BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin pesat membawa dampak signifikan bagi peradaban manusia. Era revolusi industri 4.0 telah menciptakan berbagai inovasi yang tidak hanya memberikan manfaat besar, tetapi juga mempercepat dan mempermudah berbagai aspek kehidupan, terutama dalam dunia industri. Dalam upaya menuju industri yang lebih maju, manusia terus memanfaatkan kemajuan teknologi, salah satunya melalui pemanfaatan website. Saat ini penggunaan website telah berkembang luas di berbagai bidang, mulai dari perusahaan, pendidikan, kesehatan, hingga pemerintahan.

Salah satu inovasi yang berperan penting dalam digitalisasi dunia industri adalah pemanfaatan sistem berbasis web, seperti *Enterprise Resource Planning* (ERP). ERP merupakan pendorong utama dalam transformasi digital dengan menyediakan platform integrasi untuk mengelola berbagai proses bisnis. Dengan penerapan sistem ERP, perusahaan dapat melakukan automasi serta menyederhanakan berbagai tugas penting, termasuk keuangan, rantai pasokan, dan manajemen sumber daya manusia [1]. Kemajuan teknologi informasi ini telah membuka babak baru dalam dunia bisnis [2]. Namun, seiring dengan meningkatnya ketergantungan terhadap teknologi digital, risiko keamanan siber juga semakin besar.

Menurut Dihni [3] Indonesia menempati peringkat pertama dengan kasus serangan *ransomware* di Asia Tenggara pada periode Januari–September 2020 dengan total 1,3 juta kasus. Temuan ini sejalan dengan laporan tahunan BSSN pada 2021 [4], yang mencatat bahwa Indonesia berada di peringkat pertama dalam 10 besar sumber anomali serta 10 besar destinasi anomali di seluruh dunia, dengan lebih dari 190 juta sumber anomali dan lebih dari 1 miliar anomali sebagai tujuan serangan. Anomali trafik tertinggi tercatat pada Desember 2021. Fenomena ini dapat mengindikasikan berbagai jenis ancaman siber, seperti serangan *Denial of Service* (DoS), aktivitas *malware*, dan upaya akses tidak sah.

Menurut Rahakbauw dan Batubara [5] serangan siber yang berkepanjangan dapat menyebabkan kerusakan yang berdampak luas pada proses bisnis, menciptakan ketidakpastian ekonomi, serta menghambat pertumbuhan industri. Misalnya, serangan siber terhadap sistem keuangan dapat mengganggu operasional perbankan,

transaksi keuangan, dan stabilitas pasar. Selain itu, berdasarkan laporan yang dikutip oleh Dihni dalam Databoks Katadata [6], total kerugian akibat kejahatan siber di Indonesia mencapai Rp3,88 triliun selama periode Januari-September 2021, dengan mayoritas kasus berupa penipuan. Ancaman serangan siber tidak hanya terjadi di Indonesia, tetapi juga menjadi isu global. Menurut laporan yang dikutip oleh Petrosyan dalam Statista [7], sepanjang tahun 2022, kerugian finansial akibat serangan siber di Amerika Serikat mencapai tingkat yang signifikan. Hampir seperempat perusahaan yang terdampak mengalami kerugian antara 50.000 hingga 99.999 dolar AS. Selain itu, 22% perusahaan melaporkan kehilangan antara 100.000 hingga 499.999 dolar AS, sementara 4% lainnya mengalami kerugian lebih dari satu juta dolar AS akibat serangan siber. Data ini menunjukkan bahwa serangan siber merupakan ancaman serius yang tidak dapat diremehkan dampaknya.

Hingga saat ini, serangan siber masih terus terjadi, di mana korban dari kejahatan siber tidak hanya individu, tetapi juga perusahaan. Bahkan, perusahaan dengan tingkat keamanan tinggi, seperti perbankan dan lembaga keuangan lainnya, tetap berisiko menjadi target serangan siber. Jika maraknya serangan siber tidak ditangani dengan tepat, dampaknya dapat semakin fatal dan berpotensi mengganggu stabilitas ekonomi serta operasional perusahaan. Untuk mengatasi ancaman ini, diperlukan berbagai langkah pencegahan, seperti meningkatkan edukasi masyarakat mengenai keamanan siber, menerapkan kebijakan keamanan yang ketat, serta melakukan pengujian penetrasi terhadap sistem informasi perusahaan guna mengidentifikasi dan menutup celah kerentanan sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab.

Pengujian keamanan, atau yang lebih dikenal sebagai *penetration testing* didefinisikan sebagai serangkaian aktivitas yang dilakukan untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan dalam suatu sistem [8]. Dalam praktiknya, *penetration testing* dilakukan dengan memeriksa aspek fungsional sistem, untuk mengetahui seberapa besar tingkat kerentanan sistem terhadap serangan keamanan, intrusi jaringan, serta melihat mekanisme pertahanannya dalam menangkal sebuah serangan [9]. Agar *penetration testing* berjalan efektif dan aman, pengujian harus dilakukan secara terstruktur, sistematis, dan legal. Penggunaan metode yang tepat dapat mengurangi risiko yang tidak diinginkan serta memastikan hasil pengujian yang terarah. Oleh karena itu, pemilihan model *penetration testing* menjadi aspek yang krusial dalam mengevaluasi keamanan sistem.

