|  |
| --- |
| OFFENSIVE APPROACH TO MOBILE APPLICATION SECURITY  Insecure Data Storage |

|  |  |  |
| --- | --- | --- |
| İrem Çelik |  |  |
|  |  |  |

Contents

[Why Android? 3](#_Toc52549170)

[Background of Android Devices 3](#_Toc52549171)

[APK (Android Application Package File) 4](#_Toc52549172)

[Android Local Data Storage 6](#_Toc52549173)

[Android Security Model 7](#_Toc52549174)

[Android Mobile Pentest Tools 9](#_Toc52549175)

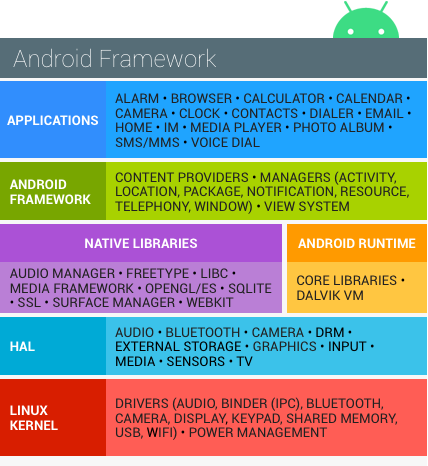
[Mobile Pentest Application 12](#_Toc52549176)

[Resources 17](#_Toc52549177)

## Why Android?

* Open source
* Based on linux
* Widespread use
* Advanced and free software development environment

## Background of Android Devices



Android provides an open source platform and app environment for mobile devices.

With the exception of a small amount of Android OS code running as root, all code above the Linux kernel is restricted by the Application Sandbox.

HAL: Hardware abstraction Layer

## APK (Android Application Package File)

Android packages contain all the necessary files for a single Android program. Below is a list of the most prominent files and folders:

**META-INF/:** Contains the manifest file, signature, and a list of resources in the archive.

**lib/:** Native libraries that run on specific device architectures.

**res/:** Resources, such as images, that were not compiled into **resources.arsc**

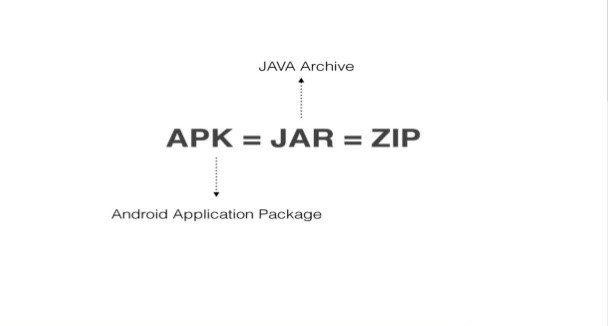
**assets/:** Raw resource files that developers bundle with the app.

**AndroidManifest.xml**: Describes the name, version, and contents of the APK file.

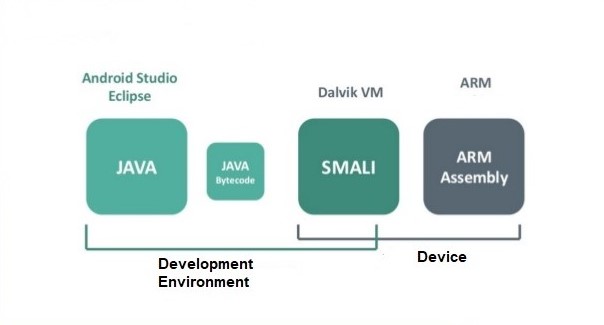
**classes.dex**: The compiled [Java](https://techterms.com/definition/java) classes to be run on the device ([.DEX](https://fileinfo.com/extension/dex) file). It is working on Dalvik VM.

**resources.arsc**: The compiled resources, such as strings, used by the app ([.ARSC](https://fileinfo.com/extension/arsc) file).

Android Application Package files are zip file format with .apk extension. After changing the extension of the APK file to .zip, the contents of the file can be viewed with archive programs such as WinZip, WinRAR.



#### Android Applications:



Smali: When you create an application code, the apk file contains a .dex file, which contains binary Dalvik bytecode. This is the format that the platform actually understands. However, it's not easy to read or modify binary code, so there are tools out there to convert to and from a human readable representation. The most common human readable format is known as Smali.

