BAB I PENDAHULUAN

I.1 Latar Belakang

Pada zaman sekarang ini, segala informasi harus memiliki akses yang lebih cepat untuk di infokan ke semua orang. Perusahaan maupun suatu organisasi menghadirkan layanan informasi secara *online* yang mana bisa lebih cepat diakses semua orang. Salah satu layanan informasi secara *online* yaitu adalah *Web*. *Web* merupakan suatu halaman yang mana didalamnya berisikan informasi penting suatu Perusahaan, perorangan maupun organisasi (Mendy, 2023). Dengan penggunaan *web* ini mempermudah perusaahan maupun organisasi untuk menjalankan bisnis mereka, meningkatkan citra dan kredibilitas, kemudahan dalam pembaruan informasi dan keunggulan kompetitif. Dengan manfaat yang banyak didapatkan melalui penggunaan *web*, ada kekurangan yang muncul dalam pemakaian *web* ini. Sering terjadi pembobolan atau mencuri data oleh orang yang tidak bertanggung jawab. Oleh sebab itu, akan muncul kerentanan terhadap *web* itu sendiri dan akan merugikan yang punya *web* tersebut.

Vulnerability merupakan kerentanan dalam sebuah sistem atau jaringan yang akan menyebabkan pihak yang tidak berwenang mendapatkan akses tanpa izin. Celah keamanan ini dapat timbul akibat pengelolaan keamanan yang kurang optimal dari pihak pengembang situs atau adanya bug yang belum terdeteksi dan diperbaiki. Apabila kerentanan pada situs tidak segera ditangani, maka risiko terkena serangan siber meningkat, yang dapat menyebabkan kerugian bagi perusahaan atau organisasi.

Berdasarkan hasil monitoring dari badan siber dan sandi negara, terdapat dugaan kasus peretasan situs di Indonesia pada bulan Agustus 2023 (Sandi, 2023).

Gambar I. 1 Data Monitoring

Berdasarkan gambar 1.1 diatas, terlihat bahwa telah terjadi 19 kasus peretasan pada situs-situs di Indonesia dalam periode tertentu. Grafik tersebut menunjukkan pola distribusi peretasan yang cukup konsisten hampir setiap hari, mengindikasikan adanya peretasan yang berlangsung terus-menerus. Kondisi ini menggarisbawahi adanya kerentanan yang cukup tinggi dalam sistem keamanan situs di Indonesia, serta perlunya upaya lebih lanjut untuk meningkatkan keamanan demi mencegah kejadian serupa di masa mendatang (Sandi, 2023).

Oleh karena itu untuk mencegah terjadi nya masalah diatas yaitu dengan memberikan solusi testing keamaan *web* itu sendiri. Dengan pengujian tersebut, kerentanan pada *web* dapat diidentifikasi, kemudian dilakukan analisis untuk menentukan rekomendasi mitigasi terhadap kerentanan yang ditemukan. Langkah ini bertujuan untuk menutup celah keamanan sebagai bentuk mitigasi dan penanganan insiden, guna mencegah potensi serangan di masa mendatang. Dalam melakukan *testing* pada *web* untuk melihat keamanannya maka diperlukan metode *Vulnerability Assessment and Penetration testing* (VAPT). Dengan menggunakan VAPT yang dapat mencari kerentanan pada sistem dan mengurangi serangan siber (Kit Arvin R. Cadiente, 2020). Setelah melakukan pengujian, akan diperoleh laporan mengenai tingkat kerentanan pada *web* tersebut, yang kemudian menjadi dasar untuk menentukan langkah mitigasi dalam menutup kerentanan yang teridentifikasi.

Metode VAPT ini akan diujikan pada *web* praktikum Fakultas Rekayasa Industri untuk mengetahui bagaimana keamanan dari data yang disimpan dalam *web*

tersebut, untuk menemukan dimana letak kerentanan *web* praktikum Fakultas Rekayasa Industri itu sendiri. Setelah menemukan masalahnya, mitigasi dapat dilakukan untuk menutup celah keamanan yang ada dan menguji ketahanan keamanan *web*site terhadap serangan terkait kerentanan yang telah ditemukan.

Web telah menjadi alat penting bagi perusahaan dan organisasi untuk menyampaikan informasi dengan cepat, meski rentan terhadap ancaman seperti pembobolan data akibat celah keamanan. Data dari BSSN menunjukkan tingginya kasus peretasan di Indonesia, menekankan perlunya langkah pencegahan. VAPT menjadi solusi efektif untuk mengidentifikasi dan menutup celah keamanan, sehingga risiko serangan dapat diminimalkan. Pengujian ini akan diterapkan pada *web* praktikum Fakultas Rekayasa Industri untuk menganalisis kerentanan, memberikan rekomendasi mitigasi, dan meningkatkan ketahanan sistem terhadap ancaman siber.

I.2 Perumusan Masalah

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

1. Bagaimana analisis dari kondisi eksisting *web* praktikum Fakultas Rekayasa Industri dengan cara VAPT*?*
2. Bagaimana rekomendasi yang dapat dilakukan untuk tahap mitigasi pada *web* praktikum Fakultas Rekayasa Industri?

I.3 Tujuan Penelitian

Adapun tujuan Penelitian ini bertujuan untuk:

1. Hasil analisis dari kondisi eksisting *web* praktikum Fakultas Rekayasa Industri dengan cara VAPT
2. Rekomendasi yang dapat dilakukan untuk tahap mitigasi *web* praktikum Fakultas Rekayasa Industri

I.4 Batasan Penelitian

Batasan dari penelitian ini adalah sebagai berikut:

1. Penelitian ini hanya dilakukan kepada *web* praktikum Fakultas Rekayasa Industri.
2. Penelitian ini akan menggunakan satu *tools network* scan yaitu *NMAP*, *tools automated scanning* yaitu Nessus,OWASP ZAP, dan Nikto.
3. Penelitian ini dilakukan sampai tahap mitigasi, dan jika terdapat *vulnerability* yang belum dapat diperbaiki, maka akan disarankan sebagai rekomendasi untuk perbaikan sistem.
4. Kategori kerentanan yang diprioritaskan untuk diberikan rekomendasi mitigasi sistem yaitu *Critical*, *High*, *Medium dan low*.

I.5 Manfaat Penelitian

Manfaat penelitian ini adalah sebagai berikut:

1. Penelitian ini bermanfaat bagi Fakultas Rekayasa Industri untuk memahami tingkat keamanan *web* yang digunakan, sehingga dapat menjadi bahan evaluasi dalam pengembangan dan pengelolaan *web* di masa depan.
2. Bermanfaat bagi penelitian lain yang bergerak pada bidang keamanan sistem dan menjadi rekomendasi dalam pemilihan *tools* untuk VAPT.
3. Hasil penelitian ini dapat menjadi dasar kolaborasi antara universitas dan industri untuk pengembangan solusi praktis, seperti layanan pengujian keamanan *web* berbasis akademik.