

Mobile Security Framework (MobSF)

Introduction

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis, and security assessment framework capable of performing static and dynamic analysis. Mobile Security Framework (MobSF) is an automated, open-source, all-in-one mobile application (Android/iOS/Windows) pen-testing framework capable of performing static, dynamic, and malware analysis. It is suggested by OWASP MSTG for static analysis of security in mobile applications. It can be used for effective and fast security analysis of Android, iOS, and Windows mobile applications and support both binaries (APK, IPA & APPX) and zipped source code. MobSF can do dynamic application testing at runtime for Android apps and has Web API fuzzing capabilities powered by CapFuzz, a Web API-specific security scanner. MobSF is designed to make your CI/CD or DevSecOps pipeline integration seamless. It has a graphic UI in the form of a web service. Web service consists of a dashboard that presents the results of the analysis, its own documentation site, an integrated emulator & an API that allows users to trigger the analysis automatically. It is hosted in a local environment, so sensitive data never interacts with the cloud.

Static Analysis

In static analysis, the application is tested from the inside out. It analyzes the source code or binary without executing the application. It does not rely on a runtime environment. It can be used to test code during development and catch vulnerabilities early on. Static analysis security testing tools must be run on the application on a regular basis, such as during daily/monthly builds, every time code is checked in, or during a code release.

Features

The following are the features of the MobSF:

- False Positive Triaging / Suppression Triaging Support for critical Android and iOS Security Analysis features.
- Android Binary & Source - Supports Code Analysis and Manifest Analysis
- iOS Binary - Supports Binary Code Analysis
- iOS Source - Supports Code Analysis
- New REST APIs for Suppression Support
- Android Certificate Analysis improvements
- Remove RELRO check from android binary analysis due to false positives
- iOS Bundle ID extraction improvements
- Feature parity - Allow IPA downloads from reports view
- Code QA: Reduce False positives in identified secrets

- Check for updates from GitHub releases
- M1 Mac support
- Disabled by default feature to support hotspots in AppSec Scorecard
- Dependency updates
- Added CodeQL scan on MobSF python code base
- Bug Fixes
- Fixes #1999, #1917, #2042 #1981 #2014 #2043
- Fixed a bug in JSON response REST API
- iOS URL view fix
- Code fixes to address minor security issues in third-party libraries.
- Handle JADX timeouts

Installation

We can install MOBSF using apt-get by running the following command:

```
sudo apt install python3 python3-pip python3-venv -y
```

```
(kali@kali)-[~]
$ sudo apt install python3 python3-pip python3-venv -y
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3-pip is already the newest version (22.2+dfsg-1).
python3-pip set to manually installed.
The following additional packages will be installed:
  libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev libc6-i386
  libpython3-dev libpython3-stdlib libpython3.10 libpython3.10-dev
  libpython3.10-minimal libpython3.10-stdlib locales python3-dev
  python3-distutils python3-lib2to3 python3-minimal python3-tk python3.10
  python3.10-dev python3.10-minimal python3.10-venv
Suggested packages:
  glibc-doc libnss-nis libnss-nisplus python3-doc tix python3-tk-dbg
  python3.10-doc
The following NEW packages will be installed:
  python3-venv python3.10-venv
The following packages will be upgraded:
  libc-bin libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev libc6-i386
  libpython3-dev libpython3-stdlib libpython3.10 libpython3.10-dev
  libpython3.10-minimal libpython3.10-stdlib locales python3 python3-dev
  python3-distutils python3-lib2to3 python3-minimal python3-tk python3.10
  python3.10-dev python3.10-minimal
23 upgraded, 2 newly installed, 0 to remove and 1031 not upgraded.
```

cd Desktop

git clone <https://github.com/MobSF/Mobile-Security-Framework-MobSF.git>

cd Mobile-Security-Framework-MobSF

ls

```
(kali@kali)-[~]
$ cd Desktop

(kali@kali)-[/Desktop]
$ git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF.git
Cloning into 'Mobile-Security-Framework-MobSF'...
remote: Enumerating objects: 18596, done.
remote: Counting objects: 100% (173/173), done.
remote: Compressing objects: 100% (132/132), done.
Receiving objects: 100% (18596/18596), 1.18 GiB | 10.55 MiB/s, done.
remote: Total 18596 (delta 79), reused 101 (delta 38), pack-reused 18423
Resolving deltas: 100% (9218/9218), done.
Updating files: 100% (402/402), done.

(kali@kali)-[~/Desktop]
$ cd Mobile-Security-Framework-MobSF

(kali@kali)-[~/Desktop/Mobile-Security-Framework-MobSF]
$ ls
docker-compose.yml  manage.py  requirements.txt  setup.bat
Dockerfile          MANIFEST.in  run.bat          setup.py
LICENSE             mobsf       run.sh          setup.sh
LICENSES            README.md   scripts         tox.ini

(kali@kali)-[~/Desktop/Mobile-Security-Framework-MobSF]
```

```
sudo ./setup.sh
```

```
(kali@kali)-[~/Desktop]
$ cd Mobile-Security-Framework-MobSF

(kali@kali)-[~/Desktop/Mobile-Security-Framework-MobSF]
$ ls
docker-compose.yml  manage.py  requirements.txt  setup.bat
Dockerfile          MANIFEST.in  run.bat          setup.py
LICENSE             mobsf       run.sh           setup.sh
LICENSES            README.md   scripts          tox.ini

(kali@kali)-[~/Desktop/Mobile-Security-Framework-MobSF]
$ sudo ./setup.sh
[INSTALL] Found Python 3.10.7
pip 22.2 from /usr/lib/python3/dist-packages/pip (python3.10)
[INSTALL] Found pip
Requirement already satisfied: pip in /usr/lib/python3/dist-packages (22.2)
Collecting pip
  Downloading pip-22.3-py3-none-any.whl (2.1 MB)
    2.1/2.1 MB 6.2 MB/s eta 0:00:00
Installing collected packages: pip
  WARNING: The scripts pip, pip3 and pip3.10 are installed in '/root/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed pip-22.3
WARNING: Running pip as the 'root' user can result in broken permissions and
```

Usage

To check or scan the “localhost:8000” server and open the MobSF tool we can execute the following command:

ls

sudo ./run.sh 127.0.0.1:8000

```
Download and Install wkhtmltopdf for PDF Report Generation - https://wkhtmltopdf.org/downloads.html
[INSTALL] Installation Complete

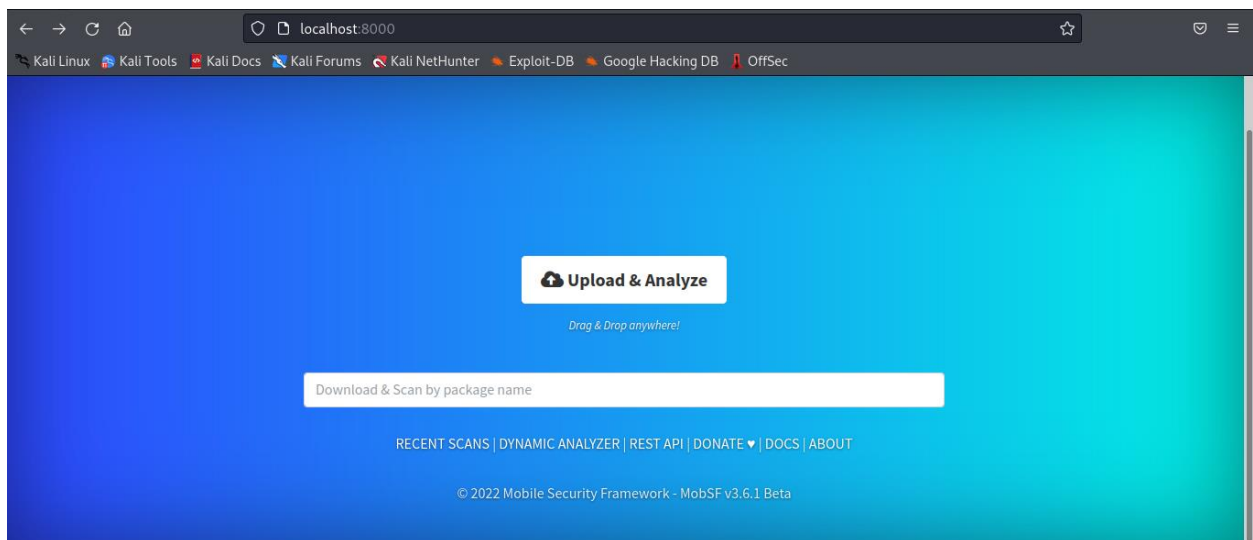
(kali@kali)-[~/Desktop/Mobile-Security-Framework-MobSF]
└─$ ls
Dockerfile      manage.py      requirements.txt  setup.bat  venv
LICENSE         MANIFEST.in   run.bat          setup.py
LICENSES        mobsf         run.sh           setup.sh
README.md       scripts       tox.ini

(kali@kali)-[~/Desktop/Mobile-Security-Framework-MobSF]
└─$ sudo ./run.sh 127.0.0.1:8000
[2022-10-20 07:55:15 -0400] [27891] [INFO] Starting unicorn 20.1.0
[2022-10-20 07:55:15 -0400] [27891] [INFO] Listening at: http://127.0.0.1:8000
[2022-10-20 07:55:15 -0400] [27891] [INFO] Using worker: gthread
[2022-10-20 07:55:15 -0400] [27892] [INFO] Booting worker with pid: 27892
[INFO] 20/Oct/2022 11:57:11 - Trackers Detection 5/428

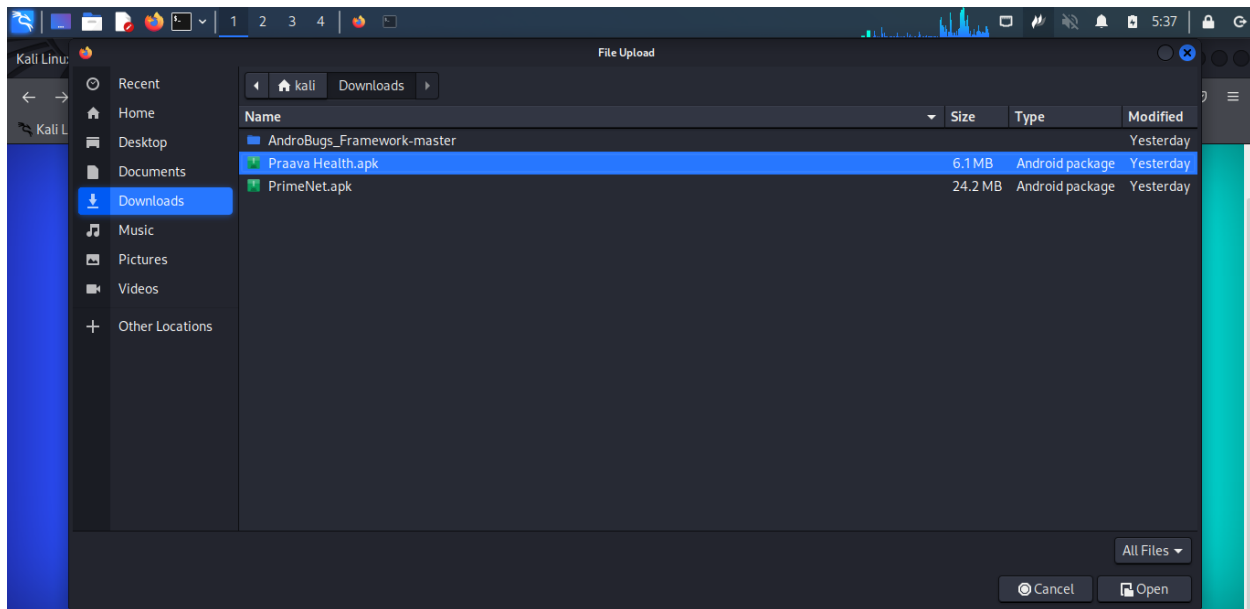
[INFO] 20/Oct/2022 11:57:11 - Mobile Security Framework v3.6.1 Beta
REST API Key: 395b1b9542f383ccc7338f2074c190e87284ebe28f6ad72d8538c7a8be84ea5
```

Write this in the browser URL in kali linux:

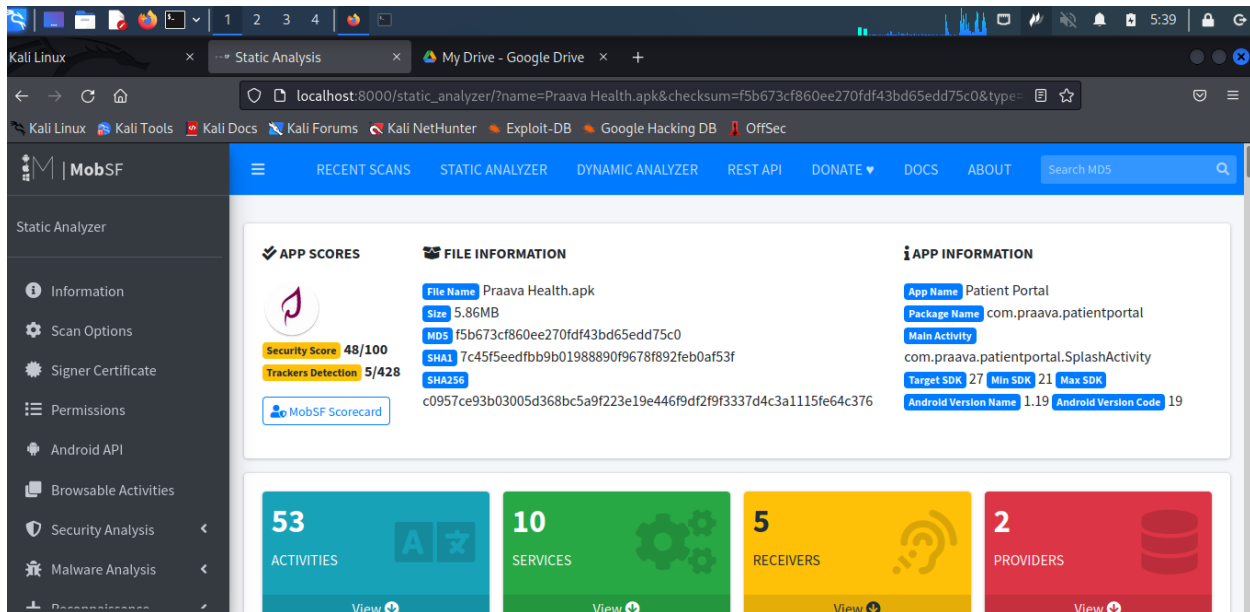
<http://localhost:8000/>



Upload your APK file:



Here is the Static Analysis:



The “Praava Health.apk” PDF report link is given below:

Drive link: <https://drive.google.com/drive/folders/1h37dhMVCHMxbC41jcKY0qXOe9OfTn7wO>

References

1. <https://mobsf.github.io/docs/#/>
2. <https://medium.com/@kshitishirke/mobile-security-framework-mobsf-static-analysis-df22fcdae46e>
3. <https://mobsf.github.io/Mobile-Security-Framework-MobSF/changelog.html>