Low Hanging Fruit On Android

Zezadas

AKA José Moreira

Currently working at S21 SEC

https://peidei.me

https://sefod.eu

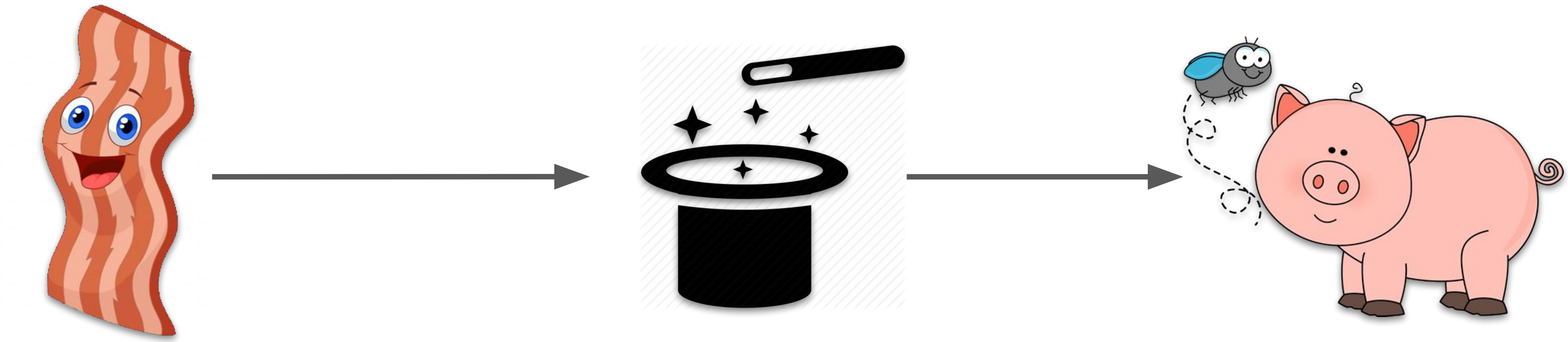
@0xz3z4d45

Reverse, patch, repack, repeat

1. Obtain and unpack APK
2. Analyze code, resources, files
3. Patch smali code
4. Rebuild and sign APK
5. Install into device / emulator
6. ???
7. PROFIT!

Reversing Android - 101

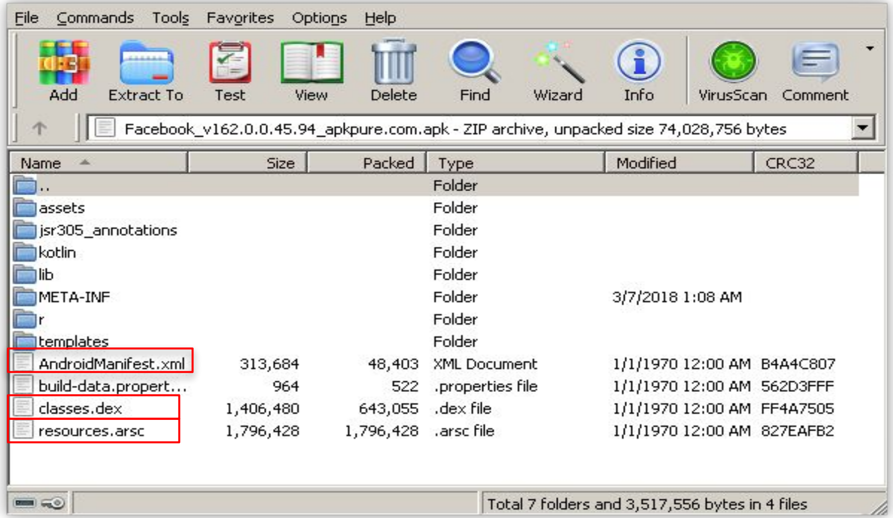
What is reversing?



