Debuggable APK

Written By Afrizal F.A - R&D incrustwerush.org

Preparation

Before performing techniques for debugging an APK, please make sure that Developer Mode and USB Debugging are enabled on your Android device. You can enable Developer Mode by navigating to Settings > About Phone and tapping on the Build Number several times. Then, go to Settings > Developer Options and activate USB Debugging. This setup is essential for successful interaction and debugging of the APK.

Decompile APK

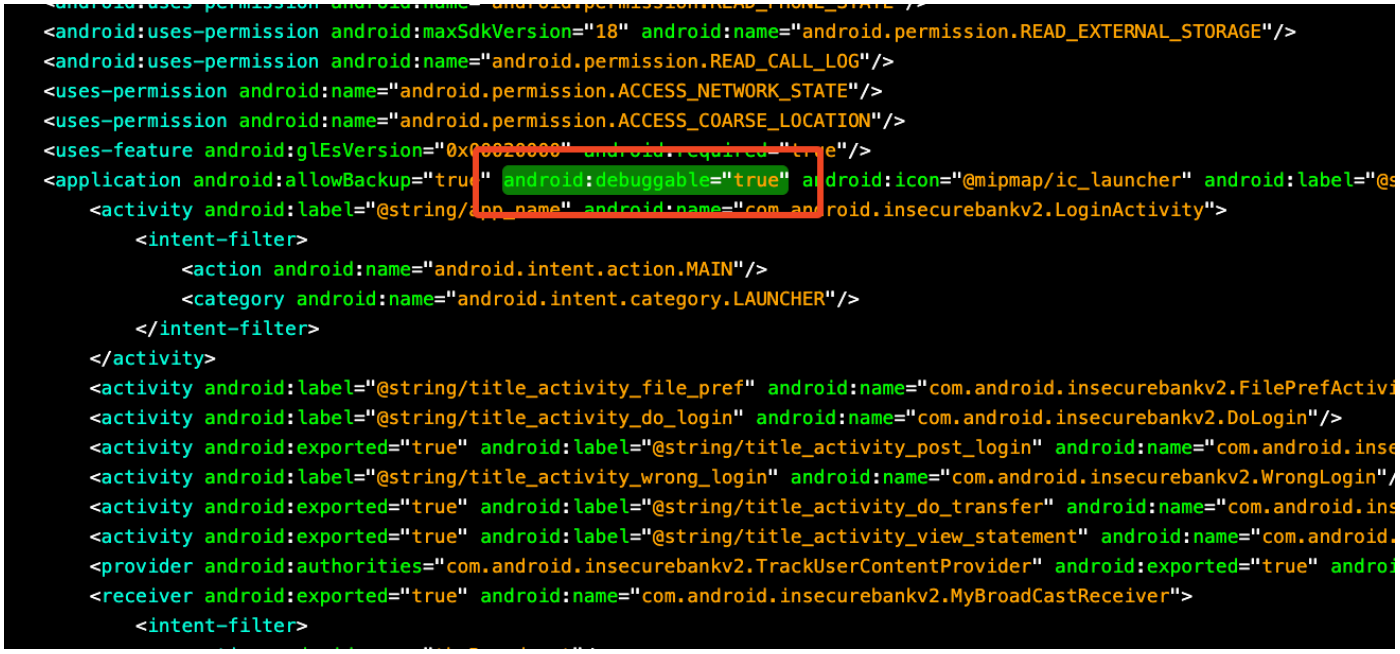
Install apktool, apksigner, keytool

```
apktool d <apk-name>.apk
ls <apk-name> # For check directory
```

```
[afrzlfa@127.0.0.1 test % apktool d InsecureBankv2.apk
I: Using Apktool 2.9.3 on InsecureBankv2.apk
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: [redacted]
I: Decoding values */* XMLs...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[afrzlfa@127.0.0.1 test % ls InsecureBankv2
AndroidManifest.xml     apktool.yml             original                res                     smali
afrzlfa@127.0.0.1 test %
```

