ASSESSMENT REPORT
MOBILE APPLICATION

One by IFG

Prepared by

SECIRON

Table of Contents

1. Pendahuluan

Aplikasi **One by IFG** merupakan salah satu kanal layanan digital yang digunakan untuk mendukung aktivitas dan layanan kepada pengguna, sehingga memproses serta menyimpan berbagai data penting di dalamnya. Kondisi tersebut menuntut penerapan aspek keamanan aplikasi yang memadai guna memastikan **kerahasiaan, integritas, dan keandalan** aplikasi tetap terjaga.

Seiring dengan meningkatnya pemanfaatan aplikasi mobile, potensi ancaman terhadap aplikasi juga semakin beragam, baik yang menargetkan struktur aplikasi, proses aplikasi saat berjalan, maupun mekanisme pertukaran data yang digunakan. Oleh karena itu, diperlukan suatu proses evaluasi keamanan yang terstruktur untuk memastikan bahwa aplikasi telah dilengkapi dengan mekanisme perlindungan yang sesuai terhadap berbagai skenario ancaman yang mungkin terjadi.

Asesmen keamanan ini dilakukan untuk mengevaluasi kondisi keamanan aplikasi **sebelum dan sesudah** penerapan mekanisme *mobile application hardening* menggunakan **SecIron**. Ruang lingkup asesmen mencakup beberapa aspek utama, antara lain **perlindungan kode aplikasi (code protection)**, **perlindungan pada saat aplikasi berjalan (runtime protection)**, **pemeriksaan integritas aplikasi**, **perlindungan terhadap intersepsi komunikasi aplikasi (MITM protection)**, serta **keamanan penyimpanan data secara lokal**.

Melalui asesmen ini, diharapkan dapat diperoleh gambaran yang lebih komprehensif mengenai **postur keamanan aplikasi** serta tingkat efektivitas mekanisme proteksi yang diterapkan dalam meningkatkan ketahanan aplikasi terhadap potensi ancaman keamanan.

2. Code Protection (Perlindungan Statis)

a. Before Hardened

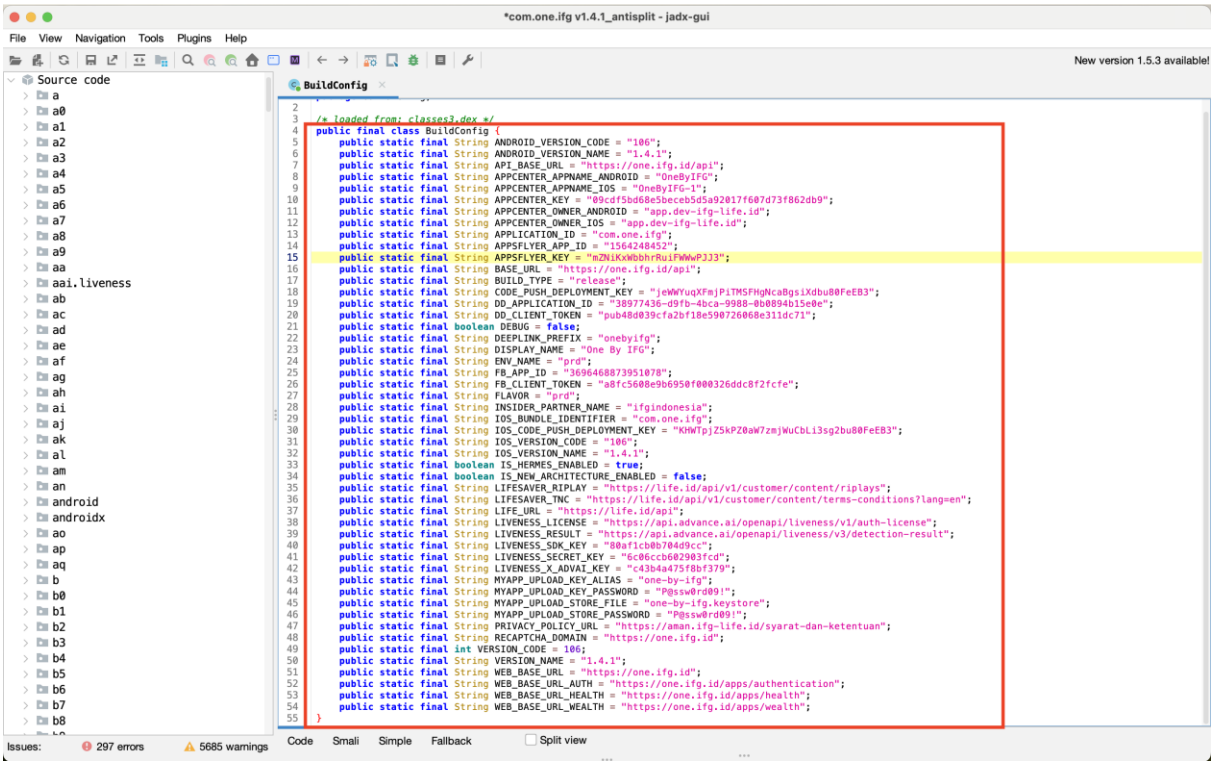
Pada tahap *reverse engineering* menggunakan tools seperti **JADX**, diketahui bahwa aplikasi **belum menerapkan mekanisme proteksi kode secara optimal**. Kondisi ini menyebabkan struktur source code masih dapat dibaca dengan relatif mudah melalui proses dekompilasi.

Sebagai dampaknya, sejumlah informasi sensitif berhasil diidentifikasi secara langsung di dalam kode aplikasi, antara lain:

- URL endpoint API
- API key

Eksposur informasi tersebut meningkatkan risiko keamanan, khususnya terhadap aktivitas *reverse engineering* lanjutan serta potensi penyalahgunaan kredensial API oleh pihak tidak berwenang. Dalam skenario terburuk, hal ini dapat dimanfaatkan untuk melakukan akses ilegal maupun pengiriman data ke server tanpa kontrol yang semestinya.

[Gambar: Cuplikan source code hasil dekompilasi dari JADX]



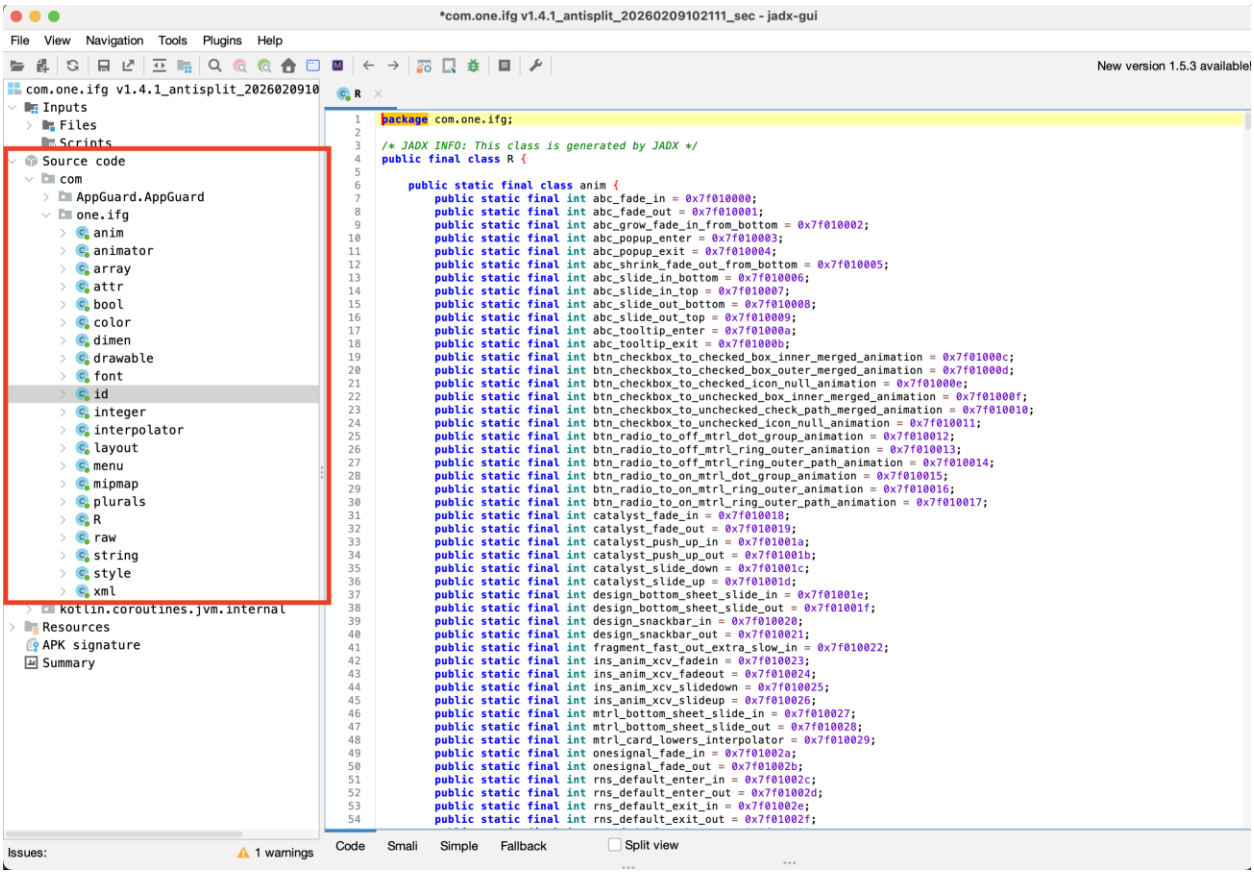
b. After Hardened

Setelah proses *hardening* diterapkan menggunakan **SecIron**, terlihat perbedaan yang signifikan dibandingkan kondisi sebelumnya. Kode aplikasi tidak hanya mengalami proses **obfuscation**, tetapi juga telah melalui mekanisme **enkripsi dan penyembunyian (code hiding)**.