APK

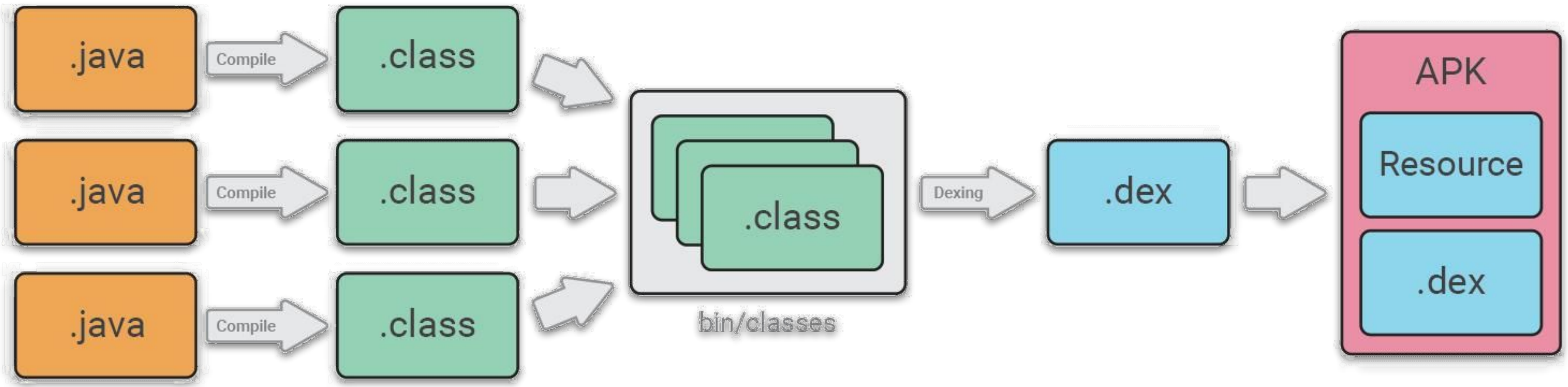
APK

APK

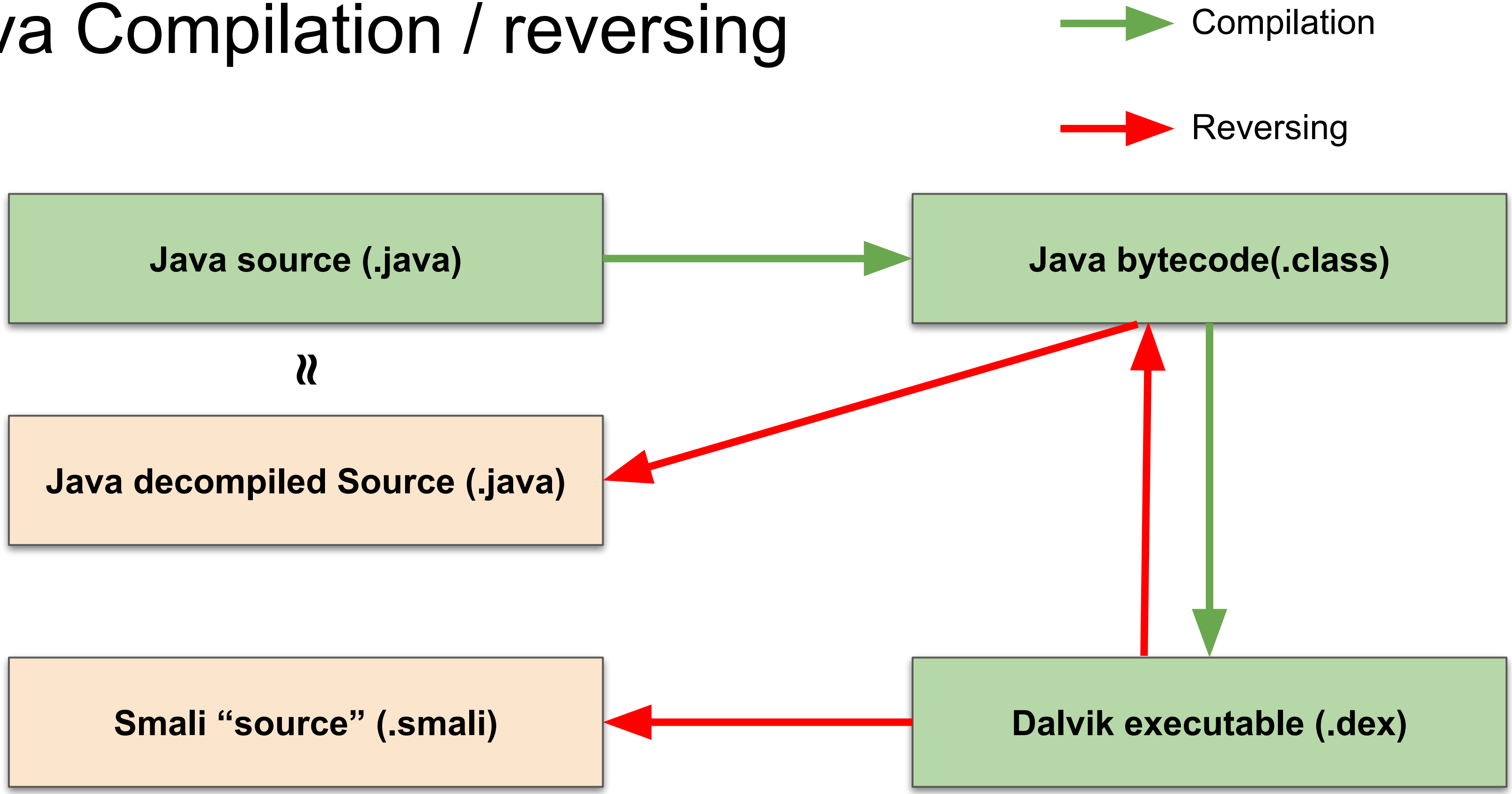


File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find
Wizard
Info
VirusScan
Comment
Facebook_v162.0.0.45.94_apkpure.com.apk - ZIP archive, unpacked size 74,028,756 bytes
Name Size Packed Type Modified CRC32
.. Folder
assets Folder
jsr305_annotations Folder
kotlin Folder
lib Folder
META-INF Folder 3/7/2018 1:08 AM
r Folder
templates Folder
AndroidManifest.xml 313,684 48,403 XML Document 1/1/1970 12:00 AM B4A4C807
build-data.propert... 964 522 .properties file 1/1/1970 12:00 AM 562D3FFF
classes.dex 1,406,480 643,055 .dex file 1/1/1970 12:00 AM FF4A7505
resources.arsc 1,796,428 1,796,428 .arsc file 1/1/1970 12:00 AM 827EAFB2
Total 7 folders and 3,517,556 bytes in 4 files

