BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian dan analisis statis menggunakan *Mobile Security Framework* terhadap aplikasi marketplace Tokopedia, Shopee, dan Lazada, dapat disimpulkan bahwa ketiga platform tersebut masih berada pada tingkat risiko menengah dengan kategori keamanan yang baik namun belum optimal. Tidak satu pun aplikasi yang sepenuhnya memenuhi standar keamanan tertinggi. Dari sisi struktur dan kualitas kode, Shopee menunjukkan tingkat kekokohan yang relatif lebih baik dibandingkan dua aplikasi lainnya, dengan jumlah temuan kerentanan tingkat tinggi yang lebih sedikit. Tokopedia berada pada posisi menengah dengan karakteristik risiko yang didominasi oleh kerentanan tingkat menengah. Sementara itu, Lazada memperlihatkan tingkat kerentanan yang relatif lebih tinggi pada aspek struktural dibandingkan kompetitornya.

Penelitian ini juga mengungkap adanya dinamika antara keamanan kode dan praktik perlindungan privasi pengguna. Aplikasi dengan skor keamanan kode yang lebih baik justru menunjukkan kecenderungan lebih aktif dalam melakukan pelacakan data pengguna melalui integrasi berbagai layanan pihak ketiga, termasuk jaringan periklanan global. Sebaliknya, aplikasi yang memiliki tingkat kerentanan kode lebih tinggi justru menerapkan pendekatan yang lebih minimal dalam penggunaan pelacak pihak ketiga. Namun demikian, pola aliran datanya memiliki karakteristik berbeda karena terhubung dengan ekosistem teknologi tertentu yang berasal dari kawasan Asia Timur. Tokopedia sendiri berada di antara keduanya, dengan ketergantungan yang cukup signifikan terhadap layanan periklanan dan analitik global.

Dari sisi manajemen perizinan, ketiga aplikasi menunjukkan pola permintaan akses yang cenderung berlebihan dibandingkan kebutuhan fungsional dasar platform jual-beli daring. Seluruh aplikasi meminta akses terhadap data sensitif seperti lokasi presisi, kamera, serta informasi perangkat. Shopee tercatat

meminta izin akses terhadap daftar kontak, yang berpotensi membuka ruang pemetaan relasi sosial pengguna secara lebih luas. Di sisi lain, Lazada menunjukkan permintaan akses tambahan seperti kalender dan daftar akun, yang berpotensi bersinggungan langsung dengan ranah privasi personal di luar konteks transaksi perdagangan elektronik.

Sebagai temuan akhir, penelitian ini juga mengidentifikasi adanya penggunaan algoritma kriptografi yang telah dinyatakan usang dalam mekanisme penandatanganan digital aplikasi. Algoritma tersebut diketahui memiliki kelemahan terhadap serangan tertentu dan secara umum telah direkomendasikan untuk digantikan dengan standar kriptografi yang lebih modern. Belum optimalnya migrasi ke algoritma yang lebih kuat mencerminkan perlunya peningkatan komitmen terhadap penerapan praktik keamanan kriptografi yang mutakhir dalam pengembangan aplikasi e-commerce di Indonesia.

5.2 Saran

Berdasarkan temuan kelemahan di atas, peneliti merumuskan saran-saran perbaikan yang ditujukan kepada tiga entitas utama:

1. Bagi Pengembang Aplikasi (Tokopedia, Shopee, Lazada)
    - Peningkatan Standar Kriptografi: Segera melakukan migrasi sertifikat penandatanganan aplikasi dari algoritma SHA-1 ke SHA-256 untuk menjamin integritas paket aplikasi yang lebih kuat dan memenuhi standar keamanan Google Play terbaru.
    - Penerapan *Least Privilege*: Meninjau ulang dan menghapus permintaan izin yang tidak krusial. Khususnya izin READ_PHONE_STATE (akses IMEI) sebaiknya diganti dengan *Advertising ID* yang dapat di-reset, serta menghapus izin READ_CONTACTS jika tidak ada fitur sosial yang benar-benar esensial.

- Pengurangan Pihak Ketiga: Shopee dan Tokopedia disarankan untuk mengurangi jumlah pustaka pelacak (*trackers*) iklan dan analitik untuk meminimalisir permukaan serangan (*attack surface*) dan risiko kebocoran data ke pihak ketiga.
- Mitigasi Temuan Kritis: Lazada perlu memprioritaskan penambalan (*patching*) terhadap 15 kerentanan kritis (*High Severity*) yang ditemukan MobSF, terutama yang berkaitan dengan konfigurasi manifes dan eksposur komponen.

2. Bagi Pengguna (*End-Users*)
   - Manajemen Izin Mandiri: Pengguna disarankan untuk secara manual mematikan izin yang tidak diperlukan melalui menu *Settings* di Android. Izin seperti Lokasi, Kamera, dan Mikrofon sebaiknya diatur ke opsi *"Only while using the app"* (Hanya saat aplikasi digunakan) atau *"Ask every time"* (Selalu tanya).
   - Kewaspadaan Privasi: Menghindari penggunaan fitur sinkronisasi kontak ("Temukan Teman") pada aplikasi belanja untuk mencegah pengunggahan buku telepon pribadi ke server aplikasi.
   - Isolasi Identitas: Disarankan menggunakan alamat *email* sekunder khusus untuk belanja *online* guna memisahkan identitas transaksi dari identitas pribadi/profesional utama.
3. Bagi Peneliti Selanjutnya
   - Analisis Dinamis: Penelitian ini terbatas pada analisis statis kode. Disarankan bagi peneliti selanjutnya untuk melakukan Analisis Dinamis (*Dynamic Analysis*) guna melihat perilaku aplikasi saat dijalankan secara *real-time*, termasuk memantau lalu lintas jaringan (*traffic analysis*) untuk membuktikan apakah data pengguna benar-benar dikirim tanpa enkripsi.

- Komparasi OS: Melakukan studi komparasi antara versi Android dan iOS untuk melihat apakah terdapat perbedaan standar keamanan yang diterapkan pengembang pada ekosistem Apple.

Uji Penetrasi API: Memperluas cakupan penelitian ke sisi *backend* dengan melakukan pengujian keamanan pada API (*Application Programming Interface*) yang digunakan oleh aplikasi seluler tersebut.