Rhombixtechnologies_tasks2

# *Mobile Application Security Assessment*

*Name:  Qamash Bashir*

*Domain:Cyber Security*

*Month 2*

# *Mobile Security Framework

It’s a free, open-source tool that works for both **Android** and **iOS** apps. Whether you’re building apps from scratch or reviewing ones already out in the wild, MobSF is your go-to for finding and fixing security weaknesses. It handles two main types of analysis:

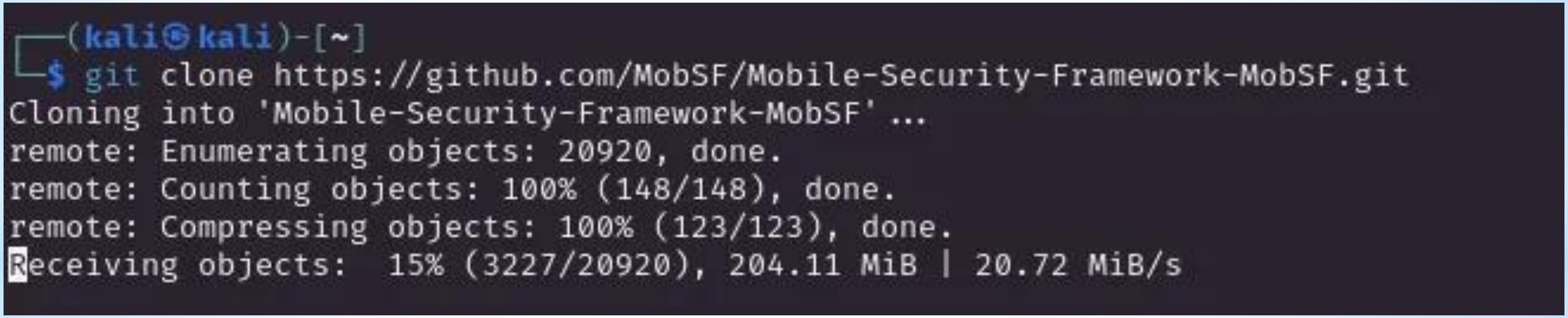
- **Static analysis** (looking at the app’s code and structure without running it)
- **Dynamic analysis** (checking how the app behaves while it’s running)

# Setting Up MobSF

Now that you know what MobSF can do, let's walk through how to set it up.

### ❖Step 1: Cloning the MobSF Repository

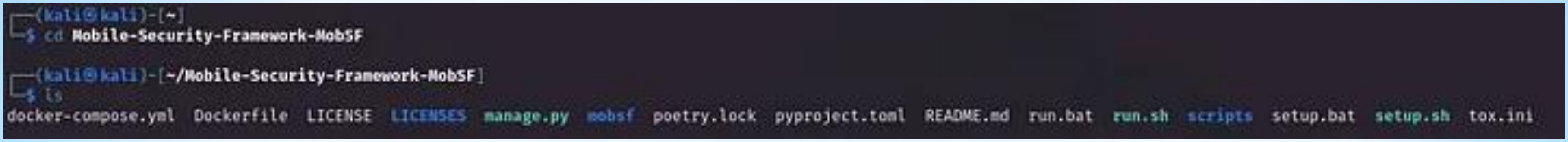
git clone [https://github.com/MobSF/Mobile- Security-Framework-MobSF.git](https://github.com/MobSF/Mobile-Security-Framework-MobSF.git)



```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF.git
Cloning into 'Mobile-Security-Framework-MobSF'...
remote: Enumerating objects: 20920, done.
remote: Counting objects: 100% (148/148), done.
remote: Compressing objects: 100% (123/123), done.
Receiving objects:  15% (3227/20920), 204.11 MiB | 20.72 MiB/s
```

