BAB I
PENDAHULUAN

1.1 Latar Belakang

Sebuah organisasi yang berkembang membutuhkan teknologi informasi untuk mendukung aktivitas operasionalnya[1]. PT. Sekar Laut Tbk. adalah perusahaan yang bergerak di industri, pertanian, perdagangan, dan pembangunan, khususnya di sektor manufaktur makanan dan minuman. PT. Sekar Laut Tbk menggunakan situs *web* sebagai teknologi sistem informasi perusahaan yang menyimpan banyak data penting, termasuk data karyawan, produksi, investor, dan pembayaran. Namun, dengan adanya teknologi tersebut, keamanan menjadi aspek penting yang harus diwaspadai oleh setiap pihak yang memiliki sistem terpusat. Pembobolan, manipulasi, atau kehilangan data dapat terjadi jika hacker berniat mencuri data sensitif dari sebuah organisasi[1]. Perkembangan teknologi yang pesat sering kali membuat developer terlewat dalam melakukan pengujian pada aplikasi yang mereka kembangkan. Pengujian adalah proses krusial dalam pengembangan perangkat lunak berkualitas tinggi, karena beberapa kesalahan yang dianggap sepele bisa menjadi risiko besar. Kesalahan tersebut dapat menjadi celah (*vulnerability*) yang dimanfaatkan oleh attacker untuk mencuri informasi melalui serangan terhadap aplikasi.[2]

Penetration testing adalah serangkaian metode dan prosedur yang dilakukan untuk menguji atau melindungi keamanan suatu organisasi. Pengujian ini membantu mengidentifikasi kerentanan yang ada dalam organisasi dan memeriksa apakah penyerang dapat mengeksploitasi kerentanan tersebut untuk mendapatkan akses secara ilegal [3].

Penetration testing pada website dapat dilakukan dengan berbagai metode, salah satunya menggunakan parameter keamanan yang dibuat oleh organisasi OWASP. OWASP Top 10 adalah daftar yang disusun oleh komunitas OWASP yang mencakup sepuluh kerentanan utama yang dapat mengancam keamanan sebuah *website*. Daftar ini bertujuan untuk meningkatkan kesadaran individu dan organisasi tentang keamanan perangkat lunak,

sehingga mereka dapat membuat keputusan yang tepat mengenai risiko keamanan[3]. Penelitian sebelumnya dilakukan oleh (Yudiana et al., 2021) analisis kualitas keamanan sistem informasi e-office berbasis website di STMIK ROSMA menggunakan OWASP ZAP, pengujian yang dilakukan dalam penelitian ini menunjukkan bahwa sistem informasi e-office memiliki 13 kerentanan. Berdasarkan OWASP TOP 10, ditemukan 4 kerentanan utama, yaitu *Sensitive Data Exposure, Security Misconfiguration, Cross-Site Scripting, dan Insecure Deserialization*.[4]

Menurut penelitihan Muh. Amirul Mu'min tahun 2022, Analisis Keamanan Sistem Informasi Akademik Menggunakan *Open Web Application Security Project Framework.* Ditemukan 12 kerentanan menggunakan OWASP Zap, dengan empat di antaranya berada pada tingkat kerentanan sedang, enam pada tingkat rendah, dan dua pada tingkat informasional. Hasil penelitian ini sesuai dengan tujuan yang diharapkan. Dari empat tahap pengujian yang menggunakan beberapa alat, *website* ini masih tergolong cukup aman dari serangan *hacker*.[5]

Menurut penelitihan Muhammad Rafi Ramdani tahun 2022, *Penetration Testing* pada *Website* Universitas Singaperbangsa Karawang Menggunakan *Open Web Application Security Project* (OWASP). Berdasarkan daftar 10 kerentanan OWASP Top-10 2021, *website* Universitas Singaperbangsa Karawang dengan domain journal.unsika.ac.id tidak memiliki celah keamanan berisiko tinggi. *Website* ini hanya memiliki kerentanan pada celah *broken access control* yang termasuk dalam daftar OWASP, dan celah tersebut hanya menampilkan direktori pada *website* yang tidak terlalu sensitif, yaitu hanya menunjukkan informasi tentang *plugins* yang digunakan.[6]

Dalam penelitihan ini, peneliti menggunakan tools OWASP ZAP sebagai penetrations testing untuk menguji kerentanan *website* PT Sekar Laut TBK. dengan menggunakan *standart* OWASP Top 10. Hasil *Reporting* dapat di deteksi dan dianalisa serangan *cyber* yang memungkinkan bisa dilakukan *attacker* pada kerentanan yang ditemukan. Hasil tersebut diharapkan dapat

memberikan informasi terkait celah-celah keamanan dan dapat menjadi evaluasi bagi instasi lain dalam membantu memperkuat keamanan *website*.

1.2 Rumusan Masalah

Berdasarkan uraian masalah pada bagian latar belakang, rumusan masalah pada penelitian ini yaitu:

a. Bagaimana menganalisis *website* PT. Sekar Laut Tbk. dengan menggunakan *standart* OWASP Top 10?

b. Bagaimana hasil *report* metode Penetration Testing yang dapat memberikan informasi kepada *developer website* PT. Sekar Laut Tbk?

1.3 Tujuan Penelitian

Tujuan yang diharapkan dari penelitihan ini adalah:

a. Memberikan hasil analisa terkait keamanan *website* PT. Sekar Laut Tbk. dengan standart OWASP Top 10.

b. Diharapkan dapat menambah tingkat keamanan dari hasil *report* dengan menggunakan metode penetration testing kepada *developer website* PT. Sekar Laut Tbk.

1.4 Batasan Masalah

Untuk menghindari penyelesaian masalah yang tidak sesuai dengan rumusan masalah dan juga agar tugas akhir ini mudah dipahami pembaca, maka peneliti membuat batasan permasalahan sebagai berikut:

a. Penelitian pengunakan Metode penetration testing dengan beberapa pengujian sesuai kerentanan yang ditemukan.

b. Objek penelitian adalah PT. Sekar Laut Tbk.

c. Pendeteksian celah keamanan menggunakan *tools* OWASP ZAP dan tidak melakukan perbandingan atau menggunakan *tools* yang lain

d. Standart kerentanan yang digunakan metode mengacu pada standart OWASP Top 10.

e. Hasil akhir penelitian berupa analisis dan *report* dari *tools* yang digunakan