* Developed with Java + Android SDK (Software Development Kit).

Note:

The Android SDK (software development kit) is a set of development tools used to develop applications for Android platform. The Android SDK includes the following:

* Required libraries
* Debugger
* An emulator
* Relevant documentation for the Android application program interfaces (APIs)
* Sample source code
* Tutorials for the Android OS
* Runs with Android Dalvik VM.

Note:

Dalvik is a discontinued [process virtual machine](https://en.wikipedia.org/wiki/Process_virtual_machine) (VM) in [Android operating system](https://en.wikipedia.org/wiki/Android_(operating_system)) that executes applications written for Android.

## Android Local Data Storage

Android apps usually store data locally on these places:

* SQLite databases
* Shared preferences
* Internal storage
* External storage

#### #SQLite Databases

SQLite is an open source database with a lot of functionalities that are similar to other relational databases such as SQL. They usually have the extension “.db” or “.sqlite”. Android provides full support for SQLite databases. Databases we create in the application will be accessible to any class in the application. Other apps cannot access them.

The common location where databases are stored in Android apps is:

**/data/data/<package name>/databases/<databasename.db>**

#### #Shared Preferences

Shared Preferences are XML files to store private primitive data in key-value pairs. Data Types include Booleans, floats, ints, longs, and strings.They are stored in the app’s data folder under the shared\_prefs folder.

#### #Internal Storage

Internal storage is another way in which we can save files directly on the device. By default, files saved to internal storage are private to your application, and other applications cannot access them. When the user uninstalls your application, these files are removed.

#### #External Storage

External storage is a location that you can use to save files. This can be a removable storage media (such as an external SD card) or an internal (non-removable) storage. External SD cards are world readable. External storage is world readable and writable, any app with the WRITE\_EXTERNAL\_STORAGE and READ\_EXTERNAL\_STORAGE permissions.

## Android Security Model

* Based on Linux security model (UID / GUID).
* Application-based permissions are used.
* Application permissions are defined in the AndroidManifest.xml file.
* For application installation, the application must be signed with a certificate.
* Each application runs in a different DVM (Dalvik Virtual Machine).
* The user plays a key role in terms of system security.
* Root access is not possible for an unrooted device. "su" application is not included in the system.

#### #App Sandboxing

On Android each app does only have access to its own data. Each app belongs to a single user. Each application has an entry in /data/data/<package-name>. The folder are not readable and writable by an other user other than the owner of the app.

Only the root user have access to any part of the system. Once the device is rooted, an app with root permissions can access any data on the system.

#### #Rooting Android Devices

Android is built on Linux. In Linux they are different users but the super user is called root. This user can perform any operation on the Android device. The process is enabling the root on the device is called rooting. Once a device is rooted you will have full root access to the device.

#### #Check for root access

To check for root access, first open a shell on the device.

**$ adb shell**

Then, then run the su command, switch user.

**$ su**

If the device is rooted your prompt will change into a # symbol, if not you will get an error that the command is not found.

By default, the Android emulator is already rooted, it gives you root access to the device.

#### #Rooting an android device

Note:

**Unlocking boot loader**

By default, most devices come with their boot loaders locked. In order, root the device, the boot loader needs to be unlocked first. The process to unlock the boot loader is dependant on the device manufacturer. For example, the Google Nexus phones are the easiest to unlock since Google seems to lax the rules on rooting the device. Some devices like Sony and Huawei requires a vendor provided code to unlock the boot loader.

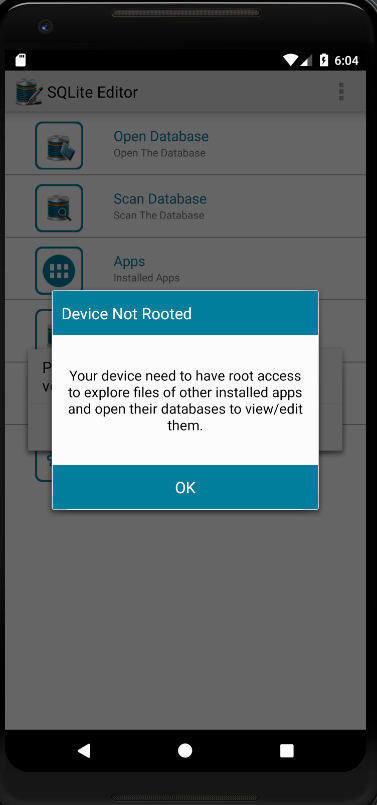
Rooting an Android devices requires a few steps:

* Unlocking the boot loader.
* Install recovery software like TWRP(Team Win Recovery Project).
* Install the Super Su app.