Android compilation (simplified)



Java Compilation / reversing



Java Vs Smali Vs Byte Code

Java code:

```
import java.io.PrintStream;

public class HelloWorld
{
  public static void main(String[] paramArrayOfString)
  {
    System.out.println("Hello World!");
  }
}
```

Java Bytecode:

???

Dalvik Bytecode:

???

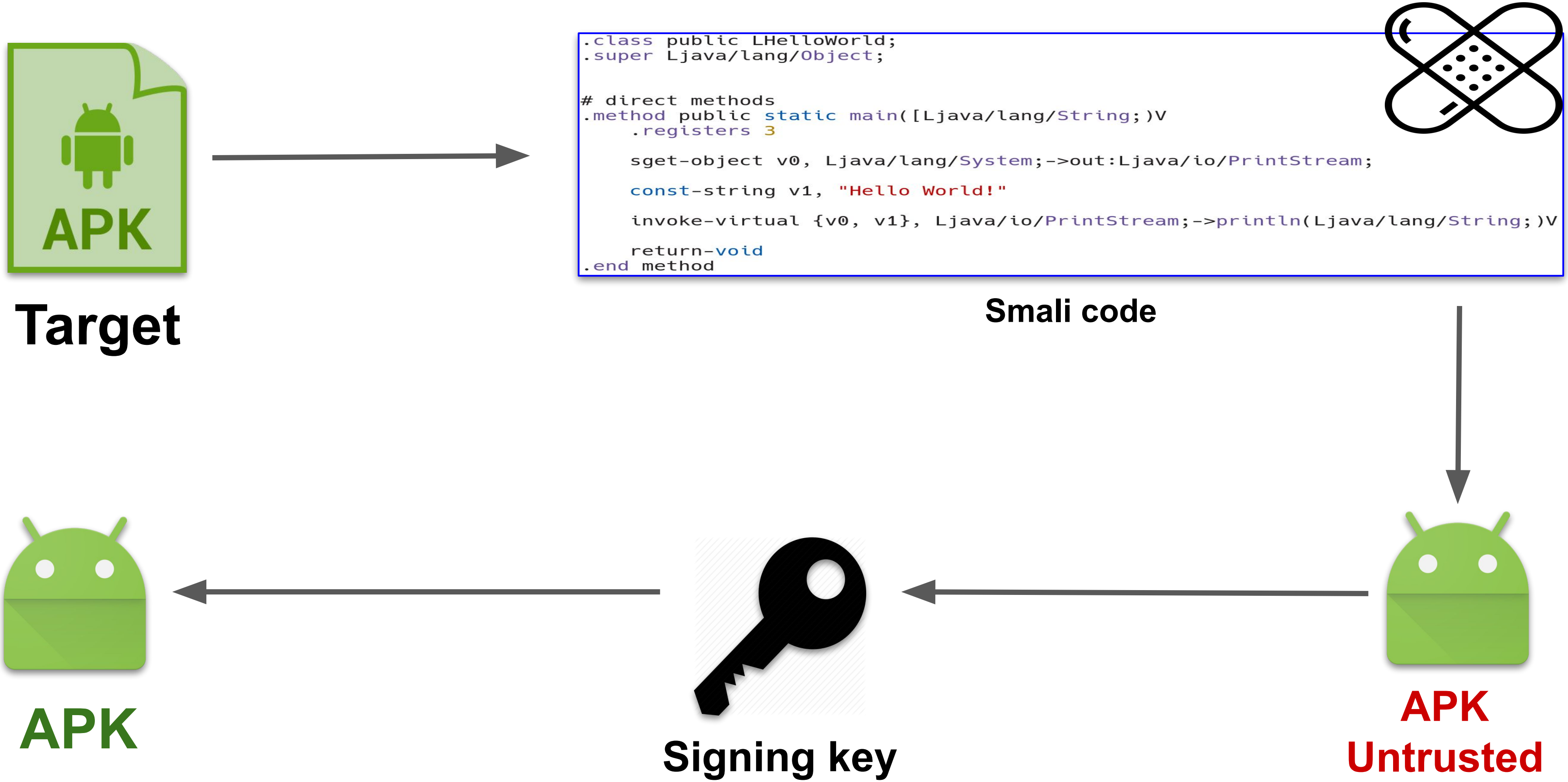
Decompiled Java bytecode:

```
public class HelloWorld {

    public static main(java.lang.String[] arg0) { //([Ljava/lang/String;)V
            getstatic java/lang/System.out:java.io.PrintStream
            ldc "Hello World!" (java.lang.String)
            invokevirtual java/io/PrintStream println((Ljava/lang/String;)V);
            return
    }
}
```