Penetration Testing Execution Standard (PTES) adalah standar yang dirancang untuk memberikan panduan umum bagi perusahaan dan penyedia layanan keamanan dalam melakukan *penetration testing* [10]. Metode PTES adalah salah satu metode *penetration testing* yang mudah digunakan [11] [12]. Hal ini dibuktikan oleh penelitian yang dilakukan Syarif dan Jatmiko [12] yang menyebut bahwa metode OWASP dan PTES lebih memiliki sistem pelaporan berbasis level-level yang mudah dipahami oleh user.

Selian PTES, Open Web Application Security Project (OWASP) Top 10 menjadi salah satu referensi utama dalam pengujian keamanan aplikasi web. Menurut Riberu dsn Emanuel [13], OWASP Top 10 merupakan sumber yang diakui secara luas dan terpercaya di bidang keamanan aplikasi web, yang berfungsi sebagai panduan praktis bagi pengembang, profesional keamanan, dan organisasi untuk memprioritaskan dan mengatasi kerentanan ini secara efektif. Pada OWASP Top 10 2021 [14], daftar 10 kerentanan teratas antara lain meliputi *Broken Access Control*, *Cryptographic Failures*, *Injection*, dan lain sebagainya. Beberapa penelitian menyebut bahwa OWASP Top 10 terbukti efektif dijadikan sebagai standard keamanan untuk melakukan *penetration testing* [15] [16].

Berdasarkan permasalahan yang telah diuraikan, serta temuan dari penelitian terdahulu, penelitian ini bertujuan untuk mengidentifikasi kerentranan dan memberikan rekomendasi keamanan aplikasi ERP perusahaan dalam mengurangi risiko eksploitasi dan meningkatkan ketahanan sistem. Untuk mencapai tujuan tersebut, penelitian ini akan melakukan pengujian keamanan pada website ERP menggunakan teknik *penetration testing* dengan metode PTES berdasarkan OWASP Top 10 sebagai kategorisasi kerentanan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, terdapat beberapa permasalahan yang akan dibahas dalam penelitian ini adalah sebagai berikut :

1. Bagaimana penerapan pengujian keamanan pada website ERP PT. XYZ yang dapat diakses oleh pengguna dengan *role* SPV Marketing menggunakan metode PTES berdasarkan OWASP Top 10?
2. Apa saja kerentanan yang ditemukan dalam website ERP PT. XYZ yang dapat diakses oleh pengguna dengan *role* SPV Marketing berdasarkan hasil pengujian keamanan berdasarkan OWASP Top 10?

1.3 Tujuan Penelitian

Berdasarkan uraian rumusan masalah diatas, maka tujuan yang ingin dicapai penulis dari penelitian ini adalah sebagai berikut :

1. Menerapkan pengujian keamanan pada website ERP PT. XYZ yang dapat diakses oleh pengguna dengan *role* SPV Marketing menggunakan metode PTES berdasarkan daftar kerentanan OWASP Top 10.
2. Mengidentifikasi dan menganalisis kerentanan yang ditemukan dalam website ERP PT. XYZ yang dapat diakses oleh pengguna dengan *role* SPV Marketing berdasarkan hasil pengujian keamanan yang mengacu pada OWASP Top 10.

1.4 Manfaat Penelitian

Berdasarkan tujuan penelitian yang telah dijelaskan, penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Memberikan kontribusi dalam pengembangan ilmu pengetahuan di bidang keamanan sistem informasi, khususnya dalam penerapan metode *penetration testing* menggunakan PTES dan referensi OWASP Top 10.
2. Menambah literatur ilmiah mengenai analisis kerentanan pada sistem ERP berbasis web dengan pendekatan standar keamanan terkini.
3. Menjadi referensi akademik bagi penelitian selanjutnya yang ingin mengkaji efektivitas pengujian keamanan dengan kombinasi pendekatan PTES dan OWASP Top 10.

1.5 Batasan Penelitian

Dalam peneltian ini, ada beberapa batasan masalah yang perlu diperhatikan adalah sebagai berikut:

1. Lingkungan pengujian terbatas pada *staging*/*testing environment*, sehingga tidak menganalisis risiko keamanan di sistem produksi.
2. Penelitian ini hanya berfokus pada pengujian keamanan aplikasi website, tidak mencakup pengujian keamanan jaringan atau infrastruktur server.
3. Eksploitasi kerentanan dilakukan pada kerentanan dengan level *high*, *medium*, dan *low* berdasarkan hasil pemindaian OWASP ZAP.
4. Identifikasi ancaman pada *threat modeling* dilakukan pada jenis ancaman *human* berdasarkan ISO 27005:2022.