Sebagai hasilnya, kelas-kelas yang sebelumnya dapat diidentifikasi melalui proses dekompilasi kini **tidak lagi terlihat**. Struktur kode menjadi jauh lebih bersih, di mana hanya komponen yang berkaitan langsung dengan kebutuhan **UI** yang masih dapat terdeteksi. Informasi sensitif serta logika inti aplikasi berhasil disembunyikan secara efektif, sehingga **tidak dapat dianalisis secara langsung melalui tools reverse engineering seperti JADX**.

Kondisi ini secara signifikan menurunkan risiko *reverse engineering*, penyalahgunaan kredensial, serta kebocoran informasi sensitif dari sisi aplikasi.

[Gambar: Cuplikan source code hasil dekompilasi dari JADX]



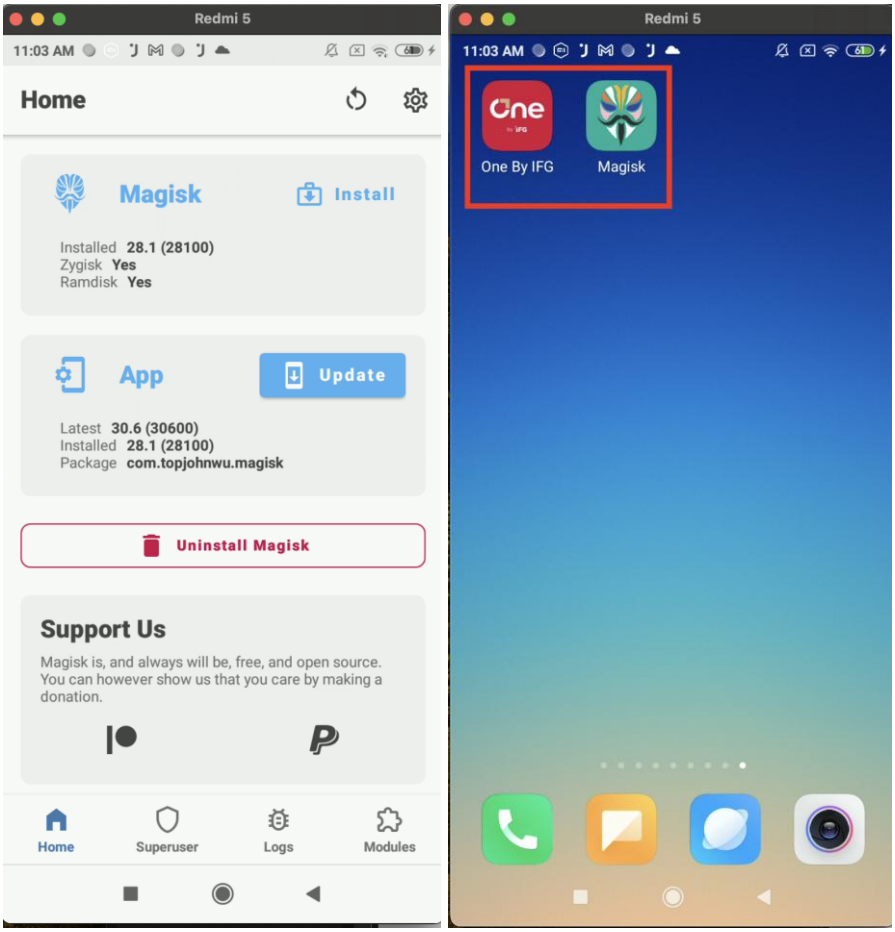
3. Runtime Protection (Perlindungan Saat Aplikasi Berjalan)

a. Before Hardened

Pada kondisi sebelum penerapan *runtime protection*, aplikasi **belum dilengkapi dengan mekanisme deteksi dan mitigasi terhadap lingkungan perangkat yang tidak aman**. Hal ini dibuktikan dengan aplikasi yang masih dapat berjalan secara normal pada perangkat yang telah di-*root* menggunakan **Magisk**.

Ketiadaan kontrol ini membuka celah keamanan yang signifikan, khususnya terhadap potensi serangan pada saat aplikasi berjalan (*runtime attack*), seperti **code injection**, *method hooking*, maupun manipulasi perilaku aplikasi melalui framework pihak ketiga. Dalam kondisi tersebut, integritas aplikasi tidak dapat terjamin karena lingkungan eksekusinya telah berada di luar kontrol keamanan yang semestinya.

[Gambar: Device yang telah di-root menggunakan magisk]

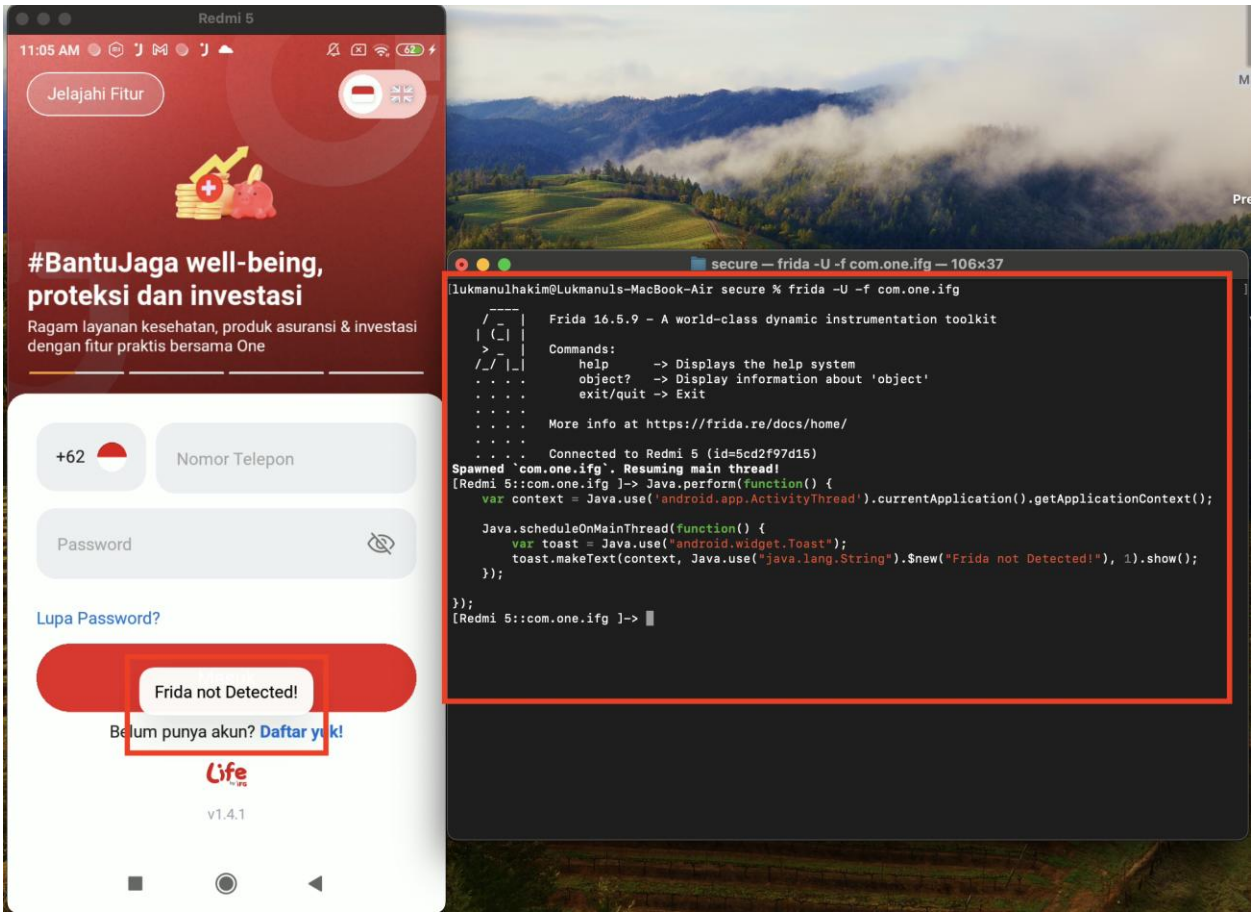


Sebagai tindak lanjut, dilakukan pengujian *runtime attack* menggunakan **Frida** untuk mensimulasikan skenario **code injection**. Pada pengujian ini, skrip Frida di-inject ke dalam aplikasi dengan tujuan menampilkan *toast message* bertuliskan **"Frida not detected"**.

Hasil pengujian menunjukkan bahwa proses injeksi **berhasil dilakukan** dan aplikasi **tetap berjalan secara normal** tanpa adanya indikasi pemblokiran, peringatan, maupun terminasi aplikasi. Kondisi ini mengindikasikan bahwa aktivitas injeksi melalui Frida **tidak terdeteksi oleh aplikasi**, serta tidak terdapat mekanisme proteksi yang mampu mendeteksi atau mencegah penggunaan *dynamic instrumentation framework* tersebut.

Temuan ini menegaskan bahwa pada kondisi *before hardened*, aplikasi **rentan terhadap serangan injeksi pada saat runtime**, termasuk manipulasi fungsi, pengambilan data sensitif, maupun perubahan alur logika aplikasi.