For more: https://guides.peruzal.com/mobile-device-security-and-penetration-testing-guide/rooting-android-devices/

Note:

There are some specific applications which run only on rooted devices such as SQLite.

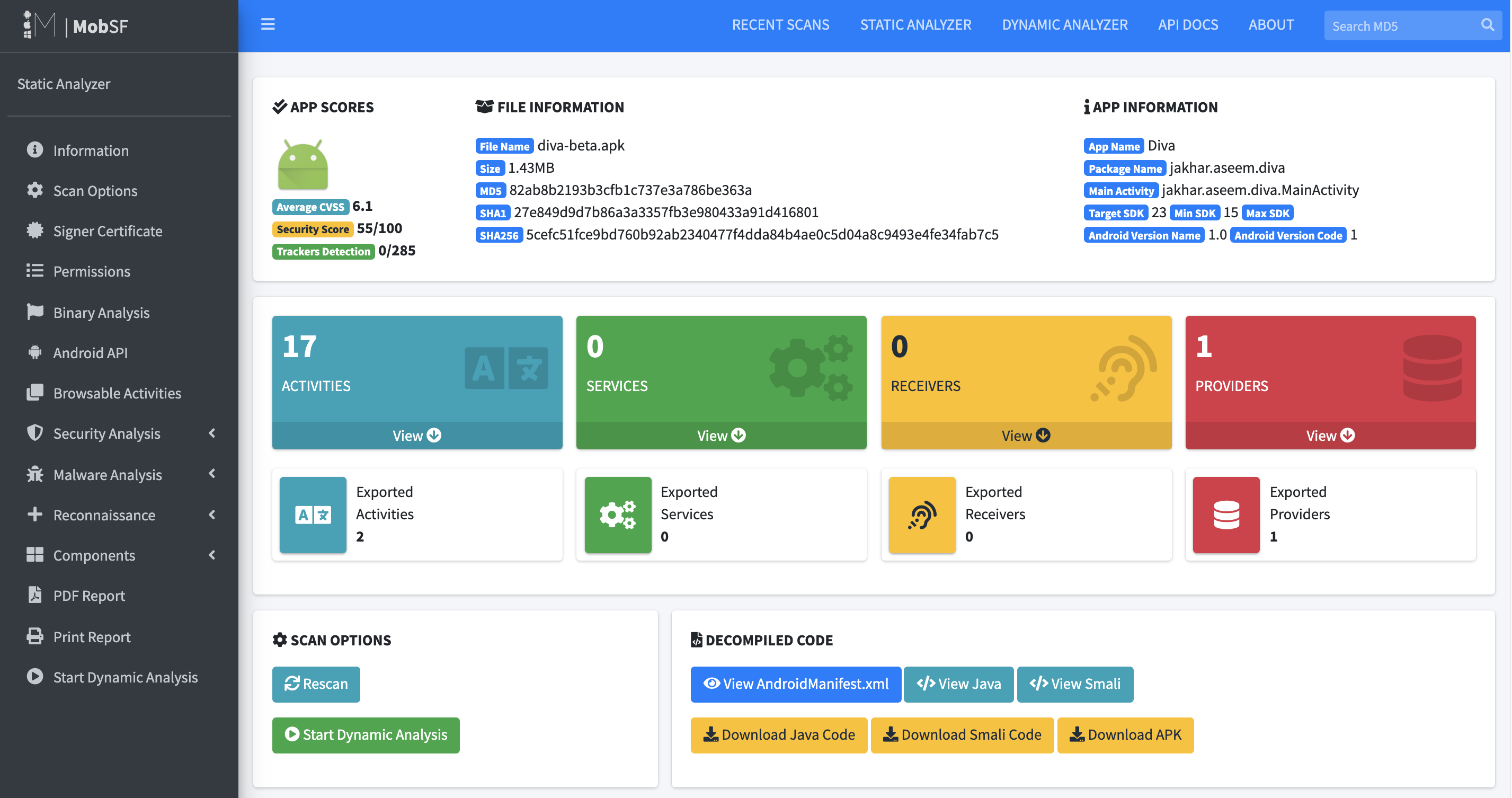


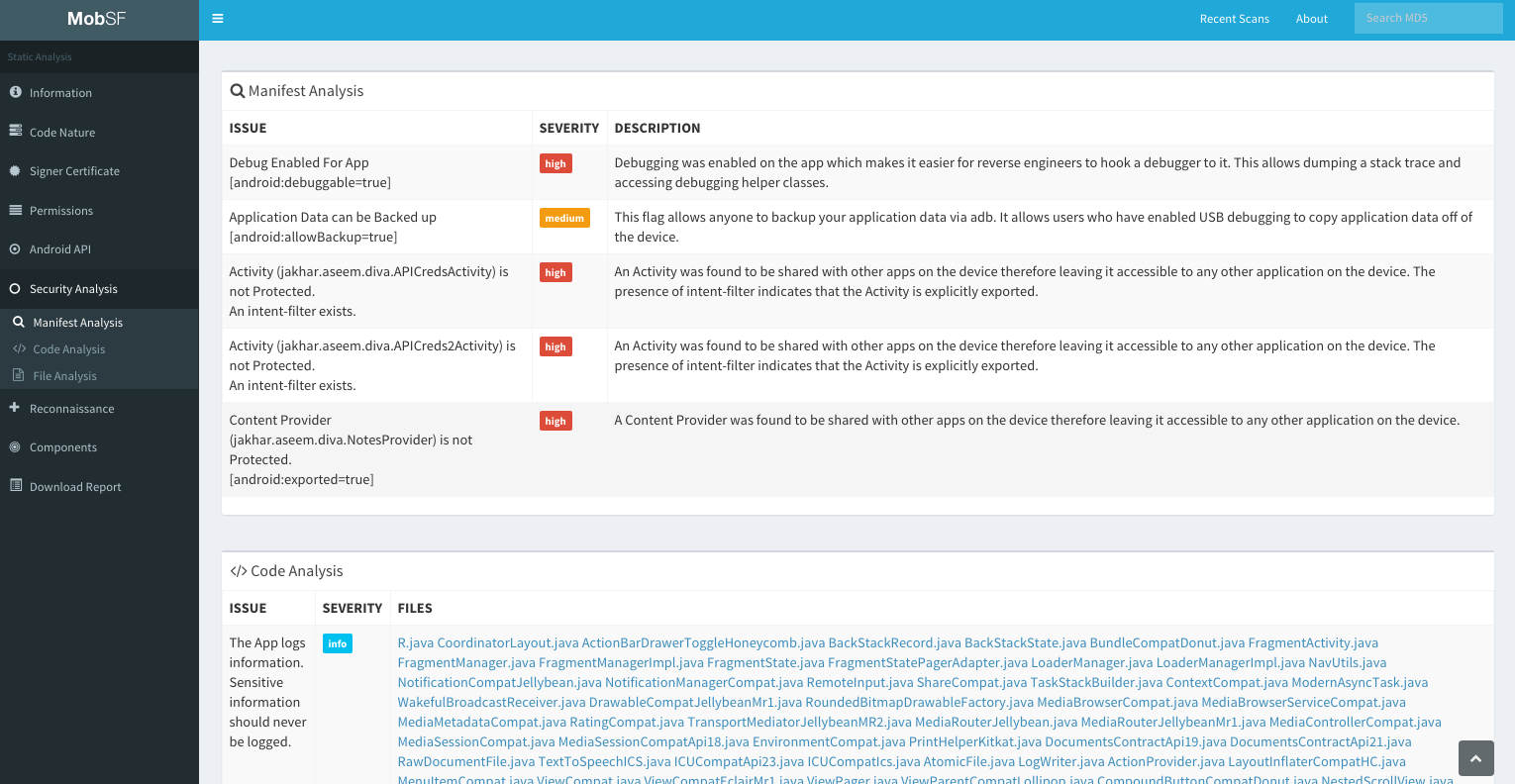
## Android Mobile Pentest Tools

#### MobSF (Mobile Security Framework)

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.

