

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi digital yang pesat dan semakin maju telah mengubah cara masyarakat berbelanja. Perkembangan *digital marketing* dan *e-commerce* semakin pesat seiring dengan globalisasi serta kemajuan teknologi. Secara global, *e-commerce* menjadi salah satu sektor dengan pertumbuhan paling cepat (Ain dkk., 2024). Indonesia termasuk negara dengan pertumbuhan *e-commerce* paling pesat di Asia Tenggara yang telah mengalami peningkatan signifikan dalam penggunaan platform *e-commerce*. *E-commerce* kini menjadi pilihan populer bagi masyarakat Indonesia dalam memenuhi kebutuhan sehari-hari (Nida dkk., 2024). Jumlah transaksi *e-commerce* di Indonesia pada tahun 2023 telah mencapai Rp 476 triliun dengan lebih dari 200 juta pengguna internet yang aktif berbelanja *online*. Hal tersebut menjadikan Indonesia sebagai salah satu pasar digital paling berkembang di dunia sekaligus menjadi kontributor utama pertumbuhan ekonomi digital di kawasan Asia Tenggara (Direktorat Statistik Keuangan, 2025).

Platform *e-commerce* lokal seperti Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak telah mendominasi pasar di Indonesia. Jumlah kunjungan ke 5 platform *e-commerce* terbesar di Indonesia yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak mencapai 462,9 juta pada Juni 2024. Jumlah kunjungan masyarakat Indonesia ke platform Shopee mencapai 261 juta pada Juni 2024. Berikutnya, kunjungan ke Tokopedia bertambah 4 juta (3,41%) menjadi 121,3 juta pada Juni 2024 dari 117,3 juta Maret 2024. Kunjungan ke platform Lazada 45,6 juta, kunjungan ke platform Blibli 27,6 juta, dan kunjungan ke platform Bukalapak 5,6 juta pada Juni 2024 (Abdul Muslim, 2024). Pertumbuhan platform-platform *e-commerce* lokal ini didukung oleh meningkatnya penetrasi internet dan penggunaan *smartphone*. Lebih dari 90% pengguna internet di Indonesia mengakses platform *e-commerce* melalui internet dan penggunaan *smartphone* (APJII, 2024).

Namun, seiring dengan pesatnya pertumbuhan *e-commerce* juga diiringi dengan tantangan peningkatan risiko keamanan siber (Asrul, 2025). Sektor *e-commerce* merupakan salah satu yang paling rentan dengan 43% serangan siber global pada tahun 2022 menargetkan bisnis *online*. Di balik pertumbuhan pesat *e-commerce* di Indonesia juga diiringi oleh meningkatnya serangan keamanan siber. Badan Siber dan Sandi Negara (BSSN) menyebutkan bahwa serangan siber di Indonesia meningkat sebesar 38% pada tahun 2022 dan terdapat 403 juta kasus serangan siber pada tahun 2023 dengan *e-commerce* sebagai salah satu sektor yang paling rentan dan menjadi salah satu target utama. Serangan seperti *phishing*, *malware*, *bruteforce attack*, serangan *ransomware*, dan kebocoran data pribadi sering menargetkan pengguna *e-commerce*, mengancam keamanan data pribadi, dan transaksi finansial (BSSN, 2023).

Dampak dari serangan siber juga sangat merugikan, misalnya pada tahun 2023 kerugian yang terjadi akibat *phishing* dan pemalsuan situs web yang marak ditemukan situs tiruan Tokopedia dan Shopee yang menyamar sebagai halaman promosi yang membuat pengguna tergoda untuk memasukkan data *login* yang menyebabkan pencurian akun dan saldo. Selain itu, pada April tahun 2024 sebanyak 1,3 juta data pengguna Shopee Indonesia bocor dan dijual melalui forum *dark web* yang mencakup informasi pribadi seperti nama, nomor telepon, email, dan riwayat transaksi. Kerugian bagi pengguna termasuk penipuan via SMS, pembajakan akun, dan pencurian dana besar. Kerugian ekonomi akibat serangan siber di sektor *e-commerce* Asia Tenggara mencapai USD 1,75 miliar, dengan Indonesia sebagai salah satu kontributor tertinggi (Redaksi, 2024).

Selain masalah teknis, minimnya kesadaran pengguna terhadap risiko keamanan juga menjadi faktor penyebab meningkatnya kerentanan. Kurangnya edukasi tentang keamanan siber menyebabkan pengguna rentan terhadap serangan *phishing* dan penipuan *online*, hanya 30% pengguna *e-commerce* di Indonesia yang menggunakan kata sandi kuat dan autentikasi dua faktor sebagai perlindungan akun mereka. Kerentanan keamanan pada platform *e-commerce* dapat menyebabkan kerugian finansial dan reputasi bagi perusahaan dan pengguna. Sebagian besar aplikasi *e-commerce* di Indonesia masih memiliki celah keamanan terutama dalam

hal enkripsi data dan manajemen pengguna (Hanifurohman & Durbin Hutagalung, 2020). Beberapa aplikasi *e-commerce* di Indonesia ditemukan masih menyimpan data sensitif dalam bentuk *plaintext*, tidak mengimplementasikan *SSL pinning*, dan meminta izin akses berbahaya seperti lokasi, kontak, serta penyimpanan tanpa kejelasan penggunaan.