### ❖Step 2: Running the Setup Script

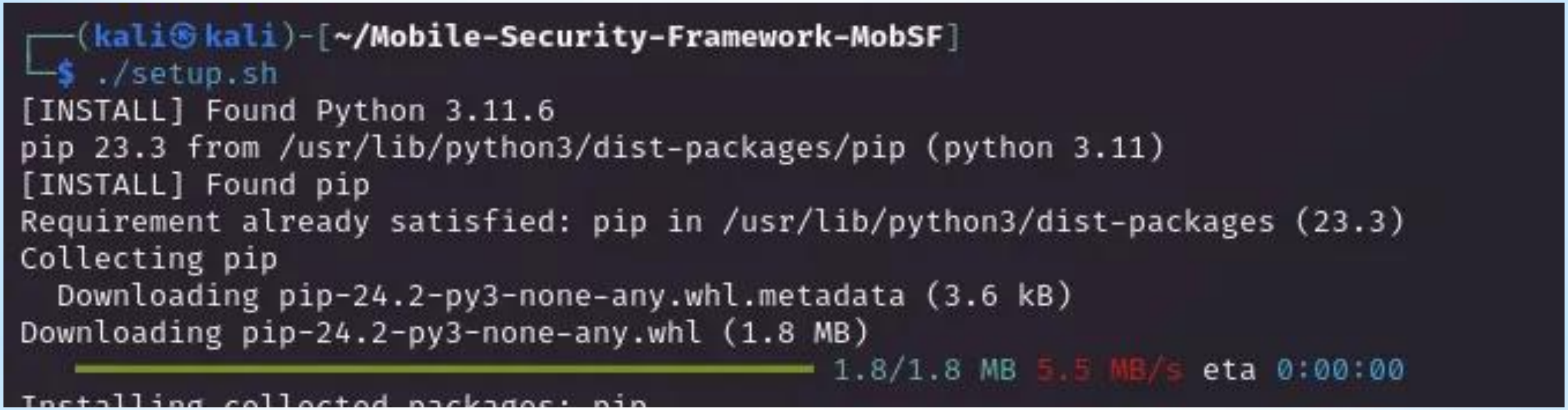
cd Mobile-Security-Framework-MobSF



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

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

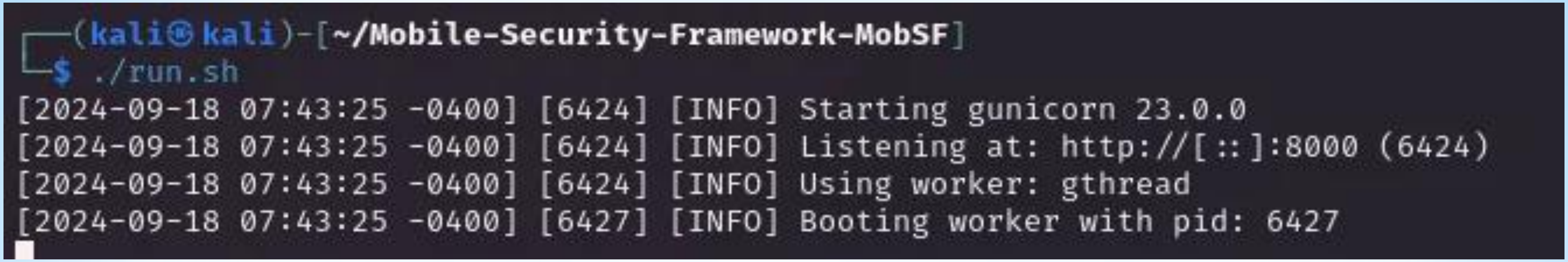
- **For Kali Linux:** Run the setup.sh script.



```
┌──(kali㉿kali)-[~/Mobile-Security-Framework-MobSF]
└─$ ./setup.sh
[INSTALL] Found Python 3.11.6
pip 23.3 from /usr/lib/python3/dist-packages/pip (python 3.11)
[INSTALL] Found pip
Requirement already satisfied: pip in /usr/lib/python3/dist-packages (23.3)
Collecting pip
  Downloading pip-24.2-py3-none-any.whl.metadata (3.6 kB)
Downloading pip-24.2-py3-none-any.whl (1.8 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.8/1.8 MB 5.5 MB/s eta 0:00:00
Installing collected packages: pip
```

## Step 3: Running MobSF

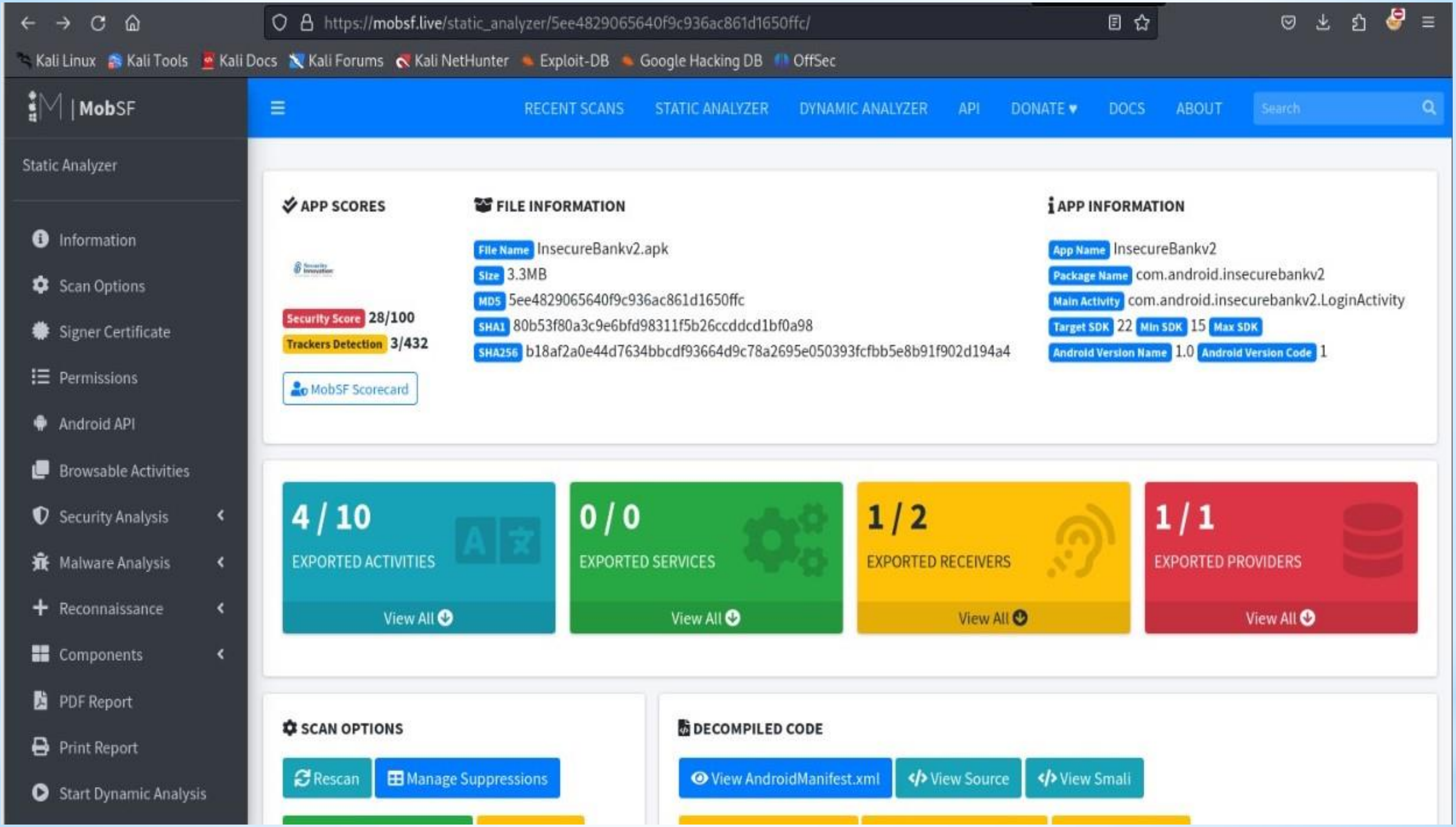
- Once the setup is complete, you can start MobSF.



```
┌──(kali㉿kali)-[~/Mobile-Security-Framework-MobSF]
└─$ ./run.sh
[2024-09-18 07:43:25 -0400] [6424] [INFO] Starting gunicorn 23.0.0
[2024-09-18 07:43:25 -0400] [6424] [INFO] Listening at: http://[::]:8000 (6424)
[2024-09-18 07:43:25 -0400] [6424] [INFO] Using worker: gthread
[2024-09-18 07:43:25 -0400] [6427] [INFO] Booting worker with pid: 6427
```

