

BAB I

PENDAHULUAN

1.1 Latar Belakang

Era globalisasi yang semakin pesat saat ini seiring dengan perkembangan teknologi informasi yang selalu digunakan oleh Masyarakat memiliki peran penting sebagai peningkat kualitas hidup untuk membantu aktivitas sehari-hari. Menurut data dari internet *live stats*, pada saat ini pengguna internet telah mencapai lebih 5 miliar pengguna [1]. Era yang serba canggih ini menuntut banyaknya pertumbuhan dari sekian banyak bidang Teknologi Informasi (IT). Sudah banyak sektor bisnis yang memanfaatkan TI sebagai pengembangan bisnisnya, seperti pada bidang telekomunikasi, transportasi, pendidikan, kesehatan, perbankan, serta perdagangan.[2]. Perkembangan teknologi yang sudah semakin canggih dan semakin mudah diakses kapanpun dan dimanapun, memberikan dampak positif ke sektor perdagangan. Di Indonesia saat ini ada banyak sekali *e-commerce* sebagai media jual beli secara *online*.

Perdagangan elektronik atau *e-commerce* di Indonesia adalah kegiatan mendistribusikan, menjual, membeli dan memperdagangkan barang (barang dan jasa) dengan menggunakan jaringan komunikasi seperti internet, televisi atau jaringan komputer lainnya. Penggunaan *e-commerce* saat ini berkembang pesat seiring dengan pergeseran perilaku konsumen, dengan semakin banyaknya orang yang melakukan pembelian secara *online*. Perubahan pola perilaku belanja ini juga ditunjukkan dengan volume transaksi *e-commerce* yang meningkat.[3] Menurut laporan terbaru *We Are Social*, sekitar 178,9 juta orang Indonesia telah terlibat dalam belanja online dari awal tahun 2022 hingga akhir tahun 2023, menunjukkan pertumbuhan sebesar 12,8% dari tahun ke tahun. Hal ini juga didukung oleh perkiraan belanja *online* penduduk Indonesia yang mencapai US\$55,97 juta atau sekitar Rp 851 triliun pada tahun yang sama.[4] *E-commerce* memberikan banyak manfaat bagi pelaku bisnis dan konsumen karena memberikan kemudahan interaksi tanpa batasan tempat, jarak dan waktu.

Namun, dengan meningkatnya keuntungan, maka resiko keamanan akan semakin meningkat. Hal ini dibuktikan dengan masuknya Indonesia ke dalam peringkat 21 kategori keamanan siber terburuk di dunia. Sekecil apa pun skala *cyber-attack* pasti akan tetap merugikan pihak yang terkena serangan tersebut jika tidak berhati-hati. [5] Keamanan dalam melakukan berbelanja online merupakan hal yang sangat utama dan penting dalam *e-commerce*. Keamanan adalah kemampuan toko online dalam melakukan pengontrolan dan penjagaan keamanan atas transaksi data. Keamanan yang diharapkan konsumen yaitu privasi identitas konsumen, keamanan transaksi *online*, tidak menyalah gunakan data konsumen, dan bukti pengiriman barang.[6]

Jika keamanan dalam *e-commerce* sangat tinggi, maka semakin percaya konsumen untuk melakukan pembelian di toko *online* tersebut. Dalam melakukan pembelian *online*, keamanan merupakan hal yang sangat diperhatikan, karena keamanan berupa data pribadi seperti nama, alamat, nomor telepon, dan informasi keuangan bisa dengan mudah dicuri atau disalah gunakann oleh pihak yang tidak bertanggung jawab. Ancaman keamanan data pribadi pada pengguna *e-commerce* sangatlah beragam, termasuk serangan *SQL Injection*, *XSS*, dan pencurian identitas.[7] Tersebar nya data informasi konsumen merupakan hal yang fatal dalam suatu perusahaan *e-commerce*. Kenyamanan konsumen menjadi memudar jika privasi konsumen tersebut tidak bisa dijaga dengan baik. Keamanan dalam transaksi *online* perlu diantisipasi karena banyak kasus pengembalian uang atau *refund* tidak dilakukan dengan baik, bahkan uang *refund* tersebut tidak masuk ke rekening konsumen.[8]

