BAB I
PENDAHULUAN

1.1 Latar Belakang

Website adalah kumpulan halaman yang menyajikan berbagai jenis informasi melalui jaringan internet [1]. Penggunaan internet menghadapi tantangan yang signifikan terkait keamanan informasi. Tingginya penggunaan internet [2] menimbulkan kekhawatiran akan kerentanan pada *website,* terutama dengan laporan kasus peretasan website oleh pihak yang tidak bertanggung jawab. Badan Siber Sandi Negara (BSSN) mencatat serangan siber di Indonesia mencapai 100 juta kasus pada tahun 2022. Ancaman ini menggaris bawahi tingkat urgensi dalam menjaga keamanan informasi di era digital saat ini.

Keamanan informasi adalah upaya untuk melindungi informasi dari akses, penggunaan, penyalahgunaan, gangguan, atau modifikasi yang tidak sah [3]. Aspek-aspek kunci keamanan sistem informasi, seperti kerahasiaan, integritas, dan ketersediaan, menjadi pokok perhatian [2], keamanan *website* sangat penting terutama bagi organisasi atau perusahaan yang harus memastikan kerahasiaan, integritas, dan otentikasi data sesuai dengan standar keamanan [4]. Hal ini disebabkan meningkatnya ketergantungan masyarakat pada *website,* sehingga mendorong perlunya evaluasi dan peningkatan terhadap keamanan sistem. Namun, kerentanan pada keamanan website menjadi perhatian bagi semua entitas untuk melindungi diri dari ancaman tindakan kejahatan di dunia maya [5].

Kerentanan pada keamanan *website* dapat disebabkan oleh beberapa faktor, di antaranya kesalahan dalam penulisan kode dan konfigurasi yang tidak tepat. Jenis serangan seperti *SQL Injection*, Autentikasi, dan *Cross-Site Scripting* (XSS) menjadi ancaman utama, dengan tingkat kerentanan yang signifikan [2]. Penting bagi organisasi dan entitas lainnya untuk memahami dan mengatasi faktor-faktor ini guna mencegah potensi risiko dan melindungi integritas serta keamanan informasi *website*.

Soodu.id merupakan *marketplace* yang menyediakan platform digital bagi Usaha Mikro, Kecil dan Menengah (UMKM) untuk memasarkan produk secara luas. *Website* ini menyediakan fasilitas bagi UMKM untuk menjual produk langsung kepada konsumen dan membuka toko online. Namun, rendahnya pemahaman IT oleh pelaku UMKM, dapat meningkatkan risiko keamanan informasi, seperti kebocoran data, penipuan online, peretasan dan pemalsuan identitas. Oleh sebab, itu keamanan informasi *website* Soodu.id memegang peranan penting dalam melindungi data dan integritas bisnis UMKM yang menggunakan platform tersebut.

Metode *vulnerability assessment* dipilih sebagai pendekatan utama, karena memiliki keunggulan dalam mengidentifikasi ancaman yang perlu diwaspadai dan memerlukan perbaikan segera. Menggunakan *tools* OWASP ZAP dan OpenVAS, untuk melakukan pemeriksaan terhadap celah kerentanan. *tools* OWASP ZAP fokus pada pengujian kerentanan website, sementara OpenVAS fokus pengujian kerentanan pada *port*. Oleh sebab itu perlu dilakukan identifikasi kerentanan keamanan pada *website*. Serta memberikan rekomendasi tindakan perbaikan yang berguna bagi pengelola *website* dan pemilik bisnis UMKM untuk menjaga keamanan informasi mereka.

1.2 Rumusan Masalah

Berdasarkan penjelasan dari latar belakang yang diberikan di atas, maka rumusan masalah yaitu bagaimana melakukan analisis kerentanan pada *website* soodu.id menggunakan *tools* OWASP ZAP dan OpenVAS.

1.3 Batasan Masalah

Dalam penulisan skripsi ini, analisis keamanan sistem informasi pada website Soodu.id dibatasi pada penggunaan metode *vulnerability assessment* tanpa melakukan penetration testing. Selain itu, penelitian ini tidak melakukan *vulnerability assessment* pada subdomain yang ditemukan dari proses *information gathering*.

1.4 Tujuan

Tujuan dari penelitian ini adalah melakukan analisis keamanan informasi website menggunakan metode *vulnerability assessment* dengan tools OWASP ZAP dan OpenVAS, studi kasus pada website soodu.id.

1.5 Manfaat

Manfaat yang dapat dihasilkan dari penelitian ini adalah sebagai berikut:

a. Dapat memungkinkan pengambilan langkah-langkah pencegahan yang mampu meningkatkan keamanan *website*.
b. Mampu mengungkapkan celah keamanan pada *website* yang dapat dieksploitasi oleh pihak yang tidak berwenang.
c. Mampu melindungi data pelanggan dan informasi sensitif dari risiko penyalahgunaan atau kebocoran.
d. Mampu meningkatkan kesadaran akan pentingnya keamanan informasi di kalangan pemilik *website* dan pengguna.