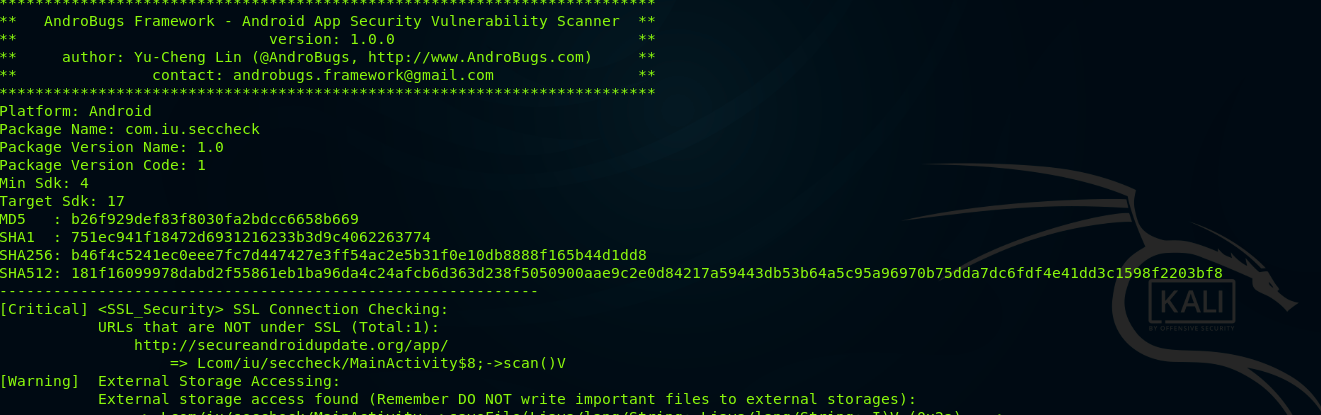
**Running address:127.0.0.1/8000.**





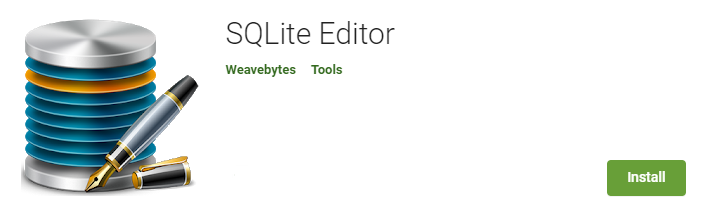
#### AndroBugs

AndroBugs Framework is an Android vulnerability analysis system that helps developers or hackers find potential security vulnerabilities in Android applications. No splendid GUI interface, but the most efficient (less than 2 minutes per scan in average) and more accurate.



#### SQLite Editor

Allows you to edit and delete records in any SQLite database on your phone. For root users, lists all installed apps which have local internal databases. You can then select an app and edit any of its databases.



#### ADB (Android Debug Bridge)

Android Debug Bridge (adb) is a versatile command-line tool that lets you communicate with a device. The adb command facilitates a variety of device actions, such as installing and debugging apps, and it provides access to a Unix shell that you can use to run a variety of commands on a device. It is a client-server program that includes three components:

**A client**, which sends commands. The client runs on your development machine. You can invoke a client from a command-line terminal by issuing an adb command.

**A daemon (adbd)**, which runs commands on a device. The daemon runs as a background process on each device.

**A server**, which manages communication between the client and the daemon. The server runs as a background process on your development machine.