[Gambar: Hooking menggunakan Frida untuk menampilkan toast message]



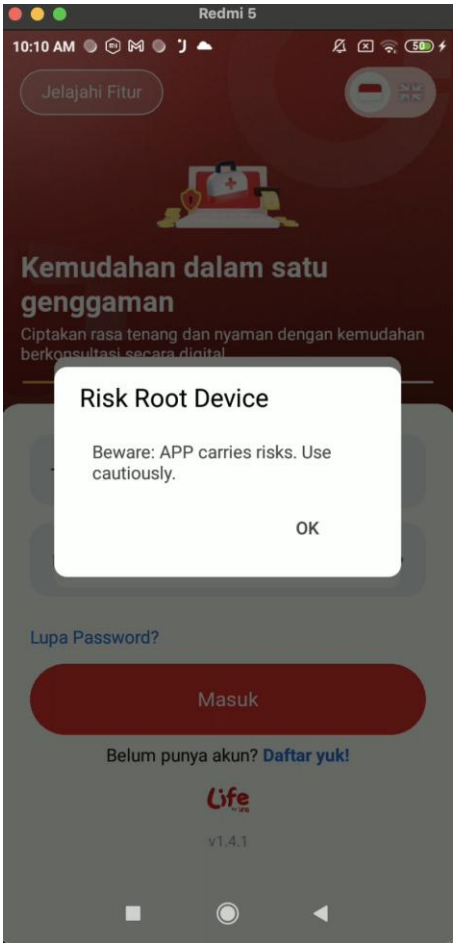
b. After Hardened

Setelah proses *hardening* diterapkan menggunakan **SecIron**, aplikasi kini telah dilengkapi dengan mekanisme **deteksi aktivitas hooking, manipulasi runtime, serta kondisi perangkat yang tidak aman (rooted device)**. Mekanisme ini memungkinkan aplikasi untuk mengidentifikasi upaya serangan yang dilakukan melalui *dynamic instrumentation*, teknik hooking, maupun eksekusi aplikasi pada lingkungan perangkat yang telah di-*root*.

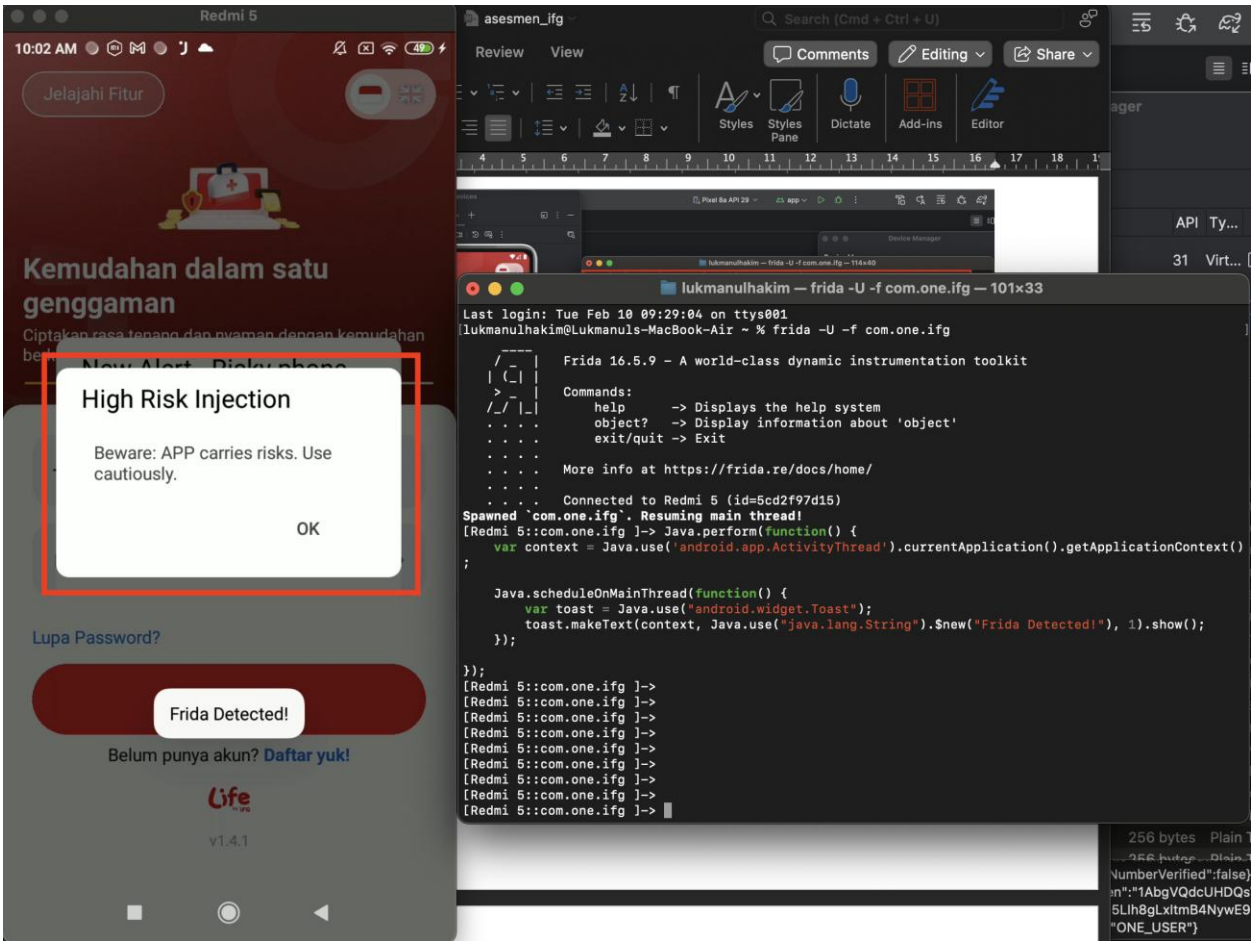
Pada saat aktivitas hooking atau indikasi perangkat *rooted* terdeteksi, aplikasi secara otomatis **melakukan tindakan mitigasi**, seperti **penghentian eksekusi aplikasi**, sehingga upaya serangan tidak dapat dilanjutkan. Selain itu, informasi terkait insiden keamanan tersebut **tercatat dan terkirim ke dashboard IronSKY**, memungkinkan tim keamanan untuk melakukan pemantauan, analisis, serta respons lanjutan secara terpusat dan real-time.

Penerapan proteksi ini secara signifikan meningkatkan **ketahanan aplikasi terhadap serangan pada saat runtime**, sekaligus memberikan **visibilitas yang lebih baik terhadap pola serangan, kondisi perangkat, dan sumber ancaman** yang terjadi di sisi klien.

[Gambar: Aplikasi mendeteksi device root setelah di-hardened]



[Gambar: Aplikasi mendeteksi aktivitas hooking yang terjadi setelah di-hardened]



[Gambar: Data monitoring yang tercatat pada dashboard IronSKY]

e23441a5-4f4a-38ee-9f5d-7e2c412c5052	unknow	1141	One By IFG	1.4.1	High Risk Injection Behavior	1770692987355	Android 8.1.0	5.5.1	Pop-up message with close button	True

THREAT ID	THREAT NAME	THREAT DETAILS
MS100002	Injection attack	Reason：["dlopen"]; Type：dlopen;
MR100002	Root/Jailbreak	root_manage_apps:#com.tsng.hidemyapplist; su_paths_exist:/sbin/su; which_su:/sbin/su; su_files_exist:/sbin/su; magisk_root:fileStat:[/sbin/magisk]magisk app install,;