Edit file `AnrdoidManifest.xml`

Add `android:debuggable="true"` to application tag



Recompile APK

```
apktool b <apk-name-directory>
keytool -genkey -v -keystore key.keystore -alias alias_name -keyalg RSA -
keysize 2048 -validity 10000
apksigner sign --ks key.keystore <apk-name-directory>/dist/<apk-name>.apk
```

```
afrzlfa@127.0.0.1 test % apktool b InsecureBankv2
I: Using Apktool 2.9.3
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: InsecureBankv2/dist/InsecureBankv2.apk
afrzlfa@127.0.0.1 test % keytool -genkey -v -keystore key.keystore -alias alias_name -keyalg RSA -keysize 2048 -validity 10000
Enter keystore password:
Re-enter new password:
Enter the distinguished name. Provide a single dot (.) to leave a sub-component empty or press ENTER to use the default value in braces.
What is your first and last name?
  [Unknown]:
What is the name of your organizational unit?
  [Unknown]:
What is the name of your organization?
  [Unknown]:
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
  [Unknown]:
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
  [no]:  yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA384withRSA) with a validity of 10,000 days
        for: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
[Storing key.keystore]
afrzlfa@127.0.0.1 test % apksigner sign --ks key.keystore InsecureBankv2/dist/InsecureBankv2.apk
Keystore password for signer #1:
afrzlfa@127.0.0.1 test %
```

Restart adb server & connect

Command:

```
adb kill-server
adb start-server
adb tcpip 5555 # With IP
adb connect <IP>:<PORT> # Connect With IP
```

```
127.0.0.1 ~ % adb kill-server
127.0.0.1 ~ % adb start-server
* daemon not running; starting now at tcp:5037
* daemon started successfully
127.0.0.1 ~ % adb tcpip 5555
restarting in TCP mode port: 5555
127.0.0.1 ~ % adb connect 10.10.1.123:5555
connected to 10.10.1.123:5555
127.0.0.1 ~ %
```

Install APK

Command:

```
cd <apk-name-directory>
adb devices # Check Connection
adb install dist/<apk-name>.apk
```

```
[127.0.0.1 test % cd InsecureBankv2
[127.0.0.1 InsecureBankv2 % adb devices
List of devices attached
10.10.1.123:5555        device

[127.0.0.1 InsecureBankv2 % adb install dist/InsecureBankv2.apk
Performing Incremental Install
Serving...
All files should be loaded. Notifying the device.
Success
Install command complete in 7624 ms
127.0.0.1 InsecureBankv2 %
```

ADB Shell: Connect and Access APK Data Directory

Enter Shell

```
adb devices
adb shell
# Android Shell
uname -a
run-as <package-directory>
ls -al
```

```
[afrzlfa@127.0.0.1 InsecureBankv2 % adb devices
List of devices attached
10.10.1.123:5555        device

[afrzlfa@127.0.0.1 InsecureBankv2 % adb shell
[a12:/ $ uname -a
Linux localhost 4.19.188-25463247-abA125FXXS4CWK1 #1 SMP PREEMPT Tue Nov 21 18:23:05 KST 2023 aarch64
[a12:/ $ run-as com.android.insecurebankv2
[a12:/data/user/0/com.android.insecurebankv2 $ ls -al
total 49
drwxr-x--x   4 u0_a655 u0_a655        3488 2024-09-05 16:29 .
drwxrwx--x 473 system  system        53248 2024-09-05 16:29 ..
drwxrws--x   2 u0_a655 u0_a655_cache  3488 2024-09-05 16:29 cache
drwxrws--x   2 u0_a655 u0_a655_cache  3488 2024-09-05 16:29 code_cache
a12:/data/user/0/com.android.insecurebankv2 $
```

Package Directory on `AndroidManifest.xml`

```
    <android:uses-permission android:name="android.permission.READ_CALL_LOG"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-feature android:glEsVersion="0x00020000" android:required="true"/>
    <application android:allowBackup="true" android:debuggable="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:theme="@android:style/Theme.Holo.Light.DarkAction
        <activity android:label="@string/app_name" android:name="com.android.insecurebankv2.LoginActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/title_activity_file_pref" android:name="com.android.insecurebankv2.FilePrefActivity" android:windowSoftInputMode="adjustNothing|stateVisible"/>
        <activity android:label="@string/title_activity_do_login" android:name="com.android.insecurebankv2.DoLogin"/>
        <activity android:exported="true" android:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin"/>
        <activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin"/>
        <activity android:exported="true" android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer"/>
        <activity android:exported="true" android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement"/>
        <provider android:authorities="com.android.insecurebankv2.TrackUserContentProvider" android:exported="true" android:name="com.android.insecurebankv2.TrackUserContentProvider"/>
        <receiver android:exported="true" android:name="com.android.insecurebankv2.MyBroadCastReceiver">
```