BAB 4
HASIL PENELITIAN

4.1 Ringkasan Hasil Penelitian

Penelitian ini bertujuan untuk melakukan penilaian risiko (*risk assessment*) keamanan informasi terhadap lima aplikasi *e-commerce* populer di Indonesia, yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak. Proses penelitian dimulai dengan identifikasi aplikasi dan aset informasinya, kemudian dilakukan pemindaian kerentanan menggunakan *Mobile Security Framework* (MobSF) dengan pendekatan analisis statis. Hasil pemindaian menunjukkan bahwa semua aplikasi memiliki nilai *security score* di bawah 51 dari skala 100, dengan skor tertinggi dimiliki oleh Shopee (50/100) dan skor terendah oleh Blibli (39/100), yang menandakan tingkat keamanan yang masih belum optimal pada seluruh aplikasi yang dianalisis.

Setelah itu dilakukan pemetaan kerentanan ke OWASP Mobile Top 10 2024, ditemukan bahwa kerentanan paling dominan berada pada kategori M10: *Insufficient Cryptography*, M9: *Insecure Data Storage*, dan M8: *Security Misconfiguration*. Selanjutnya, dilakukan analisis risiko berdasarkan *framework* NIST SP 800-30, yang mencakup penilaian *likelihood* dan *impact* untuk menentukan *risk level* keseluruhan dari kerentanan yang ditemukan. Hasil evaluasi risiko menyimpulkan bahwa kelima aplikasi berada dalam kategori *High Risk*, yang berarti bahwa masing-masing aplikasi masih memiliki banyak celah keamanan signifikan yang berpotensi dieksploitasi. Oleh karena itu, diperlukan peningkatan pengamanan terutama dalam aspek kriptografi, pengelolaan kredensial, serta pembatasan izin akses aplikasi untuk melindungi data pribadi pengguna secara lebih efektif dan menyeluruh.

4.2 Pembahasan

Berikut adalah pembahasan secara rinci hasil yang diperoleh dari tahapan penelitian yang telah dilakukan:

4.2.1 Identifikasi Aplikasi

Tahapan ini merupakan tahapan paling awal dalam melakukan *risk assessment* keamanan informasi pada aplikasi *e-commerce* di Indonesia menggunakan *framework* NIST SP 800-30 dan OWASP Mobile 2024. Pada tahapan identifikasi aplikasi meliputi:

1. Menggunakan *smartphone* android untuk mengunduh aplikasi *e-commerce* yang akan dianalisis

Gambar 4. 1 *Smartphone* android

Smartphone android yang digunakan adalah OPPO A12 seperti pada Gambar 4.1. Adapun spesifikasi dari *smartphone* android yang digunakan dapat dilihat pada Tabel 4.1.

Tabel 4. 1 Spesifikasi *smartphone* android

Detail Perangkat	Spesifikasi
Nama perangkat	OPPO A12
Nomor model	CPH2083
Versi android	9.0
Processor	Delapan *core*
RAM	3 GB
Internal	32 GB

2. Mengunduh aplikasi *e-commerce* yang akan dianalisis melalui Google Play Store dan *install* di *smartphone* android

A. Shopee

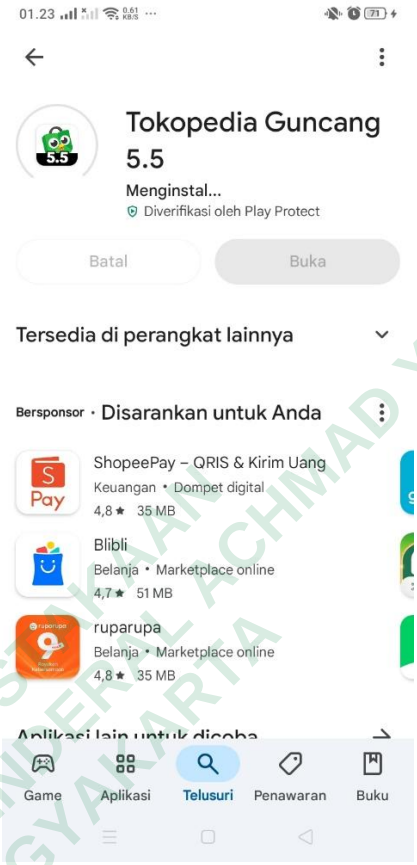
Gambar 4. 2 *Download* dan *install* aplikasi Shopee

Pada Gambar 4.2 adalah hasil setelah *download* dan *install* aplikasi Shopee di *smartphone* android. Spesifikasi dari aplikasi Shopee yang telah diunduh melalui Google Play Store dan di *install* di *smartphone* android dapat dilihat pada Tabel 4.2.

Tabel 4. 2 Spesifikasi aplikasi Shopee

Komponen	Info Aplikasi
Versi aplikasi	3.48.31
Ukuran file	79 MB
Penyedia aplikasi	Shopee
Tanggal rilis	21 April 2025
Kompatibel dengan OS	Android 5.0 dan yang lebih baru

B. Tokopedia



Gambar 4. 3 *Download* dan *install* aplikasi Tokopedia

Pada Gambar 4.3 adalah hasil setelah *download* dan *install* aplikasi Tokopedia di *smartphone* android. Spesifikasi dari aplikasi Tokopedia yang telah diunduh melalui Google Play Store dan di *install* di *smartphone* android dapat dilihat pada Tabel 4.3.

Tabel 4. 3 Spesifikasi aplikasi Tokopedia

Komponen	Info Aplikasi
Versi aplikasi	3.306.0
Ukuran file	63 MB
Penyedia aplikasi	Tokopedia
Tanggal rilis	12 April 2025
Kompatibel dengan OS	Android 5.0 dan yang lebih baru

C. Lazada

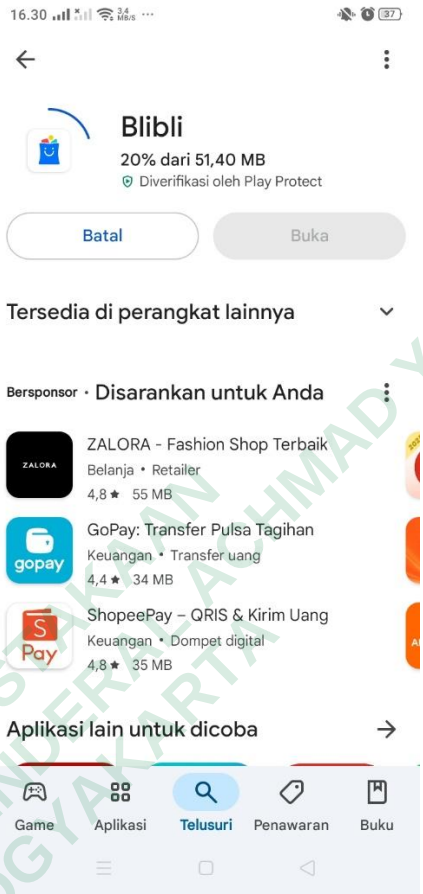
Gambar 4. 4 *Download* dan *install* aplikasi Lazada

Pada Gambar 4.4 adalah hasil setelah *download* dan *install* aplikasi Lazada di *smartphone* android. Spesifikasi dari aplikasi Lazada yang telah diunduh melalui Google Play Store dan di *install* di *smartphone* android dapat dilihat pada Tabel 4.4.

Tabel 4. 4 Spesifikasi aplikasi Lazada

Komponen	Info Aplikasi
Versi aplikasi	7.73.0
Ukuran file	30 MB
Penyedia aplikasi	Lazada Mobile
Tanggal rilis	8 April 2025
Kompatibel dengan OS	Android 5.0 dan yang lebih baru

D. Blibli



Gambar 4. 5 *Download* dan *install* aplikasi Blibli

Pada Gambar 4.5 adalah hasil setelah *download* dan *install* aplikasi Blibli di *smartphone* android. Spesifikasi dari aplikasi Blibli yang telah diunduh melalui Google Play Store dan di *install* di *smartphone* android dapat dilihat pada Tabel 4.5.

Tabel 4. 5 Spesifikasi aplikasi Blibli

Komponen	Info Aplikasi
Versi aplikasi	12.2.0
Ukuran file	56 MB
Penyedia aplikasi	Blibli.com
Tanggal rilis	26 Maret 2025
Kompatibel dengan OS	Android 8.0 dan yang lebih baru

E. Bukalapak

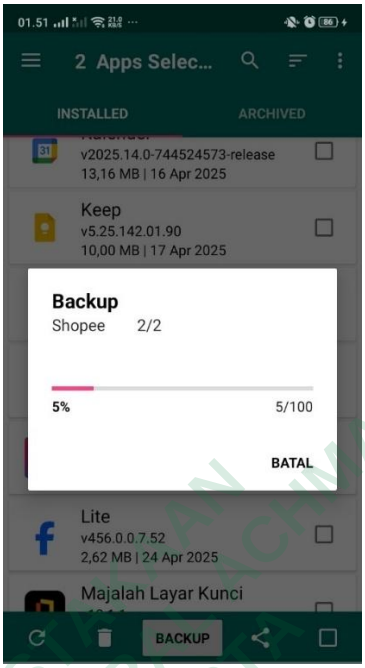
Gambar 4. 6 *Download* dan *install* aplikasi Bukalapak

Pada Gambar 4.6 adalah hasil setelah *download* dan *install* aplikasi Bukalapak di *smartphone* android. Spesifikasi dari aplikasi Bukalapak yang telah diunduh melalui Google Play Store dan di *install* di *smartphone* android dapat dilihat pada Tabel 4.6.

Tabel 4. 6 Spesifikasi aplikasi Bukalapak

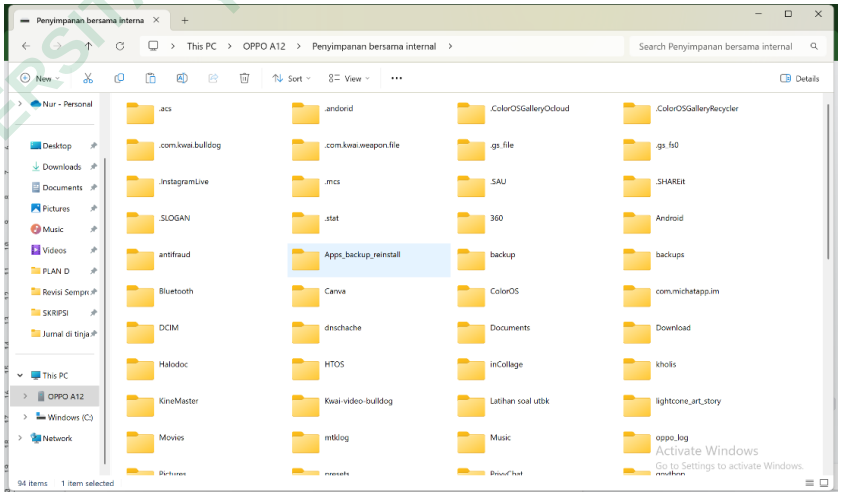
Komponen	Info Aplikasi
Versi aplikasi	11.5.1
Ukuran file	30 MB
Penyedia aplikasi	PT Bukalapak.com
Tanggal rilis	13 Maret 2025
Kompatibel dengan OS	Android 5.0 dan yang lebih baru

3. *Backup* data aplikasi dari *smartphone* android ke laptop



Gambar 4. 7 *Backup* data aplikasi di *smartphone*

Proses *backup* data aplikasi yang akan dianalisis yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak di *smartphone* menggunakan Apps Backup and Restore seperti yang ditunjukkan pada Gambar 4.7.



Gambar 4. 8 Pemindahan hasil *backup* ke laptop

Pada Gambar 4.8 adalah proses pemindahan hasil *backup* data aplikasi yang akan dianalisis dari *smartphone* ke laptop untuk proses analisis selanjutnya.

4. Mengidentifikasi aset informasi dari aplikasi *e-commerce* yang akan dianalisis terkait info aplikasi, izin aplikasi, data pengguna yang dibagikan dan dikumpulkan, fitur keamanan, dan mekanisme autentikasi yang diterapkan pada setiap aplikasi

A. Shopee

Gambar 4. 9 Logo aplikasi Shopee

Aplikasi Shopee yang digunakan adalah versi 3.48.31 dengan logo seperti pada Gambar 4.9 yang merupakan versi terbaru dan telah di *download* di Google Play Store untuk memastikan keaslian dan keamanan nya. Hasil identifikasi terkait izin aplikasi, data pengguna yang dibagikan dan dikumpulkan, fitur keamanan, dan mekanisme autentikasi dari aplikasi Shopee dapat dilihat pada Tabel 4.7.

Tabel 4. 7 Identifikasi aset informasi Shopee

No	Komponen	Data Aplikasi
1.	Izin akses	a. Kalender b. Kamera c. Kontak d. Lokasi e. Mikrofon f. Penyimpanan
2.	Data yang dibagikan	a. Info keuangan: info pembayaran pengguna dan histori pembelian

No	Komponen	Data Aplikasi
		b. Perangkat atau ID lainnya c. Aktivitas aplikasi d. File dan dokumen e. Foto dan video f. Lokasi g. Info pribadi: alamat email, alamat, dan nomor telepon
3.	Data yang dikumpulkan	a. Penjelajahan web b. Info keuangan: info pembayaran pengguna dan histori pembelian c. Kontak d. Perangkat atau ID lainnya e. Aktivitas aplikasi f. Pesan g. Info dan performa aplikasi h. File dan dokumen i. Foto dan video j. Lokasi k. Info pribadi: nama, alamat email, ID pengguna, alamat, dan nomor telepon
4.	Fitur keamanan	Data dienkripsi saat dalam pengiriman
5.	Mekanisme autentikasi	a. Verifikasi akun: nomor handphone, *password*, SMS, email, dan whatsapp b. Verifikasi identitas: KTP c. Verifikasi tambahan: sidik jari, wajah, dan PIN shopeepay

B. Tokopedia

Gambar 4. 10 Logo aplikasi Tokopedia

Aplikasi Tokopedia yang digunakan adalah versi 3.306.0 dengan logo seperti pada Gambar 4.10 yang merupakan versi terbaru dan telah di *download* di Google Play Store untuk memastikan keaslian dan keamanannya. Hasil identifikasi terkait izin aplikasi, data yang dibagikan dan dikumpulkan, fitur keamanan, dan mekanisme autentikasi dari aplikasi Tokopedia dapat dilihat pada Tabel 4.8.

Tabel 4. 8 Identifikasi aset informasi Tokopedia

No	Komponen	Data Aplikasi
1.	Izin akses	a. Kamera b. Kontak c. Lokasi d. Mikrofon e. Ponsel f. Penyimpanan
2.	Data yang dibagikan	a. Aktivitas aplikasi b. Foto dan video c. Perangkat atau ID lainnya d. Info pribadi: nama, Alamat email, dan ID pengguna e. Info keuangan: info pembayaran pengguna dan skor kredit f. Lokasi g. Info dan performa aplikasi: *log error*, diagnostik, dan data lainnya terkait performa aplikasi

No	Komponen	Data Aplikasi
3.	Data yang dikumpulkan	a. Aktivitas aplikasi b. Foto dan video c. Perangkat atau ID lainnya d. Info pribadi: nama, alamat email, ID pengguna, alamat, dan nomor telepon e. Info keuangan: info pembayaran pengguna dan histori pembelian f. Lokasi g. Info dan performa aplikasi: *log error* dan diagnostik
4.	Fitur keamanan	Data dienkripsi saat dalam pengiriman
5.	Mekanisme autentikasi	a. Verifikasi akun: nomor handphone, *password*, dan SMS b. Verifikasi identitas: KTP c. Verifikasi tambahan: PIN dan Google *authenticator* (2FA)

C. Lazada

Gambar 4. 11 Logo aplikasi Lazada

Aplikasi Lazada yang digunakan adalah versi 7.73.0 dengan logo seperti pada Gambar 4.11 yang merupakan versi terbaru dan telah di *download* di Google Play Store untuk memastikan keaslian dan keamanannya. Hasil identifikasi terkait izin aplikasi, data yang

dibagikan dan dikumpulkan, fitur keamanan, dan mekanisme autentikasi dari aplikasi Lazada dapat dilihat pada Tabel 4.9.

Tabel 4. 9 Identifikasi aset informasi Lazada

No	Komponen	Data Aplikasi
1.	Izin akses	a. Kalender b. Kamera c. Kontak d. Lokasi e. Mikrofon f. Penyimpanan
2.	Data yang dibagikan	Info pribadi: nama, alamat email, alamat, dan nomor telepon
3.	Data yang dikumpulkan	a. Lokasi b. Info pribadi: nama, alamat email, ID pengguna, alamat, dan nomor telepon c. Info keuangan: info pembayaran pengguna, histori pembelian, skor kredit, dan info keuangan lainnya d. Info dan performa aplikasi e. Audio f. Kesehatan dan kebugaran g. Foto dan video h. Aktivitas aplikasi i. Pesan
4.	Fitur keamanan	Data dienkripsi saat dalam pengiriman
5.	Mekanisme autentikasi	a. Verifikasi akun: nomor handphone, *password*, SMS, email, dan whatsapp b. Verifikasi identitas: KTP c. Verifikasi tambahan: PIN, sidik jari, dan wajah

D. Blibli

Gambar 4. 12 Logo aplikasi Blibli

Aplikasi Blibli yang digunakan adalah versi 12.2.0 dengan logo seperti pada Gambar 4.12 yang merupakan versi terbaru dan telah di *download* di Google Play Store untuk memastikan keaslian dan keamanannya. Hasil identifikasi terkait izin aplikasi, data yang dibagikan dan dikumpulkan, fitur keamanan, dan mekanisme autentikasi dari aplikasi Blibli dapat dilihat pada Tabel 4.10.

Tabel 4. 10 Identifikasi aset informasi Blibli

No	Komponen	Data Aplikasi
1.	Izin akses	a. Kamera b. Kontak c. Lokasi d. Mikrofon e. Ponsel f. Penyimpanan
2.	Data yang dibagikan	a. Perangkat atau ID lainnya b. Info pribadi: alamat email
3.	Data yang dikumpulkan	a. Info pribadi: nama, alamat email, ID pengguna, alamat, dan nomor telepon b. Lokasi c. Foto dan video d. Info keuangan: info pembayaran pengguna dan histori pembelian e. Aktivitas aplikasi

No	Komponen	Data Aplikasi
4.	Fitur keamanan	Data dienkripsi saat dalam pengiriman
5.	Mekanisme autentikasi	a. Verifikasi akun: nomor handphone, *password*, SMS, email, dan whatsapp b. Verifikasi identitas: KTP c. Verifikasi tambahan: PIN, sidik jari, dan wajah

E. Bukalapak

Gambar 4. 13 Logo aplikasi Bukalapak

Aplikasi Bukalapak yang digunakan adalah versi 11.5.1 dengan logo seperti pada Gambar 4.13 yang merupakan versi terbaru dan telah di *download* di Google Play Store untuk memastikan keaslian dan keamanannya. Hasil identifikasi terkait izin aplikasi, data yang dibagikan dan dikumpulkan, fitur keamanan, dan mekanisme autentikasi dari aplikasi Bukalapak dapat dilihat pada Tabel 4.11.

Tabel 4. 11 Identifikasi aset informasi Bukalapak

No	Komponen	Data Aplikasi
1.	Izin akses	a. Kalender b. Kamera c. Kontak d. Lokasi e. Mikrofon f. Ponsel g. Penyimpanan

No	Komponen	Data Aplikasi
2.	Data yang dibagikan	a. Info keuangan: info pembayaran pengguna dan histori pembelian b. Foto dan video c. Lokasi d. Aktivitas aplikasi e. File dan dokumen f. Info pribadi: nama, alamat email, ID pengguna, alamat, dan nomor telepon g. Kontak
3.	Data yang dikumpulkan	a. Info keuangan: info pembayaran pengguna dan histori pembelian b. Foto dan video c. Lokasi d. Pesan e. Aktivitas aplikasi f. Info dan performa aplikasi g. File dan dokumen h. Info pribadi: nama, alamat email, ID pengguna, alamat, dan nomor telepon
4.	Fitur keamanan	Data tidak dienkripsi
5.	Mekanisme autentikasi	a. Verifikasi akun: nomor handphone, *password*, SMS, email, dan whatsapp b. Verifikasi identitas: KTP c. Verifikasi tambahan: PIN, sidik jari, wajah, dan *Two Factor Authentication* (TFA)

4.2.2 Pemindaian Kerentanan dengan MobSF

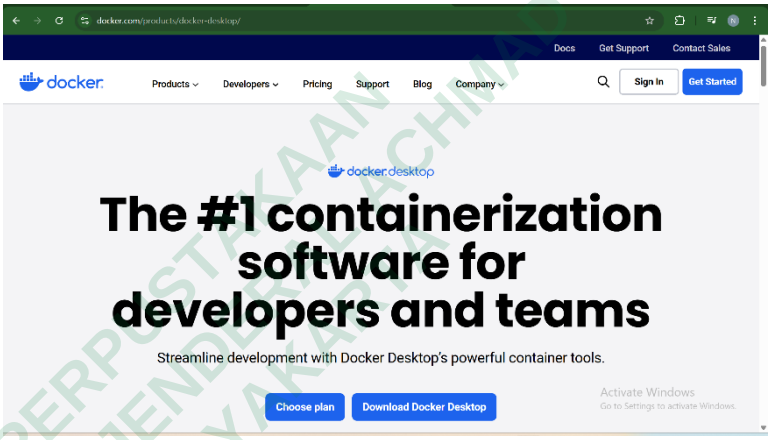
Pada tahap ini dilakukan pemindaian kerentanan terhadap file APK dari aplikasi *e-commerce* yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak menggunakan MobSF dengan pendekatan analisis statis. Dalam penelitian ini, analisis statis dilakukan terhadap file APK dari setiap aplikasi *e-commerce* dan tidak mencakup pemeriksaan langsung terhadap *source code* asli aplikasi. Tujuan dari tahapan ini adalah untuk mengidentifikasi potensi kerentanan keamanan pada file aplikasi *e-commerce* yang dianalisis. Fokus pada tahapan pemindaian

kerentanan ini yaitu pada *hardcoded secrets*, *weak cryptography*, *insecure data storage*, *dangerous permissions*, SSL/TLS *Misconfiguration*. Pada tahapan pemindaian kerentanan dengan MobSF ini meliputi:

1. Menginstal *Mobile Security Framework* (MobSF)

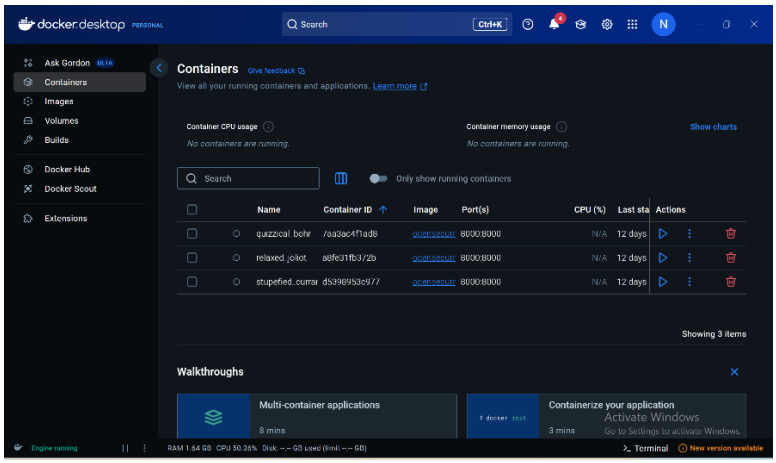
   A. *Install* Docker Desktop

   Unduh dan *install* Docker Desktop untuk windows melalui https://www.docker.com/products/docker-desktop/ kemudian pilih *Download* Docker Desktop *for Windows* seperti pada Gambar 4.14.