Smali code:

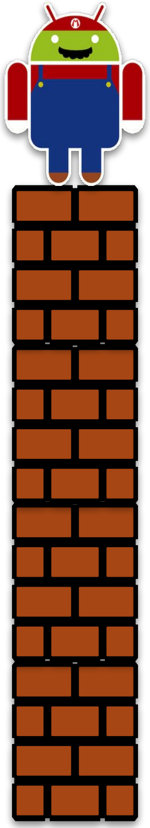
```
.class public LHelloWorld;
.super Ljava/lang/Object;


# direct methods
.method public static main([Ljava/lang/String;)V
    .registers 3

    sget-object v0, Ljava/lang/System;->out:Ljava/io/PrintStream;

    const-string v1, "Hello World!"

    invoke-virtual {v0, v1}, Ljava/io/PrintStream;->println(Ljava/lang/String;)V

    return-void
.end method
```

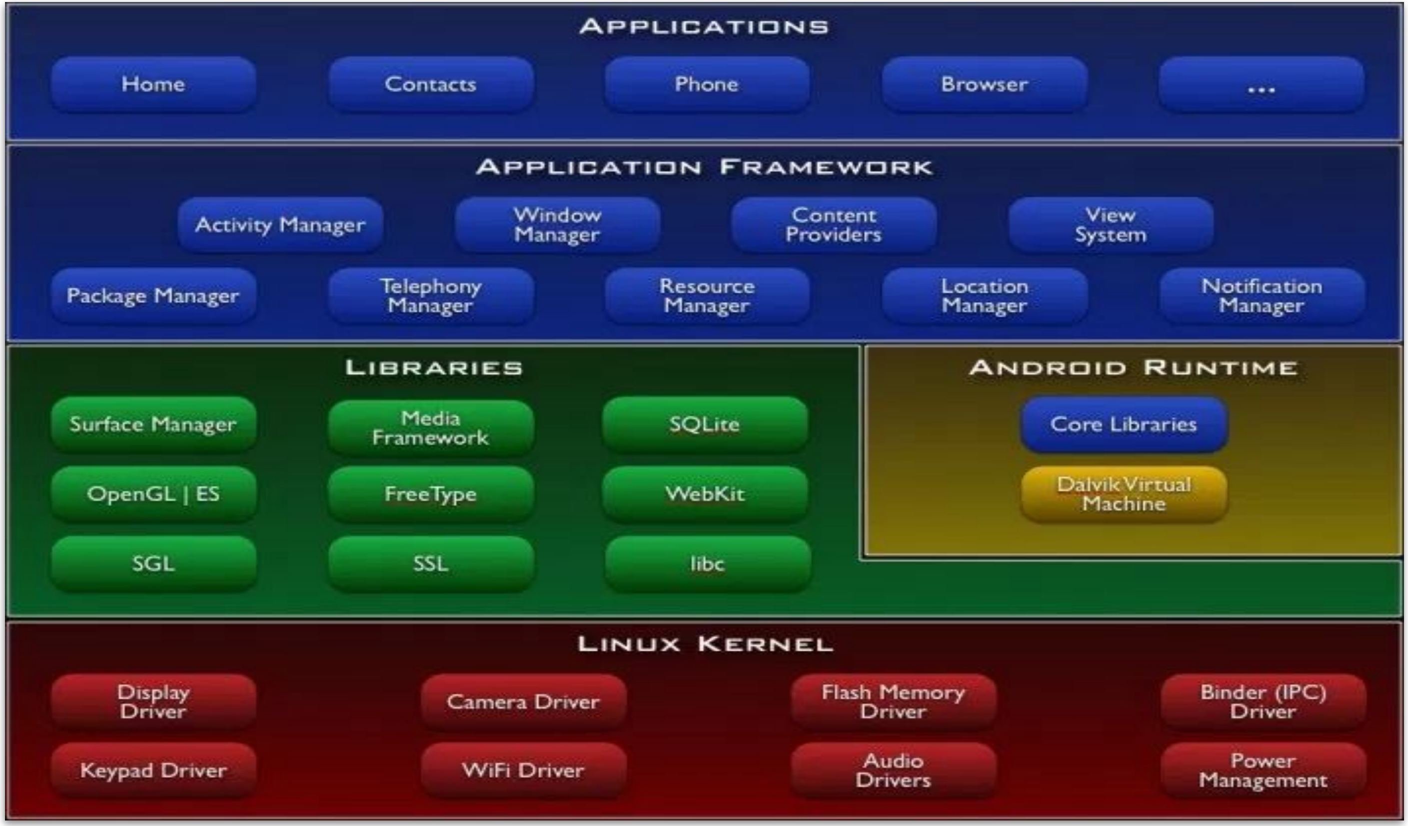
Patching Android - 101



APK
Target
.class public LHelloWorld;
.super Ljava/lang/Object;
direct methods
.method public static main([Ljava/lang/String;)V
.registers 3
sget-object v0, Ljava/lang/System;->out:Ljava/io/PrintStream;
const-string v1, "Hello World!"
invoke-virtual {v0, v1}, Ljava/io/PrintStream;->println(Ljava/lang/String;)V
return-void
.end method
Smali code
APK
Untrusted
Signing key
APK

