BAB 4
HASIL PENELITIAN

4.1 COLLECTION

Merupakan tahapan paling awal dari metode NIST, hal-hal yang dilakukan dalam tahapan *collection* yaitu koleksi, dokumentasi, isolasi, preservasi dan preservasi barang bukti. Adapun langkah pada *Collection* sebagai berikut.

1. Menggunakan perangkat *Smartphone* Andorid Xiaomi

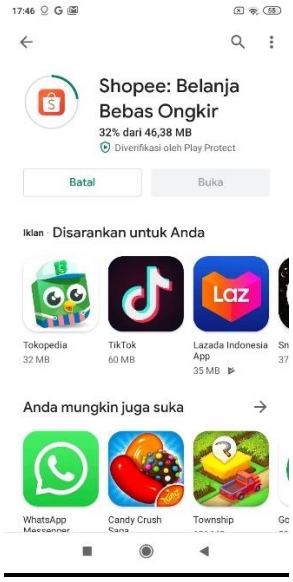
Gambar 4.1 *Smartphone* Android xiaomi

Adapun spesifikasi dari *smartphone* sebagai perangkat, dapat dilihat pada Tabel 4.1.

Tabel 4.1 Spesifikasi *smartphone* Android

DETAIL PERANGKAT	SPESIFIKASI
Xiaomi Redmi	6A
Nomor model	M1804C3CE
Versi Android	9.0
Processor	Quadcore Max 2.00GHz
RAM	2 GB
Memori *internal*	16 MB

2. Pengumpulan data aplikasi Shopee didapatkan dengan mengunduh aplikasi Shopee di PlayStore dengan *smartphone* Android, ditunjukkan pada Gambar 4.2.

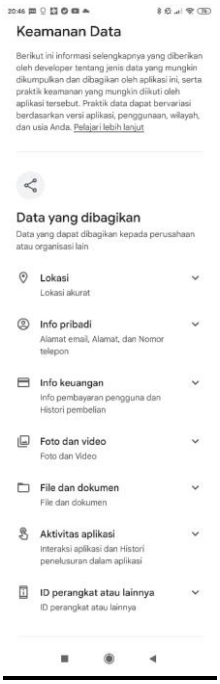


Gambar 4.2 Download aplikasi Shopee

Adapun spesifikasi aplikasi Shopee yang telah diunduh pada PlayStore, dapat dilihat pada Tabel 4.2.

Tabel 4.2 Spesifikasi aplikasi

Komponen	Info Aplikasi
Penyedia aplikasi	Shopee
Ukuran *file*	280 MB
Versi aplikasi	2.92.08
Kompatibel dengan OS	Android 4.4 sampai lebih terbaru
Tanggal rilis	4 Juni 2015
Izin akses	Kalender, kamera, kontak, lokasi, mikrofon, penyimpanan,

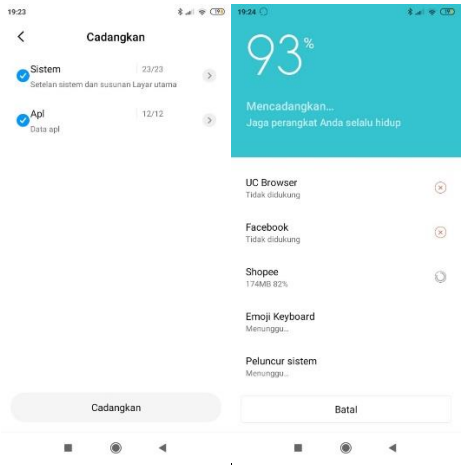


Gambar 4.3 Data yang dibutuhkan pada aplikasi

Dari uraian diatas pada Gambar 4.3 dapat disimpulkan bahwa pengumpulan data yang dibutuhkan aplikasi Shopee adalah lokasi, informasi pribadi (berisi email, alamat pengguna, dan nomor telepon), info keuangan (berisi info pembayaran pengguna, dan riwayat pembelian), foto, file dan dokumen, aktivitas aplikasi (berisi interaksi aplikasi dan riwayat penelusuran pada aplikasi), dan ID perangkat.

