MobSF Tool

Aakash R

CB.SC.P2CYS23011

Installing Mobsf Tool in Kali Linux VM

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

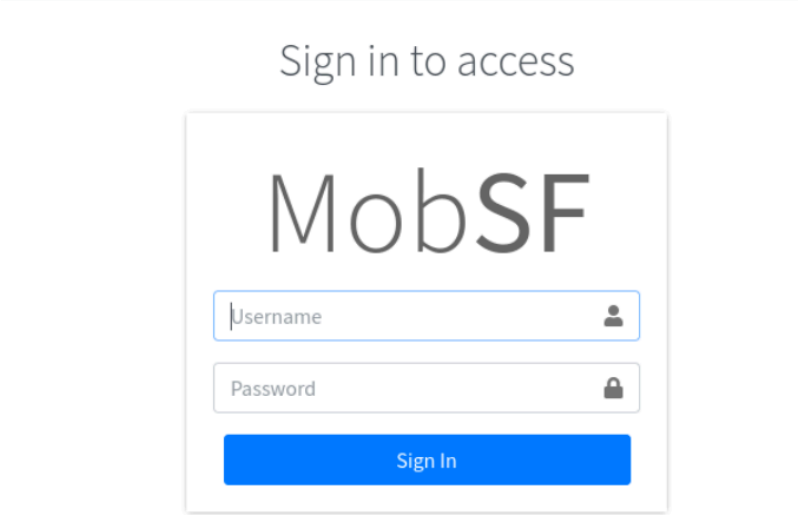
```
└─$ git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF.git
Cloning into 'Mobile-Security-Framework-MobSF' ...
remote: Enumerating objects: 20756, done.
remote: Counting objects: 100% (281/281), done.
remote: Compressing objects: 100% (187/187), done.
Receiving objects:  11% (2307/20756), 14.40 MiB | 1.13 MiB/s
```

