BAB I
PENDAHULUAN

1.1 Latar Belakang

Pemanfaatan teknologi seperti komputer dan ponsel telah meningkat pesat seiring dengan kemajuan zaman, di mana perangkat ini menjadi pendukung utama aktivitas masyarakat sehari-hari. Salah satu pendorong utama perkembangan ini adalah kemunculan internet yang dimanfaatkan oleh pelaku bisnis untuk mengembangkan usahanya, termasuk sektor perdagangan elektronik atau e-commerce [1]. Di Indonesia, pengguna internet mengalami peningkatan setiap tahunnya, yang diikuti dengan tren penggunaan internet melalui perangkat mobile. Hal ini memberikan dampak positif bagi sektor bisnis jual beli online dan memicu bermunculannya beragam aplikasi mobile, khususnya pada platform Android [2].

Kehadiran e-commerce telah membuat hidup menjadi lebih mudah bagi banyak orang di seluruh dunia, memungkinkan transaksi harian dilakukan secara nirkabel dengan nyaman. Pola perilaku belanja masyarakat pun berubah, ditunjukkan dengan volume transaksi e-commerce yang terus meningkat. Pelaku e-commerce kini harus memaksimalkan aplikasi mobile yang dimiliki untuk memenuhi tren perilaku konsumen saat ini. Namun, di balik kemudahan dan kenyamanan tersebut, penggunaan aplikasi mobile untuk transaksi elektronik juga menimbulkan berbagai ancaman keamanan yang tidak bisa diabaikan [2].

Permasalahan utama muncul karena aplikasi mobile mengelola informasi yang sangat penting dan berharga, yang dapat disajikan dalam berbagai format seperti catatan elektronik. Celah-celah keamanan yang terdapat di dalam aplikasi dapat digunakan oleh penyerang untuk mencuri informasi penting tersebut dari dalam smartphone pengguna. Jika informasi tidak dilindungi saat dikirim melalui jaringan nirkabel atau gateway, data tersebut kemungkinan akan terekspos dan menyebabkan ancaman serius terhadap aktivitas perdagangan [2]. Faktor ketidakamanan ini bisa berasal dari terminal seluler itu sendiri, antarmuka radio,

maupun dari sisi jaringan. Masalah keamanan pada sistem operasi Android juga menjadi sorotan khusus karena adanya mekanisme berbasis izin (permission) yang mengatur akses aplikasi pihak ketiga ke sumber daya perangkat. Mekanisme ini sering dikritik karena kontrolnya yang kasar dan manajemen izin yang tidak efisien, baik oleh pengembang maupun pengguna. Aplikasi Android yang "bocor" dapat menempatkan informasi sensitif pengguna di lokasi yang tidak aman pada perangkat, yang kemudian dapat diakses oleh aplikasi jahat lainnya [2]. Kerentanan seperti kebocoran data (data leakage) dan eskalasi hak istimewa (privilege escalation) membuat jutaan pengguna berisiko mengalami pembajakan data atau perangkat.

Meskipun popularitas *e-commerce* terus meningkat, terdapat kesenjangan pemahaman yang signifikan mengenai keamanan teknis di balik fitur-fitur canggih yang ditawarkan. Pengguna sering kali menganggap bahwa aplikasi besar seperti Tokopedia, Shopee, dan Lazada memiliki tingkat keamanan yang seragam dan mutlak. Namun, kenyataannya, pembaruan fitur yang agresif sering kali berbanding lurus dengan perluasan permukaan serangan (*attack surface*), seperti penambahan izin akses yang intrusif dan penggunaan pustaka pihak ketiga untuk pelacakan data.