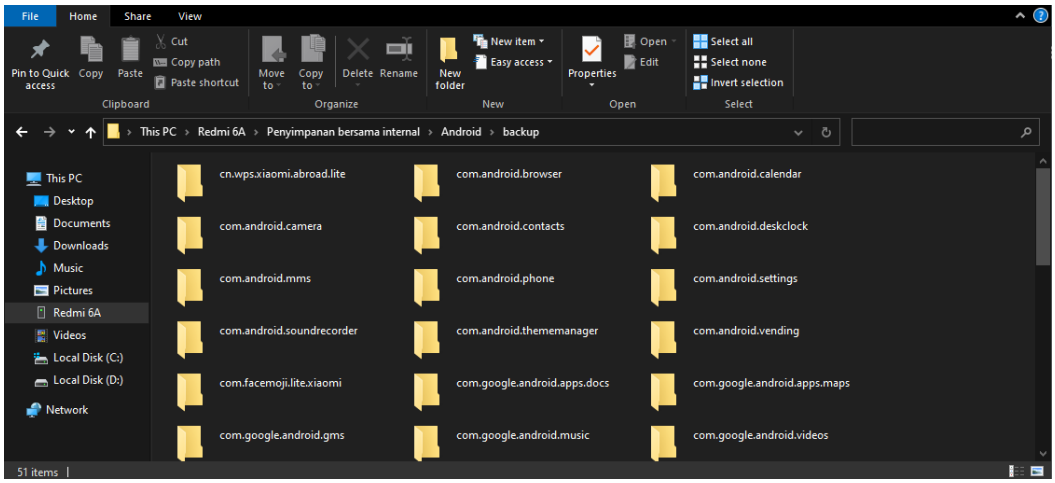
4.2 EXAMINATION

Merupakan aktivitas *backup data smartphone* dapat digunakan dengan *tool* atau dicadangkan melalui pengaturan *smartphone. Backup data smartphone* Android menggunakan fitur cadangkan dan setel ulang pada pengaturan *smartphone*, dapat dilihat pada Gambar 4.4.



Gambar 4.4 Proses pencadangan data *smartphone*

Hasil dari *backup data smartphone* ditempatkan pada penyimpanan *internal smartphone* yang dapat di salin pada *file explore* pada laptop, dapat dilihat pada Gambar 4.5.



Gambar 4.5 Hasil *backup data smartphone*

4.3 ANALYSIS

Merupakan proses untuk mendapatkan informasi yang berguna dan dapat menjawab apa yang dibutuhkan sebagai pendorong untuk melakukan pengumpulan dan pemerikasaan data. Pada langkah ini terdapat 2 macam analisis yaitu analisis statis dan analisis dinamis.

1. Analisis Statis

Analisis statis diawali dengan menginstal aplikasi ke *smartphone* Android ditunjukkan pada Gambar 4.2, kemudian data apa saja yang dimasukkan ke dalam aplikasi antara lain lokasi, informasi pribadi (berisi email, alamat pengguna, dan nomor telepon), info keuangan (berisi info pembayaran pengguna, dan riwayat pembelian), foto, file dan dokumen, aktivitas aplikasi (berisi interaksi aplikasi dan riwayat penelusuran pada aplikasi), dan ID perangkat, ditunjukkan pada Gambar 4.3. Adapun hasil analisis statis diperlukan untuk melihat sejauh mana aplikasi meminta data pengguna dalam proses membuat akun baru. ditunjukkan pada Tabel 4.3 berikut ini.