## Step 4: Logging In

- **Username:** mobsf
- **Password:** mobsf



**APP SCORES**

Security Score 28/100

Trackers Detection 3/432

**FILE INFORMATION**

File Name InsecureBankv2.apk
Size 3.3MB
MD5 5ee4829065640f9c936ac861d1650ffc
SHA1 80b53f80a3c9e6bfd98311f5b26ccddcd1bf0a98
SHA256 b18af2a0e44d7634bbcdf93664d9c78a2695e050393fcfbb5e8b91f902d194a4

**APP INFORMATION**

App Name InsecureBankv2
Package Name com.android.insecurebankv2
Main Activity com.android.insecurebankv2.LoginActivity
Target SDK 22 Min SDK 15 Max SDK
Android Version Name 1.0 Android Version Code 1

4 / 10 EXPORTED ACTIVITIES

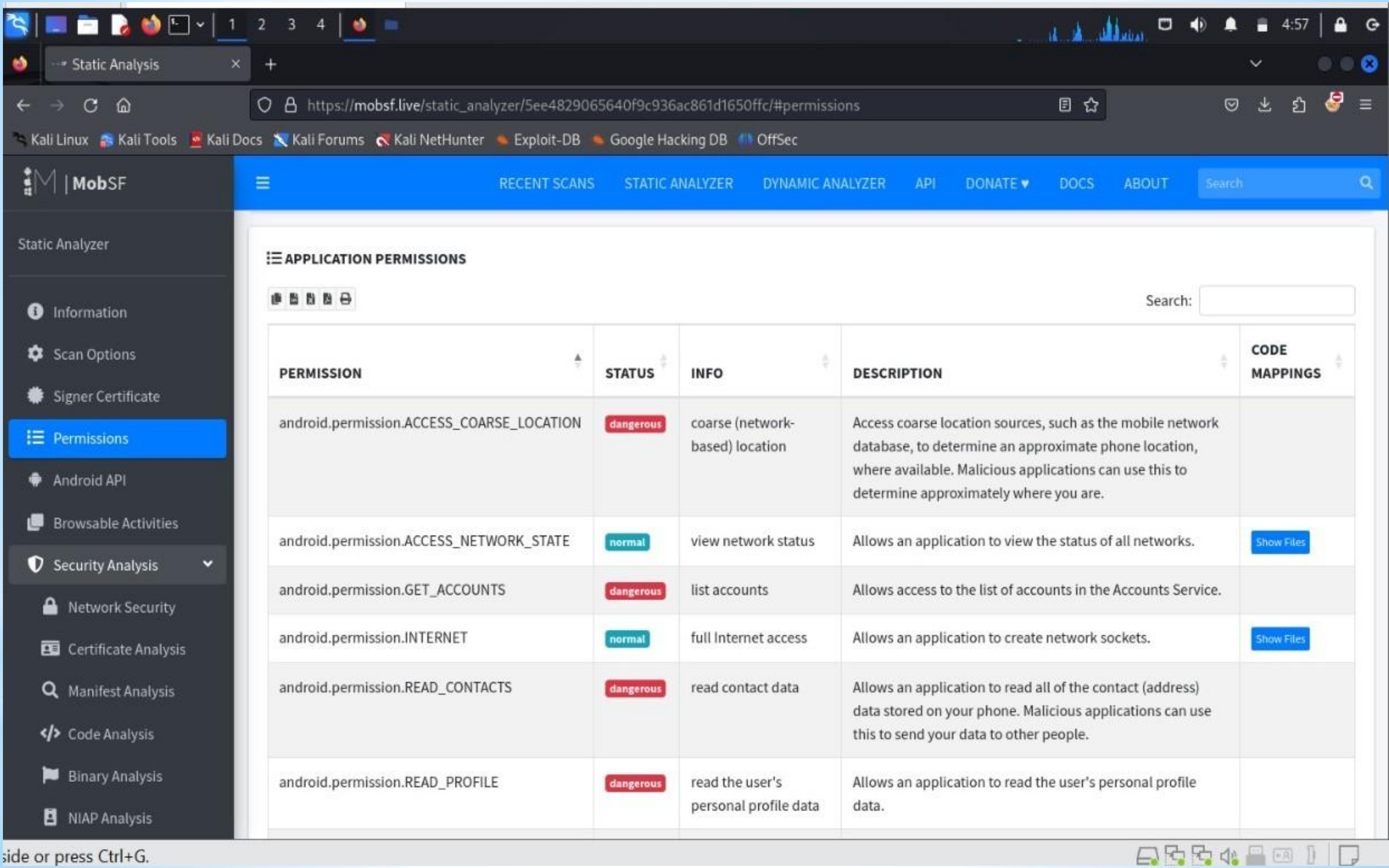
0 / 0 EXPORTED SERVICES

1 / 2 EXPORTED RECEIVERS

1 / 1 EXPORTED PROVIDERS

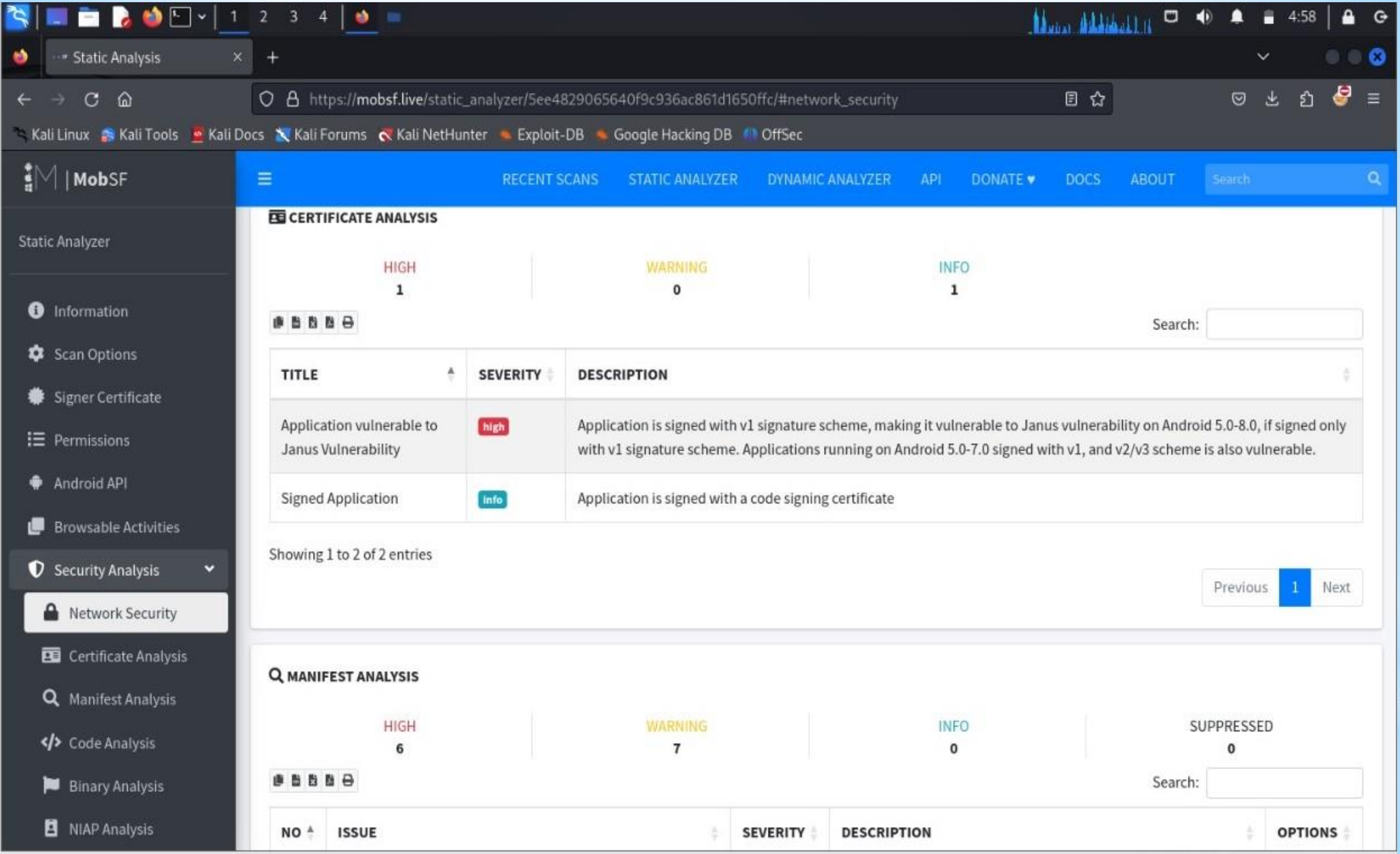
**SCAN OPTIONS**

**DECOMPILED CODE**



APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION | CODE MAPPINGS |
|---|---|---|---|---|
| android.permission.ACCESS_COARSE_LOCATION | dangerous | coarse (network-based) location | Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are. | |
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. | Show Files |
| android.permission.GET_ACCOUNTS | dangerous | list accounts | Allows access to the list of accounts in the Accounts Service. | |
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. | Show Files |
| android.permission.READ_CONTACTS | dangerous | read contact data | Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people. | |
| android.permission.READ_PROFILE | dangerous | read the user's personal profile data | Allows an application to read the user's personal profile data. | |



