# BAB I PENDAHULUAN

## I.1 Latar Belakang

Pentingnya evaluasi keamanan sistem informasi semakin mendesak mengingat eskalasi serangan siber yang telah terjadi pada tahun 2022. Menurut artikel Surfsjark, Indonesia merupakan negara dengan penduduk 275 juta jiwa per Juni 2022 dan merupakan salah satu negara dengan jumlah pengguna internet terbesar di dunia. Menurut global data breach statistics, Indonesia menempati peringkat ke 3 dunia dengan kasus kebocoran data tertinggi (Dancor, 2023). Dalam enam bulan pertama pelaku peretasan siber melakukan aksinya di Asia Tenggara pada website company sebanyak lebih dari 11,2 juta kali. Indonesia menjadi salah satu negara dengan serangan terbanyak yaitu (5 juta serangan) disusul dengan negara Vietnam (2 juta serangan) dan Thailand (1,5 juta serangan) (bumialumni, 2022), hal tersebut menandakan tingginya risiko yang harus diatasi. Kasus serangan siber yang meningkat signifikan membuka peluang bagi kebocoran data dan akses yang tidak legal, mengancam operasional dan reputasi perusahaan.

Penting untuk digaris bawahi bahwa serangan siber tidak hanya mencakup ancaman terhadap keamanan data, tetapi juga dapat mengganggu kelancaran operasional dan merusak reputasi perusahaan (Agustinus Mario Damar, 2023). Keberlanjutan operasional perusahaan dan pelayanannya kepada pelanggan sangat tergantung pada ketahanan sistem informasi mereka terhadap ancaman siber.

Lebih lanjut, situasi ini semakin memperoleh urgensi mengingat perusahaan di Indonesia merupakan tulang punggung ekonomi yang berperan sebagai penggerak pertumbuhan ekonomi, membuka lapangan pekerjaan, dan memberi pelayanan kepada pelanggan (Fanny Fajarianti, 2023). Dengan mengidentifikasi dan mengatasi potensi kerentanan keamanan, diharapkan perusahaan dapat memperkuat pertahanan mereka dan memberikan contoh bagi instansi maupun perusahaan lainnya.

Salah satu platform yang memiliki peran dalam memberikan pelayanan di bidang penjualan barang dan distribusi, PT. XYZ (Abc) mempunyai sistem informasi berupa website. Pada sistem informasi tersebut memiliki beberapa fitur seperti halaman profil, fitur belanja untuk berbelanja pada *website* tersebut, fitur

*career* untuk membuka rekrutment pegawai, E-Commerce yang terhubung dengan platform Shopee dan Tokopedia. Di tengah pemberlakuan sistem informasi, seperti *website* Abc sebagai sarana interaksi dengan pelanggan, keamanan sistem informasi menjadi krusial untuk menjaga kepercayaan publik dan integritas data yang dimiliki oleh perusahaan. Jika terjadi peretasan pada *website* dan hal yang tidak diinginkan seperti kebocoran data pelanggan yang mengakibatkan ketidakpercayaan untuk melakukan transaksi dengan perusahaan, maka hal tersebut dapat merugikan baik bagi pihak pelanggan maupun pihak perusahaan.

Menurut data Statista menunjukkan, Indonesia menjadi negara dengan pengguna rokok elektrik atau biasa dikenal dengan vape terbanyak di dunia (Cindy Mutia Annur, 2023). Website Abc menjadi media penting yang menghubungkan perusahaan dengan pelanggan maupun pengguna yang memiliki minat membeli produk Abc. Namun, potensi serangan siber pada website ini menimbulkan risiko besar terhadap kerahasiaan dan integritas data. Sebelumnya website Abc pernah menjadi sasaran hacker yang mencoba masuk pada bagian admin website dan berhasil menemukan celah yang dimiliki pada website Abc. Oleh karena itu, analisis keamanan yang menyeluruh dan sistematis menjadi suatu kebutuhan yang penting untuk mengurangi resiko keamanan dan kebocoran data pada website.

Penelitian ini bertujuan untuk mencari kerentanan pada website tersebut dengan menerapkan metode penetration testing, yang merupakan pendekatan praktis dan efektif dalam mengidentifikasi dan mengevaluasi kerentanan keamanan suatu sistem. Penggunaan Open Web Application Security Project (OWASP) Top-10 2021 sebagai alat utama (Riandhanu, 2022) dalam penelitian ini dapat memberikan gambaran yang komprehensif tentang keamanan website Abc. Penelitian ini juga relevan dengan kebutuhan mendesak untuk meningkatkan literasi keamanan siber di lingkungan perusahaan. Dengan memahami kerentanan dan resiko yang mungkin dihadapi, perusahaan dapat memperkuat kapasitas internal mereka dalam melindungi informasi yang mereka kelola dan memberikan layanan yang andal kepada pelanggan (Agustinus Mario Damar, 2023).

Melalui tahapan identifikasi website, penggunaan metode OWASP Top-10 2021, serta pengujian penetration testing menggunakan pengujian blackbox testing (Fierza & Erlangga, 2021) penelitian ini diharapkan dapat memberikan pemahaman

mendalam tentang keamanan sistem informasi pada website Abc. Hasil analisis kerentanan yang dihasilkan nantinya dapat memberikan dasar untuk rekomendasi perbaikan yang tepat dan praktis, serta membantu pihak terkait dalam mengurangi resiko serangan siber dan melindungi data rahasia yang dimiliki oleh perusahaan.

Pada akhirnya, kesimpulan dari penelitian ini akan memberikan gambaran menyeluruh serta rekomendasi perbaikan tentang keamanan sistem informasi pada website Abc dan dapat menjadi panduan bagi pihak serupa yang berkomitmen untuk meningkatkan keamanan siber mereka.

## I.2 Rumusan Masalah

Dari permasalahan pada latar belakang di atas dapat di ambil kesimpulan sebagai berikut:

1. Apa saja macam kerentanan keamanan sistem informasi pada *website* abc.co.id berdasarkan OWASP Top 10 2021?
2. Bagaimana tingkat prioritas perbaikan keamanan sistem informasi *website* ABC terkait OWASP Top 10 setelah dilakukan *penetration testing*?
3. Apa saja rekomendasi perbaikan yang harus dilakukan untuk meningkatkan keamanan sistem informasi pada perusahaan?

## I.3 Tujuan dan Manfaat

Adapun tujuan dan manfaat dari dilakukannya penelitian ini:

1. Menganalisis tingkat kerentanan keamanan sistem informasi *website* abc.co.id.
2. Mengevaluasi tingkat prioritas perbaikan keamanan sistem informasi pada *website* abc.co.id.
3. Memberikan rekomendasi perbaikan untuk mengatasi potensi kerentanan terhadap *website* abc.co.id.

## I.4 Batasan Masalah

Supaya penelitian ini dapat berjalan dengan optimal maka dapat dirumuskan beberapa batasan sebagai berikut:

1. Pengujian hanya dilakukan pada aplikasi berbasis *website* pada abc.co.id.

2. Pengujian menggunakan metode *penetration testing* dengan OWASP Top-10 2021 dan berfokus pada sepuluh kerentanan utama yang diidentifikasi oleh OWASP.
3. Analisis dan rekomendasi perbaikan dari hasil pengujian dilakukan berdasarkan OWASP Top 10.