Android Stack





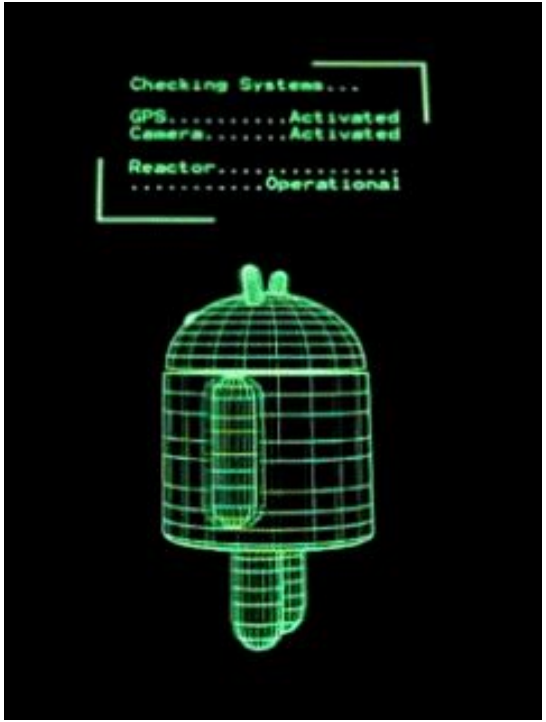
START HACKING! - Tools

- Install:
  - Android Studio (emulator && platform-tools) - https://developer.android.com/studio
  - JDK - https://jdk.java.net/
  - APKtool - https://ibotpeaches.github.io/Apktool/
  - Burp - https://portswigger.net/burp
  - Dex2jar - https://github.com/pxb1988/dex2jar
  - Bytecodeviewer - https://github.com/Konloch/bytecode-viewer
  - jadx-gui - https://github.com/skylot/jadx