**CERTIFICATE ANALYSIS**

| HIGH | WARNING | INFO |
|---|---|---|
| 1 | 0 | 1 |

Search:

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| Application vulnerable to Janus Vulnerability | high | Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable. |
| Signed Application | info | Application is signed with a code signing certificate |

Showing 1 to 2 of 2 entries

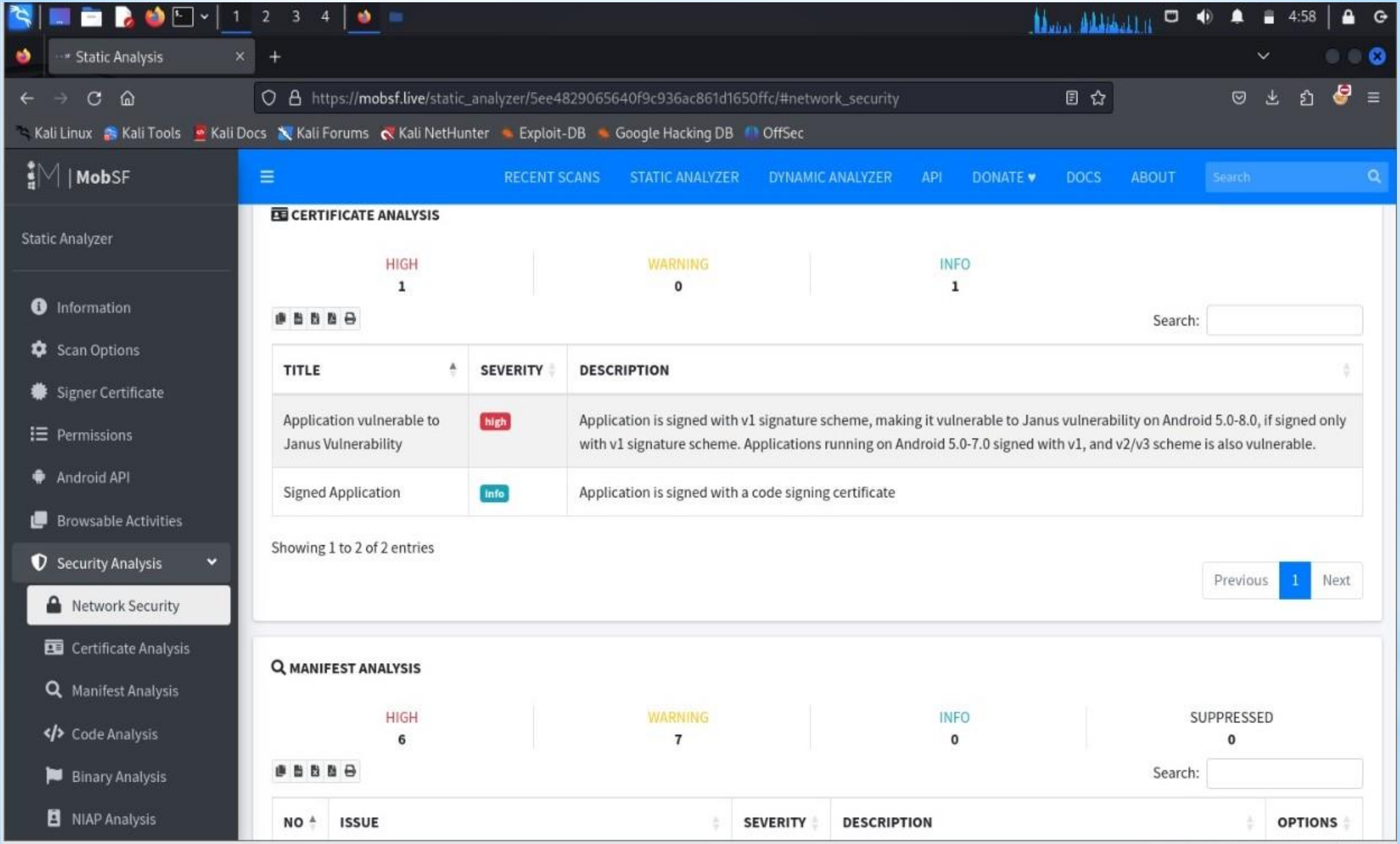
Previous 1 Next

**MANIFEST ANALYSIS**

| HIGH | WARNING | INFO | SUPPRESSED |
|---|---|---|---|
| 6 | 7 | 0 | 0 |

Search:

| NO | ISSUE | SEVERITY | DESCRIPTION | OPTIONS |
|---|---|---|---|---|



**CERTIFICATE ANALYSIS**

| HIGH | WARNING | INFO |
|---|---|---|
| 1 | 0 | 1 |

Search:

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| Application vulnerable to Janus Vulnerability | high | Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable. |
| Signed Application | info | Application is signed with a code signing certificate |

Showing 1 to 2 of 2 entries

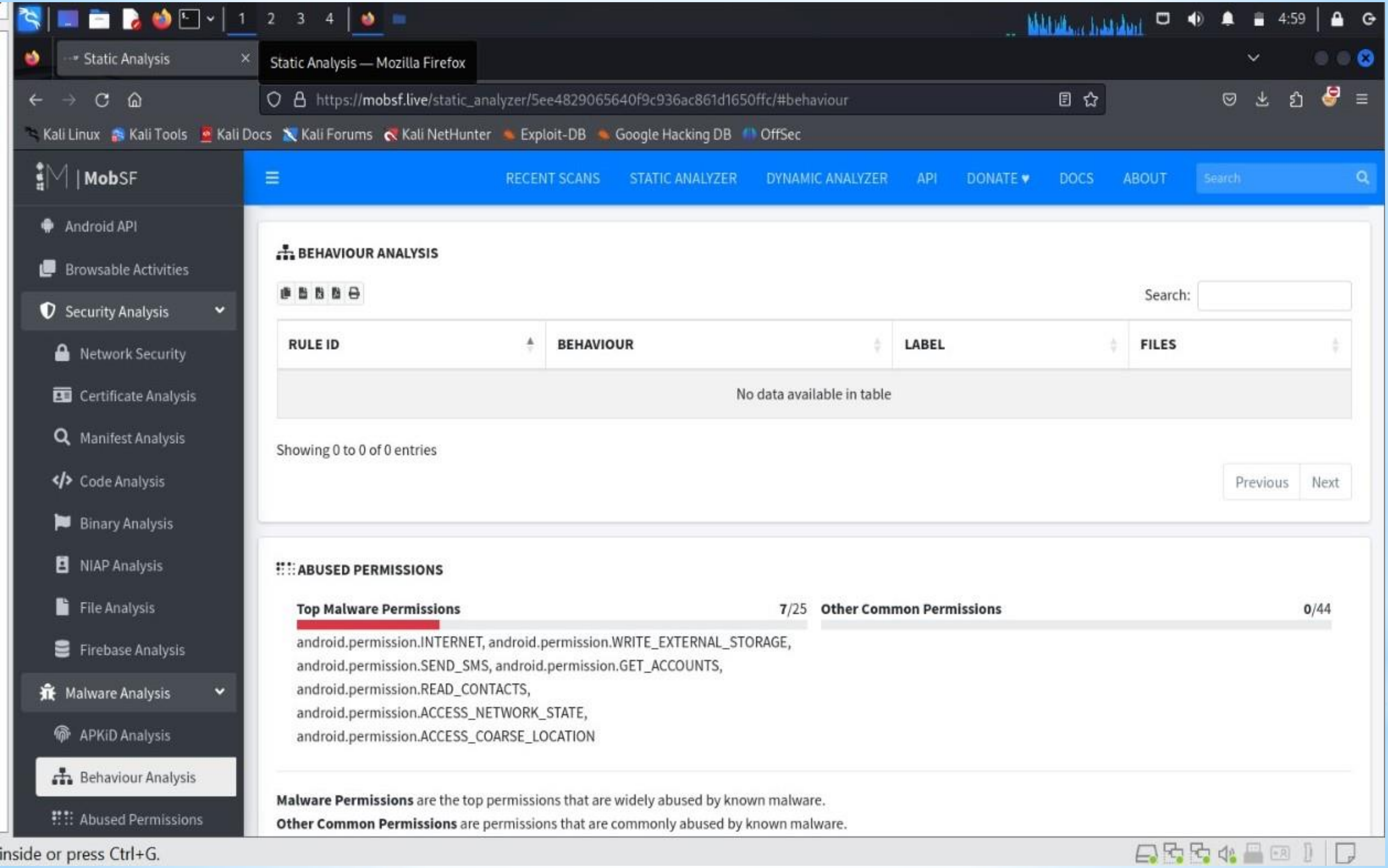
Previous 1 Next

**MANIFEST ANALYSIS**

| HIGH | WARNING | INFO | SUPPRESSED |
|---|---|---|---|
| 6 | 7 | 0 | 0 |

Search:

| NO | ISSUE | SEVERITY | DESCRIPTION | OPTIONS |
|---|---|---|---|---|



### BEHAVIOUR ANALYSIS

Search:

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| No data available in table | | | |