Tabel 4.3 Tabel analisis statis

NO	KOMPONEN	DATA APLIKASI
1.	Pengembang	Shopee
2.	URL *web*	https://droidbang.com/files30/72474/com.shopee.id_2.92.08_667.apk/
3.	Nama *file*	Shopee ID Belanja Bebas Ongkir
4.	Ukuran *file*	230 MB
5.	Penggunaan data pribadi pengguna	Yang tercantum di KTP pengguna seperti: 1. NIK 2. Nama lengkap 3. Tempat/tgl lahir 4. Jenis kelamin 5. Alamat lengkap 6. Agama 7. Status perkawinan 8. Pekerjaan 9. kewarganegaraan
6.	*File upload*	Foto muka dan foto KTP
7.	Media verifikasi	*Chat* WhatsApp

Dari hasil analisis statis pada Tabel 4.3 diatas dapat ditarik kesimpulan bahwa terdapat data penting dan proses penting yang seharusnya melalui verifikasi dan dokumentasi. Kebijakan privasi dan penggunaan data merupakan hal pertama yang harus disiapkan oleh Shopee. Kebijakan ini merupakan sebuah perjanjian awal

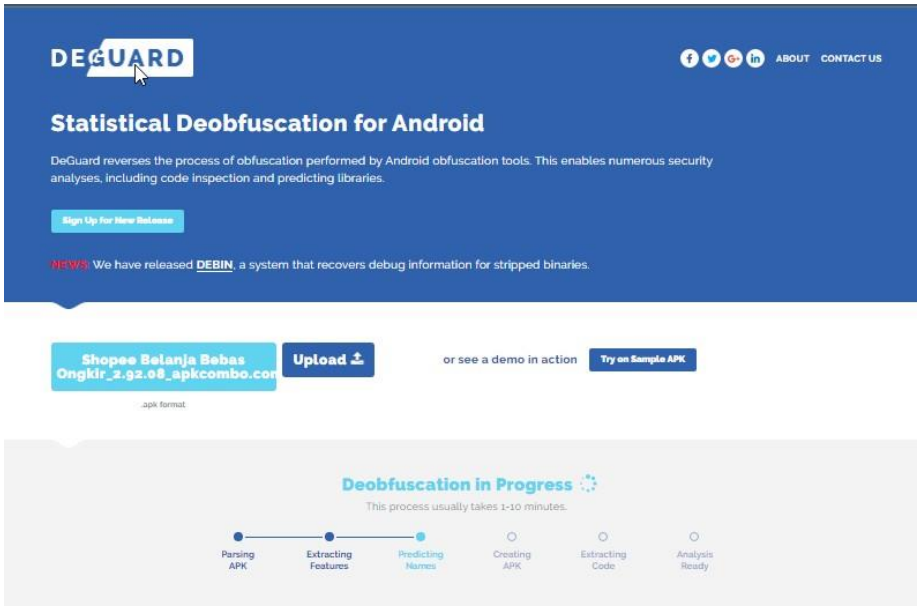
dalam penggunaan dan transaksi data informasi yang diberikan oleh calon penguna Shopee, dapat dilihat analisis diatas dalam mendaftar akun baru seseorang harus memasukkan data diri yang cukup lengkap yaitu dengan mengunggah foto KTP , hal tersebut akan berpengaruh terhadap kerahasiaan data pribadi terutama NIK.

2. Analisis Dinamis

Analisis dinamis dilakukan menggunakan dua cara, yang pertama yaitu menggunakan teknik *re-engineering file apk,* yang nantinya merubah file apk menjadi file *soure code* untuk dapat di analisis alur sistemnya. Untuk yang kedua yaitu dengan menggunakan teknik analisis proses genetik (*Genetic Malware Analysis*), teknik ini akan melihat proses apk apakah megandungaktifitas mencurigakan dalam pencurian data informasi atau tidak.

a. *Re-engineering file apk*

Tahapan proses *re-engineering file apk* menjadi *sorce code* dapat dilihat pada gambar dibawah ini yaitu dengan bantuan *tool apk-deguard.*