Untuk mengidentifikasi dan menilai tingkat risiko keamanan pada aplikasi *e-commerce* diperlukan pendekatan sistematis yang tepat, salah satunya adalah *risk assessment* atau penilaian risiko. *Risk assessment* merupakan proses sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko yang terkait dengan keamanan informasi yang berpotensi dieksploitasi oleh pihak yang tidak bertanggungjawab. Namun demikian, penelitian yang melakukan *risk assessment* terhadap aplikasi *e-commerce* masih terbatas, padahal aplikasi jenis ini sangat rentan terhadap berbagai ancaman keamanan siber akibat tingginya aktivitas transaksi dan penyimpanan data sensitif (Miltenberger & Arzt, 2023).

Salah satu kerangka kerja yang dapat digunakan dalam *risk assessment* adalah NIST SP 800-30. NIST SP 800-30 membantu menetapkan prioritas mitigasi terhadap risiko berdasarkan tingkat dampak dan probabilitas serta memberikan landasan yang kuat untuk pengambilan keputusan keamanan yang strategis (Putra Eryawan dkk., 2021). Selain itu, kerangka acuan lain yang relevan dalam mengidentifikasi kerentanan keamanan aplikasi adalah OWASP Mobile Top 10 2024. OWASP Mobile Top 10 2024 menjadi acuan penting dalam praktik pengujian keamanan karena memperbarui kategori sesuai dengan tren dan serangan terbaru (Chinnasamy, 2024). Meskipun demikian, hingga saat ini masih terbatasnya penelitian yang secara khusus mengimplementasikan kerangka NIST SP 800-30 dan OWASP Mobile Top 10 2024 dalam menilai risiko kerentanan keamanan pada aplikasi *e-commerce* di Indonesia. Dalam beberapa penelitian yang telah dilakukan untuk menganalisis kerentanan keamanan aplikasi *e-commerce* di Indonesia, sebagian besar penelitian fokus pada analisis keamanan secara umum pada aplikasi *e-commerce* tertentu tanpa membandingkan implementasi keamanan pada beberapa aplikasi *e-commerce* yang berbeda. Beberapa penelitian yang telah dilakukan untuk menganalisis kerentanan aplikasi lebih banyak menggunakan analisis statis.

Analisis statis merupakan proses pemeriksaan terhadap aplikasi tanpa perlu menjalankannya secara langsung. Dalam konteks aplikasi *mobile*, analisis statis dilakukan dengan menganalisis file instalasi aplikasi (APK) untuk mengidentifikasi potensi kerentanan yang terdapat di dalam struktur internal aplikasi, seperti izin akses, penggunaan algoritma kriptografi, dan *hardcoded secrets* (Hussain dkk., 2024).

Melihat adanya kesenjangan dalam penelitian sebelumnya maka diperlukan penelitian lebih lanjut yang tidak hanya fokus pada satu aplikasi saja tetapi dengan membandingkan beberapa aplikasi *e-commerce* di Indonesia dengan melakukan *risk assessment* menggunakan pendekatan analisis statis. Berdasarkan permasalahan diatas, maka perlu dilakukan penelitian untuk melakukan *risk assessment* pada aplikasi *e-commerce* di Indonesia seperti Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak dengan pendekatan analisis statis berdasarkan NIST SP 800-30 dan OWASP Mobile 2024. Penelitian ini diharapkan dapat memberikan solusi untuk meningkatkan keamanan aplikasi *e-commerce* di Indonesia dan keamanan data pribadi bagi pengguna aplikasi *e-commerce* di Indonesia.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah penelitian ini adalah masih tingginya kebocoran data dan terdapat celah keamanan pada beberapa aplikasi *e-commerce* di Indonesia terutama dalam hal enkripsi data dan perlindungan informasi pengguna. Selain itu, penelitian yang melakukan *risk assessment* pada aplikasi *e-commerce* di Indonesia masih terbatas.

1.3 Pertanyaan Penelitian

1. Bagaimana penerapan NIST SP 800-30 dan OWASP Mobile 2024 dalam melakukan *risk assessment* pada aplikasi *e-commerce* di Indonesia?
2. Bagaimana analisis statis dapat digunakan untuk mengidentifikasi kerentanan keamanan pada aplikasi *e-commerce* di Indonesia?
3. Bagaimana perbandingan tingkat keamanan antara aplikasi *e-commerce* di Indonesia yang dianalisis?

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk melakukan *risk assessment* pada aplikasi *e-commerce* di Indonesia dengan mengidentifikasi celah keamanan serta membandingkan tingkat keamanannya diantara beberapa platform, yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak dengan pendekatan analisis statis menggunakan *framework* NIST SP 800-30 dan OWASP Mobile 2024.

1.5 Manfaat Hasil Penelitian

1. Bagi pengguna aplikasi *e-commerce*

Memberikan informasi kepada pengguna aplikasi *e-commerce* tentang pentingnya keamanan siber dan keamanan aplikasi untuk melindungi data pribadi.

2. Bagi Perusahaan *e-commerce*

Memberikan rekomendasi serta dapat digunakan sebagai bahan pertimbangan untuk meningkatkan keamanan aplikasi *e-commerce* dan melindungi data pengguna.