BAB I PENDAHULUAN

I.1 Latar Belakang

Perkembangan dunia teknologi saat ini semakin pesat seiring dengan adanya kemudahan akses informasi melalui berbagai cara baik melalui aplikasi berbasis *mobile* ataupun *website*. Adapun informasi tersebut pada awalnya adalah sekumpulan fakta yang memberikan suatu gambaran ataupun bukti dari persoalan yang kemudian dikelola agar dapat diterima oleh pengguna (Umar et al., 2021). Informasi tentu diakses oleh banyak orang, maka keamanan dari informasi sangat penting agar hanya orang yang memiliki wewenang saja yang dapat mengakses data informasi tersebut. Jika data tersebut diakses oleh pihak yang tidak bertanggung jawab maka banyak pihak akan merasa dirugikan akan hal itu. Oleh karena itu keamanan informasi merupakan suatu hal yang harus dilindungi dari resiko serangan yang mungkin akan terjadi di masa yang akan datang (Shah & Mehtre, 2013).

Dengan kemudahan dalam mengakses informasi saat ini maka semakin tinggi juga serangan keamanan terhadap informasi pengguna dengan berbagai teknik ataupun metode ancaman yang menyerang *website*. Tingkat kerentanan dari tiap *website* tentu berbeda-beda, dengan perbedaan itu menyebabkan ancaman di setiap *website* memiliki berbagai faktor serangan yang berbeda. Umumnya dalam keamanan informasi terdapat tiga aspek yang perlu diperhatikan yaitu *Confidentiality*, *Integrity*, dan *Availability* (CIA).

Serangan pada *website* umumnya berdasarkan pada tiga aspek keamanan informasi tersebut, adapun serangan yang sering dilakukan untuk mengeksploitasi data pengguna yaitu serangan *Man in The Middle Attack* (MITM), *Denial of Services* (DOS), dan *SQL Injection*. Pada serangan *Man in the Middle* (MITM) berfokus dalam mengubah data yang dikirimkan ke suatu *website* dengan melakukan *intercept* lalu di teruskan ke alamat yang dituju, hal ini tentunya akan menyerang pengguna dari aspek *integrity* dimana seharusnya informasi diterima secara lengkap tanpa ada data yang diubah oleh pihak tertentu. Lalu serangan *Denial of Services* (DOS) menyerang pada aspek *availability* sehingga jika

pengguna mengakses suatu *website* maka *website* yang terkena serangan DOS mengakibatkan *server down* dan menjadi tidak dapat di akses. Serangan *SQL Injection* merupakan serangan yang cukup berbahaya jika terjadi dalam sistem *website*, serangan ini menyerang dalam tiga aspek yaitu *Confidentially*, *Integrity* dan *Availability*. Dengan serangan tersebut penyerang dapat melakukan serangan yang lebih berbahaya ke sistem seperti *backdoor.* Serangan tersebut membuat penyerang dapat mengakses *database website* sehingga dapat mengubah dan menghapus data yang menyebabkan terganggunya *server* dan infrastruktur *back-end website.*

Oleh karena itu diperlukan solusi untuk mengantisipasi serangan yang terjadi dengan dilakukannya *Security Testing* pada *website* sehingga dari pengujian tersebut dapat ditemukan kerentanan pada *website* lalu melakukan analisis untuk menentukan rekomendasi mitigasi kerentanan yang ditemukan agar dapat menutup celah keamanan sebagai bentuk mitigasi dan penanganan insiden dari serangan yang mungkin terjadi kedepannya.

Website Kerja Praktek dan Pengabdian Masyarakat merupakan salah satu *website* administrasi pada fakultas XYZ dimana portal ini berfungsi untuk mengelola data mahasiswa yang melakukan kegiatan kerja praktek maupun pengabdian masyarakat. Dengan adanya portal ini mahasiswa dan dosen menjadi lebih mudah dalam memilih topik, mencatat *logbook*, mengunggah laporan kegiatan serta memantau kemajuan penilaian kegiatan kerja praktek atau pengabdian masyarakat. Portal ini dibangun dengan *framework* sails.js yang berbasis bahasa javascript dan berjalan pada *Virtual Private Server* (VPS) milik fakultas xyz. Pada penelitian yang telah dilakukan sebelumnya telah dilakukan pengujian untuk menemukan kerentanan yang ada pada *website* ini namun kerentanan tersebut belum dilakukan mitigasi lebih lanjut sehingga diperlukan *security testing* kembali untuk menemukan kerentanan lebih mendalam dan rekomendasi mitigasi agar mengamankan data pengguna serta mengurangi resiko adanya serangan yang mengancam sistem *website*.

Dalam melakukan *security testing* diperlukan metode dalam pengujian, pada penelitian ini menggunakan metode *Vulnerability Assesment and Penetration Testing* (VAPT). Dengan menggunakan VAPT sebagai teknologi pertahanan siber, maka dapat menghapus kerentanan pada sistem dan mengurangi kemungkinan serangan siber (Goel & Mehtre, 2015). Hasil akhir dari metode ini adalah laporan kerentanan yang dapat menjadi dasar dalam menentukan rekomendasi mitigasi untuk menutup kerentanan yang ditemukan.