Showing 0 to 0 of 0 entries

Previous Next

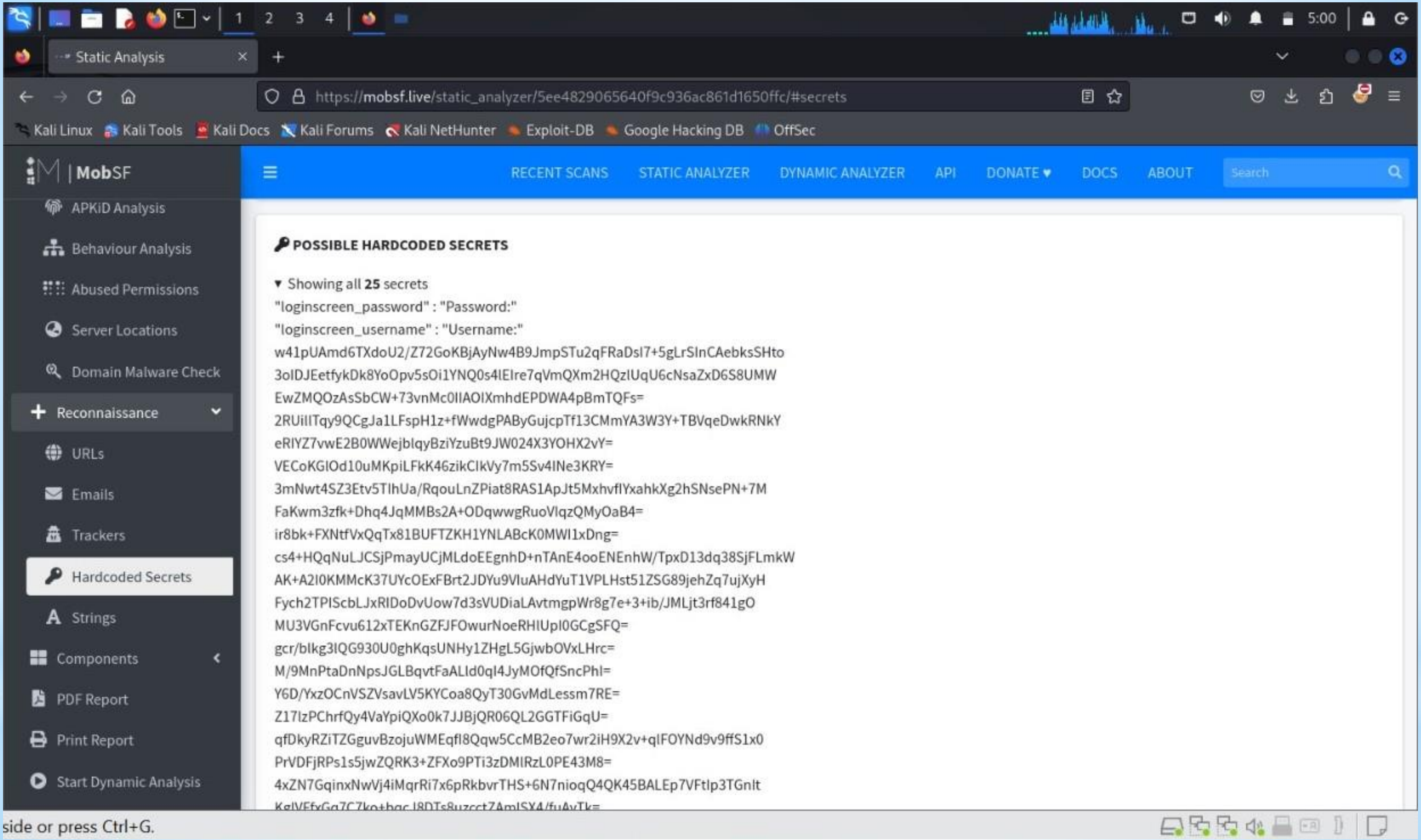
### ABUSED PERMISSIONS

**Top Malware Permissions** 7/25

android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.SEND_SMS, android.permission.GET_ACCOUNTS, android.permission.READ_CONTACTS, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION

**Other Common Permissions** 0/44

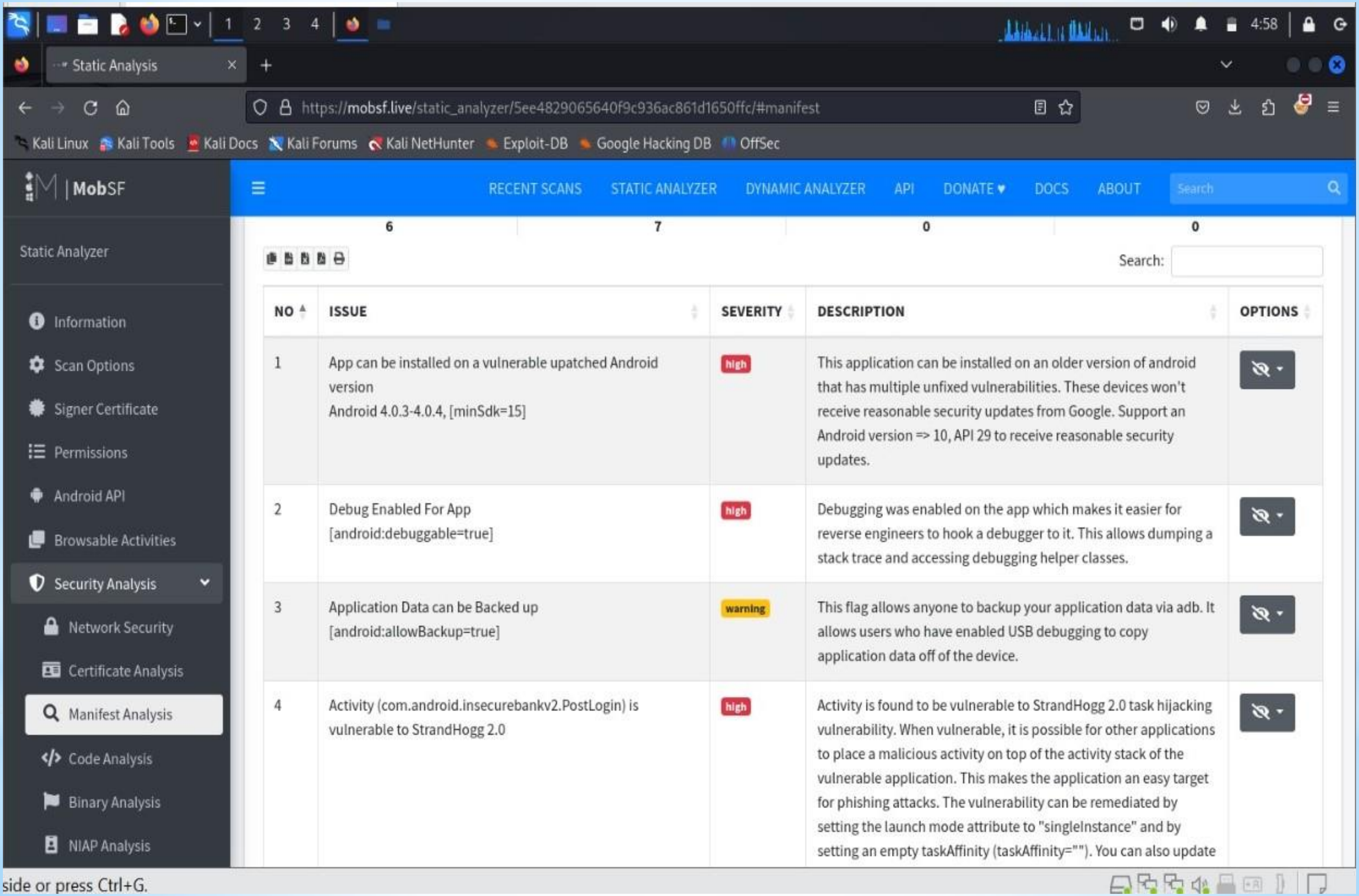
**Malware Permissions** are the top permissions that are widely abused by known malware.
**Other Common Permissions** are permissions that are commonly abused by known malware.