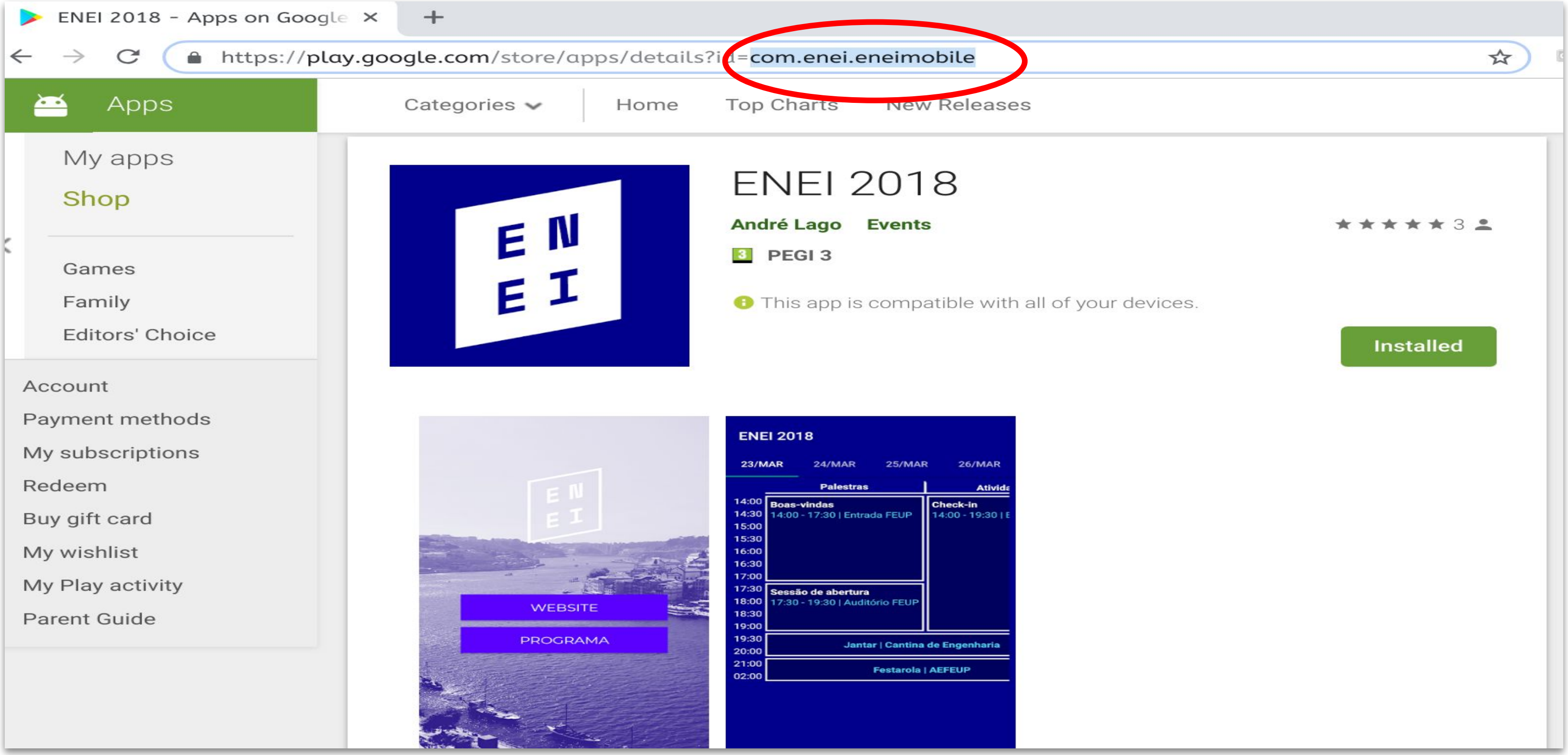
Practical - ENEI App 2018

Ways to obtain APKs:

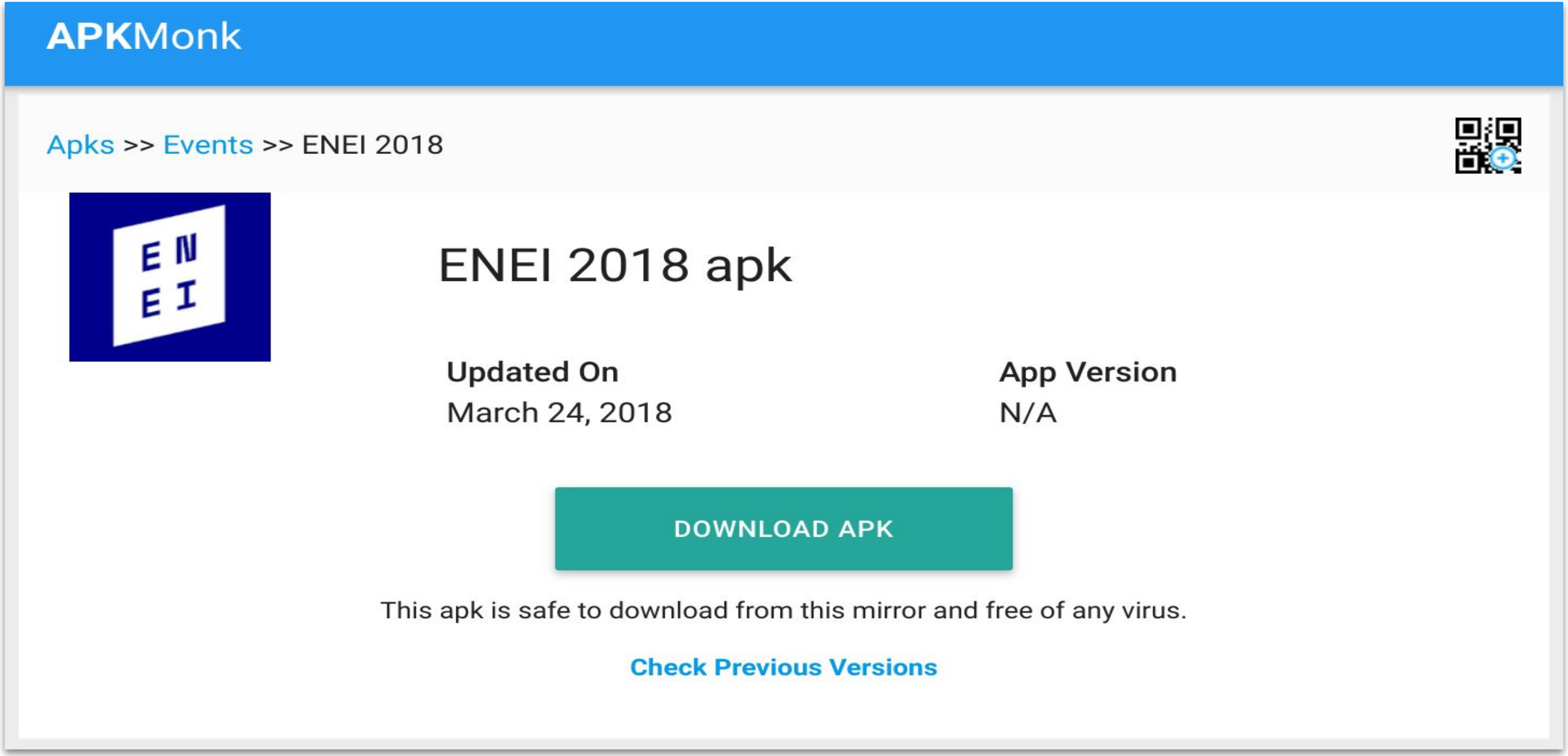
- https://apk-dl.com
- http://www.aptoide.com/
- https://www.apkmonk.com/
- Pull from android phone:
  - `$ adb shell pm list packages`
  - `$ adb shell pm path com.package.name`
  - `$ adb pull /full/path/to/apk`