Vulnerability assesment adalah proses pemindaian sistem atau perangkat lunak atau jaringan untuk mengetahui kelemahan dan celah di dalamnya. *Penetration testing* adalah langkah berikutnya setelah *vulnerability assessment* (Goel & Mehtre, 2015). *Penetration Testing* adalah proses terstruktur untuk menguji basis komputasi organisasi yang meliputi perangkat keras, perangkat lunak, dan manusia. Proses ini mencakup analisis keseluruhan sistem komputasi organisasi untuk mencari kerentanan seperti konfigurasi sistem, perangkat lunak dan kesalahan perangkat keras, dan proses operasionalnya dengan tujuan untuk mengetahui kelemahan dari sistem tersebut. (Al Shebli & Beheshti, 2018).

Penelitian ini menerapkan teknik *penetration testing* dengan *grey box testing* yaitu penguji mengetahui sebagian informasi dari infrastruktur jaringan atau aplikasi yang akan diuji (Goel & Mehtre, 2015). Untuk membantu dalam menemukan kerentanan pada Kerja Praktek dan Pengabdian Masyarakat (KPPM) digunakan *tools* seperti Nmap, Maltego, Burp Suite, Nessus, dan Acunetix.

Berdasarkan permasalahan tersebut maka diperlukan solusi untuk mencegah dan mengamankan data mahasiswa serta dosen pada *website* Kerja Praktek dan Pengabdian Masyarakat di fakultas XYZ. *Security mitigation* adalah jawaban untuk permasalahan tersebut agar kerentanan dapat ditemukan lebih awal sehingga dapat dilakukan mitigasi untuk menutup celah keamanan yang ada dan menguji tingkat ketahanan keamanan pada *website* terhadap serangan dari kerentanan yang ditemukan.

I.2 Perumusan Masalah

Adapun rumusan masalah yang mendasari penelitian ini diantaranya adalah:

a. Bagaimana analisis keamanan eksisting pada *website* Kerja Praktek dan Pengabdian Masyarakat menggunakan *tools* Burp Suite, Nessus dan Acunetix?
b. Bagaimana implementasi *security mitigation* yang dapat diberikan pada *website* Kerja Praktek dan Pengabdian Masyarakat?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah, adapun tujuan penelitian yang akan dicapai adalah sebagai berikut:

a. Hasil analisis dari pengujian *keamanan* pada *web* Kerja Praktek dan Pengabdian Masyarakat menggunakan *tools* Burp Suite, Nessus dan Acunetix
b. Rekomendasi apa saja yang akan diberikan pada web Kerja Praktek dan Pengabdian Masyarakat dari pengujian celah keamanan yang telah dilakukan.

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. Penelitian ini dalam implementasinya akan menggunakan *tools Burp suite professional* versi 8.2, *Nessus* versi 8.15 dan Acunetix versi 15.3.23.
b. Objek penelitian ini terbatas pada *website* Kerja Praktek dan Pengabdian Masyarakat pada Universitas XYZ.
c. Parameter yang diukur pada penelitian ini adalah tingkat kerentanan serta solusi berdasarkan hasil *vulnerability scan* yang dihasilkan dengan *tools Burp Suite*, *Nessus* dan Acunetix
d. Kerentanan dengan tingkat *informational* tidak akan dilanjutkan ke tahap eksploitasi lebih lanjut
e. Penelitian ini terbatas dari *vulnerable detection* hingga tahap eksploitasi dan dilanjutkan ke tahap mitigasi, jika ditemukan kerentanan dari segi *server* maka langkah mitigasi yang dilakukan hanya sampai memberikan rekomendasi mitigasi

I.5 Manfaat Penelitian

Adapun manfaat yang didapat dari adanya penelitian ini adalah sebagai berikut

a. Bagi Fakultas xyz Universitas xyz, penelitian ini bermanfaat untuk mengetahui kerentanan-kerentanan yang ada pada portal akademik 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.
b. 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 Burp suite, Nessus dan Acunetix.

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, menjelaskan tentang hal yang melatarbelakangi pembuatan sebuah karya ilmiah ini. Bab ini membahas latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, serta sistematika penulisan.
2. Bab kedua, membahas mengenai literatur yang sesuai dengan permasalahan yang diangkat pada penelitian karya ilmiah, penelitian terdahulu yang memiliki keterkaitan dengan penelitian yang sekarang serta berisi teori-teori pendukung yang berkaitan dengan penelitian
3. Bab ketiga, membahas metodologi yang digunakan dalam penelitian, model konseptual yang diambil dalam merumuskan solusi dari penelitian yang diambil serta menjelaskan tentang alur penelitian yang akan dilakukan yang disusun dalam sistematika penelitian dari tahap awal hingga tahap akhir
4. Bab keempat, membahas mengenai instrument hardware dan software yang digunakan dalam implementasi penelitian ini, serta 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 berdasarkan literatur yang sudah ditetapkan pada penelitian serta memberikan rekomendasi dari hasil analisis.
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