POSSIBLE HARDCODED SECRETS

▾ Showing all **25** secrets

```
"loginscreen_password" : "Password:"
"loginscreen_username" : "Username:"
w41pUAmd6TXdoU2/Z72GoKBjAyNw4B9JmpSTu2qFRaDsl7+5gLrSlnCAebksSHto
3olDJEetfykDk8YoOpv5sOi1YNQ0s4lElre7qVmQXm2HQzlUqU6cNsaZxD6S8UMW
EwZMQOzAsSbCW+73vnMc0IIAOIXmhdEPDWA4pBmTQFs=
2RUilITqy9QCgJa1LFspH1z+fWwdgPAByGujcpTf13CMmYA3W3Y+TBVqeDwkRNkY
eRIYZ7vwE2B0WWejblqyBziYzuBt9JW024X3YOHX2vY=
VECoKGlOd10uMKpiLFkK46zikClkVy7m5Sv4INe3KRY=
3mNwt4SZ3Etv5TlhUa/RqouLnZPiat8RAS1ApJt5MxhvflYxahkXg2hSNsePN+7M
FaKwm3zfk+Dhq4JqMMBs2A+ODqwwgRuoVlqzQMyOaB4=
ir8bk+FXNtfVxQqTx81BUFTZKH1YNLABcK0MWI1xDng=
cs4+HQqNuLJCSjPmayUCjMLdoEEgnhD+nTAnE4ooENEnhW/TpxD13dq38SjFLmkW
AK+A2I0KMMcK37UYcOExFBrt2JDYu9VluAHdYuT1VPLHst51ZSG89jehZq7ujXyH
Fych2TPIScbLJxRIDoDvUow7d3sVUDiaLAvtmgpWr8g7e+3+ib/JMLjt3rf841gO
MU3VGnFcvu612xTEKnGZFJFOwurNoeRHIUpl0GCgSFQ=
gcr/blkg3IQG930U0ghKqsUNHy1ZHgL5GjwbOVxLHrc=
M/9MnPtaDnNpsJGLBqvtFaALId0ql4JyMOfQfSncPhl=
Y6D/YxzOCnVSZVsavLV5KYCoa8QyT30GvMdLessm7RE=
Z17lzPChrfQy4VaYpiQXo0k7JJBjQR06QL2GGTFiGqU=
qfDkyRZiTZGguvBzojuWMEqfl8Qqw5CcMB2eo7wr2iH9X2v+qIFOYNd9v9ffS1x0
PrVDFjRPs1s5jwZQRK3+ZFXo9PTi3zDMIRzL0PE43M8=
4xZN7GqinxNwVj4iMqrRi7x6pRkbvrTHS+6N7nioqQ4QK45BALEp7VFtlp3TGnlt
KglVEfxGq7C7ko+bqcJ8DTs8uzcct7AmISX4/fuAvTk=
```



| NO | ISSUE | SEVERITY | DESCRIPTION | OPTIONS |
|---|---|---|---|---|
| 1 | App can be installed on a vulnerable upatched Android version<br>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. | |
| 2 | Debug Enabled For App<br>[android:debuggable=true] | high | Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes. | |
| 3 | Application Data can be Backed up<br>[android:allowBackup=true] | warning | This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device. | |
| 4 | Activity (com.android.insecurebankv2.PostLogin) is vulnerable to StrandHogg 2.0 | high | Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update | |

Thank you