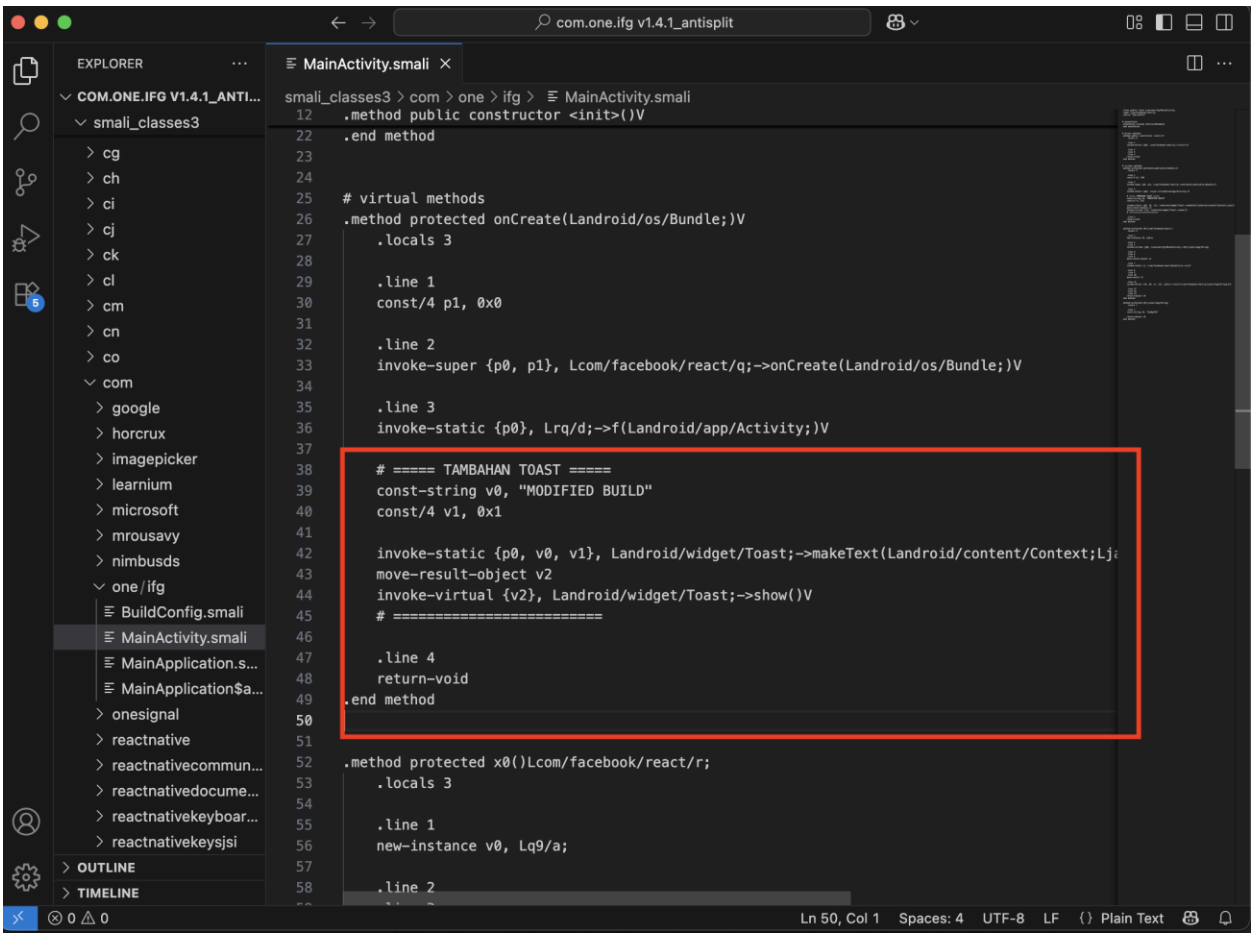
4. Integrity Protection

a. Before Hardened

Selain pengujian pada aspek *runtime protection*, dilakukan pula evaluasi terhadap **integrity protection** aplikasi. Hasil pengujian menunjukkan bahwa pada kondisi *before hardened*, aplikasi **belum dilengkapi dengan mekanisme pemeriksaan integritas** untuk mendeteksi perubahan pada kode atau struktur aplikasi.

Pada skenario pengujian ini, aplikasi didekompilasi dan dilakukan modifikasi dengan menambahkan *toast message* pada **Main Activity** berupa teks **"Modified Build"**, kemudian aplikasi dibangun ulang (*rebuild*) dan diinstal kembali ke perangkat uji.

[Gambar: Aplikasi setelah di dekompilasi dan ditambahkan Toast dengan teks Modified Build]



Setelah aplikasi terpasang, hasil pengujian menunjukkan bahwa aplikasi **tetap dapat dijalankan secara normal** tanpa adanya peringatan, pemblokiran, maupun terminasi aplikasi. *Toast message* yang ditambahkan muncul sebagaimana fungsi bawaan aplikasi, seolah-olah merupakan bagian dari aplikasi yang sah (*legitimate*).

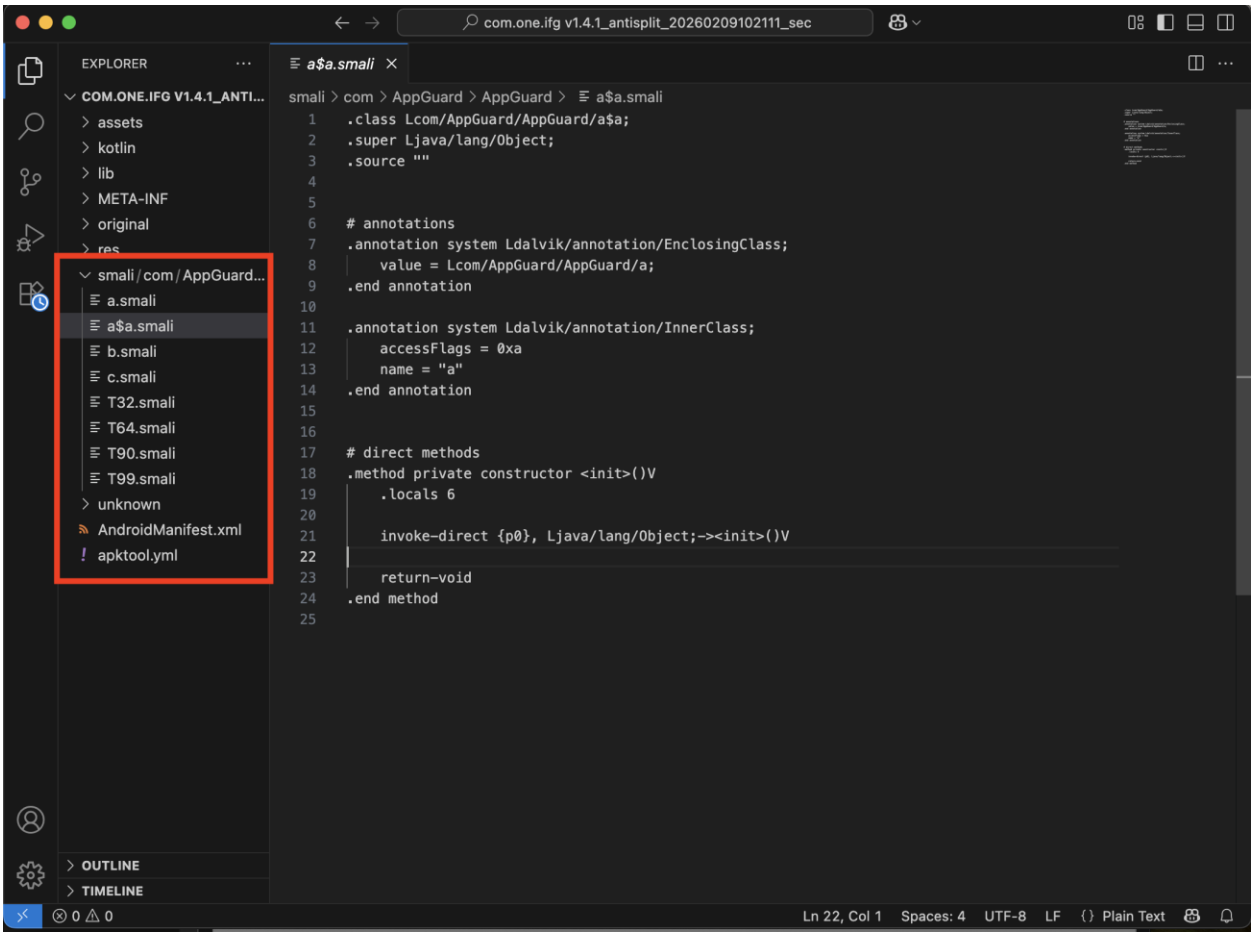
[Gambar: Aplikasi tetap berjalan setelah dimodifikasi]

Kondisi ini menunjukkan bahwa aplikasi **tidak mendeteksi adanya modifikasi kode**, sehingga membuka risiko keamanan yang serius. Dalam skenario penyalahgunaan, penyerang dapat memodifikasi satu halaman penuh agar menyerupai tampilan asli aplikasi, namun pada kenyataannya mengarahkan pengguna ke **endpoint berbahaya milik pihak tidak berwenang**. Risiko ini berpotensi menyebabkan pencurian data, penyalahgunaan kredensial, hingga kompromi akun pengguna.

b. After Hardened

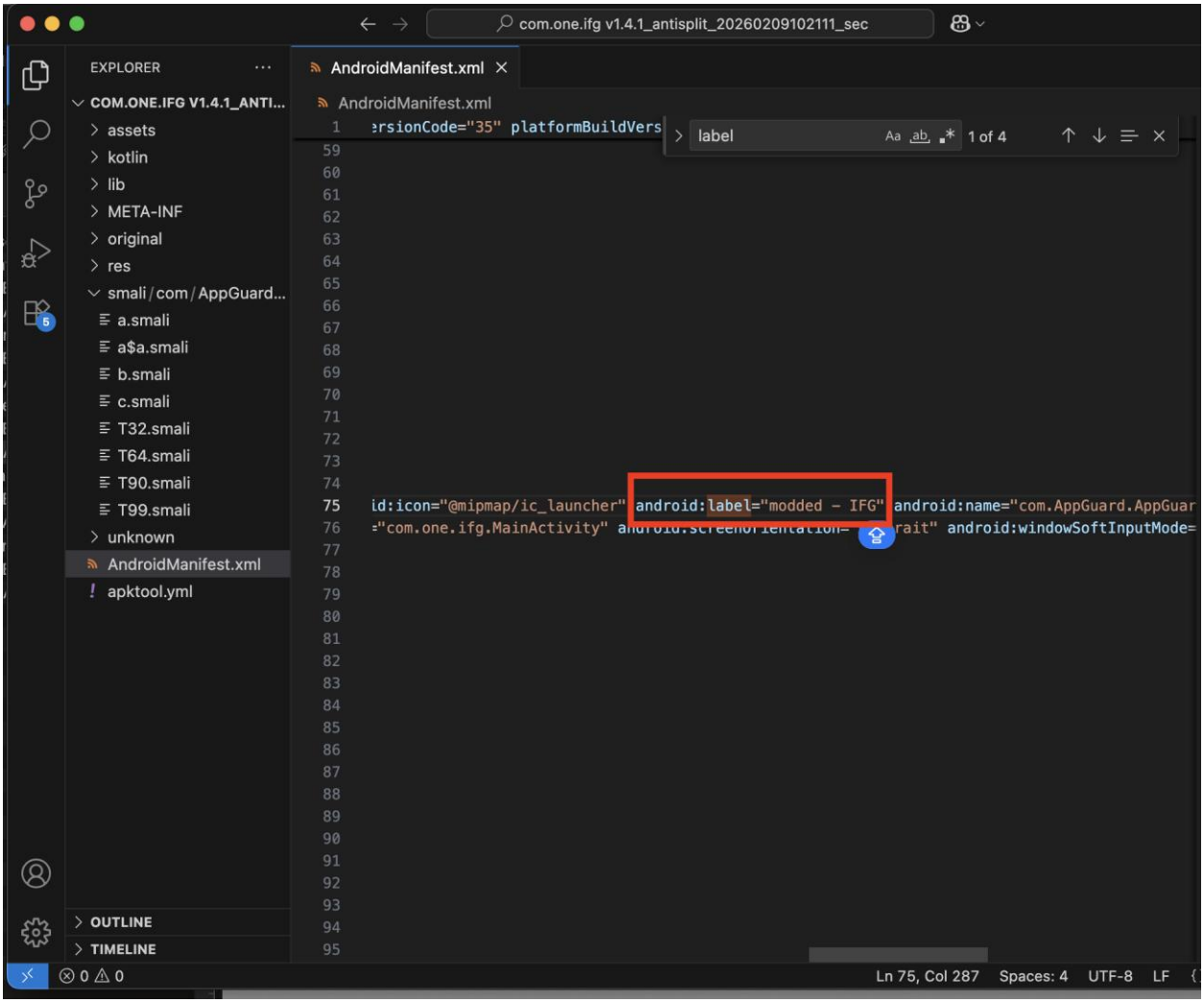
Pada saat dilakukan upaya modifikasi terhadap aplikasi yang telah di-*harden* menggunakan **SecIron**, seluruh kelas yang sebelumnya dapat diakses, termasuk **Main Activity**, **tidak lagi dapat dilihat maupun dianalisis melalui proses dekompilasi**. Hal ini menunjukkan bahwa mekanisme proteksi kode telah diterapkan secara efektif, sehingga menyulitkan pihak tidak berwenang untuk melakukan *reverse engineering* terhadap logika inti aplikasi.