Gambar 4. 14 *Install* docker desktop

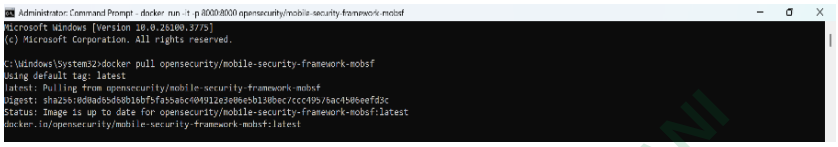
Setelah itu aktifkan WSL 2 *Backend* dan *restart* PC. Ketika Docker Desktop berhasil di *install* maka tampilan akan seperti pada Gambar 4.15.



Gambar 4. 15 Tampilan docker desktop

B. *Download Image* MobSF dari Docker Hub

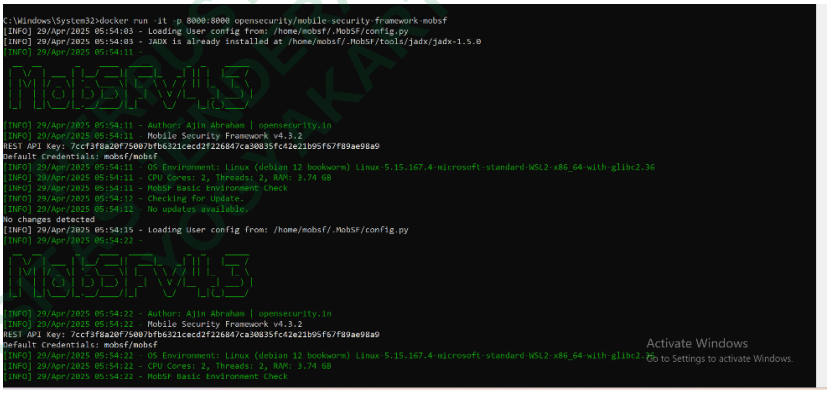
Untuk *download image* mobSF dari Docker Hub yaitu dengan melalui *command prompt* kemudian ketikkan “docker pull opensecurity/mobile-security-framework-mobsf”, untuk hasilnya seperti pada Gambar 4.16.



Gambar 4. 16 *Download image* MobSF

C. Jalankan MobSF *container*

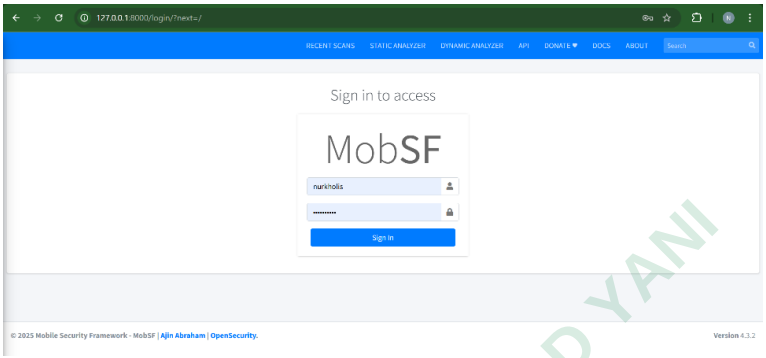
Untuk menjalankan MobSF *container* yaitu melalui *command prompt* kemudian ketikkan “docker run -it -p 8000:8000 opensecurity/mobile-security-framework-mobsf”, untuk hasilnya seperti pada Gambar 4.17.



Gambar 4. 17 Menjalankan MobSF *container*

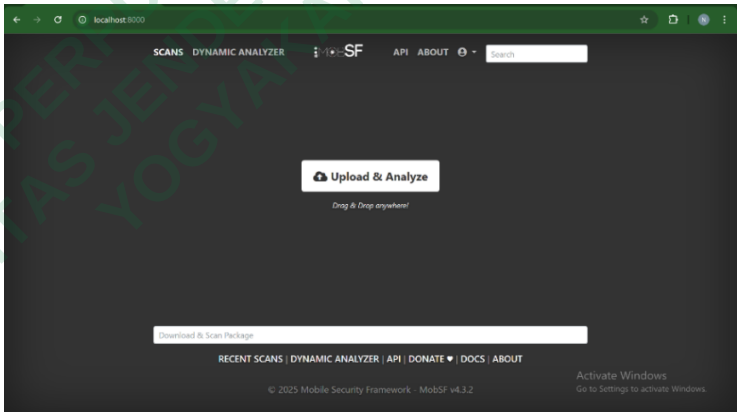
D. Membuka MobSF di browser

Setelah menjalankan MobSF *container* dan sudah berjalan, kemudian buka di browser http://localhost:8000.



Gambar 4. 18 Tampilan MobSF di browser

Setelah muncul tampilan seperti Gambar 4.18, kemudian *login* sesuai dengan *username* dan *password* untuk masuk ke halaman MobSF untuk melakukan analisis seperti pada Gambar 4.19.



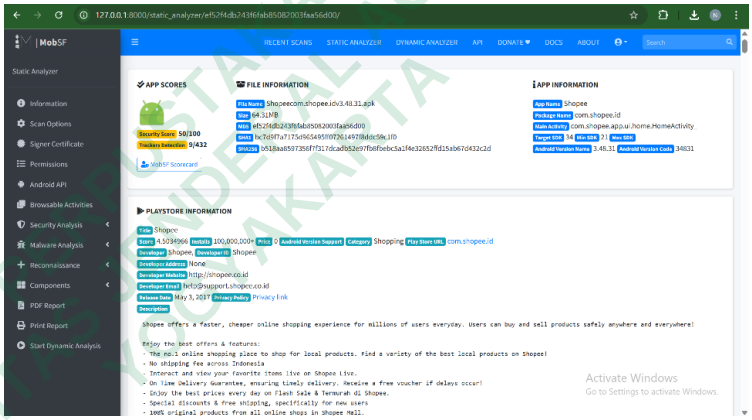
Gambar 4. 19 Tampilan MobSF setelah *login*

Ketika sudah berhasil masuk ke halaman seperti pada Gambar 4.19, maka selanjutnya yaitu untuk melakukan analisis statis dengan *upload* file APK dari aplikasi *e-commerce* yang akan dianalisis yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak pada bagian *upload* & *analysis*.

3. Pemindaian kerentanan aplikasi dengan MobSF

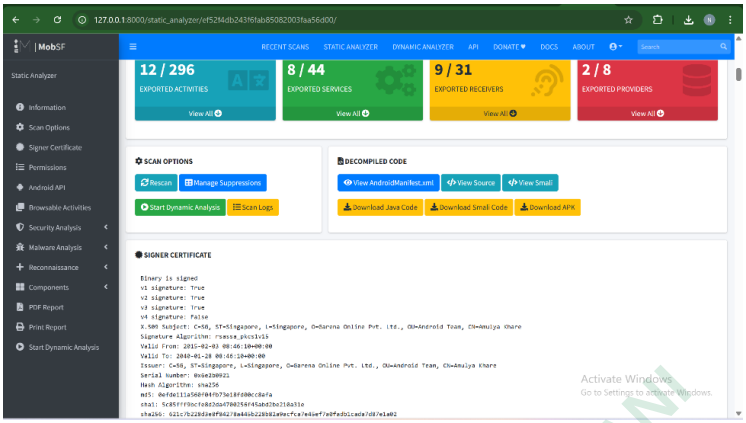
Pada tahap ini dilakukan pemindaian kerentanan terhadap aplikasi *e-commerce* yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak menggunakan *Mobile Security Framework* (MobSF) melalui pendekatan analisis statis (*static analysis*) dengan memeriksa struktur internal dari file APK tanpa perlu mengeksekusi aplikasi secara langsung. Tahap ini bertujuan untuk mengidentifikasi potensi kerentanan dalam aplikasi dengan fokus pada aspek *hardcoded secrets, weak cryptography, insecure data storage, dangerous permissions*, dan SSL/TLS *misconfiguration*. Berikut adalah hasil dari pemindaian kerentanan aplikasi dengan MobSF:

A. Shopee



Gambar 4. 20 Hasil MobSF Shopee (1)

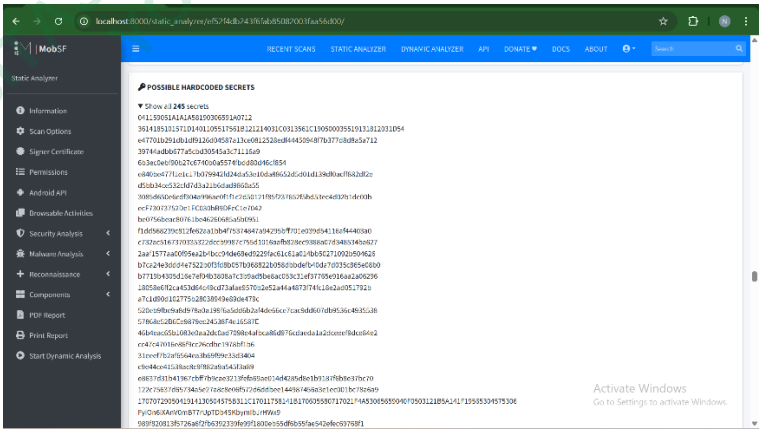
Berdasarkan pemindaian kerentanan dengan MobSF pada aplikasi Shopee seperti ditunjukkan Gambar 4.20, aplikasi Shopee yang dianalisis adalah versi 3.48.31 dengan nama paket com.shopee.id. Skor keamanan pada aplikasi Shopee sebesar 50/100.



Gambar 4. 21 Hasil MobSF Shopee (2)

Aplikasi Shopee terdapat 296 *Exported Activities* dimana 12/296 aktivitas dapat diakses eksternal dan berpotensi dieksploitasi jika rentan. Terdapat 44 *Exported Services* dimana 8/44 layanan dapat dipanggil oleh aplikasi lain. Terdapat 31 *Exported Receivers* dimana 9/31 *broadcast receiver* dapat di *trigger* dari luar. Terdapat 8 *Exported Providers* dimana 2/8 *content providers* dapat diakses eksternal dan berisiko kebocoran data seperti ditunjukkan pada Gambar 4.21.

a) *Hardcoded Secrets*



Gambar 4. 22 *Hardcoded secrets* Shopee

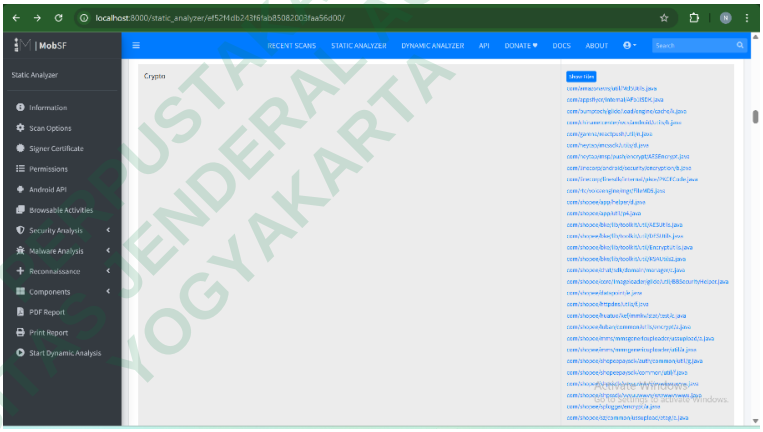
Gambar 4.22 menunjukkan bahwa aplikasi Shopee terdapat penyimpanan informasi sensitif secara langsung (*hardcoded*) di dalam kode sumber aplikasi. informasi yang disimpan secara *hardcoded* berupa nilai-nilai yang menyerupai token, API *key*,

identifier, *password*, *username*, dan kredensial lain yang berpotensi digunakan untuk mengakses layanan *backend* Shopee. Contoh string yang ditemukan yaitu:

- ecF73073752De1EC030bB9DFeC1e7042
- e47701b291db1df9126d04587a13ce0812528edf44450948f7b377d8d8a5a712

Penyimpanan informasi secara *hardcoded* dapat memungkinkan pihak luar untuk mengambil dan menyalahgunakan informasi tersebut. Risiko dari kerentanan ini meliputi akses ilegal terhadap API internal, kebocoran data pengguna, dan eksploitasi sistem *backend* aplikasi.

b) *Weak Cryptography*

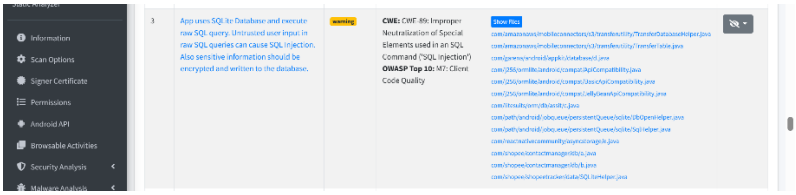


Gambar 4. 23 *Weak cryptography* Shopee

Gambar 4.23 menunjukkan bahwa aplikasi Shopee masih menggunakan algoritma kriptografi yang telah usang dan tidak direkomendasikan seperti MD5, SHA-1, dan AES/CBC dengan PKCS5 *Padding*. Penggunaan MD5 terdeteksi dalam Md5Utils.java dan algoritma AES/CBC ditemukan dalam AESUtils.java. Algoritma MD5 dan SHA-1 memiliki kelemahan terhadap serangan *collision* dimana dua input berbeda dapat menghasilkan hash yang sama. Penggunaan AES dengan mode CBC tanpa integritas membuka potensi terhadap *padding oracle attack*. Hal ini menunjukkan bahwa mekanisme proteksi terhadap data pengguna

belum memadai dan dapat dikompromikan oleh pelaku dengan kemampuan kriptografi.

c) *Insecure Data Storage*



Gambar 4. 24 *Insecure data storage* Shopee (1)

Pada Gambar 4.24 menunjukkan bahwa aplikasi Shopee menyimpan informasi pada SQLite *database* yang merupakan sistem basis data lokal bawaan android. Penyimpanan ini dilakukan tanpa mekanisme enkripsi atau proteksi tambahan yang memadai. Praktik ini menimbulkan potensi risiko keamanan, khususnya apabila data yang disimpan mencakup informasi sensitif seperti riwayat transaksi, kredensial *login*, atau preferensi pengguna. Apabila perangkat pengguna mengalami kehilangan, pencurian, atau disusupi oleh *malware*, maka data tersebut dapat diakses oleh pihak ketiga tanpa hambatan, sehingga berpotensi menyebabkan kebocoran data dan pelanggaran privasi.

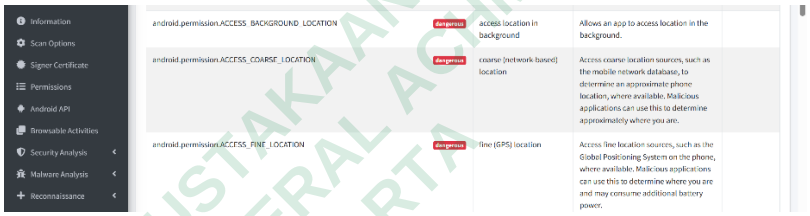
Gambar 4. 25 *Insecure data storage* Shopee (2)

Gambar 4.25 menunjukkan bahwa aplikasi Shopee dapat membaca atau menulis data pada penyimpanan eksternal tanpa enkripsi atau proteksi tambahan. Hal ini menunjukkan bahwa data yang disimpan, baik dalam bentuk file *cache*, konfigurasi, maupun data transaksi, berpotensi dapat diakses oleh aplikasi lain yang terdapat dalam perangkat yang sama dan dapat mengakibatkan eksposur data pengguna apabila perangkat hilang, dicuri, atau terinfeksi oleh *malware*.

Gambar 4. 26 *Insecure data storage* Shopee (3)

Gambar 4.26 menunjukkan bahwa aplikasi Shopee teridentifikasi membuat file sementara (*temporary* file) dan menyimpan data sensitif di dalamnya tanpa mekanisme proteksi yang memadai. Praktik ini berisiko karena file sementara yang bersifat tidak terenkripsi dapat dengan mudah diakses oleh aplikasi lain atau dimanfaatkan oleh perangkat lunak berbahaya yang dapat menyebabkan kebocoran informasi pribadi pengguna.

d) *Dangerous Permissions*

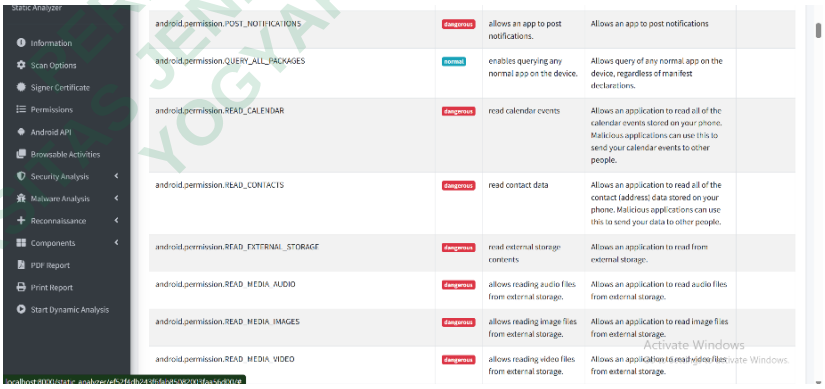


Gambar 4. 27 *Dangerous permissions* Shopee (1)

Gambar 4.27 menunjukkan bahwa aplikasi Shopee terdeteksi meminta akses terhadap beberapa izin lokasi, yaitu *ACCESS_BACKGROUND_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_FINE_LOCATION*. Ketiga izin ini memungkinkan aplikasi untuk memperoleh informasi lokasi pengguna dengan tingkat akurasi berbeda mulai dari perkiraan lokasi berbasis jaringan (*coarse*) hingga lokasi presisi tinggi menggunakan GPS (*fine*), bahkan saat aplikasi berjalan di latar belakang (*background*). Permintaan izin lokasi secara terus-menerus ini dapat menimbulkan risiko terhadap privasi pengguna, terutama apabila tidak disertai dengan transparansi tujuan penggunaan atau pengendalian yang memadai.

Gambar 4. 28 *Dangerous permissions* Shopee (2)

Gambar 4.28 menunjukkan bahwa aplikasi Shopee meminta izin akses terhadap Izin *BLUETOOTH_CONNECT* yang memberikan kemampuan bagi aplikasi untuk terhubung dan berkomunikasi dengan perangkat bluetooth yang terpasang, sementara izin *CAMERA* memungkinkan aplikasi untuk mengakses fitur kamera perangkat, termasuk mengambil foto dan merekam video. Permintaan akses terhadap sumber daya perangkat keras yang sensitif ini mengandung potensi risiko keamanan dan privasi. Tanpa adanya tujuan yang jelas serta pengendalian akses yang tepat, penggunaan izin ini dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan pelacakan, pengintaian, atau pengambilan data visual tanpa persetujuan pengguna.



Gambar 4. 29 *Dangerous permissions* Shopee (3)

Gambar 4.29 menunjukkan bahwa aplikasi Shopee teridentifikasi meminta akses terhadap berbagai izin sensitif (*dangerous permissions*), antara lain izin *POST_NOTIFICATIONS* yang memungkinkan aplikasi mengirimkan notifikasi kepada pengguna, yang jika disalahgunakan dapat menyebabkan gangguan atau serangan *notification spam*.

Izin *READ_CALENDAR* dan *READ_CONTACTS* memberikan akses ke informasi personal seperti jadwal aktivitas dan daftar kontak pengguna, yang dapat menimbulkan risiko pelanggaran privasi apabila data tersebut dikumpulkan tanpa transparansi. Sementara itu, izin *READ_EXTERNAL_STORAGE* serta izin media terkait (*READ_MEDIA_AUDIO, READ_MEDIA_IMAGES*, dan *READ_MEDIA_VIDEO*) memberikan akses ke berbagai file pribadi yang tersimpan di perangkat, seperti foto, video, dan rekaman suara. Tanpa adanya pembatasan dan pengelolaan yang tepat, akses ini dapat menimbulkan eksposur data pribadi, pelanggaran privasi, dan potensi penyalahgunaan oleh pihak ketiga atau *malware*.

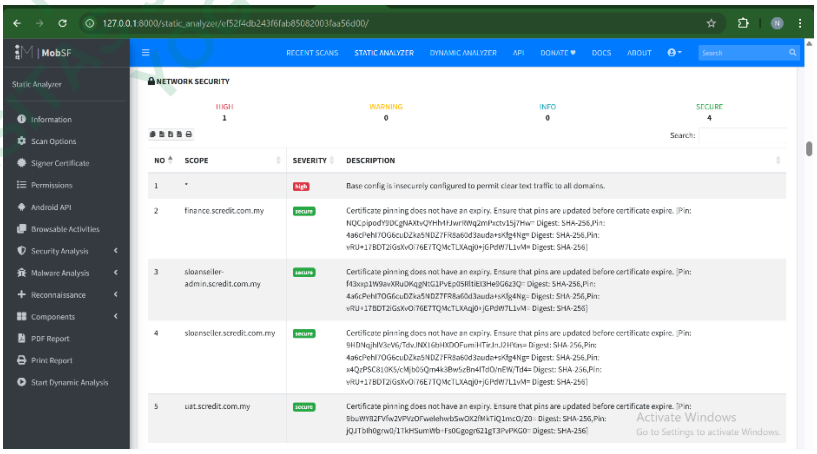
Gambar 4. 30 *Dangerous permissions* Shopee (4)

Gambar 4.30 menunjukkan bahwa aplikasi Shopee juga meminta akses terhadap izin *READ_MEDIA_VISUAL_USER_SELECTED* yang memungkinkan aplikasi mengakses file media visual tertentu seperti gambar atau video yang secara spesifik dipilih oleh pengguna. Sedangkan izin *READ_PHONE_STATE* memberikan kemampuan bagi aplikasi untuk membaca status telepon, status jaringan, serta informasi operator. Permintaan terhadap kedua izin ini menunjukkan potensi risiko privasi apabila tidak disertai transparansi penggunaan dan perlindungan data yang memadai.

Gambar 4. 31 *Dangerous permissions* Shopee (5)

Gambar 4.31 menunjukkan bahwa aplikasi Shopee terdeteksi memiliki izin *WRITE_CALENDAR* yang memungkinkan aplikasi untuk menambahkan, memodifikasi, atau menghapus entri pada kalender pengguna. Jika tidak digunakan secara tepat, akses ini berpotensi disalahgunakan untuk menyisipkan informasi palsu atau mengganggu aktivitas pribadi pengguna. Sementara itu, izin *WRITE_EXTERNAL_STORAGE* memberikan kemampuan bagi aplikasi untuk menyimpan, mengubah, dan menghapus file di penyimpanan eksternal perangkat. Kedua izin tersebut termasuk dalam kategori *dangerous permissions* yang dapat mempengaruhi keamanan dan privasi data pengguna apabila tidak dikelola dengan benar.

e) SSL/TLS *Misconfiguration*

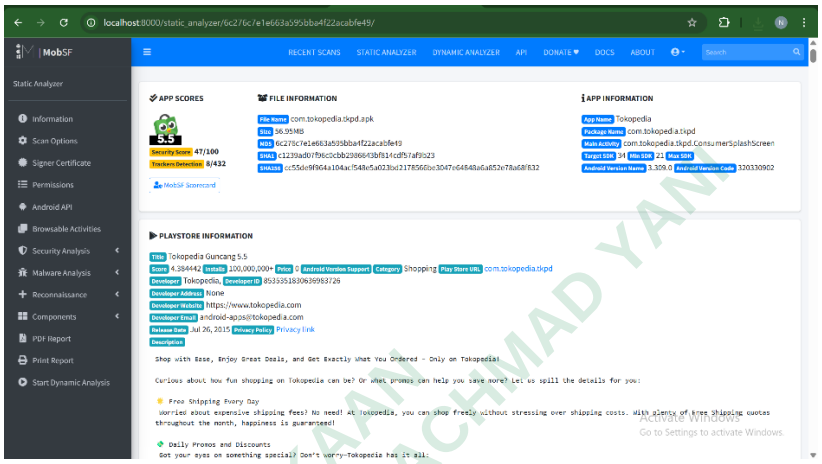


Gambar 4. 32 SSL/TLS *Misconfiguration* Shopee

Gambar 4.32 menunjukkan bahwa aplikasi Shopee mengizinkan komunikasi menggunakan *cleartext traffic* yaitu koneksi HTTP yang tidak terenkripsi ke semua domain. Hal ini terindikasi dari konfigurasi jaringan yang tidak membatasi

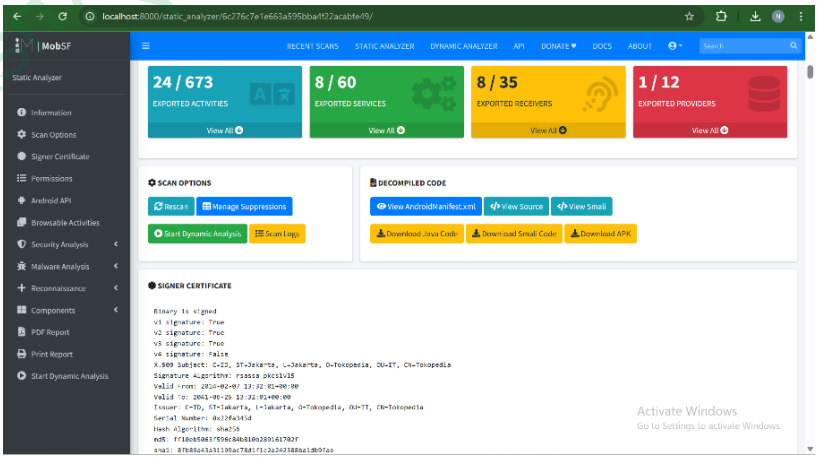
penggunaan protokol HTTP yang ditunjukkan dalam peringatan "*Base config is insecurely configured to permit clear text traffic to all domains"*.

B. Tokopedia



Gambar 4. 33 Hasil MobSF Tokopedia (1)

Berdasarkan pemindaian kerentanan dengan MobSF seperti ditunjukkan Gambar 4.33, aplikasi Tokopedia yang dianalisis adalah versi 3.309.0 dengan nama paket com.tokopedia.tkpd,. Hasil dari pemindaian aplikasi Tokopedia memiliki skor keamanan sebesar 47/100.



Gambar 4. 34 Hasil MobSF Tokopedia (2)

Gambar 4.34 menunjukkan bahwa aplikasi Tokopedia terdapat 673 *Exported Activities* dimana 24/673 aktivitas dapat dipanggil dari luar aplikasi dan wajib dicek apakah dilindungi

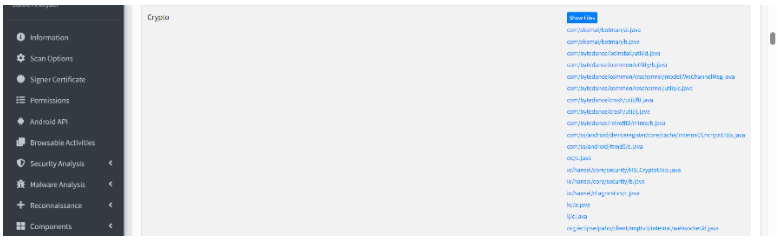
permission. Terdapat 60 *Exported Services* dimana 8/60 *services* dapat diakses oleh aplikasi lain dan berpotensi penyalahgunaan layanan. Terdapat 35 *Exported Receivers* dimana 8/35 *broadcast receiver* aktif secara publik yang dapat dipicu pihak luar. Terdapat 12 *Exported Providers* dimana 1/12 *content provider* dapat diakses publik yang berisiko kebocoran data antar aplikasi.

a) *Hardcoded Secrets*

Gambar 4. 35 *Hardcoded secrets* Tokopedia

Berdasarkan pemindaian kerentanan dengan MobSF, Gambar 4.35 menunjukkan bahwa aplikasi Tokopedia teridentifikasi adanya informasi sensitif yang disimpan secara langsung dalam *source code* aplikasi. Informasi sensitif yang tersimpan secara *hardcoded* meliputi token, API key, dan *identifier* layanan pihak ketiga. Penyimpanan informasi sensitif secara *hardcoded* memberikan celah bagi pihak luar untuk mengeksploitasi akses ke *backend* atau database aplikasi. Risiko yang ditimbulkan berupa akses ilegal ke API, manipulasi sistem, dan kebocoran data pengguna jika informasi sensitif tersebut disalahgunakan oleh pihak yang tidak bertanggungjawab.

b) *Weak Cryptography*



Gambar 4. 36 *Weak cryptography* Tokopedia

Gambar 4.36 menunjukkan bahwa aplikasi Tokopedia menggunakan beberapa teknik atau pendekatan yang mencurigakan

dalam pengolahan kriptografi seperti MD5 dan SHA-1 dan tidak adanya verifikasi penggunaan algoritma kriptografi yang kuat dan modern serta terdapat penggunaan *compiler* R8 tanpa *marker* yang menunjukkan indikasi *obfuscation* tanpa kontrol terhadap komponen kriptografi yang digunakan. Penggunaan algoritma kriptografi yang lemah dapat mempermudah penyerang untuk melakukan *brute-force attack*, *collision attack*, dan mengungkap data terenkripsi.

c) *Insecure Data Storage*

Gambar 4. 37 *Insecure data storage* Tokopedia (1)

Berdasarkan hasil analisis seperti ditunjukkan pada Gambar 4.37, aplikasi Tokopedia memiliki kemampuan untuk membaca dan menulis pada penyimpanan eksternal perangkat. Namun, implementasi tersebut terdeteksi menggunakan konfigurasi izin bawaan (*default permission*) yang tidak tepat, sehingga membuka potensi risiko keamanan. Ketidaktepatan dalam pengaturan izin ini memungkinkan file yang disimpan di penyimpanan eksternal dapat diakses oleh aplikasi lain yang dapat menyebabkan kebocoran data pengguna, khususnya apabila file yang disimpan berisi informasi sensitif seperti *cache* transaksi, gambar, atau dokumen pribadi.

Gambar 4. 38 *Insecure data storage* Tokopedia (2)

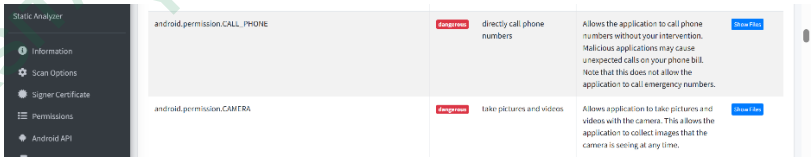
Gambar 4.38 menunjukkan bahwa aplikasi Tokopedia teridentifikasi membuat file sementara (*temporary* file) dan menyimpan data sensitif di dalamnya tanpa mekanisme proteksi yang memadai. Praktik ini berisiko karena file sementara yang bersifat tidak terenkripsi dapat dengan mudah diakses oleh aplikasi

lain atau dimanfaatkan oleh perangkat lunak berbahaya yang dapat menyebabkan kebocoran informasi pribadi pengguna.

d) *Dangerous Permissions*

Gambar 4. 39 *Dangerous permissions* Tokopedia (1)

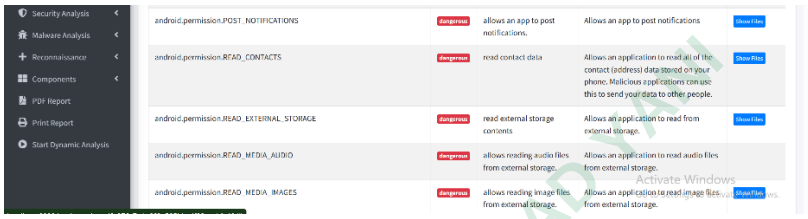
Gambar 4.39 menunjukkan bahwa aplikasi Tokopedia teridentifikasi meminta akses terhadap izin *ACCESS_COARSE_LOCATION* dan *ACCESS_FINE_LOCATION* yang memungkinkan aplikasi untuk memperoleh informasi lokasi pengguna baik dalam tingkat akurasi rendah (berbasis jaringan) maupun tingkat akurasi tinggi (menggunakan GPS). Permintaan izin ini mengandung potensi risiko privasi apabila tidak disertai transparansi dalam penggunaannya. Akses lokasi secara terus-menerus atau tanpa pengendalian dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan pelacakan aktivitas pengguna secara *real time*.



Gambar 4. 40 *Dangerous permissions* Tokopedia (2)

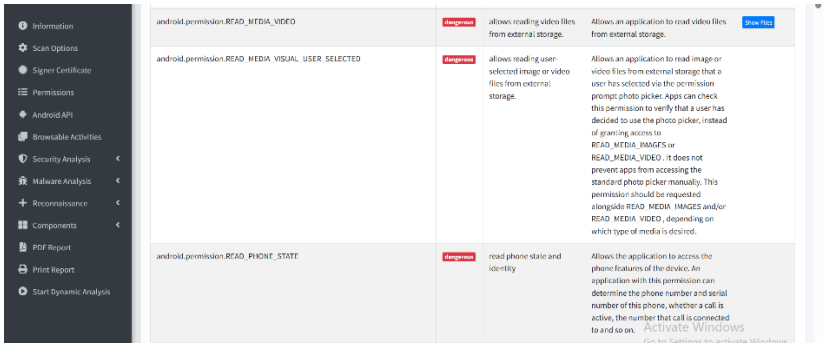
Gambar 4.40 menunjukkan bahwa aplikasi Tokopedia meminta akses terhadap izin *CALL_PHONE* dan *CAMERA*. Izin *CALL_PHONE* memungkinkan aplikasi untuk melakukan panggilan telepon secara langsung dari perangkat tanpa melalui antarmuka dialer bawaan. Meskipun fitur ini dapat digunakan untuk menghubungi layanan pelanggan atau mitra penjual, implementasinya tetap perlu diawasi secara ketat agar tidak menimbulkan risiko penyalahgunaan seperti *auto-dialing* tanpa

persetujuan pengguna. Sementara itu, izin *CAMERA* memberikan akses terhadap perangkat kamera yang digunakan untuk mengambil gambar atau merekam video. Penggunaan fitur kamera merupakan titik rawan dalam keamanan aplikasi karena dapat dimanfaatkan untuk aktivitas pengintaian apabila tidak disertai kontrol akses yang memadai.



Gambar 4. 41 *Dangerous permissions* Tokopedia (3)

Gambar 4.41 menunjukkan bahwa aplikasi Tokopedia meminta akses terhadap sejumlah izin sensitif (*dangerous permissions*) antara lain izin *POST_NOTIFICATIONS* yang memberikan kemampuan bagi aplikasi untuk mengirimkan notifikasi ke perangkat pengguna. Meskipun fitur ini dapat meningkatkan interaksi dan penyampaian informasi, jika tidak dikelola dengan baik, dapat menyebabkan gangguan atau risiko *notification spam*. Izin *READ_CONTACTS* memungkinkan aplikasi mengakses data kontak pengguna, termasuk informasi pribadi seperti nama, nomor telepon, dan alamat email. Akses ini sangat sensitif dan dapat menimbulkan pelanggaran privasi apabila data dikumpulkan atau digunakan tanpa persetujuan yang jelas. Sementara itu, izin *READ_EXTERNAL_STORAGE*, *READ_MEDIA_AUDIO*, dan *READ_MEDIA_IMAGES* memberikan akses ke file pribadi pengguna yang disimpan di penyimpanan eksternal, seperti dokumen, rekaman audio, dan gambar. Tanpa penerapan enkripsi atau kontrol akses yang ketat, akses ini berisiko menyebabkan kebocoran data pribadi melalui aplikasi pihak ketiga atau *malware*.



Gambar 4. 42 *Dangerous permissions* Tokopedia (4)

Gambar 4.42 menunjukkan bahwa aplikasi Tokopedia juga teridentifikasi meminta akses terhadap beberapa izin dengan tingkat sensitivitas tinggi, yaitu izin *READ_MEDIA_VIDEO* yang memberikan akses kepada aplikasi untuk membaca file video yang tersimpan di penyimpanan eksternal perangkat pengguna. Sementara itu, izin *READ_MEDIA_VISUAL_USER_SELECTED* memungkinkan aplikasi mengakses file media visual (seperti gambar atau video) yang secara eksplisit dipilih oleh pengguna. Selain itu, izin *READ_PHONE_STATE* memberikan aplikasi kemampuan untuk membaca status perangkat dan informasi jaringan, termasuk status panggilan serta identitas operator. Informasi ini bersifat sensitif karena dapat digunakan untuk pelacakan perangkat atau identifikasi pengguna tanpa sepengetahuan mereka. Permintaan terhadap izin-izin tersebut perlu mendapatkan perhatian serius karena menyangkut akses langsung terhadap data dan identitas pengguna.

Gambar 4. 43 *Dangerous permissions* Tokopedia (5)

Gambar 4.43 menunjukkan bahwa aplikasi Tokopedia juga meminta akses terhadap beberapa izin tingkat lanjut yang memiliki

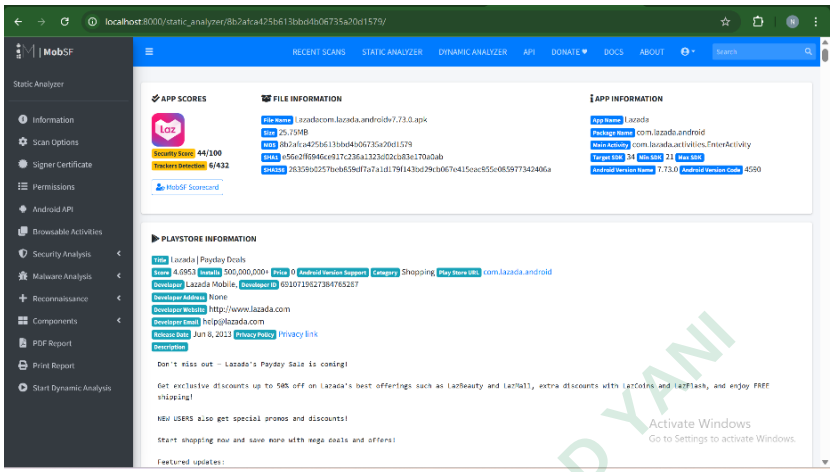
potensi dampak signifikan terhadap privasi dan keamanan pengguna, yaitu izin *RECORD_AUDIO* memungkinkan aplikasi untuk merekam suara melalui mikrofon perangkat. Jika tidak dikontrol dengan baik, akses ini dapat disalahgunakan untuk merekam percakapan pengguna tanpa sepengetahuan mereka, yang merupakan pelanggaran serius terhadap privasi. Izin *SYSTEM_ALERT_WINDOW* memberikan kemampuan bagi aplikasi untuk menampilkan elemen visual (*overlay*) di atas aplikasi lain.

Fitur ini berisiko digunakan dalam serangan *phishing overlay*, di mana aplikasi meniru antarmuka aplikasi lain untuk mencuri data pengguna seperti kredensial login. Izin *USE_BIOMETRIC* mengizinkan aplikasi menggunakan autentikasi biometrik seperti sidik jari atau pemindaian wajah. Terakhir, izin *USE_CREDENTIALS* memungkinkan aplikasi mengakses kredensial akun yang tersimpan di sistem android, yang dapat mencakup token atau data otentikasi lainnya. Akses ini sangat sensitif dan harus dijaga ketat untuk mencegah penyalahgunaan informasi akun.

e) SSL/TLS *Misconfiguration*

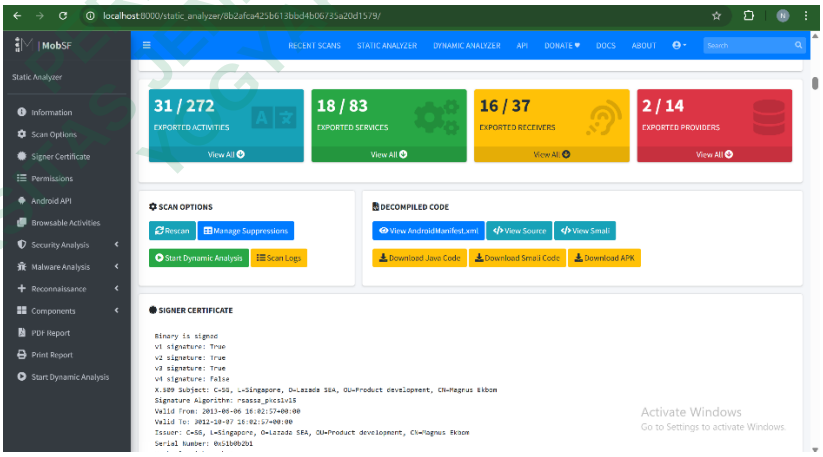
Berdasarkan hasil pemindaian kerentanan dengan MobSF pada aplikasi Tokopedia, tidak ditemukan kerentanan yang menunjukkan adanya konfigurasi SSL/TLS yang salah. Tidak ditemukan peringatan yang mengindikasikan aplikasi Tokopedia mengizinkan koneksi HTTP yang mengimplikasikan bahwa aplikasi ini kemungkinan besar telah menggunakan koneksi HTTPS secara *default* dan pengizinan *traffic cleartext* atau *trust* terhadap sertifikat yang tidak sah.

C. Lazada



Gambar 4. 44 Hasil MobSF Lazada (1)

Berdasarkan hasil pemindaian kerentanan dengan MobSF seperti ditunjukkan Gambar 4.44, aplikasi Lazada yang dianalisis adalah versi 7.73.0 dengan nama paket com.lazada.android. Berdasarkan hasil pemindaian aplikasi Lazada memiliki skor keamanan sebesar 44/100.

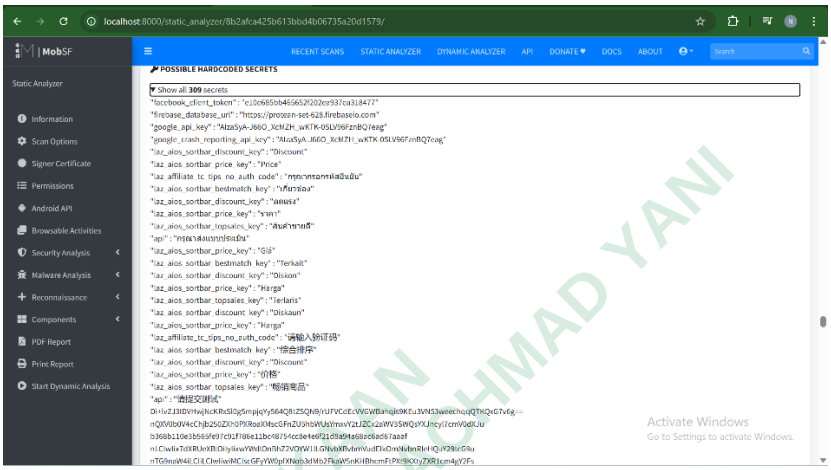


Gambar 4. 45 Hasil MobSF Lazada (2)

Gambar 4.45 menunjukkan bahwa aplikasi Lazada terdapat 272 *Exported Activities* dimana 31/272 aktivitas dapat dipanggil oleh aplikasi lain. Terdapat 83 *Exported Services* dimana 18/83 *services* berjalan di latar belakang yang dapat dipanggil eksternal. Terdapat 37 *Exported Receivers* dimana 16/37 *broadcast receiver*

dapat di *trigger* aplikasi luar. Terdapat 14 *Exported Providers* dimana 2/14 *content provider* dapat diakses aplikasi lain yang berpotensi kebocoran data.

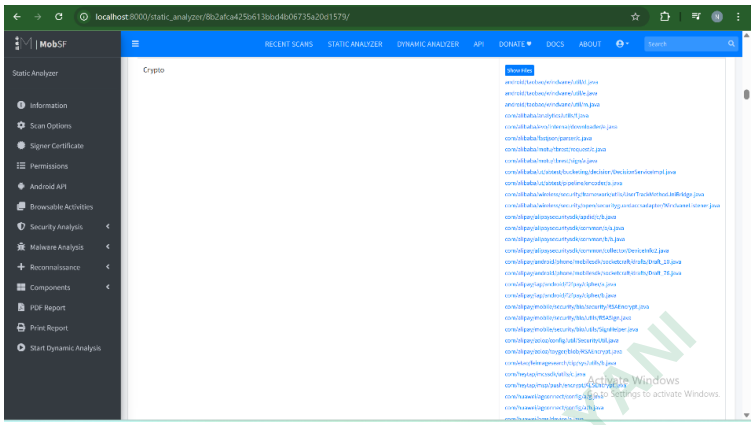
a) *Hardcoded Secrets*



Gambar 4. 46 *Hardcoded secrets* Lazada

Gambar 4.46 menunjukkan bahwa aplikasi Lazada terdeteksi keberadaan informasi sensitif yang ditanam langsung di dalam *source code* aplikasi (*hardcoded*), yang dapat mencakup token, *credential* internal, atau kunci API yang tersimpan dalam file Java/Dex. Selain itu string terenkripsi dengan metode base64 atau hex yang tidak memiliki pengamanan tambahan. Penyimpanan informasi sensitif secara *hardcoded* memungkinkan eksposur data melalui proses *reserve engineering*. Apabila informasi tersebut berhasil diekstrak oleh pihak ketiga, maka dapat terjadi akses tidak sah ke sistem *backend*, pencurian data pengguna, dan manipulasi layanan internal aplikasi.

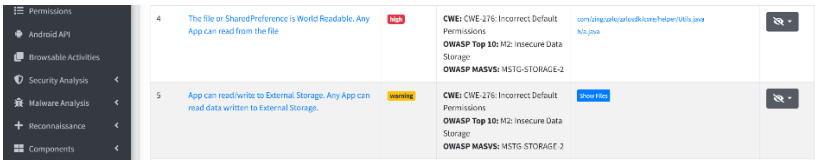
b) *Weak Cryptography*



Gambar 4. 47 *Weak cryptography* Lazada

Gambar 4.47 menunjukkan bahwa aplikasi Tokopedia terdeteksi menggunakan algoritma kriptografi yang telah usang dan tanda tangan digital dengan algoritma SHA1withRSA yang memiliki kelemahan kriptografi berupa *collision vulnerability*. Selain itu ditemukan juga penggunaan *obfuscation* menggunakan R8 *compiler* tanpa *marker* yang menyulitkan proses audit kriptografi lebih lanjut namun juga menandakan bahwa metode enkripsi belum dapat dipastikan kekuatannya. Penggunaan algoritma kriptografi usang seperti SHA-1 dapat memungkinkan serangan berbasis *hash collision* dan menurunkan integritas mekanisme autentikasi digital.

c) *Insecure Data Storage*



Gambar 4. 48 *Insecure data storage* Lazada (1)

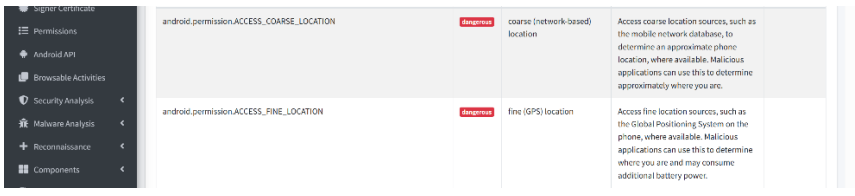
Gambar 4.48 menunjukkan bahwa aplikasi Lazada ditemukan bahwa terdapat file atau data yang disimpan melalui *shared preferences* dalam aplikasi memiliki atribut "*world readable*", yang berarti file tersebut dapat dibaca oleh aplikasi lain yang terinstal pada perangkat. Selain itu, aplikasi juga memiliki kemampuan untuk membaca dan menulis data ke penyimpanan

eksternal, di mana data yang disimpan tidak dilindungi dengan enkripsi atau kontrol akses tambahan. Kondisi ini memungkinkan aplikasi pihak ketiga untuk mengakses data tersebut secara bebas, termasuk data yang berpotensi bersifat sensitif. Kerentanan ini dapat dimanfaatkan oleh aplikasi berbahaya untuk memperoleh informasi pribadi pengguna tanpa sepengetahuan atau persetujuan mereka, sehingga meningkatkan risiko kebocoran data, pelanggaran privasi, dan eksposur terhadap serangan berbasis perangkat lunak jahat (*malware*).

Gambar 4. 49 *Insecure data storage* Lazada (2)

Gambar 4.49 menunjukkan bahwa aplikasi Lazada diketahui membuat *temporary* file (file sementara) sebagai bagian dari proses operasionalnya. Namun, ditemukan bahwa file sementara tersebut digunakan untuk menyimpan informasi sensitif, seperti data pengguna atau detail transaksi, tanpa adanya mekanisme perlindungan yang memadai sehingga dapat diakses oleh aplikasi lain atau dimanfaatkan oleh perangkat lunak berbahaya. Selain itu, file *temporary* bersifat tidak stabil dan dapat tetap tersimpan meskipun aplikasi telah ditutup, yang meningkatkan risiko eksposur data jika perangkat pengguna hilang, dicuri, atau disusupi *malware*.

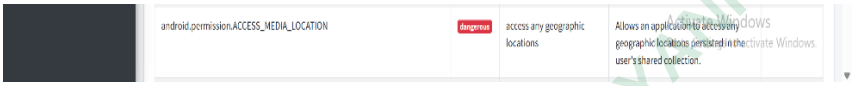
d) *Dangerous Permissions*



Gambar 4. 50 *Dangerous permissions* Lazada (1)

Gambar 4.50 menunjukkan bahwa aplikasi Lazada teridentifikasi meminta akses terhadap izin *ACCESS_COARSE_LOCATION* yang memungkinkan deteksi

lokasi dengan tingkat akurasi rendah menggunakan jaringan seluler atau Wi-Fi, sedangkan *ACCESS_FINE_LOCATION* memungkinkan pelacakan lokasi yang lebih akurat melalui GPS. Meskipun izin ini dapat digunakan untuk mendukung fitur berbasis lokasi, seperti rekomendasi produk atau penentuan wilayah pengiriman, akses terhadap data lokasi tetap memiliki implikasi serius terhadap privasi pengguna.



Gambar 4. 51 *Dangerous permissions* Lazada (2)

Gambar 4.51 menunjukkan bahwa aplikasi Lazada meminta akses terhadap izin *ACCESS_MEDIA_LOCATION*, yang memungkinkan aplikasi untuk membaca metadata lokasi geografis (*geotag*) yang disematkan pada file media seperti foto dan video yang disimpan di perangkat pengguna. Informasi lokasi yang terkandung dalam file media dapat mengungkap keberadaan pengguna dalam waktu dan tempat tertentu, yang berpotensi disalahgunakan oleh pihak yang tidak bertanggung jawab.

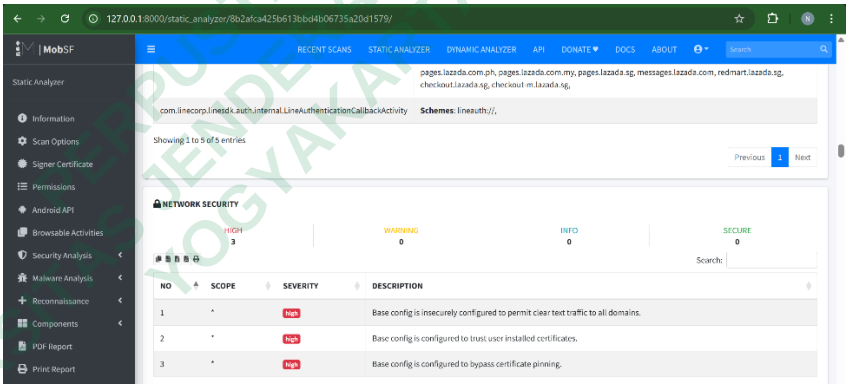
Gambar 4. 52 *Dangerous permissions* Lazada (3)

Gambar 4.52 menunjukkan bahwa aplikasi Lazada meminta akses terhadap izin *BLUETOOTH_ADVERTISE* yang memberikan kemampuan kepada aplikasi untuk mengiklankan kehadiran perangkat melalui sinyal bluetooth, sehingga perangkat lain dapat mendeteksinya. Sedangkan izin *BLUETOOTH_CONNECT* memungkinkan aplikasi untuk menjalin koneksi dengan perangkat bluetooth lain yang terhubung ke perangkat pengguna. Penggunaan yang tidak dikendalikan dapat membuka celah untuk pelacakan perangkat, pengumpulan data tanpa izin, atau potensi komunikasi yang tidak aman dengan perangkat pihak ketiga.

Gambar 4. 53 *Dangerous permissions* Lazada (4)

Gambar 4.53 menunjukkan bahwa aplikasi Lazada juga meminta akses terhadap izin *BLUETOOTH_SCAN* yang memberikan kemampuan kepada aplikasi untuk melakukan pemindaian terhadap perangkat bluetooth di sekitar, yang dapat digunakan untuk mendeteksi keberadaan dan identitas perangkat lain. Meskipun fitur ini dapat mendukung fungsi seperti konektivitas perangkat pintar atau promosi berbasis lokasi. Sementara itu, izin *CAMERA* memungkinkan aplikasi mengakses kamera perangkat untuk mengambil foto atau merekam video.

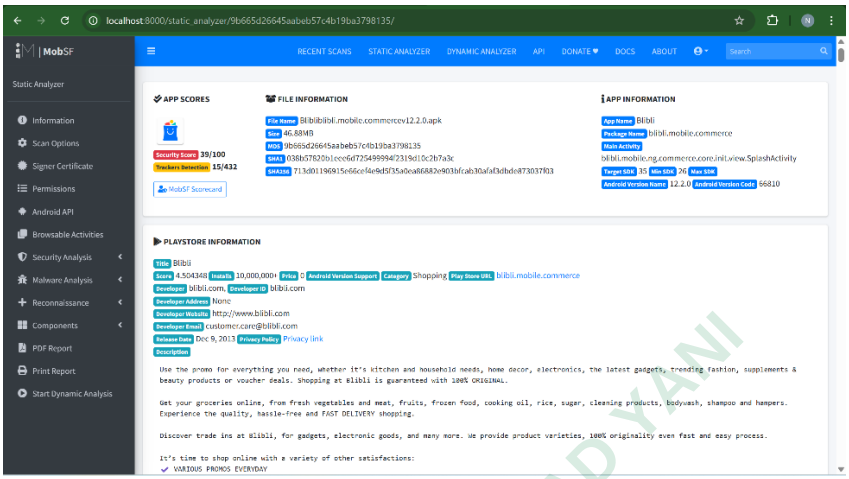
e) SSL/TLS *Misconfiguration*



Gambar 4. 54 SSL/TLS *Misconfiguration* Lazada

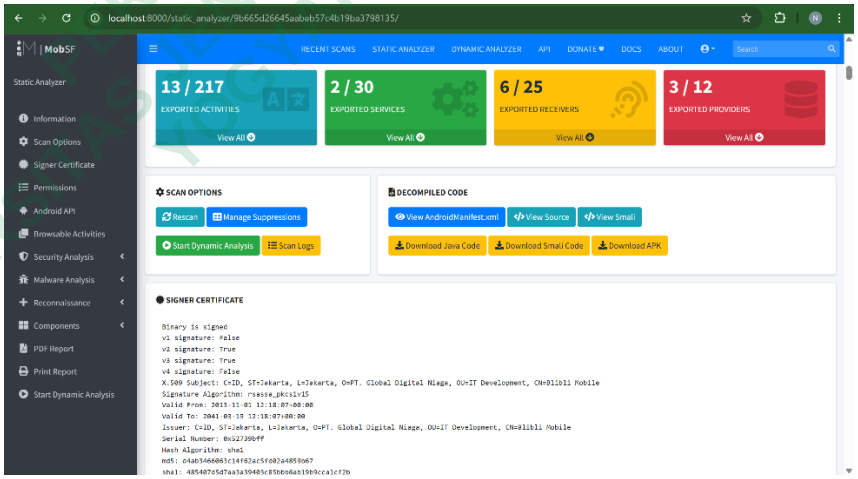
Gambar 4.54 menunjukkan bahwa aplikasi Lazada terdapat beberapa kerentanan dalam konfigurasi SSL/TLS diantaranya aplikasi mengizinkan komunikasi menggunakan *cleartext traffic* ke seluruh domain, konfigurasi keamanan jaringan mempercayai sertifikat yang di instal oleh pengguna yang berbahaya karena dapat disalahgunakan untuk menyisipkan sertifikat palsu, ditemukan *bypass* terhadap *certificate pinning* yang memungkinkan aplikasi menerima sertifikat selain dari *server* resmi tanpa validasi yang kuat.

D. Blibli



Gambar 4. 55 Hasil MobSF Blibli (1)

Berdasarkan hasil pemindaian kerentanan dengan MobSF seperti ditunjukkan Gambar 4.55, aplikasi Blibli yang dianalisis adalah versi 12.2.0 dengan nama paket Blibli.mobile.commerce. Berdasarkan hasil pemindaian aplikasi Blibli memiliki skor keamanan sebesar 39/100.

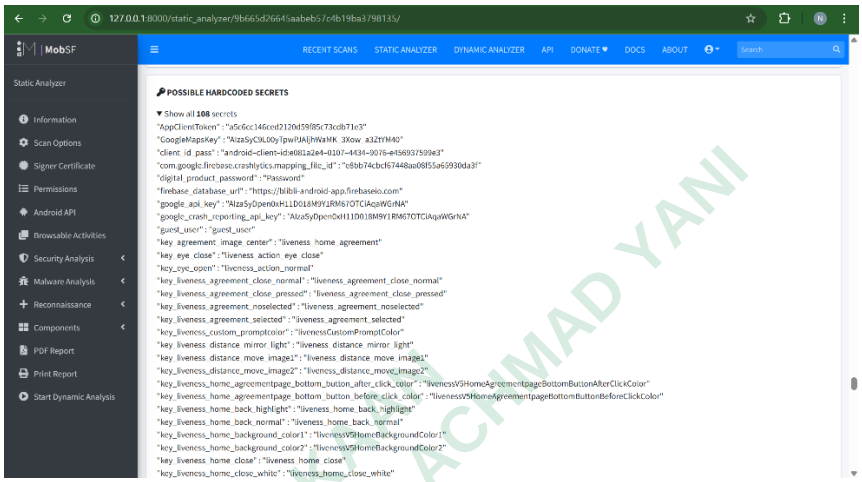


Gambar 4. 56 Hasil MobSF Blibli (2)

Gambar 4.56 menunjukkan bahwa aplikasi Blibli terdapat 217 *Exported Activities* dimana 13/217 aktivitas dapat dipanggil oleh aplikasi luar (potensi eksploitasi jika tanpa *permission*). Terdapat 30 *Exported Services* dimana 2/30 *services* dapat diakses oleh aplikasi lain. Terdapat 25 *Exported Receiver* dimana 6/25

broadcast receiver aktif secara publik. Terdapat 12 *Exported Providers* dimana 3/12 *content provider* dapat diakses eksternal (berpotensi kebocoran data).

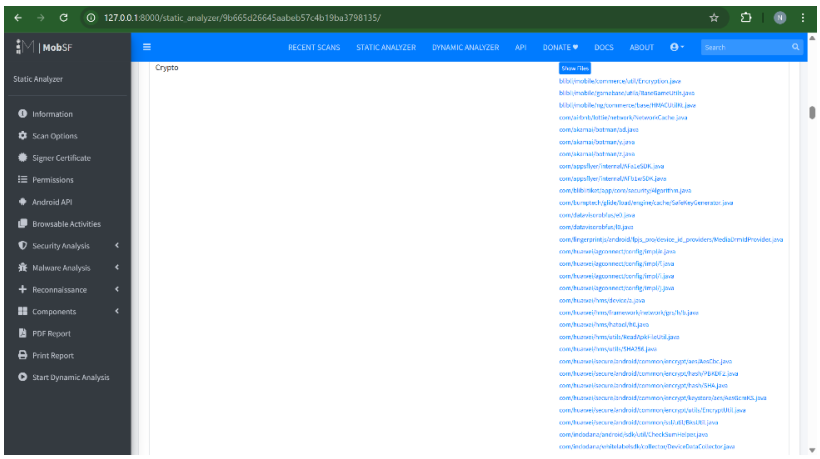
a) *Hardcoded Secrets*



Gambar 4. 57 *Hardcoded secrets* Blibli

Gambar 4.57 menunjukkan bahwa aplikasi Blibli terdeteksi adanya keberadaan *hardcoded secrets* di dalam kode sumber aplikasi. Terdapat penyisipan informasi sensitif secara langsung dalam kode seperti API *Key* Google Maps, *token firebase*, *guest user*, dan *password* statik. Penyimpanan informasi sensitif secara langsung dalam kode ini sangat berpotensi menyebabkan kebocoran data dan pembajakan akun pengguna.

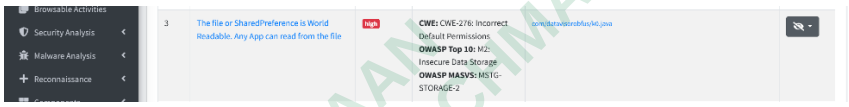
b) *Weak Cryptography*



Gambar 4. 58 *Weak cryptography* Blibli

Gambar 4.58 menunjukkan bahwa aplikasi Blibli terdeteksi menggunakan algoritma kriptografi yang sudah dianggap lemah dan usang. Penggunaan algoritma hash MD5 dan SHA-1 yang rentan terhadap serangan *collision*. Kemudian penggunaan mode enkripsi CBC (*Cipher Block Chaining*) dengan *padding* PKCS5/PKCS7 yang rentan terhadap serangan *padding oracle*. Di dalam aplikasi Blibli *Random Number Generator* (RNG) yang digunakan tidak memiliki tingkat entropi yang memadai yang meningkatkan risiko prediksi hasil acak oleh pihak ketiga.

c) *Insecure Data Storage*

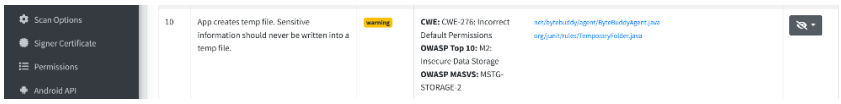


Gambar 4. 59 *Insecure data storage* Blibli (1)

Gambar 4.59 menunjukkan bahwa di dalam aplikasi Blibli ditemukan bahwa file atau *shared preferences* yang digunakan oleh aplikasi memiliki atribut "*world readable*", yang berarti file tersebut dapat diakses dan dibaca oleh aplikasi lain yang terinstal pada perangkat yang sama. Dengan konfigurasi izin yang terbuka, aplikasi pihak ketiga, termasuk aplikasi berbahaya, dapat mengeksploitasi celah ini untuk mengakses dan mencuri data pengguna.

Gambar 4. 60 *Insecure data storage* Blibli (2)

Gambar 4.60 menunjukkan bahwa aplikasi Blibli juga teridentifikasi memiliki kemampuan untuk membaca dan menulis data ke penyimpanan eksternal perangkat. Namun, aktivitas ini dilakukan dengan konfigurasi izin bawaan (*default permission*) yang tidak tepat, sehingga file yang disimpan di penyimpanan eksternal dapat diakses oleh aplikasi lain tanpa kontrol akses yang memadai.



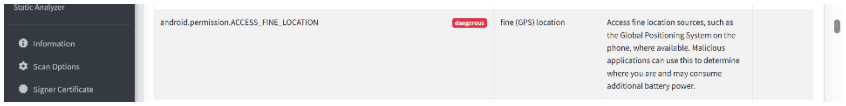
Gambar 4. 61 *Insecure data storage* Blibli (3)

Gambar 4.61 menunjukkan bahwa aplikasi Blibli terdeteksi bahwa aplikasi membuat file sementara (*temporary* file) selama proses operasionalnya. Namun, file sementara tersebut digunakan untuk menyimpan informasi yang bersifat sensitif, seperti data pengguna atau informasi sesi, tanpa adanya perlindungan tambahan seperti enkripsi atau kontrol akses. Penyimpanan data sensitif ke dalam *temporary* file tidak direkomendasikan karena file semacam ini biasanya disimpan di direktori sistem yang bersifat terbuka dan dapat diakses oleh aplikasi lain yang semakin meningkatkan potensi eksposur data dan risiko kebocoran informasi.

d) *Dangerous Permissions*

Gambar 4. 62 *Dangerous permissions* Blibli (1)

Gambar 4.62 menunjukkan bahwa aplikasi Blibli teridentifikasi meminta akses terhadap izin *ACCESS_BACKGROUND_LOCATION* yang memberikan hak akses lokasi bahkan saat aplikasi tidak sedang digunakan secara aktif oleh pengguna atau berjalan di latar depan. Sementara itu izin *ACCESS_COARSE_LOCATION* memungkinkan aplikasi memperoleh lokasi dengan akurasi rendah menggunakan sumber seperti jaringan seluler dan Wi-Fi. Permintaan terhadap izin-izin ini menimbulkan implikasi serius terhadap privasi, karena aplikasi dapat melacak pergerakan atau lokasi pengguna secara terus-menerus tanpa keterlibatan langsung dari pengguna.

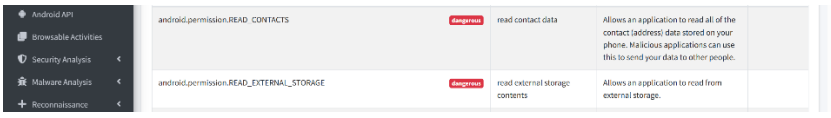


Gambar 4. 63 *Dangerous permissions* Blibli (2)

Gambar 4.63 menunjukkan bahwa aplikasi Blibli juga teridentifikasi meminta akses terhadap izin *ACCESS_FINE_LOCATION* yang memungkinkan aplikasi memperoleh informasi lokasi pengguna dengan tingkat akurasi tinggi, biasanya melalui penggunaan sensor GPS. Akses terhadap data lokasi presisi tinggi dapat menimbulkan risiko privasi, terutama jika data tersebut dikumpulkan secara terus-menerus tanpa persetujuan yang jelas atau tanpa pemberitahuan kepada pengguna.

Gambar 4. 64 *Dangerous permissions* Blibli (3)

Gambar 4.64 menunjukkan bahwa aplikasi Blibli juga meminta akses terhadap izin *BLUETOOTH_CONNECT* yang memberikan kemampuan bagi aplikasi untuk terhubung dan berkomunikasi dengan perangkat lain melalui koneksi bluetooth. Meskipun fitur ini dapat mendukung integrasi layanan tertentu, akses terhadap bluetooth tetap memiliki implikasi terhadap keamanan dan privasi, karena dapat membuka potensi interaksi dengan perangkat lain yang tidak terautentikasi atau tidak sah.

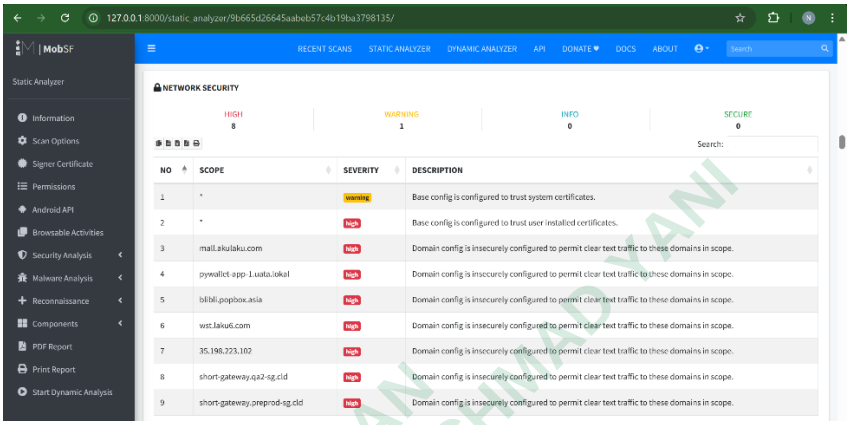


Gambar 4. 65 *Dangerous permissions* Blibli (4)

Gambar 4.65 menunjukkan bahwa aplikasi Blibli meminta izin *READ_CONTACTS*, yang memungkinkan untuk mengakses dan membaca daftar kontak pengguna yang tersimpan di perangkat. Jika tidak dikendalikan dengan baik, informasi pribadi seperti nama, nomor telepon, dan alamat email dapat terekspos dan dimanfaatkan untuk tujuan yang tidak sah, seperti spam, rekayasa sosial, atau pencurian identitas. Izin

READ_EXTERNAL_STORAGE, yang berarti mengizinkan aplikasi membaca file di penyimpanan eksternal. Jika tidak dikendalikan dengan baik dapat berpotensi kebocoran data sensitif pengguna.

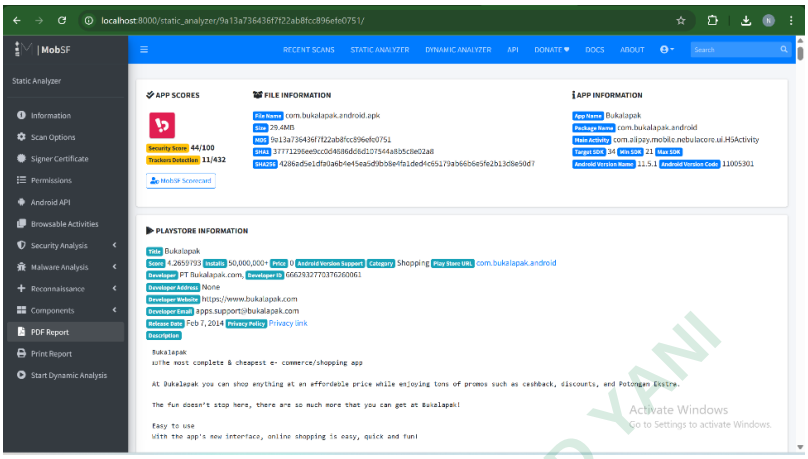
e) SSL/TLS *Misconfiguration*



Gambar 4. 66 SSL/TLS *Misconfiguration* Blibli

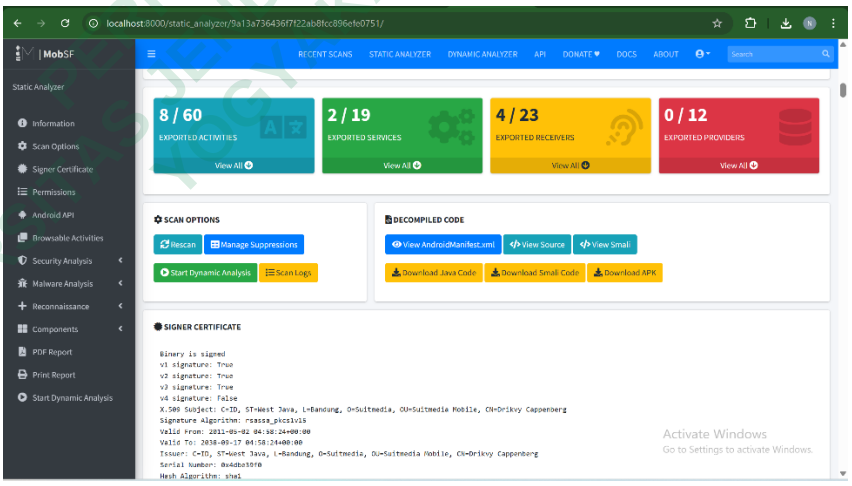
Gambar 4.66 menunjukkan bahwa aplikasi Blibli terdeteksi mempercayai sertifikat yang di instal oleh pengguna yang ditunjukkan pada "*Base config is configured to trust user installed certificates"*, hal ini memungkinkan pihak yang tidak bertanggungjawab untuk memasang sertifikat palsu untuk menyadap komunikasi TLS aplikasi. Selain itu aplikasi Blibli juga terdeteksi mengizinkan komunikasi menggunakan *cleartext traffic* yaitu koneksi HTTP yang tidak dienkripsi ke beberapa domain tertentu. Penggunaan protokol HTTP tanpa enkripsi pada aplikasi akan meningkatkan risiko penyadapan data sensitif oleh pihak ketiga yang berada dalam jaringan yang sama.

E. Bukalapak



Gambar 4. 67 Hasil MobSF Bukalapak (1)

Berdasarkan pemindaian kerentanan dengan MobSF seperti ditunjukkan Gambar 4.67, aplikasi Bukalapak yang dianalisis adalah versi 11.5.1 dengan nama paket com.bukalapak.android. Berdasarkan hasil pemindaian aplikasi Bukalapak memiliki skor keamanan sebesar 44/100.

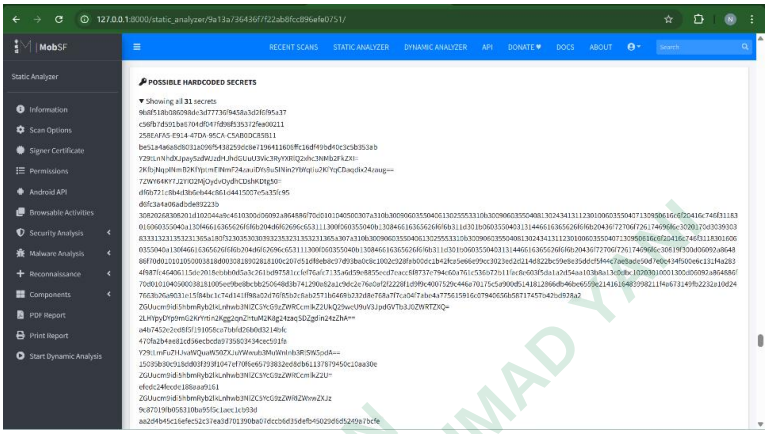


Gambar 4. 68 Hasil MobSF Bukalapak (2)

Gambar 4.68 menunjukkan bahwa aplikasi Bukalapak terdapat 60 *Exported Activities* dimana 8/60 aktivitas layar atau fungsi aplikasi dapat diakses aplikasi lain. Terdapat 19 *Exported Services* dimana 2/19 *services* dapat dijalankan oleh aplikasi luar. Terdapat 23 *Exported Receivers* dimana 4/23 *broadcast receiver*

dapat diaktifkan oleh pihak luar. Terdapat 12 *Exported Providers* dan tidak ada *content providers* yang diekspos.

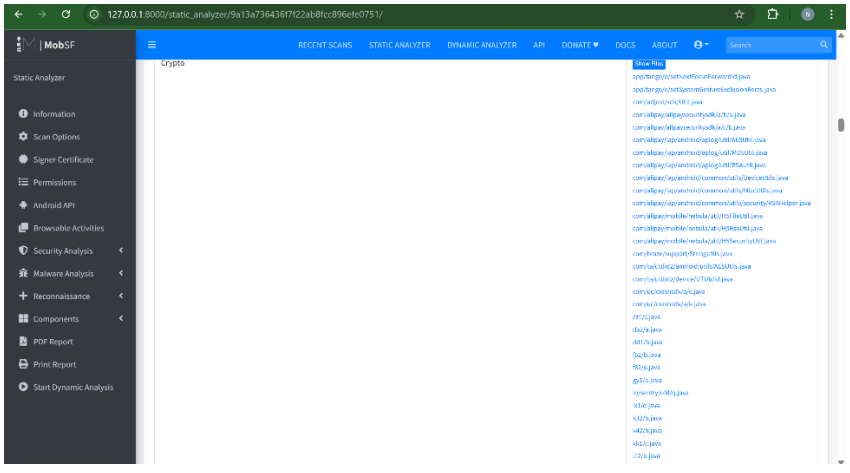
a) *Hardcoded Secrets*



Gambar 4. 69 *Hardcoded secrets* Bukalapak

Gambar 4.69 menunjukkan bahwa aplikasi Bukalapak terdeteksi adanya keberadaan informasi sensitif yang disimpan secara langsung dalam kode sumber aplikasi (*hardcoded*). Informasi sensitif yang disimpan secara *hardcoded* seperti token, *credential*, *string* yang terenkripsi dalam format base64, UUID dan API *key* serta fragmen sertifikat yang tersemat dalam string literal. Hal ini mengindikasikan risiko pencurian identitas digital dan penyalahgunaan layanan *backend*.

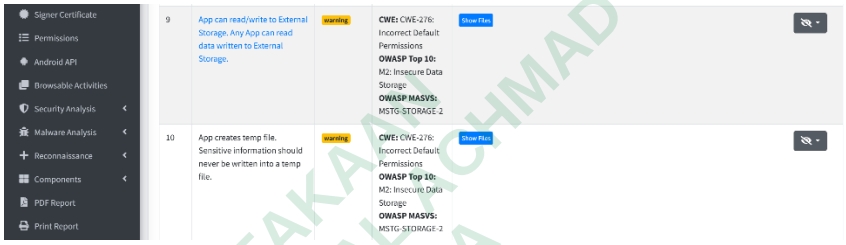
b) *Weak Cryptography*



Gambar 4. 70 *Weak cryptography* Bukalapak

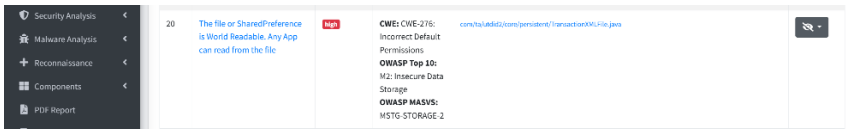
Gambar 4.70 menunjukkan bahwa aplikasi Blibli menggunakan sejumlah algoritma kriptografi yang telah usang dan tidak lagi direkomendasikan seperti MD5 dan SHA-1 yang memiliki kelemahan terhadap serangan *collision*, mode enkripsi AES-ECB dan CBC dengan PKCS5/PKCS7 *padding* yang rentan terhadap serangan *padding oracle*, serta penggunaan *Random Number Generator* (RNG) yang tidak memenuhi standar kriptografi yang kuat.

c) *Insecure Data Storage*



Gambar 4. 71 *Insecure data storage* Bukalapak (1)

Gambar 4.71 menunjukkan bahwa aplikasi Bukalapak memiliki kemampuan untuk membaca dan menulis data ke penyimpanan eksternal perangkat. Namun, aktivitas ini dilakukan dengan pengaturan izin bawaan (*default permission*) yang tidak tepat, sehingga data yang ditulis ke media penyimpanan eksternal dapat diakses secara bebas oleh aplikasi lain termasuk aplikasi pihak ketiga yang menimbulkan risiko keamanan yang signifikan, terutama apabila data yang disimpan mencakup informasi sensitif seperti file *cache* pengguna, riwayat transaksi, atau berkas yang berkaitan dengan aktivitas akun. Tanpa adanya mekanisme enkripsi atau pembatasan akses, data tersebut berpotensi dieksploitasi oleh perangkat lunak berbahaya (*malware*) atau aplikasi yang tidak sah.



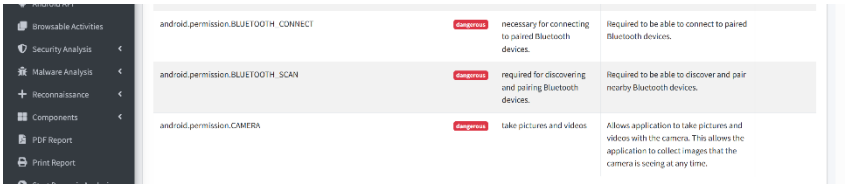
Gambar 4. 72 *Insecure data storage* Bukalapak (2)

Gambar 4.72 menunjukkan bahwa aplikasi Blibli teridentifikasi bahwa file *shared preferences* yang digunakan oleh aplikasi memiliki atribut "*world readable*", yang berarti file tersebut dapat diakses oleh aplikasi lain yang terinstal pada perangkat yang sama. Hal ini terjadi karena adanya penerapan izin akses *default* (*default permission*) yang tidak dikonfigurasi dengan benar, sehingga tidak membatasi akses hanya untuk aplikasi yang bersangkutan.

d) *Dangerous Permissions*

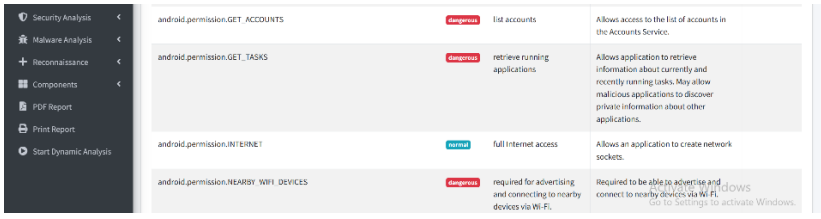
Gambar 4. 73 *Dangerous permissions* Bukalapak (1)

Gambar 4.73 menunjukkan bahwa aplikasi Bukalapak teridentifikasi meminta akses terhadap dua izin Lokasi yaitu izin *ACCESS_COARSE_LOCATION* memberikan kemampuan kepada aplikasi untuk mendeteksi lokasi pengguna dengan akurasi rendah, biasanya melalui jaringan seluler atau Wi-Fi. Sementara itu, *ACCESS_FINE_LOCATION* memungkinkan aplikasi memperoleh informasi lokasi dengan tingkat akurasi tinggi, menggunakan sensor GPS perangkat. Penggunaan kedua izin ini dapat mendukung fitur berbasis lokasi seperti penentuan alamat pengiriman, pencarian mitra terdekat, atau personalisasi konten berdasarkan wilayah pengguna. Namun demikian, akses terhadap data lokasi juga menimbulkan risiko privasi, terutama jika pengumpulan data dilakukan tanpa transparansi, persetujuan eksplisit, atau pengendalian yang memadai.



Gambar 4. 74 *Dangerous permissions* Bukalapak (2)

Gambar 4.74 menunjukkan bahwa aplikasi Bukalapak meminta akses terhadap sejumlah izin perangkat keras yaitu izin *BLUETOOTH_CONNECT* yang memungkinkan aplikasi untuk melakukan koneksi dan pertukaran data dengan perangkat bluetooth lain yang telah dipasangkan, sementara itu *BLUETOOTH_SCAN* memberikan kemampuan bagi aplikasi untuk memindai perangkat bluetooth di sekitar perangkat pengguna, termasuk yang belum terhubung sebelumnya. Kedua izin ini dapat dimanfaatkan untuk mendukung fitur tambahan berbasis konektivitas, tetapi juga memiliki implikasi terhadap privasi dan keamanan, karena membuka kemungkinan pelacakan perangkat atau interaksi dengan perangkat eksternal yang tidak sah. Sementara itu, izin *CAMERA* memberikan aplikasi akses ke fitur kamera perangkat untuk mengambil foto atau merekam video. Tanpa kontrol akses yang tepat, akses kamera dapat menimbulkan risiko pengintaian atau perekaman tanpa izin pengguna, yang merupakan pelanggaran serius terhadap privasi.



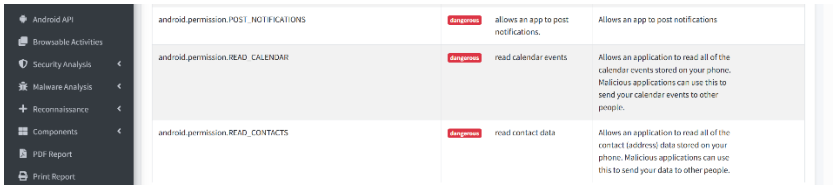
Gambar 4. 75 *Dangerous permissions* Bukalapak (3)

Gambar 4.75 menunjukkan bahwa aplikasi Bukalapak juga meminta akses terhadap beberapa izin sistem yang berpotensi mempengaruhi privasi dan keamanan informasi pengguna, yaitu izin *GET_ACCOUNTS* yang memberikan kemampuan kepada aplikasi untuk mengakses daftar akun yang tersimpan di perangkat, seperti

akun Google atau akun lainnya yang terhubung. Akses ini dapat digunakan untuk otentikasi atau sinkronisasi, namun jika tidak dikelola dengan benar, dapat menimbulkan risiko akses tidak sah terhadap informasi pribadi atau data lintas akun.

Izin *GET_TASKS* memungkinkan aplikasi untuk melihat aktivitas atau proses aplikasi lain yang sedang berjalan di perangkat. Meskipun kini penggunaannya telah dibatasi dalam versi android terbaru, pada perangkat tertentu izin ini tetap dapat menimbulkan risiko pelanggaran isolasi proses dan pengintaian aktivitas pengguna. Izin INTERNET bersifat dasar dan diperlukan agar aplikasi dapat terhubung ke jaringan dan melakukan komunikasi data. Namun, akses ini tetap relevan dalam konteks keamanan karena semua transmisi data harus dilakukan secara terenkripsi dan aman untuk mencegah intersepsi melalui serangan MITM.

Kemudian izin *NEARBY_WIFI_DEVICES* memungkinkan aplikasi mendeteksi dan berinteraksi dengan perangkat lain yang berada dalam jangkauan jaringan Wi-Fi terdekat. Penggunaan izin ini dapat mendukung fitur seperti berbagi data atau koneksi perangkat sekitar, namun juga berpotensi digunakan untuk pelacakan lokasi atau aktivitas perangkat lain apabila tidak dibatasi dengan ketat.



Gambar 4. 76 *Dangerous permissions* Bukalapak (4)

Gambar 4.76 menunjukkan bahwa aplikasi Bukalapak meminta akses terhadap beberapa izin sensitif yang berkaitan dengan interaksi dan informasi pribadi pengguna, yaitu izin *POST_NOTIFICATIONS* yang memungkinkan aplikasi mengirimkan notifikasi langsung ke perangkat pengguna. Tanpa

pengaturan yang tepat, notifikasi yang berlebihan dapat menimbulkan gangguan pengguna atau potensi *notification spam*. Izin *READ_CALENDAR* memberikan akses kepada aplikasi untuk membaca entri kalender pengguna, termasuk informasi mengenai jadwal, acara, dan kegiatan pribadi. Sementara itu, izin *READ_CONTACTS* memungkinkan aplikasi mengakses daftar kontak pengguna yang mencakup informasi sensitif seperti nama, nomor telepon, dan alamat email.

Gambar 4. 77 *Dangerous permissions* Bukalapak (5)

Gambar 4.77 menunjukkan bahwa aplikasi Bukalapak meminta akses terhadap berbagai izin yang berkaitan dengan pembacaan file media dan data pengguna yang tersimpan di perangkat izin *READ_EXTERNAL_STORAGE* yang memberikan akses umum ke seluruh file yang tersimpan di penyimpanan eksternal perangkat, termasuk dokumen, media, dan file *cache* dari aplikasi lain. Sedangkan izin *READ_MEDIA_AUDIO*, *READ_MEDIA_IMAGES*, dan *READ_MEDIA_VIDEO* secara spesifik mengizinkan aplikasi untuk membaca file media berdasarkan jenisnya, seperti rekaman audio, gambar, dan video pengguna. Sementara itu, izin *READ_MEDIA_VISUAL_USER_SELECTED* yaitu hanya mengizinkan aplikasi membaca file media visual yang secara eksplisit dipilih oleh pengguna melalui antarmuka sistem. Meskipun lebih aman, izin ini tetap berkaitan dengan akses ke informasi

pribadi pengguna. Akses terhadap file media ini memiliki implikasi terhadap privasi dan keamanan data, terutama apabila data yang dibaca berisi konten sensitif dan tidak dilindungi oleh enkripsi atau pengendalian akses tambahan dapat menimbulkan risiko kebocoran informasi pribadi atau penyalahgunaan data oleh pihak ketiga.

Gambar 4. 78 *Dangerous permissions* Bukalapak (6)

Gambar 4.78 menunjukkan bahwa aplikasi Bukalapak meminta akses terhadap izin *READ_PHONE_STATE*, yang memungkinkan aplikasi untuk memperoleh informasi terkait status perangkat dan jaringan seluler. Izin ini memberikan akses terhadap data seperti status panggilan, identitas operator jaringan, serta jenis koneksi yang sedang digunakan. Jika tidak dikelola secara aman dan transparan, akses terhadap data ini berpotensi menimbulkan risiko terhadap privasi dan keamanan pengguna, termasuk potensi penyalahgunaan oleh aplikasi pihak ketiga.

Gambar 4. 79 *Dangerous permissions* Bukalapak (7)

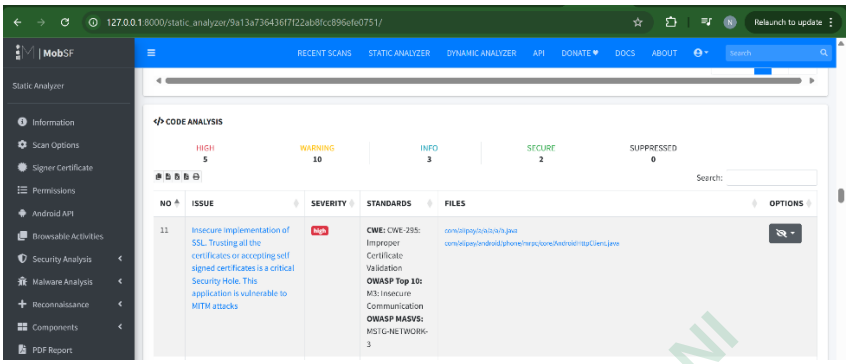
Gambar 4.79 menunjukkan bahwa aplikasi Bukalapak meminta akses terhadap izin *USE_CREDENTIALS* yang memungkinkan aplikasi untuk menggunakan kredensial akun yang tersimpan di perangkat, seperti akun Google atau akun layanan lainnya yang telah diotorisasi oleh sistem android. Meskipun dapat meningkatkan kenyamanan pengguna, izin ini memiliki tingkat sensitivitas yang tinggi karena memberikan akses terhadap data autentikasi yang berhubungan langsung dengan identitas digital pengguna. Jika tidak dikelola dengan baik, penggunaan izin ini berpotensi disalahgunakan untuk mengakses informasi akun secara tidak sah atau menyamar sebagai pengguna di dalam sistem aplikasi.

Gambar 4. 80 *Dangerous permissions* Bukalapak (8)

Gambar 4.80 menunjukkan bahwa aplikasi Bukalapak juga meminta akses terhadap beberapa izin sistem yang memiliki potensi dampak terhadap privasi dan kontrol perangkat pengguna, yaitu izin *WRITE_CALENDAR* yang memungkinkan aplikasi untuk menambahkan, mengubah, atau menghapus entri pada kalender perangkat yang dapat digunakan untuk mencatat aktivitas seperti pengingat transaksi atau jadwal promosi. Namun, jika tidak dikendalikan secara tepat akses ini dapat menyebabkan gangguan terhadap privasi pengguna, terutama jika entri kalender dimodifikasi tanpa persetujuan.

Izin *WRITE_EXTERNAL_STORAGE* memberikan kemampuan bagi aplikasi untuk menyimpan atau memodifikasi file di penyimpanan eksternal perangkat. Penyimpanan data pada media eksternal yang tidak terenkripsi berisiko tinggi terhadap kebocoran data, karena file yang ditulis dapat diakses oleh aplikasi lain termasuk aplikasi berbahaya. Sementara itu, izin *WRITE_SETTINGS* memungkinkan aplikasi untuk mengubah pengaturan sistem perangkat, seperti pengaturan jaringan, suara, atau tampilan layar. Izin ini memiliki risiko yang cukup besar karena dapat mempengaruhi fungsi dasar perangkat dan jika disalahgunakan dapat digunakan untuk mengubah perilaku sistem tanpa sepengetahuan pengguna.

e) SSL/TLS *Misconfiguration*



Gambar 4. 81 SSL/TLS *Misconfiguration* Bukalapak

Gambar 4.81 menunjukkan bahwa aplikasi Bukalapak ditemukan memiliki implementasi SSL yang mempercayai semua sertifikat tanpa validasi terhadap keresmian sertifikat tersebut. Konfigurasi seperti ini sangat berbahaya karena dapat menyebabkan serangan MITM dimana penyerang dapat menyisipkan sertifikat palsu untuk menyadap data yang dikirimkan antara aplikasi dan *server*.

Berdasarkan hasil pemindaian kerentanan menggunakan *Mobile Security Framework* (MobSF) terhadap lima aplikasi *e-commerce* populer di Indonesia yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak ditemukan bahwa seluruh aplikasi menunjukkan keberadaan kerentanan yang signifikan pada aspek keamanan. Analisis statis terhadap file APK masing-masing aplikasi mengungkapkan keberadaan *hardcoded secrets*, penggunaan algoritma kriptografi yang lemah seperti MD5 dan SHA-1, penyimpanan data sensitif tanpa enkripsi yang memadai, permintaan izin akses berbahaya, dan konfigurasi SSL/TLS yang tidak aman. Temuan kerentanan berdasarkan pemindaian dengan MobSF ini menunjukkan bahwa kelima aplikasi dalam aspek keamanan informasi masih belum sepenuhnya diperhatikan dalam praktik pengembangan dan implementasi sistem. Kerentanan-kerentanan yang ditemukan menandakan adanya kelemahan umum dalam pengelolaan kredensial, enkripsi data, dan kontrol izin aplikasi sehingga perlu meningkatkan perlindungan terhadap data pengguna dan mencegah potensi serangan yang dapat merugikan pengguna maupun penyedia layanan.