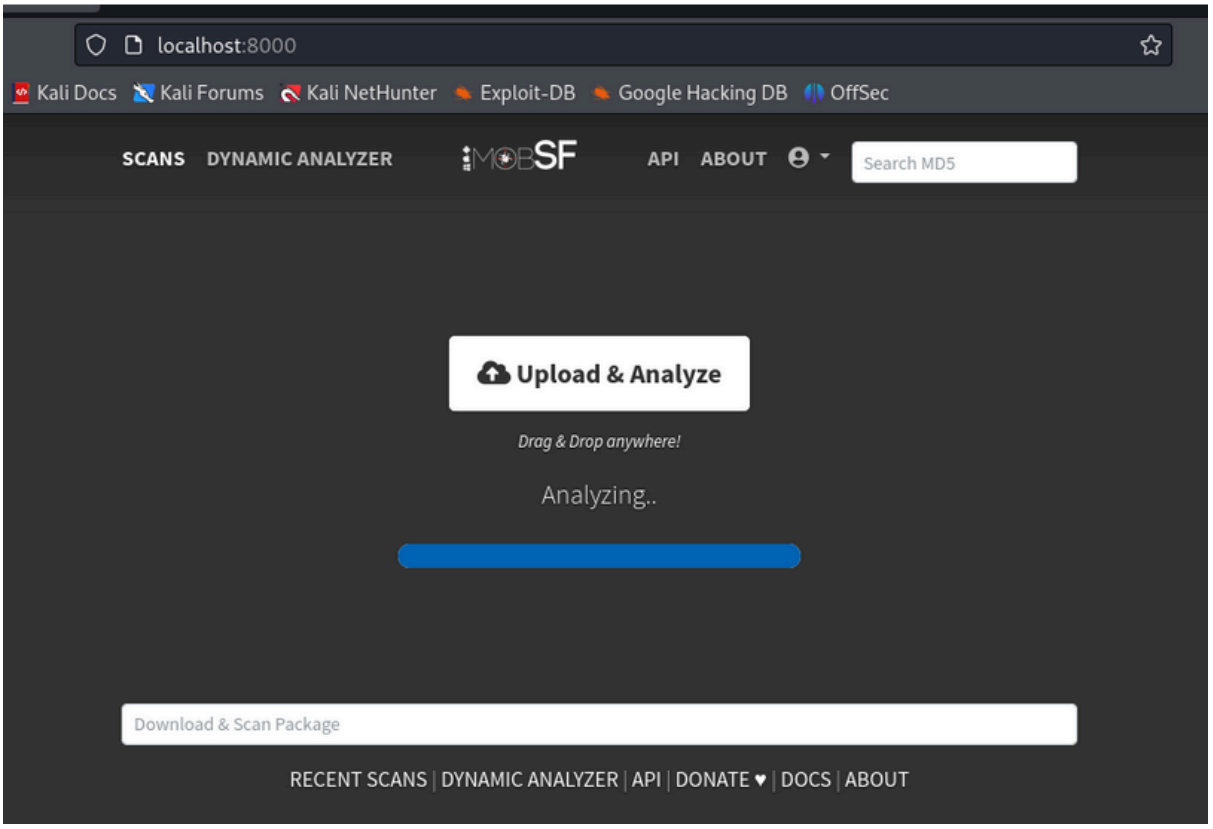
Setting Up MobSF Tool

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cd Mobile-Security-Framework-MobSF-master

┌──(kali㉿kali)-[~/Downloads/Mobile-Security-Framework-MobSF-master]
└─$ ls
docker-compose.yml  LICENSES    poetry.lock     run.bat   setup.bat
Dockerfile          manage.py   pyproject.toml  run.sh    setup.sh
LICENSE             mobsf       README.md       scripts   tox.ini
```

```
└─$ sudo ./setup.sh
[sudo] password for kali:
[INSTALL] Found Python 3.11.9
pip 24.0 from /usr/lib/python3/dist-packages/pip (python 3.11)
[INSTALL] Found pip
Requirement already satisfied: pip in /usr/lib/python3/dist-packages (24.0)
WARNING: Running pip as the 'root' user can result in broken permissions and conflic
our with the system package manager. It is recommended to use a virtual environment
tps://pip.pypa.io/warnings/venv
[INSTALL] Installing Requirements
Requirement already satisfied: wheel in /usr/lib/python3/dist-packages (0.42.0)
Collecting poetry==1.6.1
  Downloading poetry-1.6.1-py3-none-any.whl.metadata (6.8 kB)
Collecting build<0.11.0,≥0.10.0 (from poetry==1.6.1)
  Downloading build-0.10.0-py3-none-any.whl.metadata (4.1 kB)
```

```
┌──(kali㉿kali)-[~/Downloads/Mobile-Security-Framework-MobSF-master]
└─$ . ./venv/bin/activate

┌──(venv)─(kali㉿kali)-[~/Downloads/Mobile-Security-Framework-MobSF-master]
└─$ bash run.sh
[2024-06-03 06:05:19 -0400] [3323] [INFO] Starting gunicorn 22.0.0
[2024-06-03 06:05:19 -0400] [3323] [INFO] Listening at: http://[::]:8000 (3323)
[2024-06-03 06:05:19 -0400] [3323] [INFO] Using worker: gthread
[2024-06-03 06:05:19 -0400] [3374] [INFO] Booting worker with pid: 3374
```

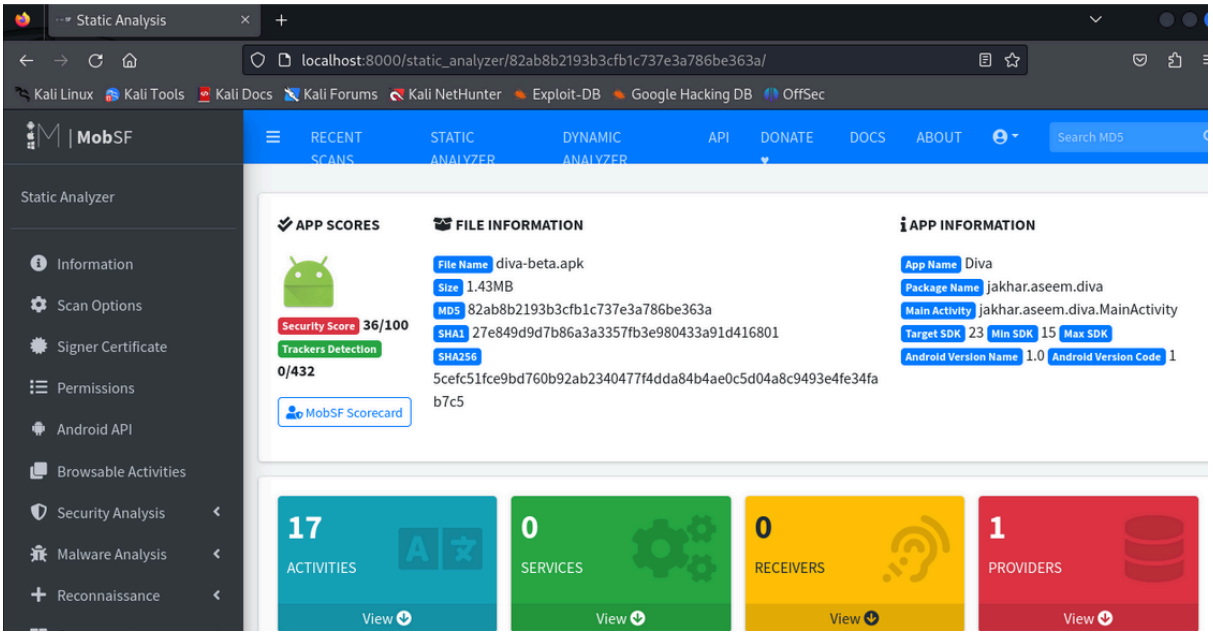

Sign in to access
MobSF
Username
Password
Sign In


localhost:8000
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
SCANS
DYNAMIC ANALYZER
MOBSF
API
ABOUT
Search MD5
Upload & Analyze
Drag & Drop anywhere!
Analyzing..
Download & Scan Package
RECENT SCANS | DYNAMIC ANALYZER | API | DONATE ♥ | DOCS | ABOUT