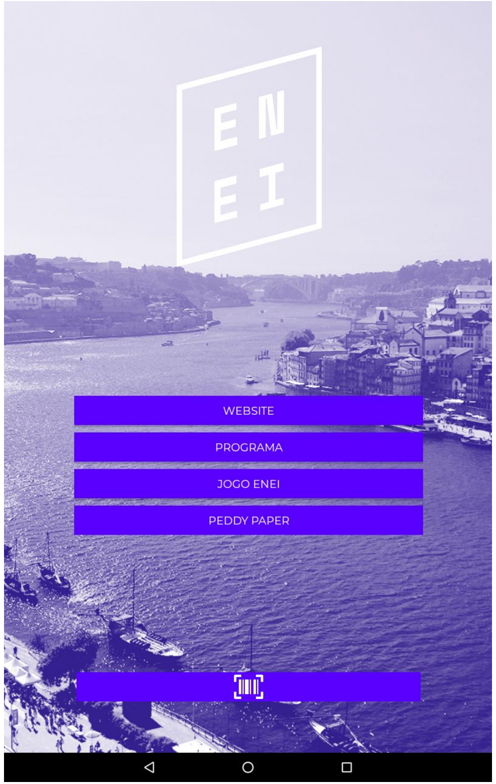
ENEI 2019 - App



Google + APKMonk



ENEI 2018 App



Extract && Decompile

```
File  Edit  View  Bookmarks  Settings  Help
anon@unknown  ~/oposec/enei  apktool d com.enei.eneimobile_2018-03-24.apk
I: Using Apktool 2.3.4 on com.enei.eneimobile_2018-03-24.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/anon/.local/share/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...
anon@unknown  ~/oposec/enei  _
```

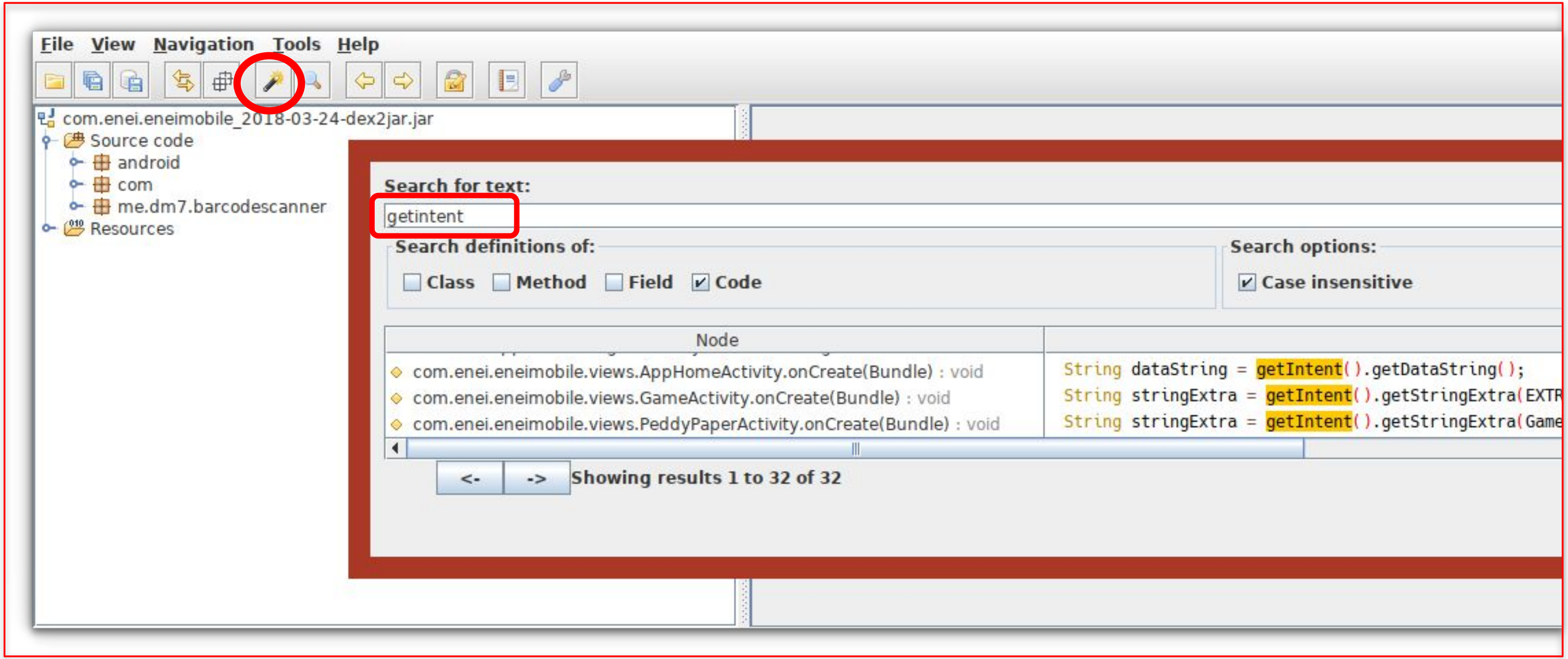
AndroidManifest.XML

```xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android"
package="com.enei.eneimobile">
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <application android:allowBackup="true" android:icon="@mipmap/ic_logo" android:label="@string/app_name"
    android:roundIcon="@mipmap/ic_logo_round" android:supportsRtl="true" android:theme="@style/AppTheme.NoActionBar">
        <activity android:name="com.enei.eneimobile.views.AppHomeActivity">
            <intent-filter>
                <action android:name="android.intent.action.VIEW"/>
                <category android:name="android.intent.category.DEFAULT"/>
                <category android:name="android.intent.category.BROWSABLE"/>
                <data android:scheme="enei"/>
            </intent-filter>
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:name="com.enei.eneimobile.views.WebViewActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/title_activity_schedule" android:name="com.enei.eneimobile.views.ScheduleActivity"
        android:theme="@style/AppTheme.NoActionBar"/>
        <activity android:name="com.enei.eneimobile.views.GameActivity"/>
        <activity android:name="com.enei.eneimobile.views.PeddyPaperActivity"/>
        <activity android:name="com.enei.eneimobile.views.CameraActivity"/>
        <meta-data android:name="android.support.VERSION" android:value="26.1.0"/>
        <meta-data android:name="android.arch.lifecycle.VERSION" android:value="27.0.0-SNAPSHOT"/>
        <meta-data android:name="com.android.vending.derived.apk.id" android:value="1"/>
    </application>
</manifest>
```