4.2.3 Pemetaan Kerentanan ke OWASP Mobile Top 10 2024

Pada tahap ini dilakukan pengklasifikasian setiap kerentanan secara sistematis dari setiap aplikasi *e-commerce* yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak berdasarkan hasil temuan dari pemindaian kerentanan dengan MobSF. Pemetaan kerentanan ke dalam kategori OWASP Mobile Top 10 2024, yaitu:

1. M1: *Improper Credential Usage*
2. M2: *Inadequate Supply Chain Security*
3. M3: *Insecure Authentication/Authorization*
4. M4: *Insufficient Input/Output Validation*
5. M5: *Insecure Communication*
6. M6: *Inadequate Privacy Controls*
7. M7: *Insufficient Binary Protections*
8. M8: *Security Misconfiguration*
9. M9: *Insecure Data Storage*
10. M10: *Insufficient Cryptography*

Pemetaan kerentanan ini bertujuan untuk mengklasifikasikan kerentanan secara standar agar memudahkan dalam proses analisis risiko dan penyusunan rekomendasi mitigasi (OWASP, 2024). Berikut adalah hasil pemetaan kerentanan ke OWASP Mobile Top 10 2024 dari setiap aplikasi berdasarkan hasil pemindaian kerentanan dengan MobSF:

A. Shopee

Tabel 4. 12 Pemetaan kerentanan Shopee

No	Temuan Kerentanan	Keterangan	Kategori OWASP Mobile Top 10 2024
1.	Penggunaan algoritma lemah atau usang seperti MD5 dan SHA-1	Algoritma *hash* yang lemah dan rentan terhadap *collision*	M10: *Insufficient Cryptography*
2.	Penggunaan *raw query* SQLite	Rentan terhadap serangan SQL *Injection* dan input pengguna dapat mempengaruhi eksekusi *query* SQL	M4: *Insufficient Input/Output Validation*

No	Temuan Kerentanan	Keterangan	Kategori OWASP Mobile Top 10 2024
3.	Terdapat *hardcoded secrets* (API *Key*, token, *password, username*)	Informasi sensitif tertahan dalam *source code*	M1: *Improper Credential Usage*
4.	Penggunaan *random values* (nilai acak) yang tidak benar-benar acak atau mudah ditebak	Menggunakan *random number* generator yang tidak aman secara kriptografis	M10: *Insufficient Cryptography*
5.	Penyimpanan data di *external storage*	Rentan diakses oleh aplikasi lain	M9: *Insecure Data Storage*
6.	Penggunaan mode enkripsi CBC + PKCS5/7	Konfigurasi rentan terhadap *padding oracle attack*	M10: *Insufficient Cryptography*
7.	Meminta izin/hak akses tidak relevan atau berbahaya	Potensi penyalahgunaan data pribadi pengguna	M6: *Inadequate Privacy Controls*
8.	Aktivitas dan komponen alamat IP tidak aman	Aplikasi dapat diakses oleh penyerang atau pihak ketiga	M8: *Security Misconfiguration*
9.	Membuat *temporary* file dan menyimpan data sensitif didalamnya	Data bisa diakses oleh pihak lain di sistem	M9: *Insecure Data Storage*
10.	Memiliki konfigurasi *debuggable* dan pengaturan yang tidak sesuai	Bisa dieksekusi dalam mode debug dan penyalahgunaan oleh penyerang	M7: *Insufficient Binary Protections*

B. Tokopedia

Tabel 4. 13 Pemetaan kerentanan Tokopedia

No	Temuan Kerentanan	Keterangan	Kategori OWASP Mobile Top 10 2024
1.	Dapat membaca atau menulis data di *external storage*	Rentan diakses oleh aplikasi lain	M9: *Insecure Data Storage*
2.	Terdapat *hardcoded secrets* (*username, password*, API *Key*)	Informasi sensitif tertahan dalam *source code*	M1: *Improper Credential Usage*

No	Temuan Kerentanan	Keterangan	Kategori OWASP Mobile Top 10 2024
3.	Penggunaan algoritma lemah atau usang seperti MD5 dan SHA-1	Algoritma *hash* yang lemah dan rentan terhadap *collision*	M10: *Insufficient Cryptography*
4.	Penggunaan *raw query* SQLite	Rentan terhadap serangan SQL *Injection* dan *input* pengguna dapat mempengaruhi eksekusi *query* SQL	M4: *Insufficient Input/Output Validation*
5.	Membuat temporary file dan menyimpan data sensitif didalamnya	Data bisa diakses oleh pihak lain di sistem	M9: *Insecure Data Storage*
6.	Penggunaan *random values* (nilai acak) yang tidak benar-benar acak atau mudah ditebak	Menggunakan *random number* generator yang tidak aman secara kriptografis	M10: *Insufficient Cryptography*
7.	Penggunaan mode enkripsi CBC + PKCS5/7	Konfigurasi rentan terhadap *padding oracle attack*	M10: *Insufficient Cryptography*

C. Lazada

Tabel 4. 14 Pemetaan kerentanan Lazada

No	Temuan Kerentanan	Keterangan	Kategori OWASP Mobile Top 10 2024
1.	Penggunaan *random values* (nilai acak) yang tidak benar-benar acak atau mudah ditebak	Menggunakan *random number* generator yang tidak aman secara kriptografis	M10: *Insufficient Cryptography*
2.	Aktivitas dan komponen alamat IP tidak aman	Aplikasi dapat diakses oleh penyerang atau pihak ketiga	M8: *Security Misconfiguration*
3.	*Shared preferences* atau aplikasi diatur dengan izin yang terlalu longgar	File dapat diakses oleh aplikasi lain dan tidak ada batasan privasi	M9: *Insecure Data Storage*
4.	Dapat membaca atau menulis data di *external storage*	Rentan diakses oleh aplikasi lain	M9: *Insecure Data Storage*

No	Temuan Kerentanan	Keterangan	Kategori OWASP Mobile Top 10 2024
5.	Terdapat *hardcoded secrets* (*username, password*, API *Key*)	Informasi sensitif tertahan dalam *source code*	M1: *Improper Credential Usage*
6.	Penggunaan algoritma lemah atau usang seperti MD5, SHA-1, dan ECB	Algoritma *hash* yang lemah dan rentan terhadap *collision*	M10: *Insufficient Cryptography*
7.	Tidak melakukan validasi sertifikat SSL dengan benar	Rentan terhadap serangan MITM	M5: *Insecure Communication*
8.	Penggunaan *raw query* SQLite	Rentan terhadap serangan SQL *Injection* dan input pengguna dapat mempengaruhi eksekusi *query* SQL	M4: *Insufficient Input/Output Validation*
9.	Membuat *temporary* file dan menyimpan data sensitif didalamnya	Data bisa diakses oleh pihak lain di sistem	M9: *Insecure Data Storage*
10.	Penggunaan mode enkripsi CBC + PKCS5/7	Konfigurasi rentan terhadap *padding oracle attack*	M10: *Insufficient Cryptography*
11.	Memiliki konfigurasi *debuggable* dan pengaturan yang tidak sesuai	Bisa dieksekusi dalam mode debug dan penyalahgunaan oleh penyerang	M7: *Insufficient Binary Protections*
12.	Menggunakan komponen *webview* dengan konfigurasi yang tidak aman	Serangan *Remote Code Execution* (RCE) dan pencurian data	M4: *Insufficient Input/Output Validation*

D. Blibli

Tabel 4. 15 Pemetaan kerentanan Blibli

No	Temuan Kerentanan	Keterangan	Kategori OWASP Mobile Top 10 2024
1.	Terdapat *hardcoded secrets* (*username, password*, API *Key*)	Informasi sensitif tertahan dalam *source code*	M1: *Improper Credential Usage*
2.	*Shared preferences* atau aplikasi diatur	*File* dapat diakses oleh aplikasi lain dan tidak ada batasan privasi	M9: *Insecure Data Storage*

No	Temuan Kerentanan	Keterangan	Kategori OWASP Mobile Top 10 2024
	dengan izin yang terlalu longgar		
3.	Aktivitas dan komponen alamat IP tidak aman	Aplikasi dapat diakses oleh penyerang atau pihak ketiga	M8: *Security Misconfiguration*
4.	Penggunaan algoritma lemah atau usang seperti MD5 dan SHA-1	Algoritma hash yang lemah dan rentan terhadap *collision*	M10: *Insufficient Cryptography*
5.	Dapat membaca atau menulis data di *external storage*	Rentan diakses oleh aplikasi lain	M9: *Insecure Data Storage*
6.	Penggunaan *random values* (nilai acak) yang tidak benar-benar acak atau mudah ditebak	Menggunakan *random number* generator yang tidak aman secara kriptografis	M10: *Insufficient Cryptography*
7.	Penggunaan mode enkripsi CBC + PKCS5/7	Konfigurasi rentan terhadap *padding oracle attack*	M10: *Insufficient Cryptography*
8.	Membuat *temporary* file dan menyimpan data sensitif didalamnya	Data bisa diakses oleh pihak lain di sistem	M9: *Insecure Data Storage*
9.	Aplikasi meminta hak akses *root* atau *superuser*	Dapat menyebabkan kerusakan sistem dan kebocoran data pengguna	M7: *Insufficient Binary Protections*
10.	Menggunakan komponen *webview* dengan konfigurasi yang tidak aman	Serangan *Remote Code Execution* (RCE) dan pencurian data	M4: *Insufficient Input/Output Validation*
11.	Penggunaan *raw query* SQLite	Rentan terhadap serangan SQL *Injection* dan *input* pengguna dapat mempengaruhi eksekusi *query* SQL	M4: *Insufficient Input/Output Validation*

E. Bukalapak

Tabel 4. 16 Pemetaan kerentanan Bukalapak

No	Temuan Kerentanan	Keterangan	Kategori OWASP Mobile Top 10 2024
1.	Terdapat *hardcoded secrets* (API *Key*, token, *password, username*)	Informasi sensitif tertahan dalam *source code*	M1: *Improper Credential Usage*
2.	Penggunaan *random values* (nilai acak) yang tidak benar-benar acak atau mudah ditebak	Menggunakan *random numbe*r generator yang tidak aman secara kriptografis	M10: *Insufficient Cryptography*
3.	Penggunaan algoritma lemah atau usang seperti MD5, SHA-1, dan ECB	Algoritma *hash* yang lemah dan rentan terhadap *collision*	M10: *Insufficient Cryptography*
4.	Aktivitas dan komponen alamat IP tidak aman	Aplikasi dapat diakses oleh penyerang atau pihak ketiga	M8: *Security Misconfiguration*
5.	Menggunakan komponen *webview* dengan konfigurasi yang tidak aman	Serangan *Remote Code Execution* (RCE) dan pencurian data	M4: *Insufficient Input/Output Validation*
6.	Dapat membaca atau menulis data di *external storage*	Rentan diakses oleh aplikasi lain	M9: *Insecure Data Storage*
7.	Membuat *temporary* file dan menyimpan data sensitif didalamnya	Data bisa diakses oleh pihak lain di sistem	M9: *Insecure Data Storage*
8.	Tidak melakukan validasi sertifikat SSL dengan benar	Rentan terhadap serangan MITM	M5: *Insecure Communication*
9.	Memiliki konfigurasi *debuggable* dan pengaturan yang tidak sesuai	Bisa dieksekusi dalam mode debug dan penyalahgunaan oleh penyerang	M7: *Insufficient Binary Protections*
10.	Penggunaan mode enkripsi CBC + PKCS5/7	Konfigurasi rentan terhadap *padding oracle attack*	M10: *Insufficient Cryptography*
11.	Aplikasi meminta hak akses *root* atau *superuser*	Dapat menyebabkan kerusakan sistem dan	M7: *Insufficient Binary Protections*

No	Temuan Kerentanan	Keterangan	Kategori OWASP Mobile Top 10 2024
		kebocoran data pengguna	
12.	*Shared preferences* atau aplikasi diatur dengan izin yang terlalu longgar	File dapat diakses oleh aplikasi lain dan tidak ada batasan privasi	M9: *Insecure Data Storage*

Berdasarkan pemetaan kerentanan pada aplikasi *e-commerce* ke OWASP Mobile Top 10 2024 memberikan gambaran yang lebih jelas mengenai ancaman utama yang dihadapi dari masing-masing aplikasi tersebut. Kerentanan yang paling sering ditemukan yaitu M10: *Insufficient Cryptography*, M9: *Insecure Data Storage*, dan M8: *Security Misconfiguration* yang menunjukkan bahwa sebagian besar aplikasi *e-commerce* di Indonesia masih memiliki kerentanan dalam hal pengelolaan data sensitif, perlindungan komunikasi, dan konfigurasi aplikasi yang aman.

4.2.4 Analisis Risiko Berdasarkan NIST SP 800-30

Pada tahap ini dilakukan penilaian risiko keamanan informasi terhadap kerentanan-kerentanan keamanan yang telah diidentifikasi sebelumnya melalui hasil pemindaian kerentanan dengan MobSF. Penilaian risiko ini berdasarkan *framework* NIST SP 800-30 yang merupakan standar acuan dalam melakukan penilaian risiko informasi secara sistematis dan komprehensif. Analisis risiko dilakukan dengan menilai dua parameter utama yaitu *likehood* (kemungkinan eksploitasi) dan *impact* (dampak terhadap aset informasi) yang kemudian dikombinasikan untuk menentukan tingkat risiko (*risk level*) dari setiap kerentanan yang ditemukan. Skala penilaian untuk *likehood* dan *impact* masing-masing terdiri dari tiga tingkatan yaitu *High*, *Medium*, dan *Low*. Sedangkan *risk level* dikategorikan ke dalam lima tingkatan yaitu *Very High, High, Medium, Low,* dan *Very Low*. Penentuan analisis risiko aplikasi berdasarkan pada framework NIST SP 800-30 yang terdapat pada Tabel 3.1. Berikut ini merupakan hasil analisis risiko terhadap aplikasi *e-commerce* yang dianalisis yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak berdasarkan penilaian risiko menurut NIST SP 800-30.

A. Shopee

Tabel 4. 17 Analisis risiko Shopee

No	Kerentanan	*Likehood*	*Impact*	*Risk Level*
1.	Penggunaan algoritma kriptografi lemah (MD5, SHA-1)	*High*	*High*	*High*
2.	Penggunaan *raw query* SQLite	*Medium*	*High*	*High*
3.	*Hardcoded secrets* (API key, token, *password, username*)	*High*	*High*	*High*
4.	*Random number* generator tidak aman	*High*	*Medium*	*High*
5.	Penyimpanan data di *external storage*	*Medium*	*High*	*High*
6.	Enkripsi CBC + PKCS5/7	*Medium*	*High*	*High*
7.	Izin akses berbahaya (*CAMERA, LOCATION, CONTACTS*)	*Medium*	*Medium*	*Medium*
8.	Komponen dan IP tidak aman	*Medium*	*Medium*	*Medium*
9.	*Temporary* file menyimpan data sensitif	*Medium*	*High*	*High*
10.	*Debuggable* aktif dan pengaturan tidak aman	*Medium*	*High*	*High*

Berdasarkan hasil analisis risiko aplikasi Shopee yang disusun berdasarkan NIST SP 800-30, mayoritas kerentanan yang teridentifikasi berada pada tingkat *Risk Level High* yang menunjukkan tingginya potensi eksploitasi serta dampak yang signifikan terhadap keamanan informasi. Kerentanan paling kritis berada pada kategori *High* yaitu penggunaan algoritma kriptografi lemah (MD5, SHA-1) dan *hardcoded secrets* yang dapat dimanfaatkan oleh penyerang untuk membobol sistem autentikasi atau integritas data. Selain itu, sejumlah kerentanan seperti penggunaan *raw query* SQLite, penyimpanan data di *external storage*, penggunaan enkripsi CBC tanpa validasi integritas, serta pengaktifan mode debug tergolong dalam kategori *High* yang mengindikasikan adanya kelemahan pada lapisan

pengamanan data dan kontrol akses. Terdapat beberapa kerentanan berada pada tingkat risiko *Medium* seperti izin akses yang berlebihan dan konfigurasi komponen tidak aman yang berpotensi penyalahgunaan data. Oleh karena itu, berdasarkan hasil analisis risiko aplikasi Shopee ini perlu penerapan kebijakan pengelolaan kredensial yang aman serta pembatasan hak akses aplikasi untuk meminimalkan keamanan yang ada.

B. Tokopedia

Tabel 4. 18 Analisis risiko Tokopedia

No	Kerentanan	*Likehood*	*Impact*	*Risk Level*
1.	Membaca/menulis data di *external storage*	*Medium*	*High*	*High*
2.	*Hardcoded secrets* (*username, password*, API *Key*)	*High*	*High*	*High*
3.	Penggunaan algoritma kriptografi lemah (MD5, SHA-1)	*High*	*High*	*High*
4.	*Raw query* SQLite	*Medium*	*High*	*High*
5.	Temporary file menyimpan data sensitif	*Medium*	*High*	*High*
6.	*Random number* generator tidak aman	*High*	*Medium*	*High*
7.	Mode enkripsi CBC + PKCS5/7	*Medium*	*High*	*High*

Berdasarkan hasil analisis risiko aplikasi Tokopedia yang disusun berdasarkan NIST SP 800-30, seluruh kerentanan yang teridentifikasi berada pada tingkat risiko *High* yang menandakan tingginya urgensi penanganan terhadap permasalahan keamanan yang ditemukan. Kerentanan dengan tingkat *High* adalah penyimpanan data sensitif secara *hardcoded* dan penggunaan algoritma kriptografi yang telah usang dan lemah yang secara langsung mengancam integritas dan kerahasiaan data pengguna. Selain itu, kerentanan lain yang berada pada kategori risiko *High* seperti akses terhadap penyimpanan eksternal, penggunaan *raw* SQL *query*, penyimpanan data sensitif dalam file sementara, serta penggunaan mode enkripsi CBC yang menunjukkan adanya kelemahan yang dapat dimanfaatkan

untuk mengakses, memanipulasi, atau mencuri data sensitif. Penggunaan *random* generator juga berada pada tingkat risiko *High* yang berpotensi terjadinya serangan terhadap mekanisme keamanan berbasis token. Oleh karena itu, berdasarkan hasil analisis risiko aplikasi Tokopedia menunjukkan bahwa aplikasi masih mengandung kerentanan serius yang perlu segera dimitigasi melalui penerapan praktik pengembangan yang aman seperti penghapusan kredensial dari kode sumber untuk mengurangi risiko terhadap aset informasi pengguna.

C. Lazada

Tabel 4. 19 Analisis risiko Lazada

No	Kerentanan	*Likehood*	*Impact*	*Risk Level*
1.	*Random number generator* tidak aman	*High*	*Medium*	*High*
2.	Komponen dan alamat IP tidak aman	*Medium*	*Medium*	*Medium*
3.	*Shared preferences* dengan izin longgar	*Medium*	*High*	*High*
4.	Akses *external storage*	*Medium*	*High*	*High*
5.	*Hardcoded secrets* (API *Key, username, password*)	*High*	*High*	*High*
6.	Penggunaan algoritma lemah (MD5, SHA-1, ECB)	*High*	*High*	*High*
7.	Validasi sertifikat SSL tidak benar	*High*	*High*	*High*
8.	*Raw query* SQLite	*Medium*	*High*	*High*
9.	*Temporary* file menyimpan data sensitif	*Medium*	*High*	*High*
10.	Enkripsi CBC + PKCS5/7	*Medium*	*High*	*High*
11.	*Debuggable* aktif dan pengaturan tidak aman	*Medium*	*High*	*High*
12.	*WebView* dengan konfigurasi tidak aman	*High*	*High*	*High*

Berdasarkan hasil analisis risiko aplikasi Lazada yang disusun berdasarkan NIST SP 800-30, diketahui sebagian besar kerentanan yang ditemukan memiliki tingkat risiko *High* dan hanya satu kerentanan yang berada pada tingkat *Medium*.

Kerentanan yang berada dalam kategori *High* yaitu *hardcoded secrets*, penggunaan algoritma kriptografi lemah, validasi sertifikat SSL yang tidak tepat, serta konfigurasi *WebView* yang tidak aman menunjukkan adanya ancaman serius terhadap aspek kerahasiaan, integritas, dan otentikasi sistem. Sementara itu kerentanan lainnya seperti akses ke *external storage*, penggunaan *random* generator yang tidak aman, penyimpanan data sensitif dalam *temporary* file, penggunaan enkripsi CBC, serta konfigurasi debug yang aktif berada dalam kategori risiko *High* yang mengindikasikan adanya celah keamanan yang dapat dimanfaatkan untuk mengeksploitasi data pengguna. Kerentanan pada *shared preferences* dengan izin longgar dan penggunaan *raw* SQL *query* juga berpotensi kebocoran data dan manipulasi basis data *internal*. Kemudian kerentanan yang berada dalam kategori risiko *Medium* yaitu adanya komponen dan alamat IP tidak aman yang memiliki risiko jika tidak segera ditangani. Oleh karena itu, berdasarkan hasil analisis risiko aplikasi Lazada penting untuk menerapkan kebijakan keamanan berlapis dan pengembangan keamanan untuk meminimalkan risiko serangan serta menjaga perlindungan data pengguna.

D. Blibli

Tabel 4. 20 Analisis risiko Blibli

No	Kerentanan	*Likehood*	*Impact*	*Risk Level*
1.	*Hardcoded secrets* (*username, password*, API *Key*)	*High*	*High*	*High*
2.	dengan izin s*hared preferences* terlalu longgar	*Medium*	*High*	*High*
3.	Komponen dan alamat IP tidak aman	*Medium*	*Medium*	*Medium*
4.	Penggunaan algoritma kriptografi lemah (MD5, SHA-1)	*High*	*High*	*High*
5.	Akses membaca/menulis ke *external storage*	*Medium*	*High*	*High*
6.	*Random number* generator tidak aman	*High*	*Medium*	*High*

No	Kerentanan	*Likehood*	*Impact*	*Risk Level*
7.	Enkripsi CBC + PKCS5/7	*Medium*	*High*	*High*
8.	*Temporary* file menyimpan data sensitif	*Medium*	*High*	*High*
9.	Permintaan hak akses *root* atau *superuser*	*Medium*	*High*	*High*
10.	*WebView* tidak dikonfigurasi dengan aman	*High*	*High*	*High*
11.	Penggunaan *raw query* SQLite	*Medium*	*High*	*High*

Berdasarkan hasil analisis risiko aplikasi Blibli yang disusun berdasarkan NIST SP 800-30, mayoritas kerentanan berada pada kategori risiko *High* dan satu kerentanan dalam kategori *Medium* yang menunjukkan tingkat urgensi tinggi dalam penanganannya. Kerentanan dalam kategori *High* terkait penyimpanan data secara *hardcoded*, penggunaan algoritma kriptografi lemah, dan konfigurasi *WebView* yang tidak aman yang secara langsung mengancam integritas, kerahasiaan, dan keamanan pengguna dari serangan pihak ketiga. Sementara itu, kerentanan yang berada dalam kategori *High* seperti *shared preferences* dengan izin terlalu longgar, akses ke penyimpanan *external*, penggunaan *random* generator yang tidak aman, enkripsi CBC, penyimpanan data sensitif dalam *temporary* file, permintaan hak akses *root*, dan penggunaan *raw query* SQLite berpotensi dieksploitasi untuk mengakses, memodifikasi, atau mencuri informasi pengguna. Kerentanan yang berada dalam kategori *Medium* yaitu komponen dan alamat IP yang tidak aman juga dapat meningkatkan risiko serangan. Oleh karena itu, berdasarkan hasil analisis risiko aplikasi Blibli mengindikasikan perlunya penerapan strategi keamanan aplikasi yang komprehensif mencakup penguatan sistem kriptografi, manajemen kredensial yang aman, dan pembatasan akses data untuk meminimalkan potensi eksploitasi dan menjaga kepercayaan pengguna terhadap aplikasi.

