FIELD NOTE / SECURITY

Android Static Analysis dengan MobSF

Petruknisme · 7 Apr, 2017 · 2 min to read

Bagi rekan-rekan yang berkecimpung dalam dunia Reverse Engineering mungkin istilah Static Analysis sudah tidak asing lagi. Static Analysis merupakan sebuah analisis terhadap sebuah aplikasi ataupun code tanpa melakukan eksekusi. Biasanya digunakan untuk menemukan bug pada sebuah code/aplikasi, coding guidelines, code quality dan beberapa security point yang seharusnya diperhatikan seperti Android Manifest contohnya bila yang kita analisis adalah android app.

Pada tulisan kali ini, kita akan membahas MobSF untuk melakukan Static Analysis Android. Pada dasarnya, MobSF dapat melakukan analysis terhadap Android, iOS, dan Windows.

Jadi Apa itu MobSF?

Menurut sumber laman MobSF menyebutkan bahwa MobSF adalah sebagai berikut:

> *"Mobile Security Framework (MobSF) is an intelligent, all-in-one open source mobile application (Android/iOS/Windows) automated pen-testing framework capable of performing static and dynamic analysis. It can be used for effective and fast security analysis of Android, iOS and Windows mobile Applications and supports both binaries (APK, IPA & APPX) and zipped source code. MobSF can also perform Web API Security testing with it's API Fuzzer that can do Information Gathering, analyze Security Headers, identify Mobile API specific vulnerabilities like XXE, SSRF, Path Traversal, IDOR, and other logical issues related to Session and API Rate Limiting."*

Pemasangan MobSF

*** Requirements**

– Python 2.7

– JDK 1.7

Dipastikan bahwa sistem yang sedang berjalan sudah memiliki python versi 2.7 dengan pip yang sudah terpasang. Bila sudah, lakukan clone dengan git:

```
1 | git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF
```

Atau, bisa juga langsung download berkas zip yang tersedia pada laman berikut:

Licensed under CC BY-SA 4.0

https://github.com/MobSF/Mobile-Security-Framework-MobSF/releases (https://github.com/MobSF/Mobile-Security-Framework-MobSF/releases)

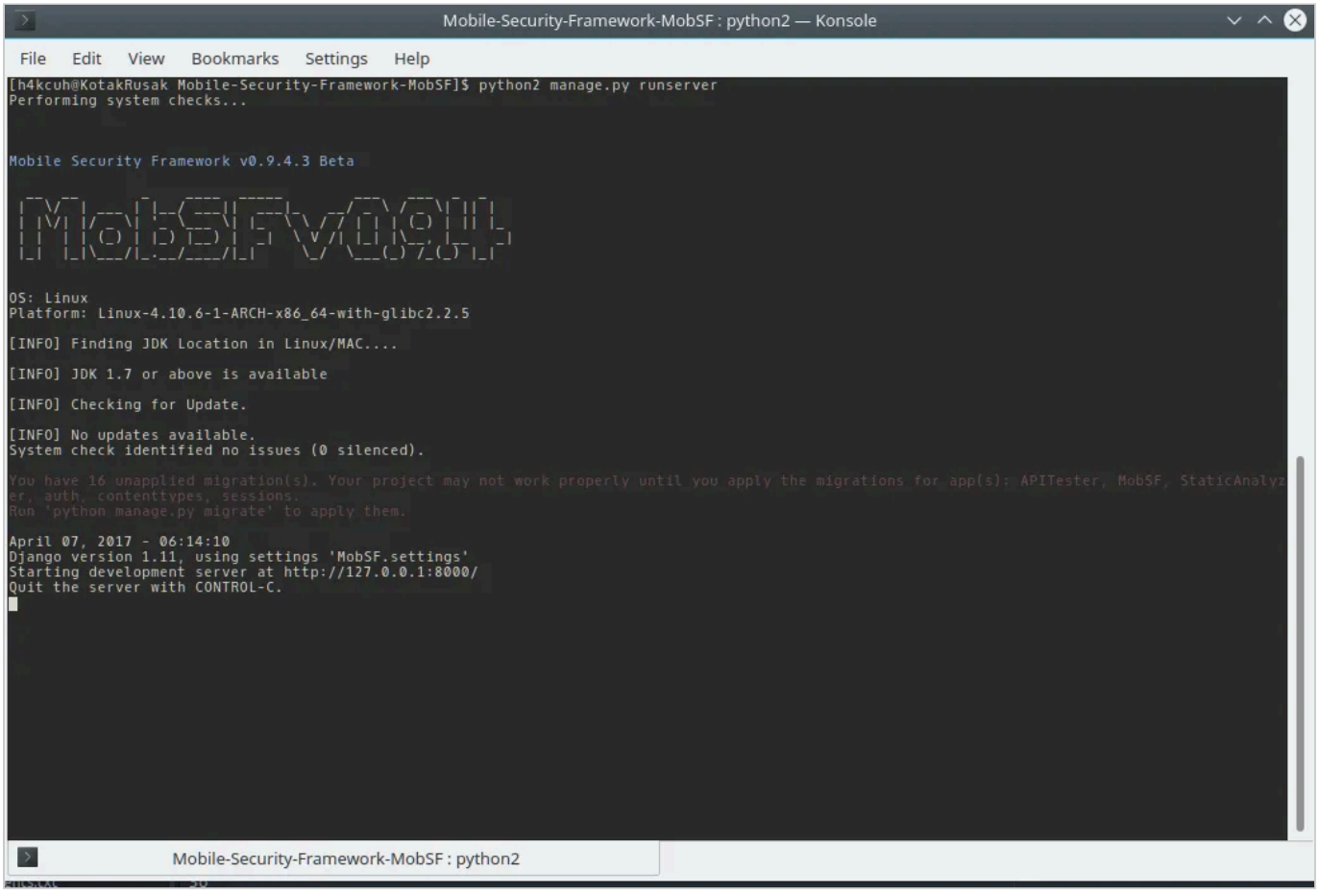
Pasang paket yang dibutuhkan oleh MobSF dengan menggunakan:

```
cd Mobile-Security-Framework-MobSF
sudo pip install -r requirements.txt
```

