BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan teknologi informasi berkembang pesat seiring dengan pertumbuhan penggunanya. Pada era internet saat ini, informasi sangat mudah diperoleh dan disebarluaskan. Oleh karena itu, informasi menjadi aset yang sangat berharga bagi berbagai macam pihak. Pentingnya sebuah informasi menimbulkan munculnya istilah keamanan informasi. Saat ini semakin banyak sumber informasi yang berasal dari internet sehingga keamanan informasi menyangkut teknologi komputer dan jaringan (Nurul et al., 2022).

Website merupakan salah satu media yang digunakan oleh banyak pihak untuk menyebarkan informasi. *Website* lebih mudah diakses oleh masyarakat di berbagai daerah hanya dengan menggunakan internet, sehingga mampu memberikan informasi menjadi lebih efisien (Hasugian, 2018). Selain tingginya manfaat yang dirasakan, tingkat risiko dan ancaman penyalaahgunaan pada teknologi informasi seperti *website* juga semakin tinggi dan kompleks sehingga lebih rentan terhadap ancaman atau serangan jaringan (Bustami & Bahri, 2020).

Tingkat kerentanan dan serangan pada setiap *website* tentu berbeda-beda, sehingga diperlukan pengujian celah keamanan pada *website*. Hanya dengan mengetahui celah keamanan sendiri tidak akan serta merta langsung meningkatkan keamanan pada aplikasi atau *website*. Perlu adanya penilaian risiko pada *website* terkait dengan mempertimbangkan faktor faktor yang ada sehingga dapat memberikan penjelasan yang lebih baik untuk mengamankan *website* (Elanda & Lintang Buana, 2020).

Pedoman untuk penilai risiko pada suatu *website* yang dapat dikatakan aman dari serangan *cyber* mengacu pada tiga aspek, yaitu *confidentially*, *integrity*, dan *availability* atau CIA TRIAD (gtslearning, 2014). Terdapat berbagai jenis serangan yang memanfaatkan celah keamanan pada suatu *website* dengan fokus penyerangan terhadap salah satu aspek CIA TRIAD atau keseluruhan aspek tersebut. Adapun serangan *cyber* yang biasa dilakukan pada aspek *confidentiality* yaitu Sniffing, cara kerja serangan *cyber* dengan metode *sniffing* yaitu penyerang akan melakukan penyadapan terhadap jaringan antara *client* dan *server website*

untuk mendapatkan informasi penting seperti *password user*, kredensial *login*, dan lainnya. Kemudian serangan *cyber* yang sering terjadi pada aspek kedua yaitu *integrity* adalah *Man in the Middle Attack*. Cara kerja *Man in the middle attack*, yaitu penyerang melakukan pembajakan terhadap *session request client* atau melakukan manipulasi data yang dikirim sehingga terjadilah perubahan integritas dari sebuah data. Selanjutnya serangan *cyber* yang sering terjadi pada aspek *availability* yaitu *Denial of Service* (DOS), cara kerja serangan *cyber* dengan metode DOS ini yaitu membanjiri *server website* dengan ribuan *request* hingga jutaan yang membuat *server* menjadi lambat hingga tidak berfungsi.

Untuk mencegah terjadi serangan *cyber*, dapat dilakukan *security testing* pada suatu *website*. Dalam melakukan *security testing* diharuskan menggunakan standarisasi dalam pengujiannya. Salah satu standarisasi yang sering digunakan, yaitu metode *Vulnerability Assessment and Penetration Testing* (VAPT). *Vulnerability assessment* adalah proses melakukan pemindaian sistem, perangkat lunak atau jaringan untuk mengetahui kelemahan dan celah yang ada di dalamnya. Sementara, *penetration testing* adalah langkah yang dilakukan setelah *vulnerability assessment*. *Penetration testing* mencoba untuk mengeksploitasi sistem untuk mengetahui kemungkinan eksploitasi dari celah keamanan yang ditemukan (Goel & Mehtre, 2015).

Dalam melakukan metode VAPT diperlukan penggunaan *software* keamanan dengan beragam pilihan *software* yang dapat digunakan sesuai dengan kebutuhan pengujiannya. Perbedaan dari setiap *software* keamanan berada pada fitur dan mekanisme yang digunakan untuk menemukan celah keamanan dengan memantau dan memindai lalu lintas jaringan serta sistem pada *website*. Terdapat beberapa *software* keamanan atau *tool* yang sering digunakan pada proses *security testing*, yaitu NMAP, Nessus, Nikto, Maltego, Burp Suite, OWASP ZAP, Acunetix, Wireshark, dan masih banyak lagi.