E. Bukalapak

Tabel 4. 21 Analisis risiko Bukalapak

No	Kerentanan	*Likehood*	*Impact*	*Risk Level*
1.	*Hardcoded secrets* (API *Key*, token, *password, username*)	*High*	*High*	*High*
2.	*Random number* generator tidak aman	*High*	*Medium*	*High*
3.	Penggunaan algoritma kriptografi lemah (MD5, SHA-1, ECB)	*High*	*High*	*High*
4.	Komponen dan alamat IP tidak aman	*Medium*	*Medium*	*Medium*
5.	*WebView* dengan konfigurasi tidak aman	*High*	*High*	*High*
6.	Akses ke *external storage*	*Medium*	*High*	*High*
7.	Penyimpanan data sensitif dalam *temporary* file	*Medium*	*Medium*	*Medium*
8.	SSL tidak tervalidasi dengan benar	*High*	*High*	*High*
9.	*Debuggable* aktif dan pengaturan tidak aman	*Medium*	*High*	*High*
10	Enkripsi CBC + PKCS5/7	*Medium*	*High*	*High*
11.	Permintaan hak akses *root/superuser*	*Medium*	*High*	*High*
12.	*Shared preferences* tanpa batasan privasi	*Medium*	*High*	*High*

Berdasarkan hasil analisis risiko aplikasi Bukalapak yang disusun berdasarkan NIST SP 800-30, ditemukan bahwa aplikasi ini memiliki sejumlah kerentanan yang berada dalam kategori risiko *High* dan sebagian kecil berada pada tingkat *Medium*. Kerentanan yang berada pada kategori *High* seperti penyimpanan data sensitif secara *hardcoded*, penggunaan algoritma kriptografi lemah, konfigurasi *WebView* yang tidak aman, dan validasi SSL yang tidak benar yang berpotensi besar untuk dimanfaatkan oleh pihak yang tidak bertanggungjawab dalam serangan yang menargetkan integritas, kerahasiaan, dan komunikasi data pengguna. Selain itu, kerentanan yang berada dalam kategori risiko *High* seperti

random generator yang tidak aman, akses penyimpanan *external*, konfigurasi debug aktif, permintaan hak akses *root* atau *superuser*, dan *shared preferences* berisiko tinggi terhadap kebocoran data maupun pengambilalihan kontrol aplikasi. Kemudian kerentanan yang berada dalam kategori risiko *Medium* yaitu komponen dan alamat IP tidak aman serta penyimpanan data sensitif dalam *temporary* file juga memiliki potensi untuk dimanfaatkan dalam melakukan serangan. Oleh karena itu, berdasarkan hasil analisis risiko aplikasi Bukalapak menekankan perlunya penguatan kontrol keamanan dalam pengembangan aplikasi termasuk penerapan enkripsi yang kuat, validasi sertifikat yang kuat, dan pengelolaan kredensial serta izin akses secara aman untuk menjaga kerahasiaan dan keamanan informasi pengguna.

4.2.5 Evaluasi Risiko

Evaluasi risiko merupakan tahap penting dalam penilaian risiko keamanan informasi yang bertujuan untuk mengidentifikasi, menilai, dan mengklasifikasikan potensi ancaman berdasarkan tingkat kerentanan yang ditemukan pada setiap aplikasi. Dalam penelitian ini, evaluasi risiko dilakukan terhadap aplikasi *e-commerce* yang dianalisis yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak dengan mengacu pada *framework* NIST SP 800-30. Evaluasi risiko dilakukan dengan menggabungkan analisis risiko per kerentanan yang telah dilakukan sebelumnya dengan *security score* yang diperoleh melalui pemindaian kerentanan dengan MobSF. Penggabungan ini bertujuan untuk memberikan penilaian risiko yang lebih menyeluruh sehingga dapat digunakan sebagai dasar dalam menentukan prioritas mitigasi dan rekomendasi peningkatan keamanan aplikasi. Hasil evaluasi risiko dari masing-masing aplikasi *e-commerce* yang telah dianalisis adalah sebagai berikut:

A. Shopee

Berikut adalah evaluasi risiko pada aplikasi Shopee berdasarkan hasil analisis kerentanan dan *security score* dari MobSF yang mengacu pada *framework* NIST SP 800-30.

1) Evaluasi berdasarkan analisis risiko per kerentanan

Tabel 4. 22 Evaluasi risiko Shopee

Risk Level	**Jumlah Kerentanan**	**Bobot Skor**
Very High	2	5
High	6	4
Medium	2	3
Low	0	2
Very Low	0	1

Dari perhitungan tersebut, diperoleh rata-rata skor risiko per kerentanan sebesar:

$$\text{Rata} - \text{rata skor risiko} = \frac{(2x5) + (6x4) + (2x3)}{10} = 4$$

Berdasarkan nilai rata-rata skor risiko per kerentanan maka aplikasi berada pada kategori *High* yang berarti aplikasi masih memiliki banyak celah keamanan yang perlu diperbaiki.

2) Evaluasi risiko berdasarkan *security score*

Security score aplikasi Shopee berdasarkan hasil pemindaian kerentanan dengan MobSF adalah 50/100. Dengan mengacu pada Tabel 3.2 klasifikasi skor risiko dari pedoman NIST SP 800-30 maka aplikasi berada pada kategori risiko *High* yang berarti aplikasi masih ada banyak celah keamanan yang perlu diperbaiki dan berdasarkan matriks penilaian evaluasi risiko pada Tabel 3.3 maka aplikasi memiliki bobot skor 4.

3) Penggabungan evaluasi risiko

Penggabungan evaluasi risiko berdasarkan hasil dari rata-rata skor risiko per kerentanan dan hasil dari *security score*.

Rata-rata skor risiko: 4

Security score: 4

$$\text{Skor gabungan} = \frac{4+4}{2} = 4.00$$

Dengan demikian, evaluasi risiko gabungan menunjukkan aplikasi Shopee berada pada tingkat risiko *High*.

Berdasarkan evaluasi risiko yang telah dilakukan menunjukkan bahwa aplikasi Shopee berada pada kategori risiko *High*. Hal ini menandakan bahwa terdapat sejumlah keamanan signifikan yang perlu segera dilakukan perbaikan untuk meningkatkan perlindungan terhadap data pengguna dan mencegah potensi eksploitasi dari pihak yang tidak bertanggungjawab.

B. Tokopedia

Berikut adalah evaluasi risiko pada aplikasi Tokopedia berdasarkan hasil analisis kerentanan dan *security score* dari MobSF yang mengacu pada *framework* NIST SP 800.30.

1) Evaluasi berdasarkan analisis risiko per kerentanan

Tabel 4. 23 Evaluasi risiko Tokopedia

Risk Level	**Jumlah Kerentanan**	**Bobot Skor**
Very High	2	5
High	5	4
Medium	0	3
Low	0	2
Very Low	0	1

Dari perhitungan tersebut, diperoleh rata-rata skor risiko per kerentanan sebesar:

$$\text{Rata} - \text{rata skor risiko} = \frac{(2\text{x}5) + (5\text{x}4)}{7} = 4.29$$

Berdasarkan nilai rata-rata skor risiko per kerentanan maka aplikasi berada pada kategori *High* yang berarti aplikasi masih memiliki banyak celah keamanan yang perlu diperbaiki.

2) Evaluasi risiko berdasarkan *security score*

Security score aplikasi Tokopedia berdasarkan hasil pemindaian kerentanan dengan MobSF adalah 47/100. Dengan mengacu pada Tabel 3.2 klasifikasi skor risiko dari pedoman NIST SP 800-30 maka aplikasi berada pada kategori risiko *High* yang berarti aplikasi masih ada banyak celah keamanan yang perlu diperbaiki dan berdasarkan matriks penilaian evaluasi risiko pada Tabel 3.3 maka aplikasi memiliki bobot skor 4.

3) Penggabungan evaluasi risiko

Penggabungan evaluasi risiko berdasarkan hasil dari rata-rata skor risiko per kerentanan dan hasil dari *security score*.

Rata-rata skor risiko: 4.29

Security score: 4

$$\text{Skor gabungan} = \frac{4.29 + 4}{2} = 4.145$$

Dengan demikian, evaluasi risiko gabungan menunjukkan aplikasi Tokopedia berada pada tingkat risiko *High*.

Berdasarkan evaluasi risiko yang telah dilakukan menunjukkan bahwa aplikasi Tokopedia berada pada kategori risiko *High*. Hal ini menandakan bahwa terdapat sejumlah keamanan signifikan yang perlu segera dilakukan perbaikan untuk meningkatkan perlindungan terhadap data pengguna dan mencegah potensi eksploitasi dari pihak yang tidak bertanggungjawab.

C. Lazada

Berikut adalah evaluasi risiko pada aplikasi Lazada berdasarkan hasil analisis kerentanan dan *security score* dari MobSF yang mengacu pada *framework* NIST SP 800-30.

1) Evaluasi berdasarkan analisis risiko per kerentanan

Tabel 4. 24 Evaluasi risiko Lazada

Risk Level	**Jumlah Kerentanan**	**Bobot Skor**
Very High	4	5

Risk Level	**Jumlah Kerentanan**	**Bobot Skor**
High	7	4
Medium	1	3
Low	0	2
Very Low	0	1

Dari perhitungan tersebut, diperoleh rata-rata skor risiko per kerentanan sebesar:

$$\text{Rata} - \text{rata skor risiko} = \frac{(4x5) + (7x4) + (1x3)}{12} = 4.25$$

Berdasarkan nilai rata-rata skor risiko per kerentanan maka aplikasi berada pada kategori *High* yang berarti aplikasi masih memiliki banyak celah keamanan yang perlu diperbaiki.

2) Evaluasi risiko berdasarkan *security score*

Security score aplikasi Lazada berdasarkan hasil pemindaian kerentanan dengan MobSF adalah 44/100. Dengan mengacu pada Tabel 3.2 klasifikasi skor risiko dari pedoman NIST SP 800-30 maka aplikasi berada pada kategori risiko *High* yang berarti aplikasi masih ada banyak celah keamanan yang perlu diperbaiki dan berdasarkan matriks penilaian evaluasi risiko pada Tabel 3.3 maka aplikasi memiliki bobot skor 4.

3) Penggabungan evaluasi risiko

Penggabungan evaluasi risiko berdasarkan hasil dari rata-rata skor risiko per kerentanan dan hasil dari *security score*.

Rata-rata skor risiko: 4.25

Security score: 4

$$\text{Skor gabungan} = \frac{4.25 + 4}{2} = 4.125$$

Dengan demikian, evaluasi risiko gabungan menunjukkan aplikasi Lazada berada pada tingkat risiko *High*.

Berdasarkan evaluasi risiko yang telah dilakukan menunjukkan bahwa aplikasi Lazada berada pada kategori risiko *High*. Hal ini menandakan bahwa terdapat sejumlah keamanan signifikan yang perlu segera dilakukan perbaikan untuk meningkatkan perlindungan terhadap data pengguna dan mencegah potensi eksploitasi dari pihak yang tidak bertanggungjawab.

D. Blibli

Berikut adalah evaluasi risiko pada aplikasi Blibli berdasarkan hasil analisis kerentanan dan *security score* dari MobSF yang mengacu pada *framework* NIST SP 800.30.

1) Evaluasi berdasarkan analisis risiko per kerentanan

Tabel 4. 25 Evaluasi risiko Blibli

Risk Level	**Jumlah Kerentanan**	**Bobot Skor**
Very High	3	5
High	7	4
Medium	1	3
Low	0	2
Very Low	0	1

Dari perhitungan tersebut, diperoleh rata-rata skor risiko per kerentanan sebesar:

$$\text{Rata} - \text{rata skor risiko} = \frac{(3\text{x}5) + (7\text{x}4) + (1\text{x}3)}{11} = 4.18$$

Berdasarkan nilai rata-rata skor risiko per kerentanan maka aplikasi berada pada kategori *High* yang berarti aplikasi masih memiliki banyak celah keamanan yang perlu diperbaiki.

2) Evaluasi risiko berdasarkan *security score*

Security score aplikasi Blibli berdasarkan hasil pemindaian kerentanan dengan MobSF adalah 39/100. Dengan mengacu pada Tabel 3.2 klasifikasi skor risiko dari pedoman NIST SP 800-30 maka

aplikasi berada pada kategori risiko *High* yang berarti aplikasi masih ada banyak celah keamanan yang perlu diperbaiki dan berdasarkan matriks penilaian evaluasi risiko pada Tabel 3.3 maka aplikasi memiliki bobot skor 4.

3) Penggabungan evaluasi risiko

Penggabungan evaluasi risiko berdasarkan hasil dari rata-rata skor risiko per kerentanan dan hasil dari *security score*.

Rata-rata skor risiko: 4.18

Security score: 4

$$\text{Skor gabungan} = \frac{4.18 + 4}{2} = 4.09$$

Dengan demikian, evaluasi risiko gabungan menunjukkan aplikasi Blibli berada pada tingkat risiko *High*.

Berdasarkan evaluasi risiko yang telah dilakukan menunjukkan bahwa aplikasi Blibli berada pada kategori risiko *High*. Hal ini menandakan bahwa terdapat sejumlah keamanan signifikan yang perlu segera dilakukan perbaikan untuk meningkatkan perlindungan terhadap data pengguna dan mencegah potensi eksploitasi dari pihak yang tidak bertanggungjawab.

E. Bukalapak

Berikut adalah evaluasi risiko pada aplikasi Bukalapak berdasarkan hasil analisis risiko dan *security score* dari MobSF yang mengacu pada *framework* NIST SP 800.30.

1) Evaluasi berdasarkan analisis risiko per kerentanan

Tabel 4. 26 Evaluasi risiko Bukalapak

Risk Level	**Jumlah Kerentanan**	**Bobot Skor**
Very High	4	5
High	6	4
Medium	2	3
Low	0	2

Risk Level	**Jumlah Kerentanan**	**Bobot Skor**
Very Low	0	1

Dari perhitungan tersebut, diperoleh rata-rata skor risiko per kerentanan sebesar:

$$\text{Rata} - \text{rata skor risiko} = \frac{(4x5) + (6x4) + (2x3)}{12} = 4.16$$

Berdasarkan nilai rata-rata skor risiko per kerentanan maka aplikasi berada pada kategori *High* yang berarti aplikasi masih memiliki banyak celah keamanan yang perlu diperbaiki.

2) Evaluasi risiko berdasarkan *security score*

Security score aplikasi Bukalapak berdasarkan hasil pemindaian kerentanan dengan MobSF adalah 44/100. Dengan mengacu pada Tabel 3.2 klasifikasi skor risiko dari pedoman NIST SP 800-30 maka aplikasi berada pada kategori risiko High yang berarti aplikasi masih ada banyak celah keamanan yang perlu diperbaiki dan berdasarkan matriks penilaian evaluasi risiko pada Tabel 3.3 maka aplikasi memiliki bobot skor 4.

3) Penggabungan evaluasi risiko

Penggabungan evaluasi risiko berdasarkan hasil dari rata-rata skor risiko per kerentanan dan hasil dari *security score*.

Rata-rata skor risiko: 4.16

Security score: 4

$$\text{Skor gabungan} = \frac{4.16 + 4}{2} = 4.08$$

Dengan demikian, evaluasi risiko gabungan menunjukkan aplikasi Bukalapak berada pada tingkat risiko *High*.

Berdasarkan evaluasi risiko yang telah dilakukan menunjukkan bahwa aplikasi Bukalapak berada pada kategori risiko High. Hal ini menandakan bahwa terdapat sejumlah keamanan signifikan yang perlu segera dilakukan perbaikan untuk meningkatkan perlindungan terhadap

data pengguna dan mencegah potensi eksploitasi dari pihak yang tidak bertanggungjawab.

Berdasarkan evaluasi risiko terhadap lima aplikasi *e-commerce* di Indonesia yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak yang dilakukan mengacu pada *framework* NIST SP 800-30, hasil evaluasi risiko menunjukkan bahwa seluruh aplikasi yang dianalisis memiliki tingkat risiko pada kategori *High*. Aplikasi Shopee dengan hasil skor gabungan 4.00, Tokopedia sebesar 4.145, Lazada sebesar 4.125, Blibli sebesar 4.09, dan Bukalapak sebesar 4.08. Kerentanan yang ditemukan umumnya mengarah pada kelemahan dalam aspek enkripsi, penyimpanan data, dan konfigurasi akses. Hal tersebut menandakan perlunya tindakan mitigasi dan penguatan sistem keamanan pada level pengembangan aplikasi. Dengan demikian, hasil evaluasi risiko ini memberikan gambaran secara menyeluruh mengenai keamanan aplikasi *e-commerce* yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak serta menjadi dasar untuk penyusunan mitigasi risiko sebagai strategi perbaikan keamanan aplikasi secara lebih sistematis.

4.2.6 Rekomendasi Mitigasi

Setelah dilakukan evaluasi risiko terhadap masing-masing aplikasi, tahap selanjutnya yaitu penyusunan rekomendasi mitigasi untuk setiap kerentanan yang telah diidentifikasi. Setiap rekomendasi mitigasi dirancang untuk memberikan langkah-langkah yang dapat membantu pengembang aplikasi dalam memperbaiki kelemahan sistem dan menurunkan tingkat risiko keamanan aplikasi yang telah dianalisis sebelumnya. Berikut adalah rekomendasi mitigasi untuk masing-masing aplikasi *e-commerce* yang dianalisis.

A. Shopee

Berdasarkan hasil analisis risiko dan evaluasi risiko yang telah dilakukan sebelumnya terhadap aplikasi Shopee, ditemukan sejumlah kerentanan yang berpotensi mengancam kerahasiaan data pengguna, integritas sistem, dan ketersediaan layanan. Berikut rekomendasi mitigasi aplikasi Shopee yang dapat dilihat pada Tabel 4. 27.

Tabel 4. 27 Rekomendasi mitigasi Shopee

No	Temuan Kerentanan	Rekomendasi Mitigasi
1.	Penggunaan algoritma kriptografi lemah (MD5, SHA-1)	Hentikan penggunaan algoritma lemah seperti MD5 dan SHA-1. Gunakan algoritma yang lebih kuat seperti SHA-256 atau SHA-3, serta mode enkripsi seperti AES-GCM yang lebih aman dan sesuai standar saat ini
2.	Penggunaan *raw query* SQLite	Gunakan *parameterized queries* atau *prepared statements* untuk mencegah SQL *Injection*. Hindari menyusun *query* SQL secara dinamis menggunakan *input* langsung dari pengguna
3.	*Hardcoded secrets* (API *key*, token, *password, username*)	Hindari menyimpan informasi sensitif seperti API *key* dan *password* secara *hardcoded* di dalam kode aplikasi. Gunakan android k*eystore* atau solusi manajemen kredensial di sisi *server*
4.	*Random number generator* tidak aman	Gunakan *secure random* untuk keperluan kriptografi agar dapat menghasilkan angka acak yang tidak diprediksi. Hindari *java.util.Random* atau pendekatan serupa yang tidak aman
5.	Penyimpanan data di *external storage*	Hindari menyimpan data sensitif pada penyimpanan eksternal. Jika tidak dapat dihindari, enkripsi data dengan AES-256 dan pastikan hanya aplikasi terkait yang dapat mengaksesnya
6.	Enkripsi CBC + PKCS5/7	Hindari penggunaan mode CBC karena rentan terhadap serangan *padding oracle*. Gunakan mode enkripsi yang

No	Temuan Kerentanan	Rekomendasi Mitigasi
		lebih amna seperti AES-GCM yang menyediakan otentikasi dan enkripsi sekaligus
7.	Izin akses berbahaya (*CAMERA, LOCATION, CONTACTS*)	Terapkan prinsip *least privilege* dengan hanya meminta izin yang benar-benar dibutuhkan oleh aplikasi. Informasikan kepada pengguna alasan permintaan izin dan gunakan *runtime permissions*
8.	Komponen dan IP tidak aman	Pastikan komponen seperti *activity* atau *broadcast receiver* yang bersifat publik disertai mekanisme autentikasi dan validasi. Validasi setiap komunikasi dengan IP eksternal dan gunakan HTTPS
9.	*Temporary* file menyimpan data sensitif	Hindari menyimpan data sensitif dalam file sementara. Jika diperlukan, gunakan direktori internal aplikasi dengan hak akses terbatas dan hapus file setelah digunakan
10.	*Debuggable* aktif dan pengaturan tidak aman	Pastikan android *debuggable* disetel ke *false* dalam versi produksi. Terapkan teknik *code obfuscation* dengan *ProGuard* atau R8, dan tambahkan proteksi anti *reserve engineering*

B. Tokopedia

Berdasarkan hasil analisis risiko dan evaluasi risiko yang telah dilakukan sebelumnya terhadap aplikasi Tokopedia, ditemukan sejumlah kerentanan yang berpotensi mengancam kerahasiaan data pengguna, integritas sistem, dan ketersediaan layanan. Berikut rekomendasi mitigasi aplikasi Tokopedia yang dapat dilihat pada Tabel 4. 28.

Tabel 4. 28 Rekomendasi mitigasi Tokopedia

No	Temuan Kerentanan	Rekomendasi Mitigasi
1.	Membaca/menulis data di *external* storage	Hindari penyimpanan data sensitif pada *external storage* yang dapat diakses oleh aplikasi lain. Sebagai gantinya, gunakan *internal storage*
2.	*Hardcodes secrets* (API *Key*, *username, password*)	Menyimpan *secrets* secara terpisah menggunakan android *keystore* system atau melalui *source backend server*, serta menerapkan *obfuscation* dan teknik pengamanan *code* (seperti *ProGuard*) untuk menghindari dekompilasi
3.	Penggunaan algoritma kriptografi lemah (MD5, SHA-1)	Hentikan penggunaan algoritma kriptografi yang telah dianggap tidak aman seperti MD5 dan SHA-1. Gantilah dengan algoritma yang lebih kuat dan direkomendasikan seperti SHA-256 atau SHA-3 untuk menjaga integritas data dan mencegah serangan *collision*
4.	Penggunaan *raw query* SQLite	Penggunaan *raw* SQL *query* yang melibatkan input pengguna membuka kemungkinan serangan SQL *Injection*. Disarankan menggunakan *parameterized query* atau *prepared statement* untuk membatasi pengaruh input pengguna terhadap eksekusi SQL. Validasi *input* juga harus diterapkan secara menyeluruh
5.	*Temporary* file menyimpan data sensitif	Aplikasi sebaiknya tidak menyimpan data sensitif dalam *temporary* file tanpa perlindungan yang aman.

No	Temuan Kerentanan	Rekomendasi Mitigasi
		Gunakan direktori internal dengan kontrol akses sistem dan pastikan *temporary* file dienkripsi dan dihapus segara setelah tidak diperlukan
6.	*Random number generator* tidak aman	Penggunaan nilai acak yang tidak aman dapat membahayakan keamanan kriptografi aplikasi. Gunakan *cryptographically secure pseudo-random number* generator (CSPRNG) seperti *secure random* untuk menghasilkan nilai acak yang tidak dapat diprediksi oleh pihak ketiga
7.	Mode enkripsi CBC + PKCS5/7	Mode enkripsi CBC dengan *padding* PKCS5/7 rentan terhadap serangan *padding oracle*. Gunakan mode enkripsi yang lebih aman seperti AES-GCM yang menyediakan integritas dan autentikasi data, serta mencegah manipulasi *ciphertext*

C. Lazada

Berdasarkan hasil analisis risiko dan evaluasi risiko yang telah dilakukan sebelumnya terhadap aplikasi Lazada, ditemukan sejumlah kerentanan yang berpotensi mengancam kerahasiaan data pengguna, integritas sistem, dan ketersediaan layanan. Berikut rekomendasi mitigasi aplikasi Lazada yang dapat dilihat pada Tabel 4. 29.

Tabel 4. 29 Rekomendasi mitigasi Lazada

No	Temuan Kerentanan	Rekomendasi Mitigasi
1.	*Random number generator* tidak aman	Gunakan *cryptographically secure pseudo random number* generator (CSPRNG) seperti *securerandom* untuk menghasilkan nilai acak yang aman secara kriptografis, terutama untuk token, sesi, atau enkripsi
2.	Komponen dan alamat IP tidak aman	Pastikan semua komponen dan *endpoint* jaringan (alamat IP) hanya dapat diakses melalui koneksi yang aman (HTTPS). Selain itu, konfigurasikan komponen di *AndoidManifest.xml* agar tidak bersifat *exported* jika tidak diperlukan
3.	*Shared preferences* dengan izin longgar	Ubah pengaturan penyimpanan *sharedpreferences* agar bersifat private dengan *MODE_PRIVATE*. Hindari menyimpan informasi sensitif tanpa enkripsi dan pertimbangkan menggunakan *EncryptedSharedPreferences*
4.	Akses ke *external storage*	Hindari menyimpan data penting di *external storage*. Jika diperlukan, lakukan enkripsi sebelum penyimpanan dan manfaatkan *internal storage* atau penyimpanan *sandbox* yang lebih aman
5.	*Hardcoded secrets* (API *Key, username, password*)	Jangan menyimpan kredensial atau *secrets* langsung dalam *source code*. Gunakan layanan penyimpanan *secure* seperti android *keystore*, atau disimpan di *backend* dengan akses terbatas melalui autentikasi token

No	Temuan Kerentanan	Rekomendasi Mitigasi
6.	Penggunaan algoritma lemah (MD5, SHA-1, ECB)	Hindari penggunaan algoritma yang telah usang seperti MD5, SHA-1, dan mode ECB. Gunakan algoritma modern seperti AES dengan mode GCM dan hash SHA-256 untuk menjamin keamanan data
7.	Validasi sertifikat SSL tidak benar	Terapkan validasi sertifikat SSL yang benar dengan menggunakan SSL pinning. Pastikan aplikasi memverifikasi sertifikat *server* untuk mencegah serangan MITM
8.	Penggunaan *raw query* SQLite	Gunakan *parameterized queries* atau *prepared statements* untuk mencegah SQL *Injection*. Lakukan validasi input secara ketat sebelum digunakan dalam eksekusi SQL
9.	*Temporary* file menyimpan data sensitif	Hindari menyimpan data sensitif dalam file sementara. Jika penyimpanan sementara diperlukan, simpan di direktori internal dan pastikan file dienkripsi serta dihapus setelah digunakan
10.	Enkripsi CBC + PKCS5/7	Gunakan mode enkripsi yang lebih aman seperti AES-GCM yang menyediakan autentikasi dan integritas data. Hindari penggunaan CBC + PKCS5/7 karena rentan terhadap serangan *padding oracle*
11.	*Debuggable* aktif dan pengaturan tidak aman	Nonaktifkan opsi *android:debuggable=”true”* pada versi produksi dan terapkan *obfuscation* kode menggunakan *ProGuard* atau R8. Tambahkan pemeriksaan

No	Temuan Kerentanan	Rekomendasi Mitigasi
		integritas aplikasi untuk mencegah *reserve engineering*
12.	*WebView* dengan konfigurasi tidak aman	Nonaktifkan Javascript jika tidak diperlukan dan hindari pemuatan konten dari sumber tak terpercaya dalam *WebView*. Gunakan *setAllowFileAccess(false)* dan *setMixedContentMode* untuk mencegah eksploitasi

D. Blibli

Berdasarkan hasil analisis risiko dan evaluasi risiko yang telah dilakukan sebelumnya terhadap aplikasi Blibli, ditemukan sejumlah kerentanan yang berpotensi mengancam kerahasiaan data pengguna, integritas sistem, dan ketersediaan layanan. Berikut rekomendasi mitigasi aplikasi Blibli yang dapat dilihat pada Tabel 4. 30.

Tabel 4. 30 Rekomendasi mitigasi Blibli

No	Temuan Kerentanan	Rekomendasi Mitigasi
1.	*Hardcoded secrets* (*username, password*, API *Key*)	Hindari menyimpan informasi sensitif dalam bentuk *hardcoded* di dalam *source code*. Gunakan layanan penyimpanan aman seperti Android *Keystore* atau enkripsi berbasis token dari *server backend* yang hanya dapat diakses melalui autentikasi.
2.	*Shared preferences* dengan izin terlalu longgar	Gunakan *MODE_PRIVATE* untuk menyimpan data di *SharedPreferences* dan enkripsi data jika menyangkut informasi sensitif. Disarankan menggunakan *EncryptedSharedPreferences* untuk tingkat keamanan lebih tinggi

No	Temuan Kerentanan	Rekomendasi Mitigasi
3.	Komponen dan alamat IP tidak aman	Pastikan konfigurasi komponen aplikasi disetel *non-exported* jika tidak dibutuhkan secara publik. Selain itu, pastikan alamat IP atau *endpoint* yang digunakan telah dibatasi aksesnya dan hanya berjalan melalui HTTPS
4.	Penggunaan algoritma kriptografi lemah (MD5, SHA-1)	Gantilah algoritma *hash* lama (MD5, SHA-1) dengan algoritma yang lebih kuat seperti SHA-256 atau SHA-3. Untuk enkripsi gunakan standar modern seperti AES dengan GCM
5.	Akses membaca/menulis ke *external storage*	Hindari penggunaan *external storage* untuk menyimpan data sensitif. Jika tidak dapat dihindari, data harus dienkripsi sebelum disimpan dan dihapus secara setelah tidak diperlukan. Disarankan menggunakan *internal storage*
6.	*Random number generator* tidak aman	Gunakan generator bilangan acak yang aman secara kriptografis seperti *SecureRandom* dari Java. Jangan gunakan *random* atau fungsi non-kriptografis lainnya untuk keperluan keamanan seperti token atau OTP
7.	Enkripsi CBC + PKCS5/7	Hindari penggunaan mode enkripsi CBC karena rentan terhadap serangan *padding oracle*. Disarankan untuk menggunakan AES-GCM yang menyediakan *authenticated encryption* dan integritas data
8.	*Temporary* file menyimpan data sensitif	Jangan menyimpan data sensitif dalam file sementara. Jika dibutuhkan, gunakan direktori *internal* aplikasi dan

No	Temuan Kerentanan	Rekomendasi Mitigasi
		pastikan file dihapus setelah digunakan. Lakukan enkripsi pada data sensitif jika harus ditulis ke *disk*
9.	Permintaan hak akses *root* atau *superuser*	Hindari permintaan akses *root* atau *superuser* kecuali benar-benar diperlukan. Akses ini membuka potensi penyalahgunaan yang sangat besar dan dapat membahayakan integritas serta kerahasiaan data pengguna
10.	*WebView* tidak dikonfigurasi dengan aman	Nonaktifkan JavaScript jika tidak diperlukan dan hindari pemuatan konten dari domain tidak terpercaya
11.	Penggunaan *raw query* SQLite	Gunakan *parameterized query* atau *prepared statement* untuk mencegah SQL *Injection*. Lakukan validasi dan sanitasi *input* dari pengguna sebelum digunakan dalam *query*

E. Bukalapak

Berdasarkan hasil analisis risiko dan evaluasi risiko yang telah dilakukan sebelumnya terhadap aplikasi Bukalapak, ditemukan sejumlah kerentanan yang berpotensi mengancam kerahasiaan data pengguna, integritas sistem, dan ketersediaan layanan. Berikut rekomendasi mitigasi aplikasi Bukalapak yang dapat dilihat pada Tabel 4. 31.

Tabel 4. 31 Rekomendasi mitigasi Bukalapak

No	Temuan Kerentanan	Rekomendasi Mitigasi
1.	*Hardcoded secrets* (API *Key*, token, *password, username*)	Hindari penyimpanan kredensial sensitif secara *hardcoded* dalam *source code*. Gunakan android *keystore* atau teknik manajemen kredensial dari sisi *server*, serta enkripsi data secara *end-to-end*

No	Temuan Kerentanan	Rekomendasi Mitigasi
2.	*Random number generator* tidak aman	Gunakan *SecureRandom* yang secara khusus dirancang untuk keperluan kriptografi. Hindari *java.util.Random* atau generator numerik yang mudah diprediksi
3.	Penggunaan algoritma kriptografi lemah (MD5, SHA-1, ECB)	Ganti algoritma kriptografi lama dengan yang lebih aman seperti SHA-256 atau SHA-3. Hindari mode enkripsi ECB karena tidak menyediakan keamanan yang memadai dan gunakan AES-GCM sebagai gantinya
4.	Komponen dan alamat IP tidak aman	Pastikan komponen seperti *activity, service*, atau *broadcast receiver* tidak disetel *exported=true* tanpa autentikasi. Gunakan komunikasi terenkripsi dan validasi alamat IP yang digunakan
5.	*WebView* dengan konfigurasi tidak aman	Nonaktifkan JavaScript jika tidak diperlukan, Batasi akses file dan cegah pemuatan konten dari sumber yang tidak terpercaya. Gunakan *WebViewClient* yang dikustomisasi untuk memverifikasi URL sebelum dimuat
6.	Akses ke *external storage*	Hindari penyimpanan data sensitif di *external storage*. Jika diperlukan enkripsi data sebelum disimpan dan pastikan akses terbatas hanya pada aplikasi yang bersangkutan
7.	Penyimpanan data sensitif dalam *temporary* file	Jangan menyimpan informasi sensitif dalam file sementara. Jika file temporer dibutuhkan, gunakan direktori internal dengan hak akses terbatas dan

No	Temuan Kerentanan	Rekomendasi Mitigasi
		hapus file segera setelah tidak digunakan
8.	SSL tidak tervalidasi dengan benar	Implementasikan validasi sertifikat SSL/TLS dengan benar menggunakan *HostnameVerifier* yang aman. Hindari mengabaikan kesalahan validasi SSL dalam *debugging* atau produksi
9.	*Debuggable* aktif dan pengaturan tidak aman	Pastikan *android:debuggable* disetel false pada build produksi. Gunakan *ProGuard* atau R8 untuk melakukan *code obfuscation* serta aktifkan fitur anti *reserve engineering*
10.	Enkripsi CBC + PKCS5/7	Hindari penggunaan mode enkripsi CBC karena rentan terhadap serangan *padding oracle*. Disarankan untuk menggunakan AES-GCM yang menyediakan *authenticated encryption* dan integritas data
11.	Permintaan hak akses *root* atau *superuser*	Hindari permintaan hak akses *root* karena dapat membuka akses terhadap seluruh sistem dan meningkatkan risiko eksploitasi. Batasi hak akses aplikasi hanya sesuai dengan kebutuhan fungsional
12.	*Shared preferences* tanpa batasan privasi	Gunakan *MODE_PRIVATE* saat menyimpan data pada *SharedPreferences*. Untuk data sensitif, gunakan *EncryptedSharedPreferences* yang menyediakan enkripsi AES-256 untuk nilai dan kunci

Berdasarkan hasil penelitian menunjukkan bahwa seluruh aplikasi *e-commerce* yang dianalisis berada dalam kategori risiko tinggi (*High Risk*), sehingga diperlukan mitigasi yang tepat guna menurunkan potensi eksploitasi. Rekomendasi teknis bagi pengembang mencakup penggantian algoritma kriptografi lemah dengan standar modern (misalnya SHA-256 dan AES), penghapusan *hardcoded secrets*, pembatasan izin akses yang tidak relevan, serta penerapan SSL *pinning* dan validasi sertifikat digital. Di sisi lain, pengguna juga berperan penting dalam menjaga keamanan informasi. Oleh karena itu, disarankan agar pengguna mengaktifkan autentikasi dua faktor (2FA), menggunakan kata sandi yang kuat, melakukan pembaruan aplikasi secara berkala, serta membatasi izin akses aplikasi terhadap data sensitif. sehingga keamanan *e-commerce* dapat terjaga secara menyeluruh melalui kolaborasi antara pengembang dan pengguna.

4.2.7 Pelaporan

Bagian ini merupakan tahap akhir dari proses penelitian yang bertujuan untuk menyampaikan secara komprehensif hasil *risk assessment* keamanan informasi terhadap kelima aplikasi *e-commerce* di Indonesia yaitu Shopee, Tokopedia, Lazada, Blibli, dan Bukalapak. Selain itu pelaporan ini juga bertujuan untuk memberikan referensi praktis yang dapat digunakan oleh pengembang aplikasi, pengguna aplikasi, dan penelitian lain dalam meningkatkan aspek keamanan informasi pada aplikasi *e-commerce* di Indonesia. Pelaporan ini disajikan dalam bentuk narasi, tabel, dan grafik yang diharapkan dapat dipahami dengan mudah dan memberikan gambaran yang jelas mengenai kondisi keamanan dari masing-masing aplikasi *e-commerce* yang dianalisis.

Pada tahap identifikasi aplikasi telah dilakukan pengumpulan data dari lima aplikasi *e-commerce* di Indonesia dari Google Play Store kemudian di *back-up* dalam bentuk file APK menggunakan *smartphone* android. Selanjutnya dilakukan identifikasi terhadap aset informasi dari masing-masing aplikasi terkait izin aplikasi, data pribadi yang dibagikan dan dikumpulkan, fitur keamanan, serta metode autentikasi yang digunakan. Identifikasi aplikasi ini menjadi landasan awal untuk memahami potensi risiko dan kerentanan dari setiap aplikasi.

Tahap pemindaian kerentanan telah dilakukan menggunakan *static analysis* dengan *Mobile Security Framework* (MobSF). Hasil pemindaian kerentanan menunjukkan bahwa seluruh aplikasi memiliki celah keamanan pada *hardcoded secrets, weak cryptography, insecure data storage, dangerous permissions*, serta SSL/TLS *Misconfiguration*. Masing-masing aplikasi memperoleh *security score* dengan nilai antara 39-50 dari skala 100 yang berarti semua aplikasi perlu dilakukan perbaikan.

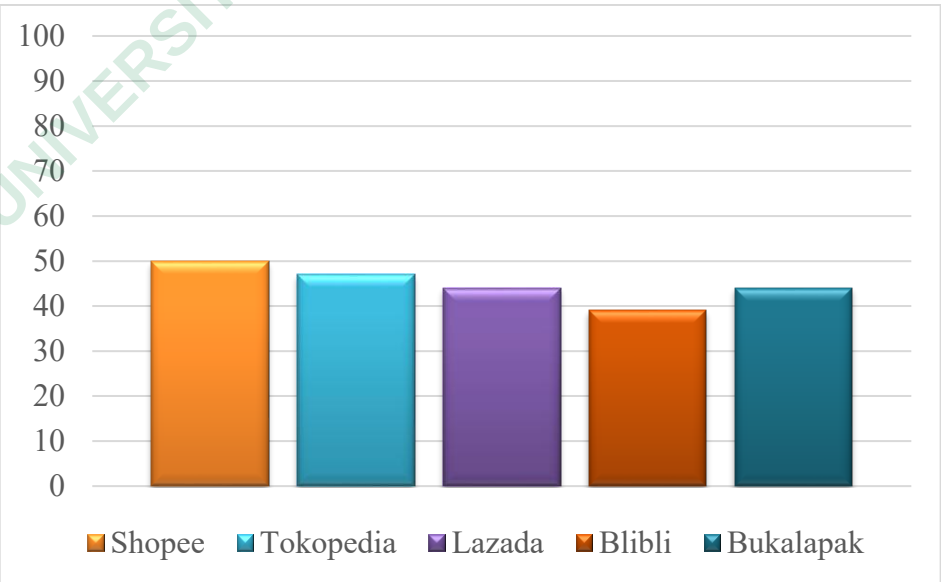
Kemudian setiap kerentanan yang didapatkan dari pemindaian kerentanan dipetakan dalam kategori OWASP Mobile Top 10 2024 yang bertujuan untuk mengklasifikasikan kerentanan secara standar berdasarkan sepuluh risiko keamanan paling kritis pada aplikasi *mobile*. Kerentanan paling dominan yang ditemukan masuk dalam kategori M10 (*Insufficient Cryptography*), M9 (*Insecure Data Storage*), dan M8 (*Security Misconfiguration*).

Selanjutnya dilakukan analisis risiko berdasarkan *framework* NIST SP 800-30 dengan mengukur *likehood* (kemungkinan eksploitasi) dan *impact* (dampak terhadap aset informasi) untuk setiap kerentanan. Hasilnya digunakan untuk menentukan *risk level* setiap temuan yang diklasifikasikan dalam lima tingkat yaitu *Very High, High, Medium, Low, Very Low*. Berdasarkan analisis risiko yang telah dilakukan terhadap kelima aplikasi berdasarkan framework NIST SP 800-30 menunjukkan bahwa semua aplikasi berada pada kategori risiko *High* (tinggi).

Tahap evaluasi risiko telah dilakukan dengan menggabungkan hasil analisis risiko per kerentanan dengan *security score* dengan MobSF. Evaluasi risiko ini bertujuan untuk menghasilkan penilaian menyeluruh terhadap keamanan masing-masing aplikasi. Berikut adalah tabel perbandingan tingkat risiko dan skor keamanan aplikasi yang telah dilakukan evaluasi risiko yang dapat dilihat pada Tabel 4.32.

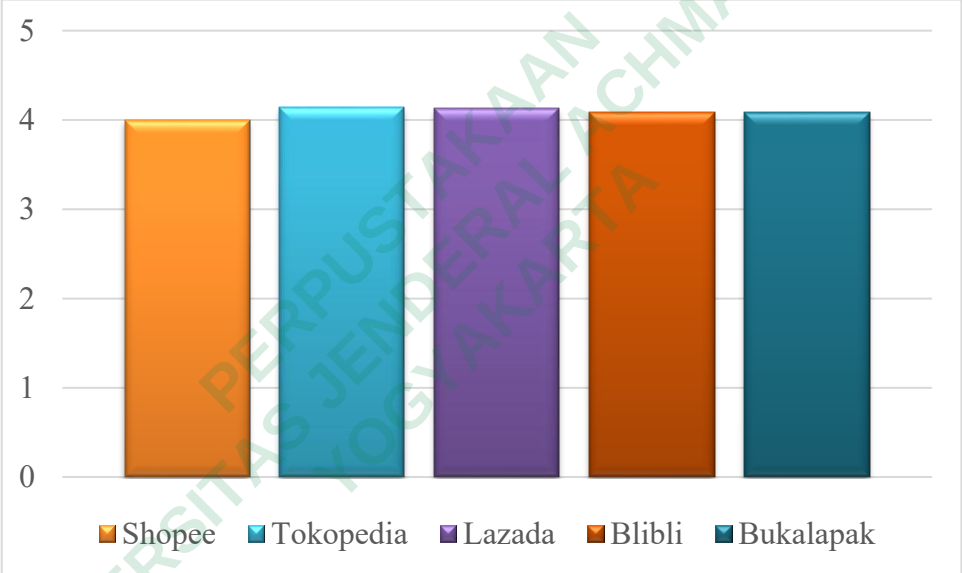
Tabel 4. 32 Perbandingan tingkat risiko dan skor keamanan aplikasi

Nama Aplikasi	*Security Score* (MobSF)	Skor Evaluasi Risiko	Kategori Risiko (NIST SP 800-30)	Kerentanan Dominan
Shopee	50/100	4.00	*High Risk*	*Weak Cryptography, Insecure Data Storage, Dangerous Permissions*
Tokopedia	47/100	4.145	*High Risk*	*Insecure Data Storage, Hardcoded Secrets, SSL/TLS Misconfiguration*
Lazada	44/100	4.125	*High Risk*	*Weak Cryptography, SSL/TLS Misconfiguration*
Blibli	39/100	4.09	*High Risk*	*Hardcoded Secrets, Dangerous Permissions*
Bukalapak	44/100	4.08	*High Risk*	SSL/TLS *Misconfiguration, Hardcoded Secrets*



Gambar 4. 82 Grafik perbandingan *security score*

Berdasarkan grafik perbandingan *security score* seperti yang ditunjukkan Gambar 4.82, aplikasi Shopee mempunyai *security score* tertinggi yaitu 50/100 menunjukkan implementasi keamanan yang paling baik namun masih perlu peningkatan signifikan. Tokopedia dengan *security score* 47/100, Lazada dan Bukalapak mempunyai *security score* sama yaitu 44/100, serta aplikasi Blibli mempunyai *security score* terendah yaitu 39/100. Blibli dengan *security score* 39 menunjukkan kerentanan yang paling serius dan memerlukan perhatian darurat untuk perbaikan keamanan. Temuan ini menggarisbawahi pentingnya regulasi dan standar keamanan yang lebih ketat untuk aplikasi *e-commerce* guna melindungi data dan privasi pengguna Indonesia.



Gambar 4. 83 Skor risiko aplikasi berdasarkan NIST SP 800-30

Berdasarkan hasil evaluasi risiko yang telah dilakukan yang mengacu pada *framework* NIST SP 800-30 terhadap lima aplikasi *e-commerce* populer di Indonesia seperti yang ditunjukkan pada Gambar 4.83, seluruh aplikasi yang dianalisis menunjukkan tingkat risiko pada kategori *High* dengan rentang skor antara 4.00 hingga 4.145. Aplikasi Shopee memperoleh skor risiko terendah dengan nilai 4.00, diikuti oleh Bukalapak dengan skor 4.08, Blibli dengan skor 4.09, Lazada dengan skor 4.125, dan Tokopedia dengan skor tertinggi yaitu 4.145. Tokopedia memiliki skor risiko tertinggi yang mengindikasikan tingkat ancaman keamanan paling kritis dengan probabilitas dan dampak yang signifikan. Shopee menunjukkan

skor risiko terendah, namun masih berada dalam kategori *High Risk*. Meskipun terdapat perbedaan skor antar aplikasi, selisih yang relatif kecil menunjukkan bahwa tingkat risiko keamanan pada kelima aplikasi tersebut berada pada level yang hampir setara.

Terakhir, disusun rekomendasi mitigasi berdasarkan hasil pemetaan kerentanan ke OWASP Mobile Top 10 2024 dan analisis risiko berdasarkan NIST SP 800-30. Rekomendasi ini mencakup perbaikan teknis seperti penerapan algoritma kriptografi yang kuat (misalnya AES dan SHA-256), penghapusan informasi sensitif dari *source code*, pengurangan penggunaan *permission* berbahaya, serta implementasi SSL *pinning* untuk memperkuat keamanan komunikasi data. Selain itu, pengembang aplikasi juga disarankan untuk melakukan pengujian keamanan secara berkala serta meningkatkan kesadaran keamanan dalam proses pengembangan aplikasi.

Secara keseluruhan, pelaporan ini bertujuan untuk menjadi referensi bagi pengembang aplikasi, pengguna aplikasi, peneliti, dan pemangku kepentingan lainnya dalam meningkatkan keamanan aplikasi *e-commerce* dan data pengguna aplikasi *e-commerce* di Indonesia. Dengan mengetahui letak dan tingkat kerentanan secara spesifik, maka upaya peningkatan keamanan dapat dilakukan secara lebih terarah, efektif, dan berkelanjutan.