Penelitian terdahulu mayoritas hanya berfokus pada analisis *malware* spesifik atau aplikasi versi lama, sehingga belum ada pemetaan keamanan komparatif yang relevan untuk versi terbaru tahun 2026. Ketiadaan data pembanding ini menyulitkan pengguna untuk mengetahui aplikasi mana yang paling menghormati privasi data mereka, dan menyulitkan pengembang untuk mengetahui standar keamanan relatif mereka terhadap kompetitor. Oleh karena itu, penelitian ini mendesak dilakukan untuk mengevaluasi dan membandingkan secara *head-to-head* postur keamanan serta risiko privasi pada ketiga aplikasi *marketplace* tersebut menggunakan pendekatan analisis statis.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini Adalah Bagaimana perbandingan kerentanan dan tingkat keamanan pada aplikasi *marketplace* (Tokopedia, Shopee, dan Lazada) berdasarkan hasil analisis statis menggunakan *Mobile Security Framework* (MobSF)?

1.3 Batasan Masalah

Untuk menjaga agar penelitian ini tetap fokus dan terarah, peneliti menetapkan batasan masalah sebagai berikut:

1. Penelitian ini hanya menggunakan metode Analisis Statis (*Static Analysis*) yang disediakan oleh *Mobile Security Framework* (MobSF). Penelitian ini tidak melakukan Analisis Dinamis (*Dynamic Analysis*).
2. Objek penelitian adalah aplikasi *marketplace* Tokopedia, Shopee, dan Lazada dalam format berkas APK (*Application Package File*) untuk platform Android.
3. Berkas APK yang digunakan adalah versi terbaru yang diunduh secara resmi dari Google Play Store pada periode Desember 2025 hingga Januari 2026.
4. Parameter analisis kerentanan yang dibandingkan terbatas pada hasil keluaran MobSF, yang mencakup (namun tidak terbatas pada) *Dangerous Permissions*, *Weak Crypto*, *Hardcode Secrets*, *SSL Bypass*, dan *Domain Malware Check* [2] [1]

1.4 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dari penelitian ini adalah:

1. Mengidentifikasi dan mendeskripsikan kerentanan keamanan yang terdapat pada aplikasi marketplace Tokopedia, Shopee, dan Lazada menggunakan tools MobSF.
2. Menyajikan perbandingan postur keamanan, temuan kerentanan, dan skor

keamanan antara ketiga aplikasi marketplace tersebut.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Bagi Akademisi: Menjadi referensi ilmiah dan bahan kajian untuk penelitian selanjutnya di bidang keamanan aplikasi *mobile*, khususnya dalam analisis komparatif aplikasi *marketplace*.
2. Bagi Pengembang Aplikasi: Memberikan masukan dan temuan konkret mengenai potensi kerentanan yang ada, yang dapat digunakan sebagai dasar untuk melakukan perbaikan (*hardening*) dan meningkatkan keamanan aplikasi demi melindungi data pengguna [2].
3. Bagi Pengguna (Masyarakat Umum): Meningkatkan pemahaman dan kesadaran (*awareness*) mengenai potensi risiko keamanan yang ada pada aplikasi *marketplace* yang mereka gunakan sehari-hari [2] [1].

1.6 Sistematika Penulisan

Penulisan skripsi ini dibagi menjadi lima bab dengan sistematika sebagai berikut:

- BAB I PENDAHULUAN: Bab ini berisi Latar Belakang Masalah, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, dan Sistematika Penulisan.
- BAB II TINJAUAN PUSTAKA: Bab ini menguraikan Studi Literatur (penelitian terdahulu yang relevan) dan Dasar Teori yang digunakan, seperti keamanan aplikasi *mobile*, analisis statis, dan *Mobile Security Framework* (MobSF).
- BAB III METODE PENELITIAN: Bab ini menjelaskan objek penelitian, alur penelitian secara sistematis, serta alat dan bahan yang digunakan dalam proses pengumpulan dan analisis data.

- BAB IV HASIL DAN PEMBAHASAN: Bab ini menyajikan data temuan hasil analisis statis dari MobSF terhadap ketiga aplikasi. Bab ini juga berisi pembahasan komparatif dari hasil temuan tersebut, membandingkan kerentanan dan skor keamanan masing-masing aplikasi.
- BAB V PENUTUP: Bab ini berisi kesimpulan yang menjawab rumusan masalah penelitian, serta saran untuk pengembangan aplikasi yang lebih aman dan untuk penelitian selanjutnya.