Gambar 4.6 Proses *re-engineering file apk*

Gambar 4.7 Hasil *re-engineering file apk*

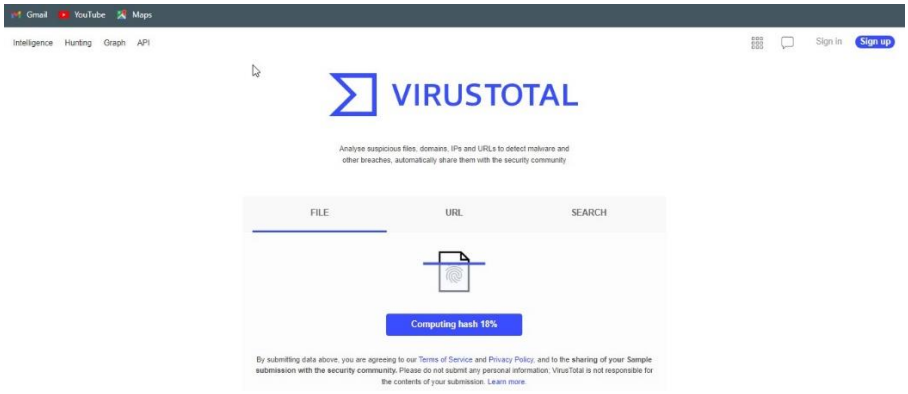
Proses *Re-engineering* file apk Shopee dan hasil yang ditampilkan dapat dilihat pada Gambar 4.6 dan Gambar 4.7 ditunjukkan bahwa aplikasi *compatible* dengan versi minimal Android 7 dan untuk memverifikasi ShopeePayLaternya dibutuhkan data dari KTP, dibutuhkan akses *proxy* untuk masuk ke dalamnya agar terhindar dari kerawanan data yang mudah terlacak.

b. Analisis Aktifitas Genetik.

Analisis genetik dilakukan untuk melihat aktifitas yang menyerupai aktifitas *backdoor*, *malware* dan *virus*. Dimana aktifitas tersebut dapat memicu pencurian data. Analisis menggunakan *tool Virustotal dan MobSF*. selain itu dapat juga untuk melihat aktifitas yang dilakukan saat aplikasi dijalankan.

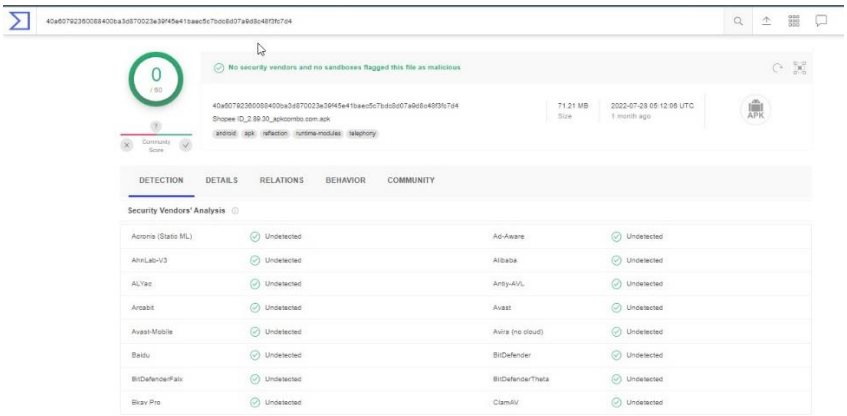
1) Virustotal

Tampilan dari Virustotal dapat dilihat pada Gambar 4.8.



Gambar 4.8 Proses upload file aplikasi Shopee

Pada penelitian ini menggunakan *tool* Virustotal untuk memindai data yang didapat dari perangkat *smartphone* yang terinstal aplikasi Shopee. Pada Gambar 4.8 menunjukkan bahwa untuk memindai data diperlukan proses *upload* untuk mendapatkan hasil dari pemindaian data pengguna Shopee.



Gambar 4.9 Hasil analisis file Shopee tampilan pertama

Berdasarkan analisis file aplikasi Shopee pada Gambar 4.9 dapat disimpulkan bahwa aplikasi dalam kondisi aman, tidak terdetekasi *malware* atau aktivitas berbahaya.