[Gambar: Hasil dekompilasi aplikasi setelah hardening, di mana kelas-kelas internal tidak lagi dapat diidentifikasi]



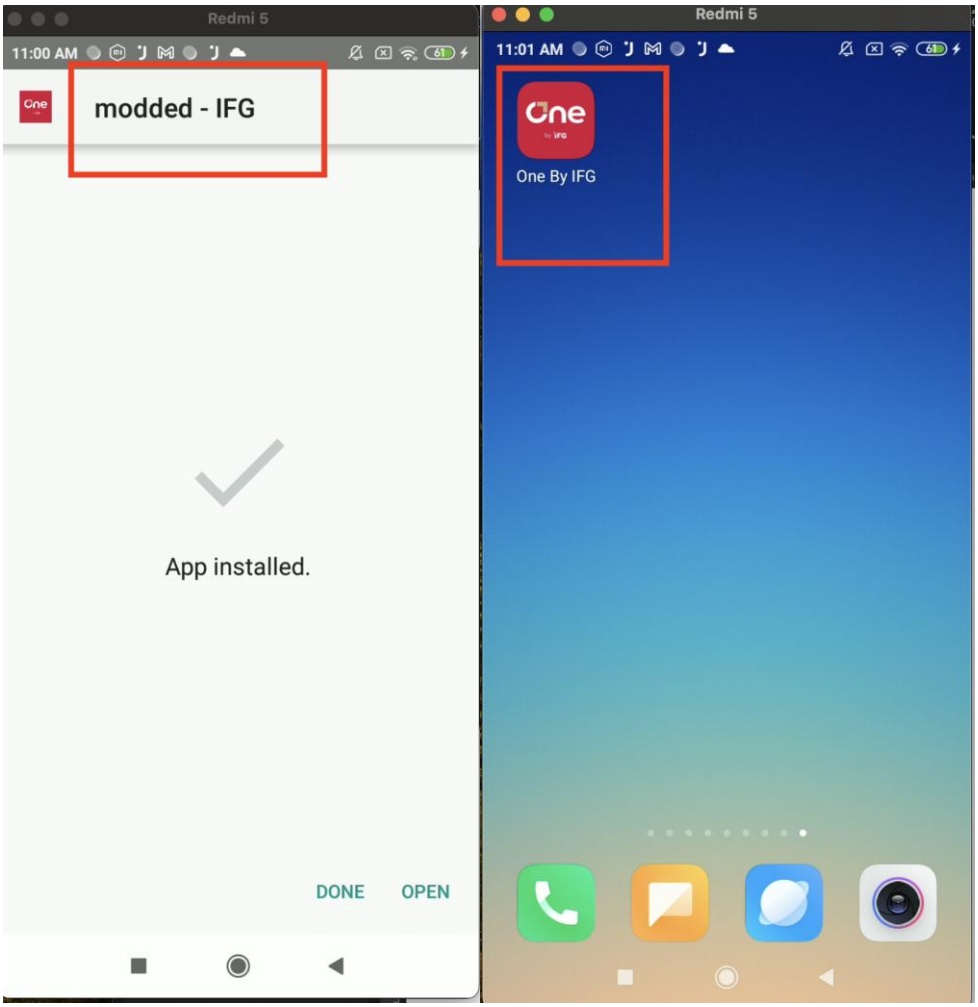
Sebagai bagian dari pembuktian (*proving*) mekanisme **integrity protection** SecIron, dilakukan pengujian lanjutan dengan melakukan perubahan minor pada aplikasi, yaitu **mengubah label aplikasi menjadi "modded – IFG"**.

[Gambar: Merubah label aplikasi menjadi "modded -IFG"]



Setelah dilakukan *rebuild* dan instalasi ulang ke perangkat uji, aplikasi **langsung mengalami *force close*** pada saat dijalankan.

[Gambar: Aplikasi hasil modifikasi yang diinstal pada perangkat dan langsung mengalami force close akibat mekanisme integrity protection]



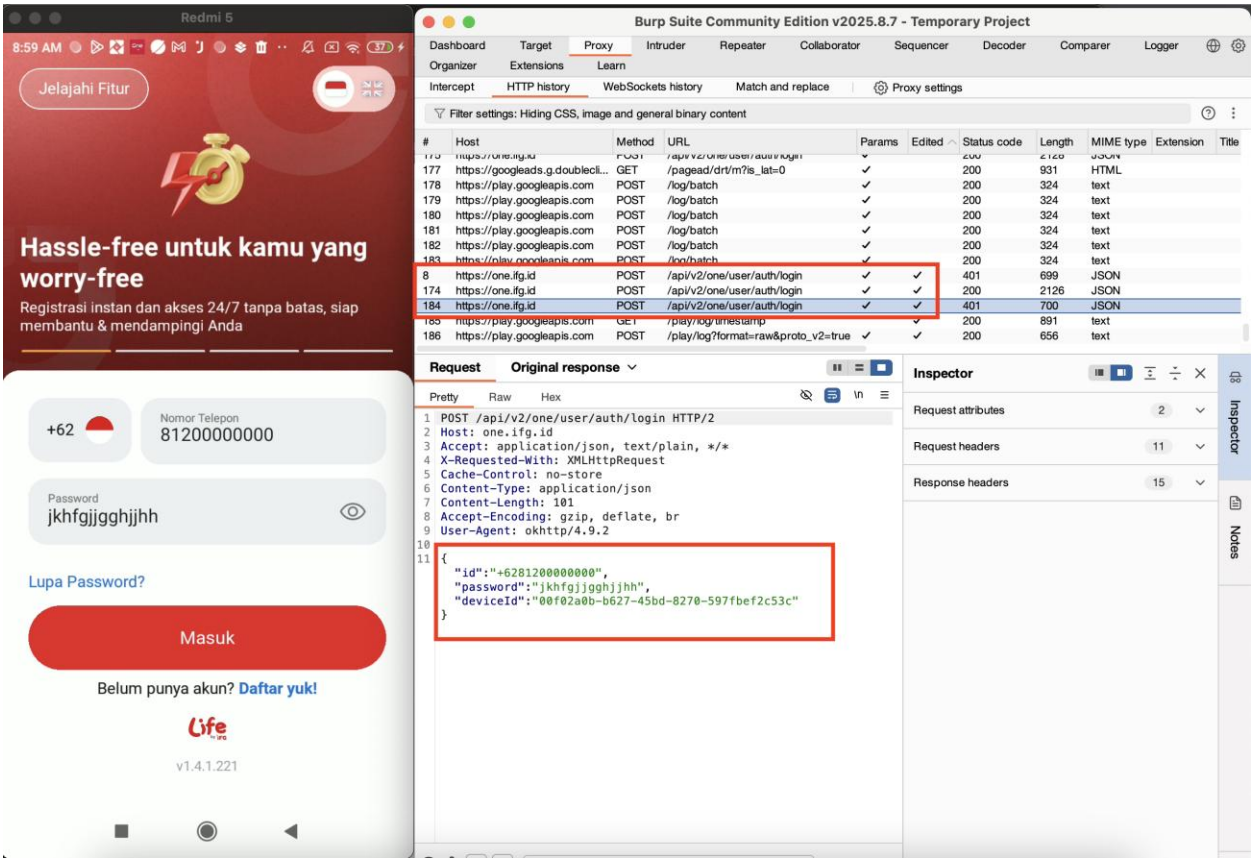
Hasil pengujian ini membuktikan bahwa SecIron **mampu mendeteksi setiap perubahan pada paket aplikasi**, termasuk modifikasi yang bersifat non-fungsional seperti perubahan label. Dengan demikian, mekanisme *integrity protection* bekerja secara menyeluruh untuk mencegah eksekusi aplikasi yang telah dimodifikasi.

5. Man-in-the-Middle (MITM) Protection

a. Before Hardened

Berdasarkan hasil pengujian **Man-in-the-Middle (MITM)** menggunakan **Burp Suite**, diketahui bahwa aplikasi **belum menerapkan mekanisme SSL Pinning maupun deteksi terhadap aktivitas MITM**. Pada kondisi ini, komunikasi antara aplikasi dan server dapat diintersepsi dengan mudah, sehingga **endpoint API dan payload komunikasi dapat terlihat secara jelas**, sebagaimana ditunjukkan pada pengujian berikut.