Tunggu sampai semua proses pemasangan paket yang dibutuhkan selesai. Pastikan tidak terjadi kesalahan saat proses melakukan pemasangan paket untuk MobSF. Selanjutnya, jalankan web server MobSF dengan menggunakan perintah:

```
python manage.py runserver #sesuaikan python exe dengan python versi 2.7
```

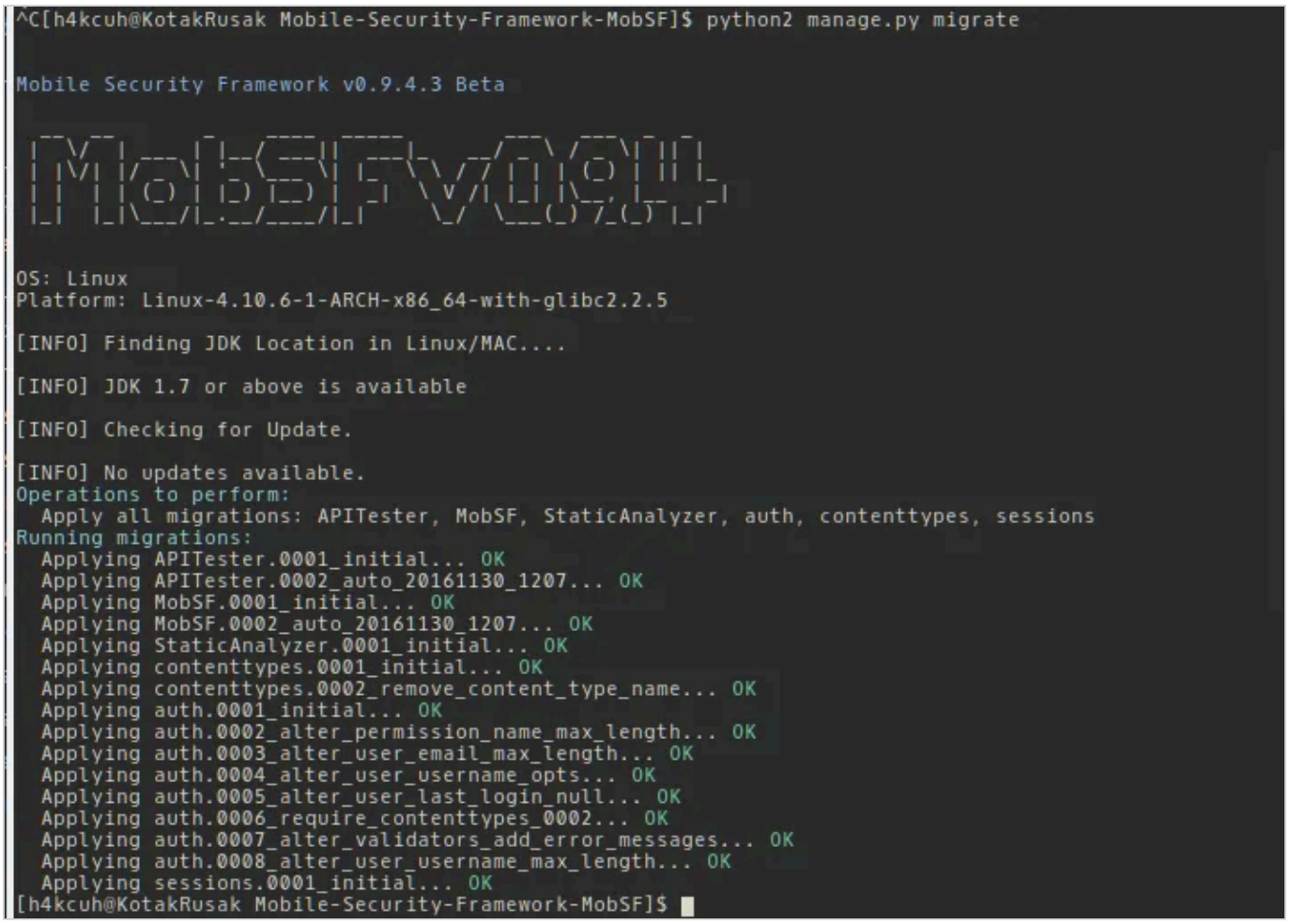
Akan tampil seperti gambar berikut:



Licensed under CC BY-SA 4.0

Nah, untuk menghindari error atau permasalahan saat melakukan analyze, lakukan `migrate` terlebih dahulu untuk memperbarui dan migrasi database pada MobSF:

```
python manage.py migrate
```