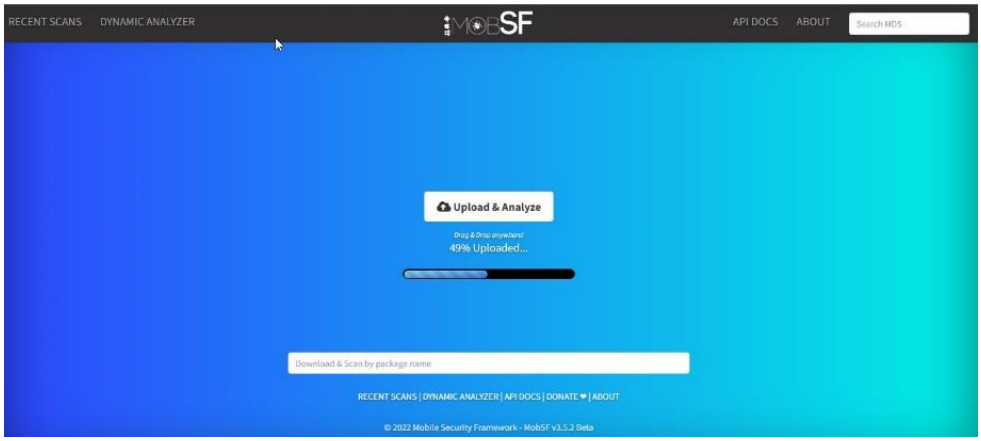
Gambar 4.10 Analisis pada perizinan aplikasi Shopee

Berdasarkan analisis file dalam bagian perizinan aplikasi pada Gambar 4.10 dijelaskan bahwa aplikasi dapat membaca dan menambahkan kalender pada Android, dapat menambah dan membaca memori eksternal, dapat membaca status telepon, dapat membaca daftar kontak yang tersimpan. Aktivitas ini dapat membuka informasi/berkas dari data pengguna Shopee.

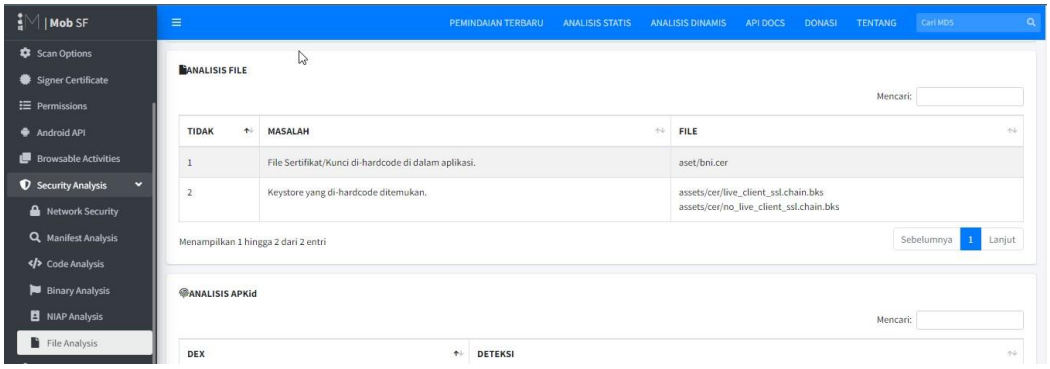
2) MobSF

Analisis menggunakan tool *MobSF* untuk menganalisis aplikasi Shopee mencakup :