[Gambar Percobaan Man-in-the-Middle menggunakan Burp Suite sebelum hardening]



Ketiadaan proteksi terhadap serangan MITM membuka risiko keamanan yang signifikan. Dalam skenario ini, penyerang berpotensi untuk:

- Mencegat dan memantau *request* serta *response* antara aplikasi dan server
- Memodifikasi data pada saat runtime
- Melakukan serangan *replay* maupun *spoofing* data

Kondisi tersebut dapat berdampak langsung pada kebocoran data sensitif, manipulasi transaksi, hingga penyalahgunaan sesi komunikasi aplikasi.

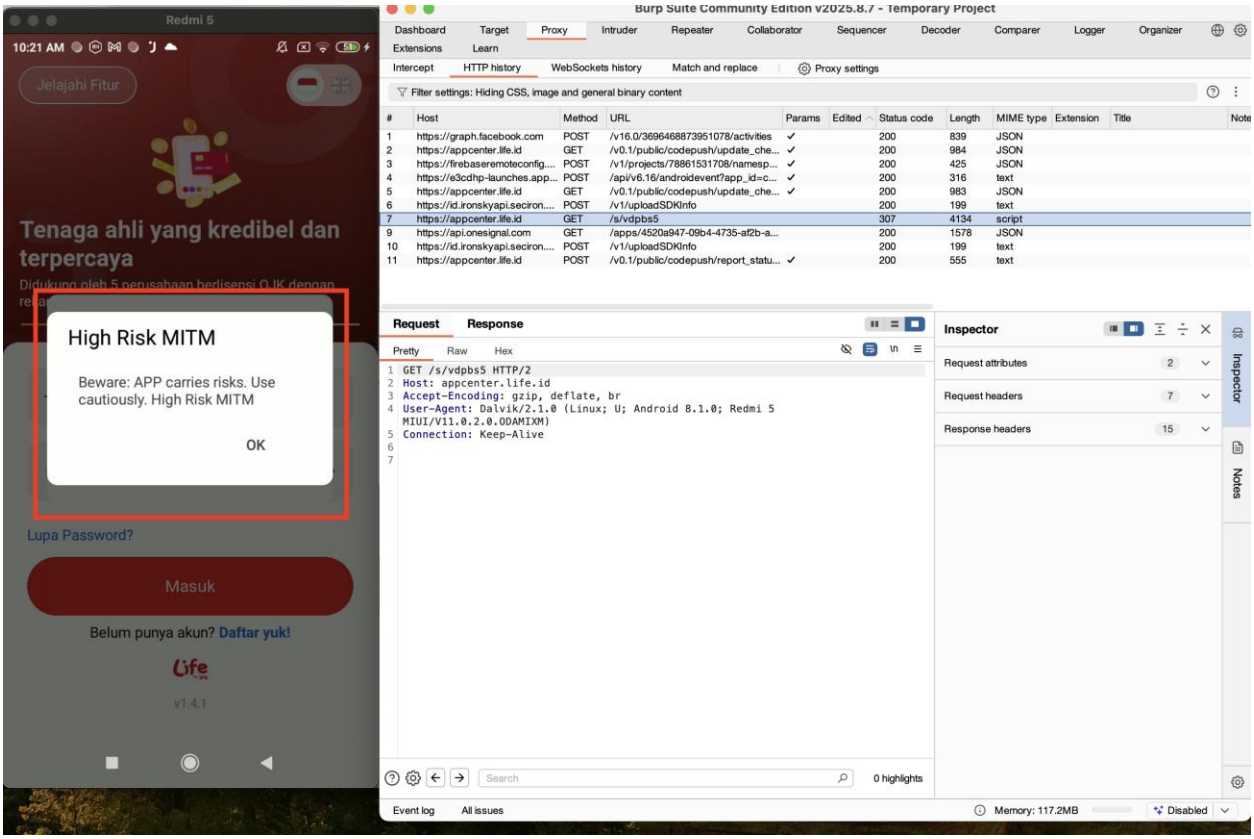
a. After Hardened

Setelah proses *hardening* diterapkan menggunakan **SecIron**, aplikasi kini mampu **mendeteksi aktivitas Man-in-the-Middle secara efektif**. Upaya intersepsi komunikasi yang dilakukan melalui Burp Suite berhasil teridentifikasi oleh mekanisme proteksi yang diterapkan.

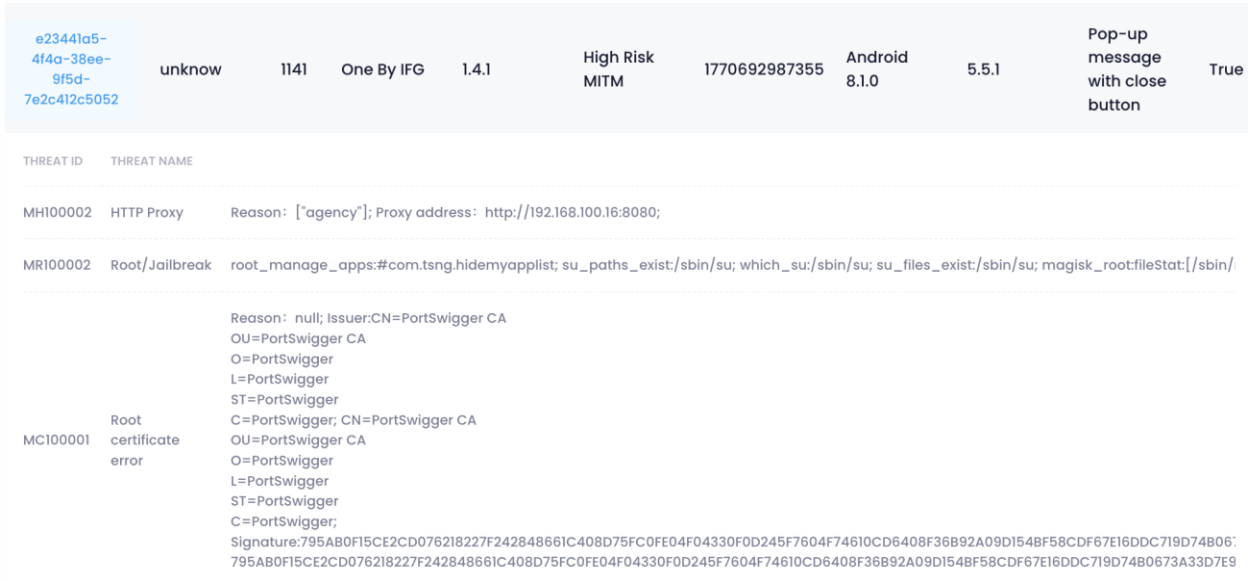
Pada saat aktivitas MITM terdeteksi, aplikasi dapat **menjalankan respons keamanan yang bersifat konfigurable**, seperti melakukan *force exit* secara langsung atau menampilkan notifikasi peringatan sebelum aplikasi dihentikan. Fleksibilitas ini memungkinkan penyesuaian kebijakan keamanan sesuai dengan kebutuhan operasional dan tingkat risiko yang ditetapkan.

Selain itu, seluruh aktivitas serangan yang terdeteksi **tercatat dan dimonitor melalui dashboard IronSKY**, sehingga tim keamanan memperoleh visibilitas penuh terhadap upaya MITM yang terjadi di sisi klien.

[Gambar: Percobaan MITM menggunakan Burp Suite yang terdeteksi setelah hardening]



[Gambar: Data monitoring aktivitas MITM pada dashboard IronSKY]



e2344la5-4f4a-38ee-9f5d-7e2c412c5052	unknow	1141	One By IFG	1.4.1	High Risk MITM	1770692987355	Android 8.1.0	5.5.1	Pop-up message with close button	True

THREAT ID	THREAT NAME	
MH100002	HTTP Proxy	Reason：["agency"]; Proxy address：http://192.168.100.16:8080;
MR100002	Root/Jailbreak	root_manage_apps:#com.tsng.hidemyapplist; su_paths_exist:/sbin/su; which_su:/sbin/su; su_files_exist:/sbin/su; magisk_root:fileStat:[/sbin/
MC100001	Root certificate error	Reason：null; Issuer:CN=PortSwigger CA OU=PortSwigger CA O=PortSwigger L=PortSwigger ST=PortSwigger C=PortSwigger; CN=PortSwigger CA OU=PortSwigger CA O=PortSwigger L=PortSwigger ST=PortSwigger C=PortSwigger; Signature:795AB0F15CE2CD076218227F242848661C408D75FC0FE04F04330F0D245F7604F74610CD6408F36B92A09D154BF58CDF67E16DDC719D74B06 795AB0F15CE2CD076218227F242848661C408D75FC0FE04F04330F0D245F7604F74610CD6408F36B92A09D154BF58CDF67E16DDC719D74B0673A33D7E9

6. Penyimpanan Data di Shared Preferences

a. Before Hardened

Berdasarkan hasil analisis, ditemukan bahwa aplikasi menyimpan sejumlah konfigurasi di dalam **SharedPreferences**. Pada kondisi *before hardened*, mekanisme penyimpanan tersebut **belum dilengkapi dengan enkripsi maupun proteksi tambahan**.