Dari permasalahan yang muncul, maka diperlukan sebuah metode yang mampu menganalisis, mensintesis, dan mengekstrak data menjadi informasi yang bermanfaat. Mengandalkan data saja tidak cukup, sehingga analisis keamanan data perlu dilakukan untuk mengungkap potensi yang ada. Untuk mengantisipasi risiko yang berhubungan dengan keamanan *website e-commerce*, di perlukan sistem analisis untuk menganalisis perkembangan keamanan *website e-commerce*.

Berdasarkan uraian di atas maka peneliti berkeinginan untuk melakukan penelitian mengenai keamanan *website* untuk mengetahui sejauh mana tingkat

keamanannya. Oleh karena itu, peneliti tertarik untuk melakukan penelitian dengan judul **Analisis Penerapan Metode *Information System Security Assessment Framework* (ISSAF) Untuk Uji Penetrasi Kualitas Keamanan Website E-Commerce**. Penelitian ini akan menggunakan metode *Penetration Testing* berjenis *Information System Security Assessment Framework* (ISSAF) melakukan pengujian terhadap *website e-commerce* untuk mengukur sejauh mana tingkat keamanan yang dimiliki oleh *website e-commerce*.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka permasalahan yang dapat dirumuskan adalah sebagai berikut:

1. Bagaimana menerapkan metode *information system security assessment framework* (ISSAF) untuk uji penetrasi keamanan *website e-commerce*?
2. Apakah hasil uji keamanan *website e-commerce* menggunakan metode *information system security assessment framework* (ISSAF)?

1.3 Tujuan Penelitian

Berikut tujuan penelitian ini berdasarkan rumusan masalah yang telah dikembangkan:

1. Mengetahui penerapan metode *information system security assessment framework* (ISSAF) untuk uji penetrasi keamanan *website e-commerce*.
2. Mengetahui hasil pengujian keamanan *website e-commerce* menggunakan metode *information system security assessment framework* (ISSAF).

1.4 Batasan Penelitian

Berdasarkan pengamatan yang di lihat oleh peneliti, maka disini peneliti akan membatasi masalah yang akan di bahas, yaitu:

1. Penelitian ini melakukan analisis kualitas keamanan *website* terhadap *website e-commerce* pada domain Tokopedia.com, Lazada.co.id, dan Blibli.com.
2. Metodologi yang digunakan adalah *Penetration Testing* berjenis *Information System Security Assessment Framework* (ISSAF)

3. Analisis kualitas keamanan dilakukan berdasarkan tahapan *Fase Planning and preparation*, *Fase assessment* dan *Fase reporting*.
4. Analisa penetrasi yang dilakukan mencakup pengujian pada *Information gathering*, *Network mapping*, *Vulnerability identification*, dan *Penetration testing*.
5. *Tools* yang digunakan untuk memperoleh data adalah Nslookup, Whois domain, SLLScan, NMap, OwaspZap, dan Manual test.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini yang ingin dicapai oleh peneliti adalah sebagai berikut:

- a. Bagi Masyarakat:
 1. Hasil penelitian ini dapat memberikan gambaran mengenai keamanan layanan e-commerce dengan menggunakan metode ISSAF.
 2. Sebagai informasi tambahan bagi Masyarakat yang akan menggunakan *e-commerce* sebagai alat pembelian.
 3. Sebagai bahan untuk penelitian selanjutnya, terutama menyangkut objek analisis keamanan *e-commerce*.

- b. Bagi Perusahaan

Hasil penelitian ini bisa dijadikan saran untuk perusahaan e-commerce agar menjaga dan meningkatkan kualitas keamanan.