a) Hardcode secrets
b) Permisions
c) Malware check

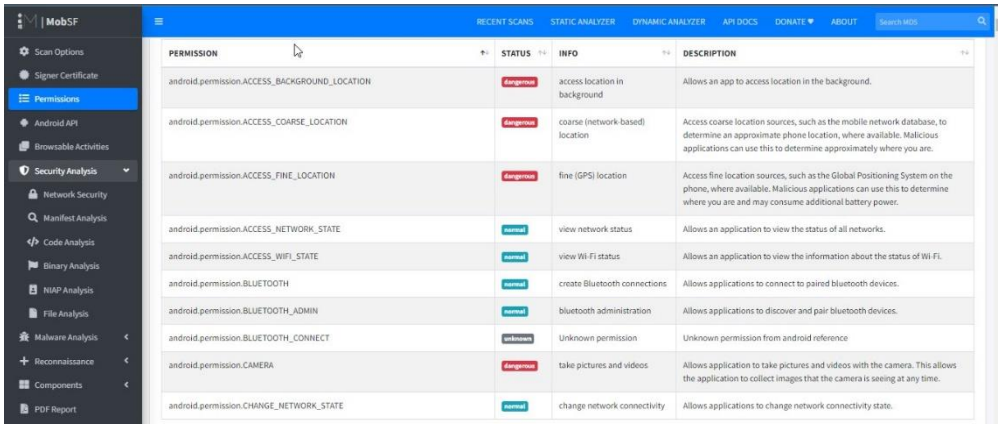


Gambar 4.11 Proses upload file aplikasi Shopee



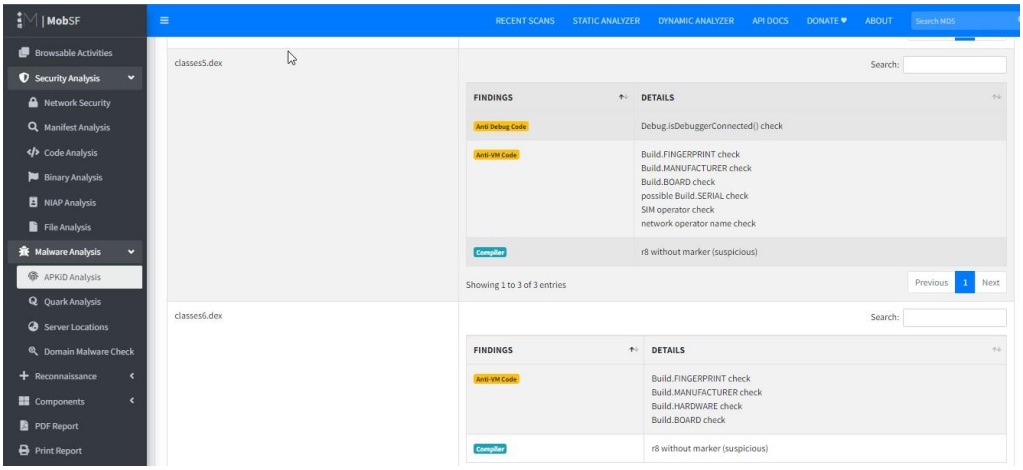
Gambar 4.12 Hasil analisis file Shopee

Pada analisis file Shopee pada Gambar 4.12 ditampilkan bahwa file aplikasi Shopee ada dua masalah pada file sertifikat/kunci di *hardcode* dalam aplikasi dan *keystore* yang di hardcode ditemukan.



Gambar 4.13 Hasil analisis pada perizinan aplikasi

Pada perizinan aplikasi pada Gambar 4.13 ditampilkan bahwa pada bagian *ACCES_BACKGROUND_LOCATION* yaitu mengizinkan aplikasi mengakses lokasi di latar belakang pada status bahaya, aktivitas tersebut sangat membahayakan data pribadi pengguna karena dapat membaca lokasi pengguna saat aplikasi tidak digunakan, pada bagian *ACCES_COARSE_LOCATION* berbahaya karena aplikasi dapat mengetahui keberadaan pengguna saat aplikasi digunakan, pada bagian *ACCES_FINE_LOCATION* yaitu jika lokasi terdeteksi bahwa jaringan GPS bagus maka aplikasi akan mengakses lokasi pengguna aplikasi dan hal tersebut dapat memperpendek penggunaan Andorid karena kehabisan baterai, pada bagian *CAMERA* yaitu mengizinkan aplikasi untuk mengakses foto dan video dari kamera Android ,aktivitas tersebut berbahaya karena dapat melihat gambar yang sudah tersimpan pada memori Android.



Gambar 4.14 Hasil analisis malware

Analisis *malware* pada Gambar 4.14 ditampilkan pada clasess5.dex dijelaskan bahwa ada hal yang mencurigakan yaitu pada FINGERPRINT, MANUFACTURE, BOARD yaitu pada build serial, SIM operator, dan jaringan operator karena pada fitur tersebut rawan pembobolan data pengguna karena mudah dalam melakukan eksekusi. Pada clasess 6 dijelaskan bahwa ada hal yang mencurigakan juga yaitu pada FINGERPRINT, MANUFACTURE, HARDWARE, dan BOARD karena pada fitur tersebut rawan pembobolan data pengguna.

Tabel 4.4 Tabel hasil analisis dinamis

NO	DATA/INFORMASI	HASIL	KETERANGAN
1.	Re-engineering file apk (apk-deguard)	Menunjukkan bahwa aplikasi *compatible* pada versi Android minimal 7, untuk memverifikasinya dibutuhkan data pribadi pengguna dari KTP	Rawan terjadi pencurian data pribadi
2.	Aktivitas genetic (apk Virustotal)	Aplikasi Shopee tidak terdeteksi *Malware* berbahaya	Aman
3.	Aktivitas genetic (apk Mobsf)	Banyak fitur yang terdeteksi mencurigakan	Rawan terjadi pencurian data pribadi, maka di anjurkan pengguna agar lebiih hati-hati

Dari Tabel 4.4 diketahui bahwa semua *tool* melakukan analisis aplikasi yang memberikan hasil masing-masing setiap langkah yang dilakukan. Sehingga dapat disimpulkan bahwa data informasi pengguna aplikasi yang tersimpan dalam Android dapat diakses oleh aplikasi deng mudah, jika diizinkan saat pertama membuat akun baru. Sehingga berpotensi data informasi yang seharusnya tidak dibutuhkan oleh aplikasi dapat ter *input* dalam aplikasi.

4.4 REPORTING

Merupakan proses pelaporan dari hasil tahapan yang meliputi penjelasan mengenai alat yang digunakan, prosedur yang digunakan, penggambaran tindakan yang dilakukan, memberikan rekomendasi untuk perbaikan prosedur atau aspek lain pada aplikasi

Tabel 4.5 Hasil reporting

NO	NAMA TOOL	LANGKAH YANG DILAKUKAN	KERAWANAN	REKOMENDASI SOLUSI
1.	Apk deguard	Melakukan *scanning* file aplikasi Shopee.	Pembobolan data pengguna dapat terjadi jika tidak adanya *proxy* khusus saat penggunaan aplikasi Shopee.	Dibutuhkan akses *proxy* agar terhindar dari kerawanan data yang mudah terlacak oleh aplikasi Shopee.
2.	Virustotal	Melakukan scanning file aplikasi Shopee.	Jika tidak diizinkan saat bagian perizinan aplikasi untuk mengakses data pada *smartphone* maka aplikasi tidak terdeteksi kerawanan data yang mudah terlacak oleh aplikasi Shopee.	Sebaiknya izinkan jika saat ingin digunakan saja seperti pembacaan kontak, kamera, dan yang lainnya.
3.	MobSF	Melakukan scanning file aplikasi Shopee	Ada kecurigaan pembacaan data yang mengancam pembobolan data pribadi pengguna.	Sebaiknya lebih berhati-hati sebagai pengguna agar tidak terjadi pembobolan data pribadi

Dari hasil reporting yang di tampilkan pada Tabel 4.5 dapat disimpulkan bahwa setiap *tool* yang digunakan untuk analisis file memliki fungsi dan hasil yang berbeda serta didapatkan rekomendasi solusi supaya pengguna dapat memahami apa yang harus dilakukan supaya tidak terjadi kerentanan data pribadi yang tersebar.