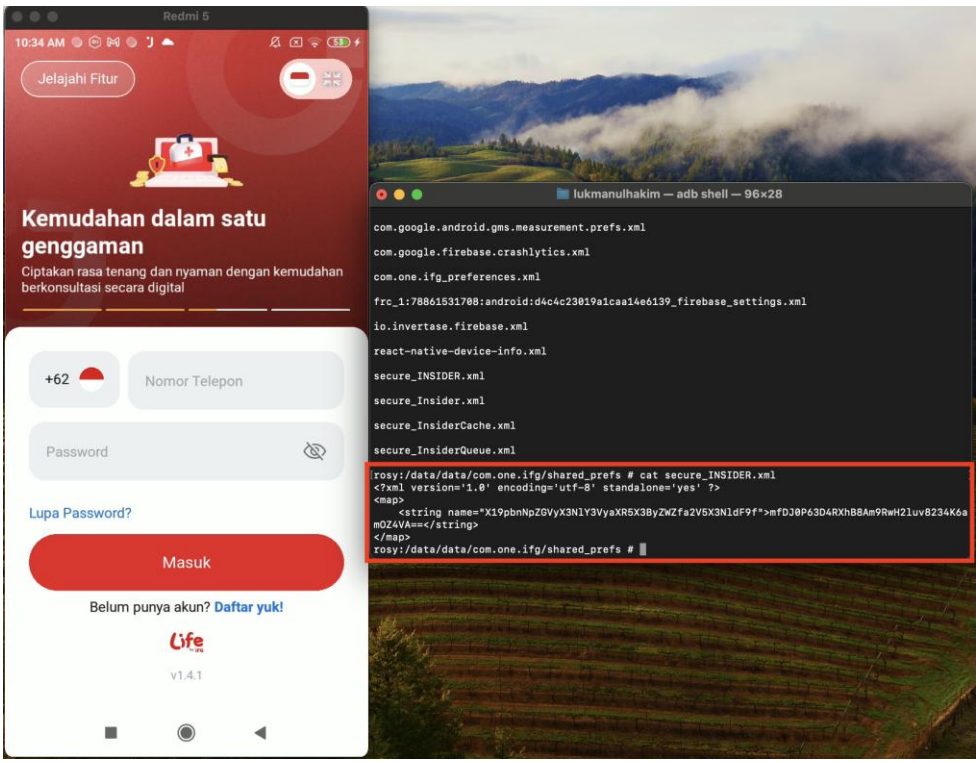
Apabila data sensitive, seperti **token autentikasi, ID pengguna, atau status login**, disimpan dalam SharedPreferences tanpa perlindungan yang memadai, maka informasi tersebut berpotensi untuk diakses maupun dimodifikasi, terutama pada perangkat yang berada dalam kondisi **rooted** atau **debuggable**.

Kondisi ini meningkatkan risiko keamanan, antara lain:

- Data dapat dibaca atau diubah secara langsung melalui akses ke penyimpanan aplikasi
- Terbukanya peluang terjadinya *spoofing* identitas pengguna
- Peningkatan risiko *session hijacking* akibat manipulasi token atau status autentikasi

Tanpa mekanisme perlindungan yang memadai, penyimpanan data pada sisi klien menjadi salah satu titik lemah yang dapat dimanfaatkan oleh pihak tidak berwenang.

[Gambar: Isi SharedPreferences hasil eksplorasi sebelum hardening]



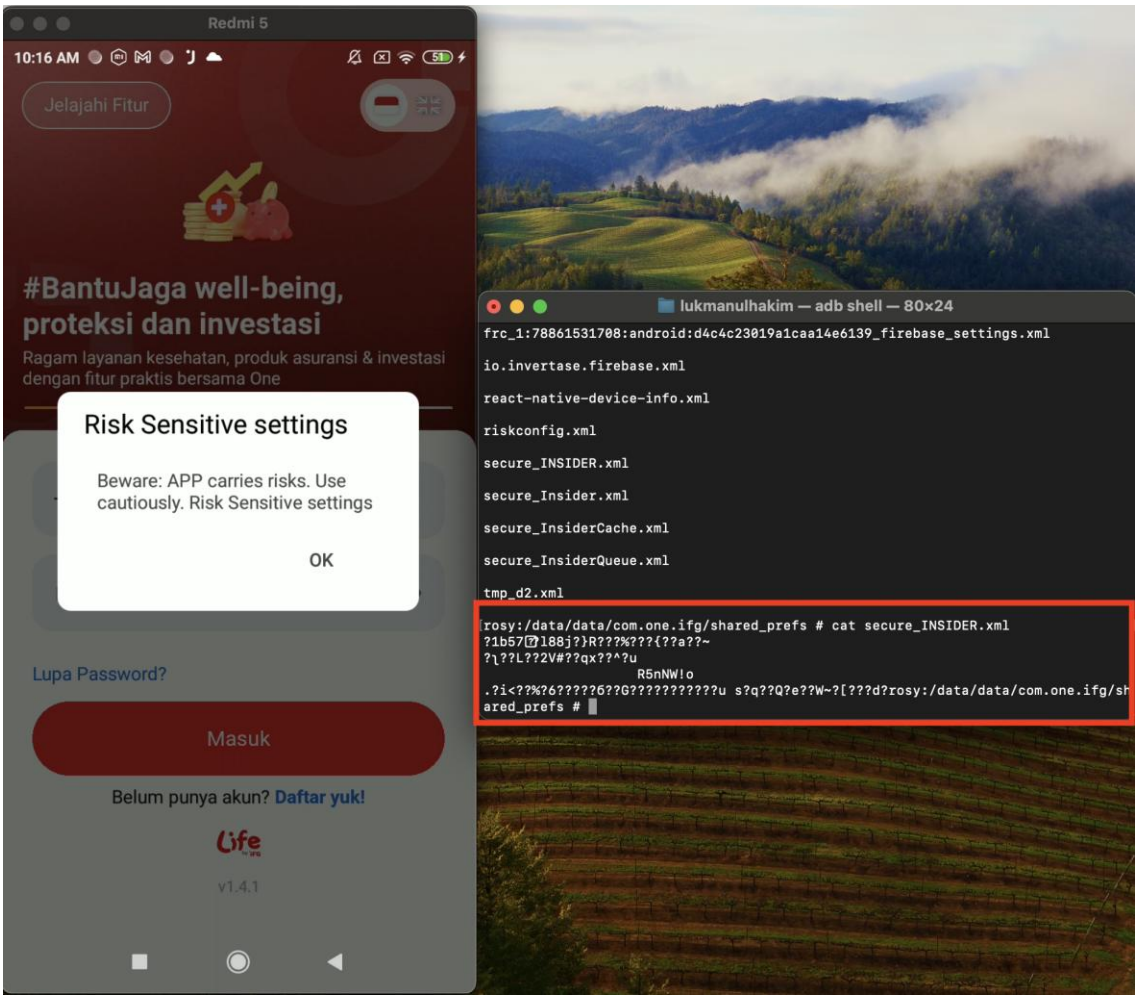
b. After Hardened

Setelah proses *hardening* diterapkan menggunakan **SecIron**, mekanisme **enkripsi pada SharedPreferences** telah diaktifkan. Dengan penerapan enkripsi ini, data yang disimpan di sisi klien **tidak lagi dapat dibaca dalam bentuk teks yang dapat dimengerti**, karena seluruh nilai tersimpan dalam format terenkripsi.

Hasil pengujian menunjukkan bahwa isi *SharedPreferences* yang sebelumnya dapat diakses dan dibaca secara langsung kini **berubah menjadi karakter acak yang tidak bermakna**, sehingga tidak dapat diinterpretasikan meskipun berhasil diakses secara tidak sah. Kondisi ini secara efektif melindungi data sensitif dari upaya pencurian informasi melalui akses langsung ke penyimpanan aplikasi.

Penerapan enkripsi *SharedPreferences* ini secara signifikan meningkatkan **keamanan penyimpanan data lokal**, serta meminimalkan risiko kebocoran informasi pada sisi perangkat pengguna.

[Gambar: Isi SharedPreferences pada aplikasi yang telah di-harden]