```
[INFO] 03/Jun/2024 10:06:52 - Author: Ajin Abraham | opensecurity.in
[INFO] 03/Jun/2024 10:06:52 - Mobile Security Framework v4.0.3
REST API Key: bdb9923c8be542799c4a18beaf8032aa86c1709fdb7eb55685f1f5d49e64dc8e
Default Credentials: mobsf/mobsf
[INFO] 03/Jun/2024 10:06:52 - OS Environment: Linux (kali 2024.1 kali-rolling) Linux-6.6.9-amd6
4-x86_64-with-glibc2.37
[INFO] 03/Jun/2024 10:06:52 - MobSF Basic Environment Check
[WARNING] 03/Jun/2024 10:06:52 - Dynamic Analysis related functions will not work.
Make sure a Genymotion Android VM/Android Studio Emulator is running before performing Dynamic
```

Static Analysis:

Code Analysis: Scans the application's code for security vulnerabilities, including insecure API usage, hardcoded secrets, and configuration issues.



List of Activities:

ACTIVITIES

▼ Showing all **17** activities

jakhar.aseem.diva.MainActivity
jakhar.aseem.diva.LogActivity
jakhar.aseem.diva.HardcodeActivity
jakhar.aseem.diva.InsecureDataStorage1Activity
jakhar.aseem.diva.InsecureDataStorage2Activity
jakhar.aseem.diva.InsecureDataStorage3Activity
jakhar.aseem.diva.InsecureDataStorage4Activity
jakhar.aseem.diva.SQLInjectionActivity
jakhar.aseem.diva.InputValidation2URISchemeActivity
jakhar.aseem.diva.AccessControl1Activity
jakhar.aseem.diva.APICredsActivity
jakhar.aseem.diva.AccessControl2Activity
jakhar.aseem.diva.APICreds2Activity
jakhar.aseem.diva.AccessControl3Activity
jakhar.aseem.diva.Hardcode2Activity
jakhar.aseem.diva.AccessControl3NotesActivity
jakhar.aseem.diva.InputValidation3Activity

Recent Scans

Recent Scans

APP	FILE	TYPE	HASH
Diva - 1.0 jakhar.aseem.diva MobSF Scorecard Static Report Dynamic Report	diva-beta.apk		82ab8b2193b3cfb1c737e3a786be363a

Previous 1 Next Items per page

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.	Show Files
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.	Show Files

Showing 1 to 3 of 3 entries

Binary Analysis: Decompiles and disassembles the application binary to identify potential security issues in the compiled code.

SHARED LIBRARY BINARY ANALYSIS

Search:

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY
1	mips/libdivajni.so Analyze	**False** high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities	**False** high This binary does not have a stack canary value added to the stack. Stack canaries	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option

Manifest Analysis (Android): Analyzes the Android manifest file for permissions, activities, services, and other components to identify potential security misconfigurations.

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
2	4	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable upatched Android version Android 4.0.3-4.0.4, [minSdk=15]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.	

Overall Analysis: