapan dari aspek keamanan informasi pada *website* Universitas XYZ dalam upaya menjaga keamanan data sudah diterapkan didalam sistem. Tetapi terdapat kekurangan dalam penerapannya dengan adanya kerentanan yang muncul dari proses *vulnerability detection*. Sehingga dalam hal ini perlu adanya evaluasi kembali dalam menjaga aspek keamanan informasi sudah diterapkan pada *website*.

Dalam pengujian dari celah keamanan *website* layanan akademik Universitas XYZ, penulis memilih menggunakan metode *Vulnerability Assessment and Penetration Testing (VAPT)* dengan menggunakan beberapa *tools* seperti *NMAP*, *Nessus*, *OWASP ZAP*, dan *Burp suite* kemudian dibuatkan *reporting*. Dengan metode ini dapat dijelaskan celah apa yang dimiliki oleh *website* berikut dengan bukti pengujian dan diberikan rekomendasi dalam melakukan mitigasi sistem.

Dari metode ini dapat memberikan evaluasi kepada pengembang *website* dalam upaya meningkatkan keamanan dan keutuhan *website* yang mendorong penulis untuk melakukan penelitian ini.

I.2 Rumusan Masalah

Adapun rumusan masalah yang mendasari penelitian ini diantaranya adalah sebagai berikut:

a. Bagaimana analisis dari kondisi eksisting *website* layanan akademik Universitas XYZ menggunakan *tools NMAP, Nessus, OWASP ZAP,* dan *Burp suite* ?
b. Bagaimana rekomendasi yang dapat dilakukan untuk tahap mitigasi *website* layanan akademik Universitas XYZ ?

I.3 Tujuan Penelitian

Adapun tujuan dari dilakukannya penelitian ini diantaranya adalah sebagai berikut:

a. Hasil analisis dari kondisi eksisting *website* layanan akademik Universitas XYZ menggunakan *tools NMAP, Nessus, OWASP ZAP,* dan *Burp suite.*
b. Rekomendasi yang dapat dilakukan untuk tahap mitigasi *website* layanan akademik Universitas XYZ

I.4 Batasan Penelitian

Batasan dari penelitian ini adalah sebagai berikut:

1. Penelitian hanya dilakukan kepada *website* layanan akademik Universitas XYZ.
2. Penelitian ini akan menggunakan 1 *tools network scan* yaitu *NMAP*, 2 *tools automated scanning* yaitu *Nessus Essentials* dan *OWASP ZAP*, dan 1 *tools penetration testing* yaitu *Burp suite Community Edition*
3. Penelitian ini dilakukan hingga tahap mitigasi dan bila terdapat *vulnerability* yang belum bisa diperbaiki, maka akan menjadi rekomendasi mitigasi perbaikan sistem.

4. Kateogri kerentanan yang diprioritaskan untuk diberikan rekomendasi mitigasi sistem yaitu *Critical, High*, dan *Medium*.

I.5 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut:

1. Bermanfaat bagi Universitas XYZ dalam mengetahui tingkat keamanan pada *website* yang digunakan sehingga bisa dijadikan evaluasi dalam pengembangan dan pengelolaan *website*.
2. Bermanfaat bagi penelitian lain yang bergerak pada bidang keamanan sistem dan menjadi rekomendasi dalam pemilihan *tools* untuk *Vulnerability Assessment and Penetration Testing (VAPT)*.

I.6 Sistematika Penulisan

Sistematika penulisan dari penelitian ini terdiri dari enam bab. Adapun uraian dari keenam bab tersebut disusun sebagai berikut:

1. Bab pertama, Bab ini berisikan tentang latar belakang penelitian, rumusan masalah dalam penelitian, tujuan penelitian, manfaat penelitian dan sistematika penulisan.
2. Bab kedua, bab ini membahas mengenai literatur yang digunakan dalam penelitian ini. Terdiri atas literatur penelitian terdahulu, Perbandingan Metode Penelitian, dan literatur yang sesuai dengan penelitian ini.
3. Bab ketiga, bab ini membahas mengenai metodologi yang digunakan dalam penelitian, model konseptual, sistematika penyelesaian masalah dari penelitian ini.
4. Bab keempat, pada bab ini membahas mengenai perancangan pengujian,*vulnerability detection*, dan penjelasan mengenai skenario pengujian yang akan digunakan.
5. Bab kelima, pada bab ini membahas mengenai penjelasan hasil pengujian yang telah dilakukan di bab sebelumnya dan melakukan analisis dari hasil yang sudah dilakukan kemudian disimpulkan dalam *reporting*.

6. Bab keenam, Bab ini menjelaskan tentang penjelasan intisari dari keseluruhan hasil pengujian dan menjawab rumusan masalah yang telah ditentukan serta berisi saran penelitian yang akan dilakukan selanjutnya.