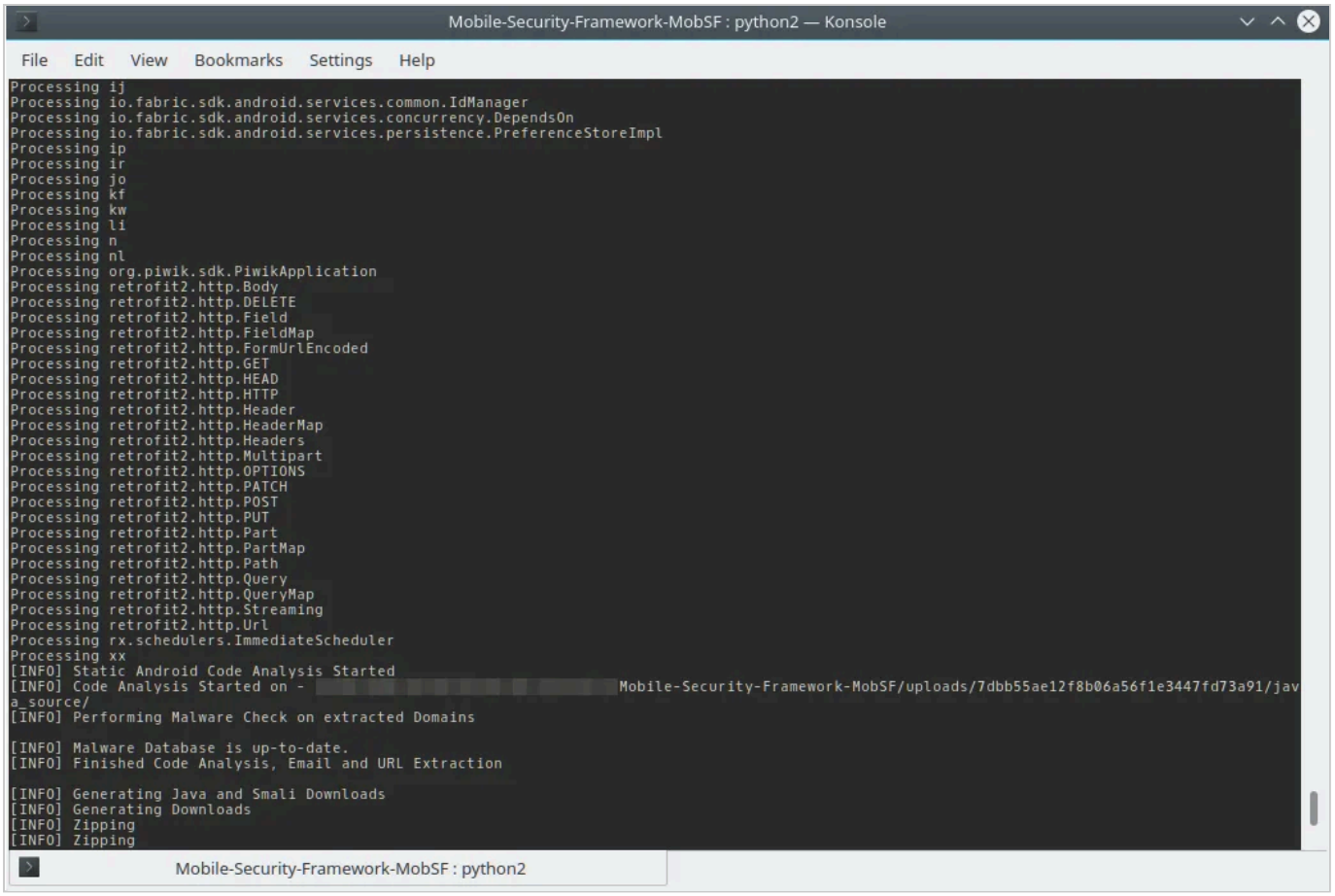
Bila sudah berhasil, kita jalankan kembali web servernya seperti yang sudah dilakukan sebelumnya. Buka url http://127.0.0.1:8000/ (http://127.0.0.1:8000/) maka akan tampil halaman utama dari MobSF sebagai berikut:

Licensed under CC BY-SA 4.0

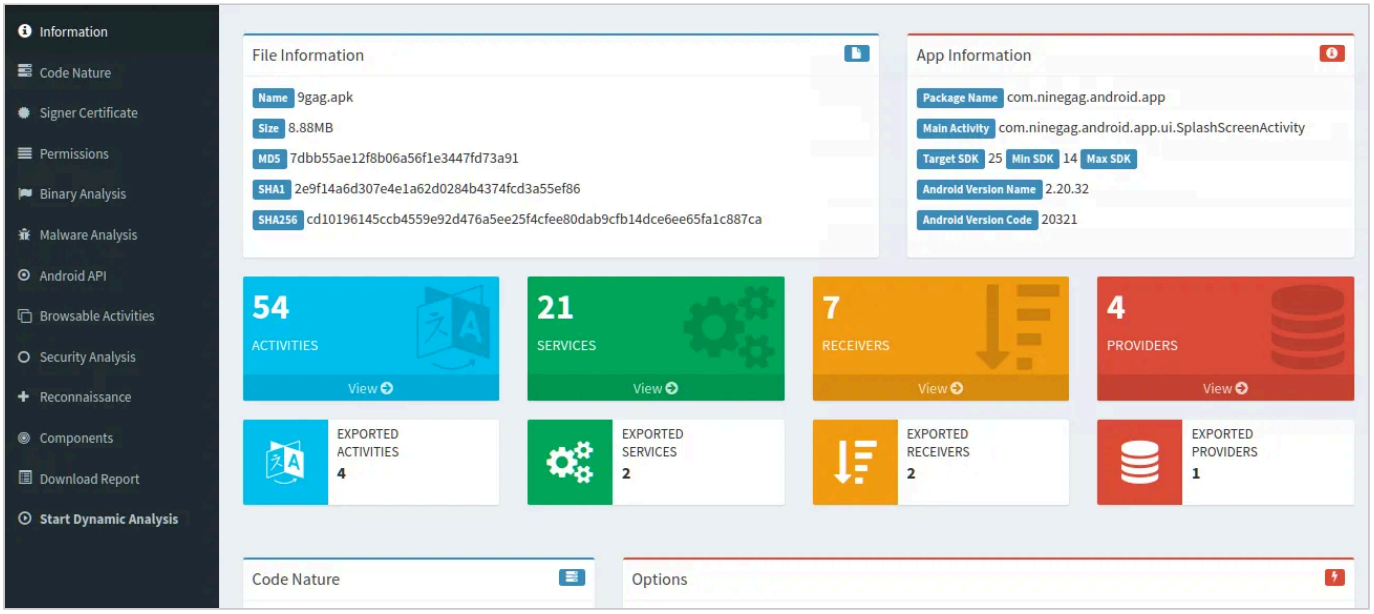


Untuk melakukan analyze, kita cukup drag and drop atau upload berkas apk dari aplikasi yang akan kita analisis. Saya disini menggunakan aplikasi 9gag sebagai bahan percobaan. Tunggu hingga proses analyze selesai dan nantinya akan disuguhkan dengan hasil reporting dari aplikasi tersebut. Bila ingin melihat proses yang sedang berjalan, bisa dicek melalui terminal saat menjalankan webserver.