##### ADB Basics:

**adb shell** (starts the backround terminal)

**adb devices** (lists connected devices)  
**adb root** (restarts adbd with root permissions)  
**adb start-server** (starts the adb server)   
**adb kill-server** (kills the adb server)  
**adb reboot** (reboots the device)  
**adb devices -l** (list of devices by product/model)  
**exit** (exits the background terminal)  
**adb help** (list all commands)  
**adb –d <command>** (directs command to only attached USB device)  
**adb –e <command>** (directs command to only attached emulator)

**adb pull** (To copy a file or directory from the device)

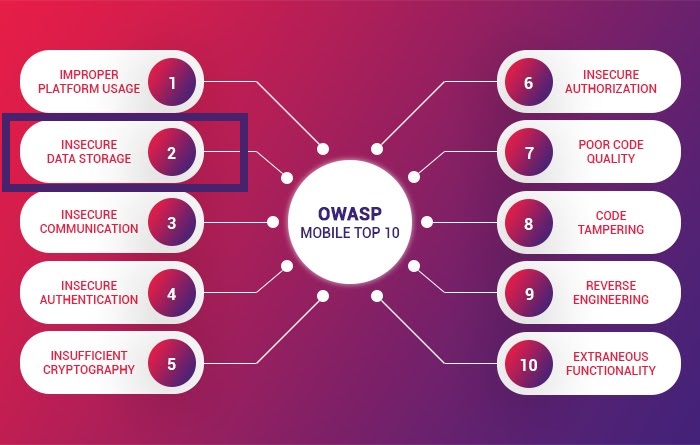
**adb push** (To copy a file or directory and its sub-directories to the device)

#### Xposed Modules

If an application does not check whether the device is rooted or not, we can bypass this control with a module like RootCloak, Amplify Battery, Bootmanager, etc.

## Mobile Pentest Application

#### Insecure Data Storage



Insecure data storage is the application which stores user sensitive data on device itself such as uncrypted database files, insecured shared storage, insecure application data storage.

Where to find?

* Shared preferences (xml files)
* Database folder (db files)
* Application resources folder (any file type)
* Sd card (any file type)

#### DIVA

(insecure and vulnerable app) is an app intentionally designed to be insecure.

Download Link: <https://apkpure.com/diva-app/com.n4labs.diva>

Installation:

**$ adb install diva.apk**

#### Application Steps:

* Go data/data/app\_directory through terminal.
* All application names are there. Find which one is yours.

**$ ls | grep diva**

**$ cd jakhar.aseem.diva**

##### #Challenge 3

* Credentials got saved we do not now where. Firstly, we will check shared preferences.

**$ ls**

**$ cd shared\_prefs**

**$ ls -l**

* There is only one jakhar.aseem.diva\_preferences.xml in shared\_prefs.
* See contents through cat command.

**$ ls**

**$ cat**

* Application stores password in shared preferences.

Results:

* Application stores user credentials natively in device.
* Shared preferences are not encrypted here which is storing user data.

##### #Challenge 4

* Firstly, check again this shared preferences. App might be storing all user info here in single xml file.
* No, it is not there. So, we have to look if application has generated new xml file in same folder to store other credentials.
* No, it is not there. So, app storing credentials outside shared preferences. So, let’s check database now.

**$ cd ..**

**$ ls**

**$ cd databases/**

**$ ls**

* Here sqli, id2 and divanotes are 2 main databases. Other are those DB journal which are not actual database files. First check divanotes.db.

**$ sqlite3 divanotes.db**

**$ .tables**

* Looks like notes might have some juicy info.

**$ select \* from notes;**

* It does not store credentials.
* Move to next database.

**$ Ctrl-z**

**$ sqlite3 ids2**

* Target myuser here.

**$ select \* from myuser;**

* We have got password saved in this db.

##### #Challenge 5

**$ Ctrl-z**

**$ ls**

**$ cd ..**

**$ ls**

**$ ls -l**

* Look for all previous places. Find if any new file is created or not.
* Basically 4 directories are there.
* Give credentials and save.
* A new file has been generated it must be a password.
* It is storing our new password.

##### #Challenge 6

If you are not able to find any information here(under data/data) then look for sdcard.

Many applications store private info on sdcard even which is more dangerous

Try to find this credentials (for user data in application resources) you will not able to find.

Then move to sdcard.