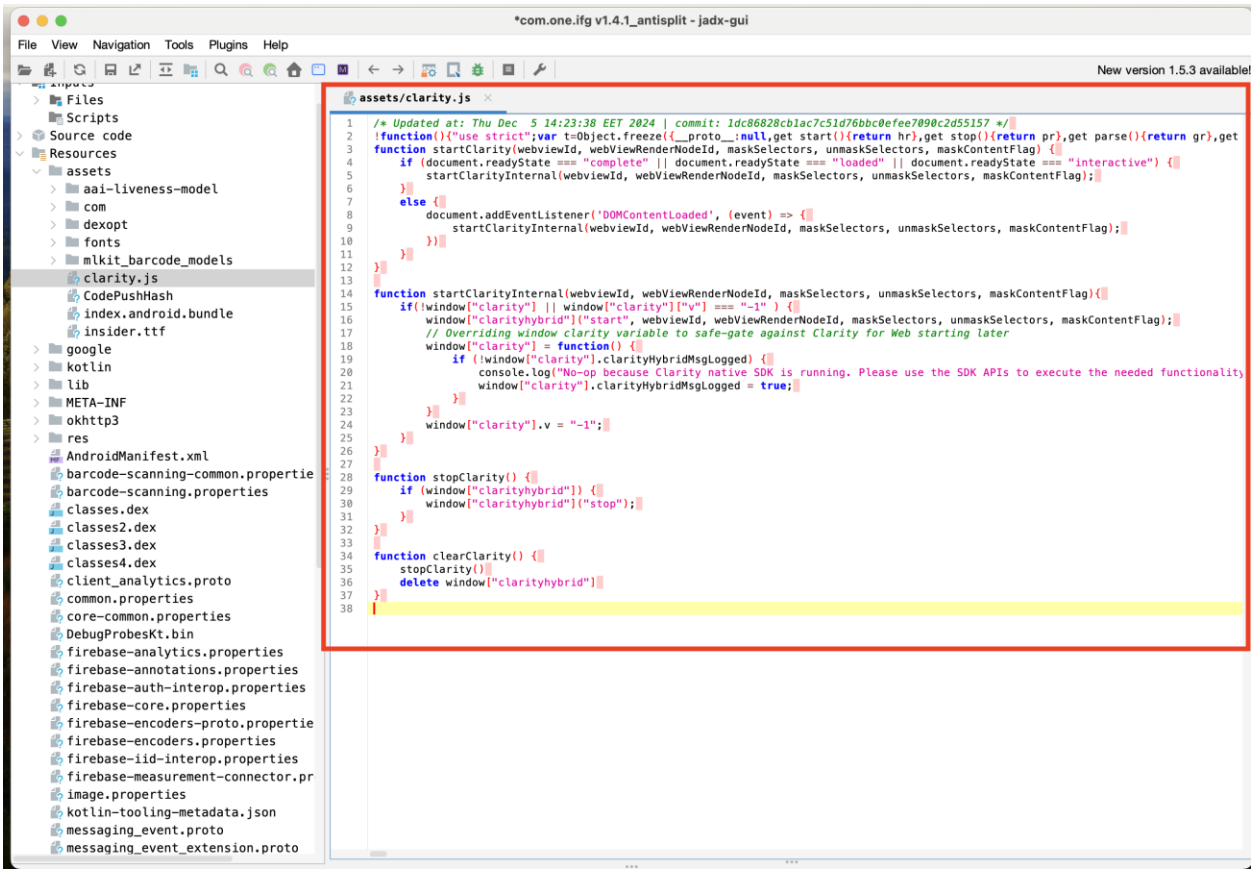
7. Resource Protection

a. Before Hardened

Berdasarkan hasil asesmen keamanan yang dilakukan, diketahui bahwa pada kondisi **sebelum penerapan mekanisme hardening**, aplikasi masih menyimpan sejumlah *resource* dalam bentuk **tidak terenkripsi**. *Resource* tersebut dapat diakses, ditampilkan, dan dianalisis secara langsung, sehingga berpotensi membuka informasi internal aplikasi.

Kondisi ini menunjukkan bahwa struktur aplikasi masih relatif mudah untuk dianalisis, yang dapat meningkatkan risiko terhadap upaya *reverse engineering* maupun penyalahgunaan *resource* oleh pihak yang tidak berwenang.

[Gambar: Contoh file resource aplikasi sebelum dilakukan hardening]

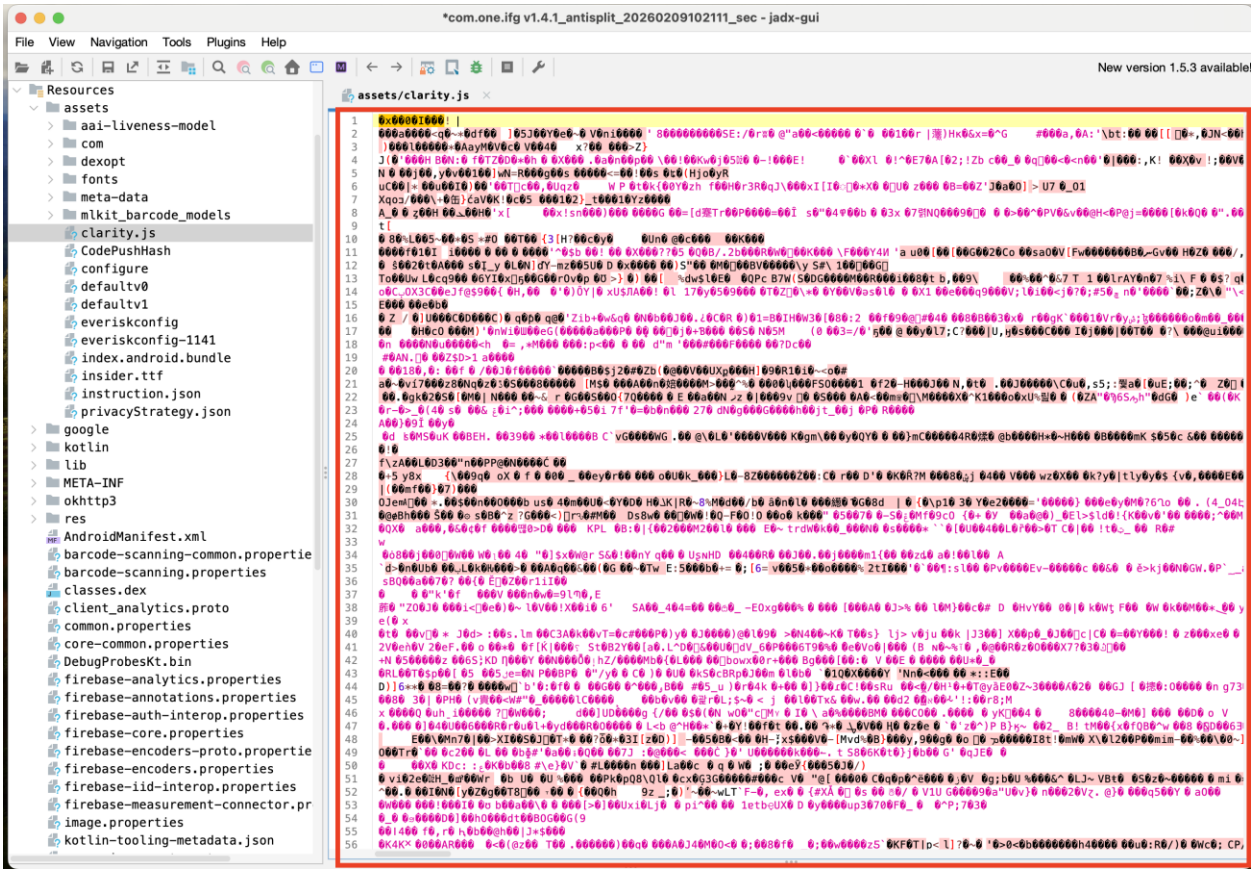


b. After Hardened

Setelah penerapan mekanisme hardening, *resource* pada aplikasi telah terenkripsi, sehingga tidak lagi dapat dianalisis secara langsung. Kondisi ini secara signifikan meningkatkan tingkat kesulitan terhadap upaya *reverse engineering* serta mengurangi risiko pemanfaatan *resource* aplikasi oleh pihak yang tidak berwenang.

Penerapan enkripsi pada *resource* aplikasi menunjukkan bahwa mekanisme hardening yang diterapkan telah berjalan dengan baik dalam melindungi komponen internal aplikasi dari proses analisis statis.

[Gambar: Contoh file resource aplikasi setelah dilakukan hardening]



8. Kesimpulan

Berdasarkan hasil asesmen keamanan yang telah dilakukan terhadap aplikasi **One by IFG**, dapat disimpulkan bahwa sebelum penerapan *hardening*, aplikasi masih memiliki sejumlah celah keamanan yang signifikan. Celah tersebut mencakup aspek *static protection*, *runtime protection*, *integrity protection*, *network security (MITM)*, serta *local data storage*, yang berpotensi dimanfaatkan oleh pihak tidak berwenang untuk melakukan *reverse engineering*, manipulasi aplikasi, pencurian data, maupun penyalahgunaan kredensial pengguna.

Setelah penerapan mekanisme *hardening* menggunakan **SecIron**, terjadi peningkatan postur keamanan aplikasi secara menyeluruh dan terukur, dengan hasil sebagai berikut:

- **Code Protection**
  Kode aplikasi berhasil diamankan melalui obfuscation, enkripsi, dan code hiding, sehingga struktur internal serta informasi sensitif tidak lagi dapat dianalisis melalui proses dekompilasi.

- **Runtime Protection**
  Aplikasi mampu mendeteksi dan memitigasi serangan pada saat runtime, termasuk aktivitas hooking, dynamic instrumentation (Frida), serta eksekusi aplikasi pada perangkat yang telah di-*root*. Upaya serangan dihentikan secara otomatis dan tercatat pada dashboard IronSKY.

- **Integrity Protection**
  Setiap perubahan pada paket aplikasi, baik perubahan logika maupun modifikasi minor seperti perubahan label aplikasi, berhasil terdeteksi dan menyebabkan aplikasi tidak dapat dijalankan (*force close*). Hal ini membuktikan bahwa integritas aplikasi terlindungi secara menyeluruh.

- **Man-in-the-Middle (MITM) Protection**
  Upaya intersepsi komunikasi jaringan berhasil dideteksi, dengan respons keamanan yang dapat dikonfigurasi sesuai kebijakan. Aktivitas MITM juga tercatat dan dapat dimonitor secara terpusat melalui IronSKY.

- **Local Data Protection (SharedPreferences)**
  Data yang disimpan secara lokal telah terenkripsi, sehingga tidak dapat dibaca atau dimodifikasi meskipun diakses secara tidak sah, secara signifikan menurunkan risiko kebocoran data dan *session hijacking*.

- **Resources Encryption**
  Resource internal aplikasi telah dienkripsi sebagai bagian dari mekanisme hardening, sehingga tidak lagi dapat dianalisis secara langsung. Penerapan enkripsi ini meningkatkan ketahanan aplikasi terhadap analisis statis dan upaya reverse engineering, serta melindungi komponen internal aplikasi dari penyalahgunaan oleh pihak yang tidak berwenang.

Secara keseluruhan, penerapan SecIron telah meningkatkan **ketahanan aplikasi terhadap berbagai vektor serangan**, memperkuat perlindungan data pengguna, serta memberikan **visibilitas dan kontrol keamanan yang lebih baik** bagi tim melalui sistem monitoring.