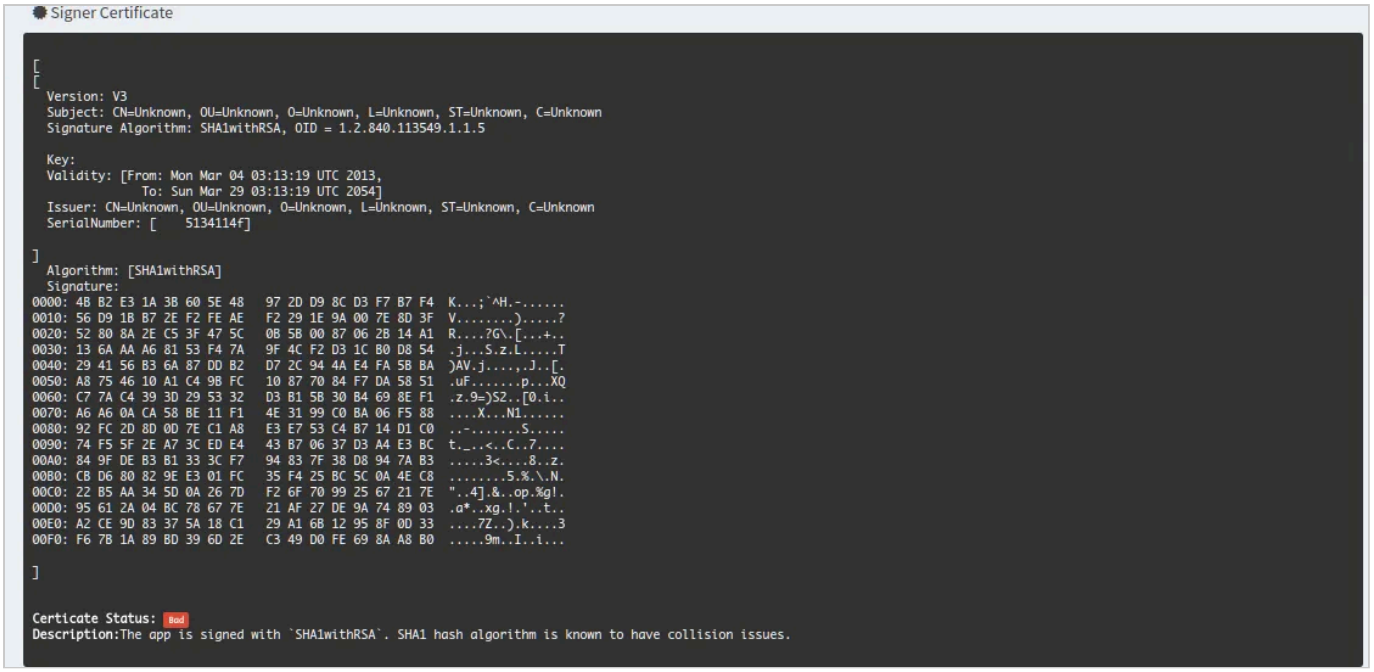
Licensed under CC BY-SA 4.0

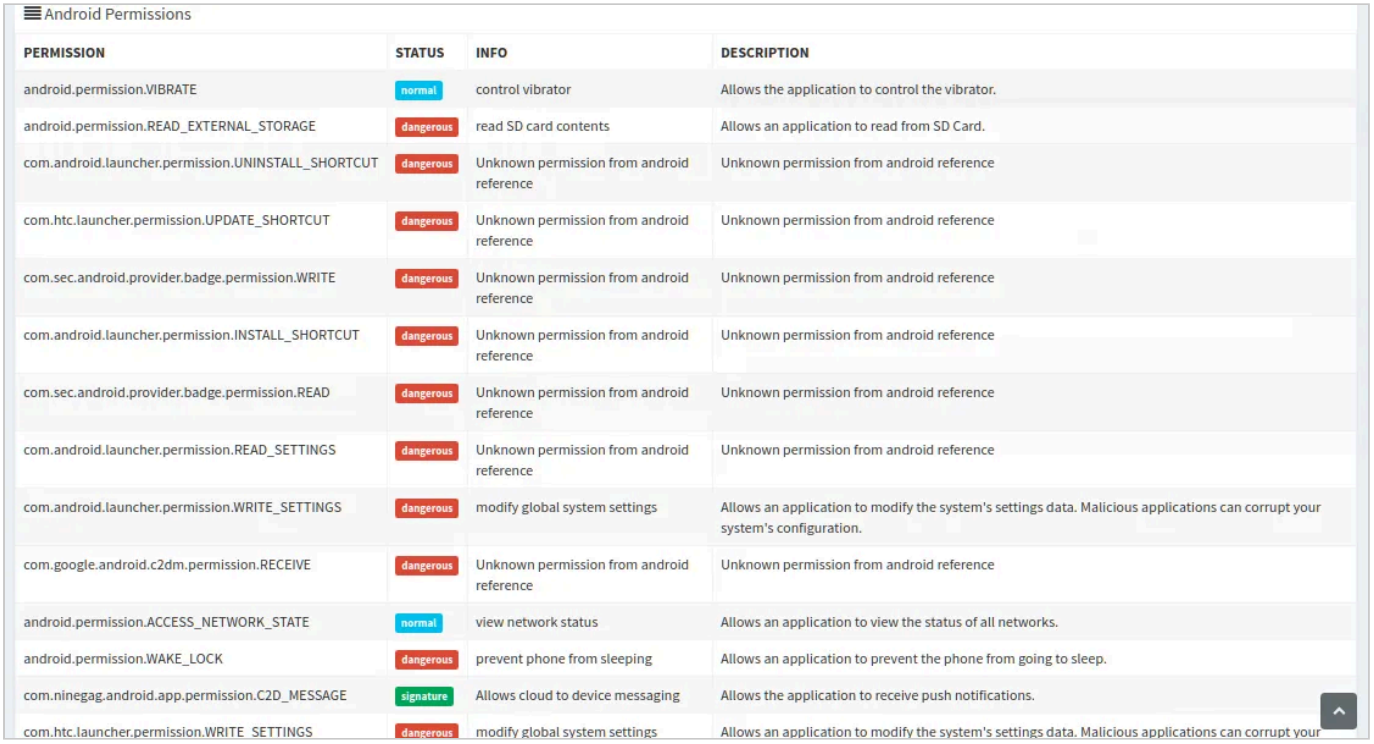


Oke, setelah proses analyzing selesai. Akan tampil seperti beberapa gambar berikut:



Licensed under CC BY-SA 4.0





Masih banyak lagi hasil report yang tidak bisa saya tampilkan disini untuk mengurangi page load 😀

Dengan MobSF, jadi lebih memudahkan Pentester ataupun security auditor dalam melakukan assessment terhadap mobile application. Akhir kata, semoga tulisan ini bermanfaat.

Security # Tutorial

Licensed under CC BY-SA 4.0

Licensed under CC BY-SA 4.0