**$ cd /mnt**

Note:

The /mnt directory and its subdirectories are intended for use as the temporary mount points for mounting [storage](http://www.linfo.org/storage.html) devices, such as CDROMs, floppy disks and USB (universal serial bus) key drives. /mnt is a standard subdirectory of the [root directory](http://www.linfo.org/root_directory.html) on [Linux](http://www.linfo.org/linuxdef.html) and other [Unix-like](http://www.linfo.org/unix-like.html) [operating systems](http://www.linfo.org/operating_systems_list.html), along with directories such as [/bin](http://www.linfo.org/bin.html), /boot, /dev, /etc, [/home](http://www.linfo.org/home.html), /proc, [/root](http://www.linfo.org/slash_root.html), [/sbin](http://www.linfo.org/sbin.html), /usr and /var.

**$ ls**

Note:

If you want to find hidden files or folders in Linux, use “cd .” with tab twice. When you try ls command it will not work.

**$ cd sdcard/**

**$ ls -al**

It will give “.uinfo.txt” file. The file starting with “.” and it means “.uinfo” file is hidden.

**$ cat .uinfo.txt**

## Resources

* [**https://www.appknox.com/blog/understanding-owasp-top-10-mobile-insecure-data-storage**](https://www.appknox.com/blog/understanding-owasp-top-10-mobile-insecure-data-storage)
* [**https://owasp.org/www-project-mobile-top-10/2016-risks/m2-insecure-data-storage**](https://owasp.org/www-project-mobile-top-10/2016-risks/m2-insecure-data-storage)
* [**https://source.android.com/security**](https://source.android.com/security)
* [**https://developer.android.com/training/articles/security-tips.html**](https://developer.android.com/training/articles/security-tips.html)
* [**https://www.youtube.com/watch?v=hXTu9kgcLUU**](https://www.youtube.com/watch?v=hXTu9kgcLUU)
* [**https://www.youtube.com/watch?v=ZPmpOEw-O2Y**](https://www.youtube.com/watch?v=ZPmpOEw-O2Y)
* [**https://www.appsealing.com/owasp-mobile-top-10-a-comprehensive-guide-for-mobile-developers-to-counter-risks/**](https://www.appsealing.com/owasp-mobile-top-10-a-comprehensive-guide-for-mobile-developers-to-counter-risks/)
* [**https://apprize.best/security/pentesting/8.html**](https://apprize.best/security/pentesting/8.html)
* [**https://guides.peruzal.com/mobile-device-security-and-penetration-testing-guide/android-insecure-data-storage/**](https://guides.peruzal.com/mobile-device-security-and-penetration-testing-guide/android-insecure-data-storage/)
* [**https://guides.peruzal.com/mobile-device-security-and-penetration-testing-guide/rooting-android-devices/**](https://guides.peruzal.com/mobile-device-security-and-penetration-testing-guide/rooting-android-devices/)
* [**https://www.slideshare.net/AhmetGrel1/mobil-pentest-eitim-dkman**](https://www.slideshare.net/AhmetGrel1/mobil-pentest-eitim-dkman)
* [**http://www.linfo.org/mnt.html#:~:text=The%20%2Fmnt%20directory%20and%20its,operating%20systems%2C%20along%20with%20directories**](http://www.linfo.org/mnt.html#:~:text=The%20%2Fmnt%20directory%20and%20its,operating%20systems%2C%20along%20with%20directories)
* [**https://www.automatetheplanet.com/adb-cheat-sheet/**](https://www.automatetheplanet.com/adb-cheat-sheet/)
* [**https://developer.android.com/studio/command-line/adb**](https://developer.android.com/studio/command-line/adb)
* [**https://www.techopedia.com/definition/4220/android-sdk**](https://www.techopedia.com/definition/4220/android-sdk)
* [**https://github.com/MobSF/Mobile-Security-Framework-MobSF**](https://github.com/MobSF/Mobile-Security-Framework-MobSF)
* [**https://github.com/AndroBugs/AndroBugs\_Framework**](https://github.com/AndroBugs/AndroBugs_Framework)
* [**https://en.wikipedia.org/wiki/Dalvik\_(software)**](https://en.wikipedia.org/wiki/Dalvik_(software))
* [**https://www.xda-developers.com/best-xposed-modules-for-2020/**](https://www.xda-developers.com/best-xposed-modules-for-2020/)
* **https://github.com/payatu/diva-android**