Berdasarkan informasi di atas, diperlukan solusi untuk mencegah serangan *cyber* terhadap *website* untuk menjaga data dan sistem yang berjalan didalamnya. Salah satu *website* yang memiliki fungsionalitas untuk memverifikasi data adalah *website* absensi praktikan dan asisten praktikum Universitas XYZ. *Website* tersebut berfungsi untuk memvalidasi data kehadiran mahasiswa dalam mengikuti

kegiatan praktikum, dikarenakan data absensi mahasiswa akan berpengaruh pada penilaian akhir semester. Maka dari itu, *website* harus dilindungi agar validasi data di dalamnya dapat berjalan dengan baik, oleh sebab itu perlu dilakukan implementasikan *vulnerability assessment* pada *website* absensi praktikan dan asisten praktikum Universitas XYZ untuk mencari celah kerentanannya. Kerentanan yang ditemukan akan dianalisis dan dilakukan mitigasi menggunakan metode VAPT. Pada penelitian ini menggunakan tiga *tools* yang akan membantu pemindaian celah keamanan pada *website* target, yaitu Nessus, Bupsuite, dan OWASP ZAP. Setelah dilakukan *vulnerability assessment* dan *penetration testing* pada *website* tersebut, diharapkan akan meminimalisir serangan *cyber* yang dapat merugikan pengguna *website*.

I.2 Perumusan Masalah

Adapun rumusan masalah yang mendasari penelitian ini diantaranya adalah:

a. Bagaimana analisis keamanan pada *website existing* absensi praktikan dan sistem praktikum Universitas XYZ menggunakan *tools* Nessus, Burp Suite, dan OWASP ZAP?
b. Bagaimana rekomendasi solusi dan tahapan mitigasi yang dapat diberikan pada *website* absensi praktikan dan sistem praktikum Universitas XYZ?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah sebelumnya, sehingga tujuan dari penelitian Tugas Akhir adalah sebagai berikut:

a. Hasil dan analisis dari pengujian celah keamanan pada *website existing* absensi praktikan dan sistem praktikum Universitas XYZ menggunakan *tools* Nessus, Burp Suite, dan OWASP ZAP.
b. Rekomendasi solusi dan tahapan mitigasi yang akan diberikan pada *website* absensi praktikan dan sistem praktikum Universitas XYZ mengenai hasil pengujian celah keamanan.

I.4 Batasan Penelitian

Agar penelitian tidak keluar dari ruang lingkupnya, pada penelitian ini diberikan beberapa batasan masalah diantaranya terbatas pada hal-hal berikut:

a. Objek penelitian ini akan terbatas pada *website* absensi praktikan dan asisten praktikum Universitas XYZ.
b. Penelitian ini akan menggunakan beberapa *automated tools scanning*, yaitu Nessus versi 10.5.0, Burp Suite *professional* versi 2022.8.2, dan OWASP ZAP versi 2.12.0. untuk melakukan pemindaian kerentanan terhadap *website* target.
c. Parameter yang diukur pada penelitian ini meliputi tingkat kerentanan dan solusi mitigasi yang diterapkan berdasarkan hasil pemindaian kerentanan.
d. Kerentanan dengan nilai risiko informasi, tidak dilakukan eksploitasi dan mitigasi lebih lanjut.
e. Penelitian ini terbatas pada tahap *vulnerability analysis* hingga tahap eksploitasi dan mitigasi. Apabila ditemukan kerentanan pada konfigurasi *server* dan kode sistem *website*, langkah mitigasi akan diambil dengan memberikan rekomendasi mitigasi.

I.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dengan adanya penelitian Tugas Akhir ini adalah sebagai berikut :

1. Bagi Fakultas XYZ Universitas XYZ, penelitian ini bermanfaat untuk mengetahui kerentanan-kerentanan yang ada pada *website* absensi praktikan dan sistem praktikum yang dapat digunakan sebagai bahan acuan serta pertimbangan dalam melakukan peningkatan di sistem *website*. Selain itu juga dengan penelitian ini akan meminimalisir potensi ancaman dan serangan yang akan terjadi dan bisa melakukan mitigasi sebelum berakibat fatal bagi sistem *website* tersebut.
2. Bagi peneliti yang bergerak di bidang sistem informasi pendidikan tinggi, penelitian ini dapat menjadi referensi dalam melakukan proses analisis celah kerentanan pada aplikasi berbasis *website* dan dapat memberikan informasi terkait *tools* yang digunakan yaitu Nessus, Burp Suite, dan OWASP ZAP.