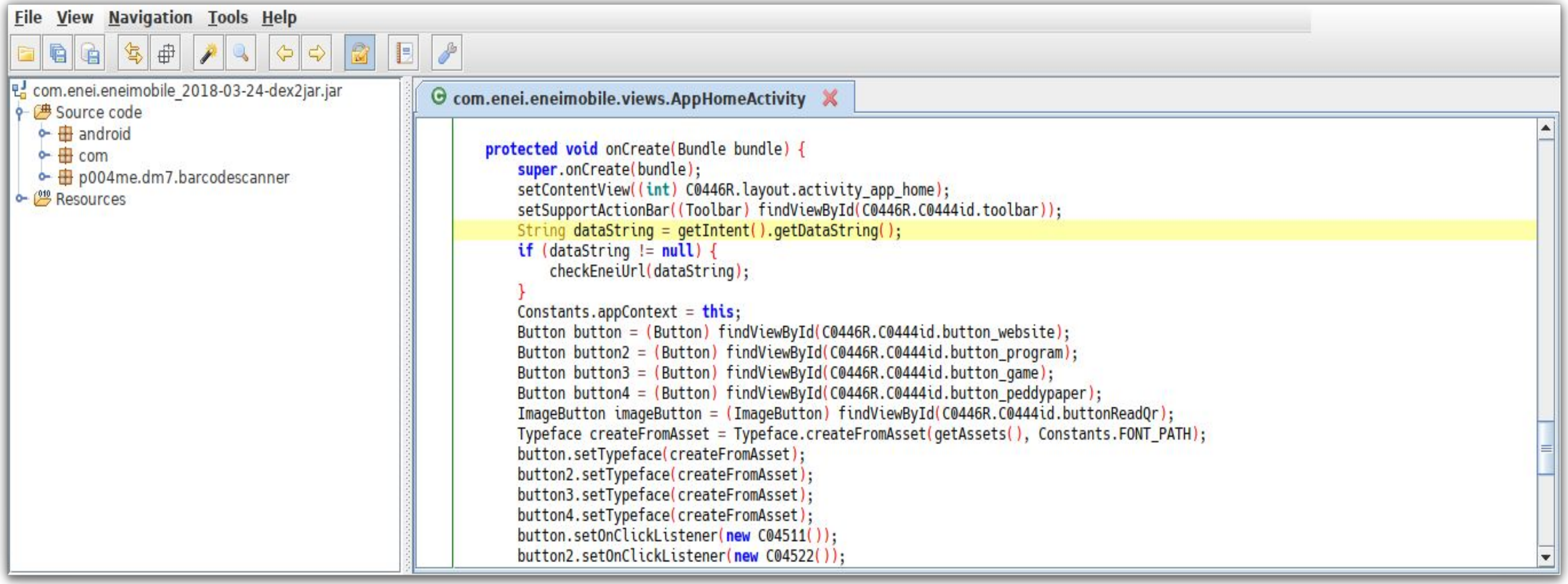
Dex2Jar && Jadx-GUI

```
File  Edit  View  Bookmarks  Settings  Help
anon@unknown  ~/oposec/enei  d2j-dex2jar com.enei.eneimobile_2018-03-24.apk
dex2jar com.enei.eneimobile_2018-03-24.apk -> ./com.enei.eneimobile_2018-03-24-dex2jar.jar
anon@unknown  ~/oposec/enei  jadx-gui com.enei.eneimobile_2018-03-24-dex2jar.jar
INFO  - output directory: com.enei.eneimobile_2018-03-24-dex2jar
INFO  - loading ...
INFO  - converting to dex: com.enei.eneimobile_2018-03-24-dex2jar.jar ...
```

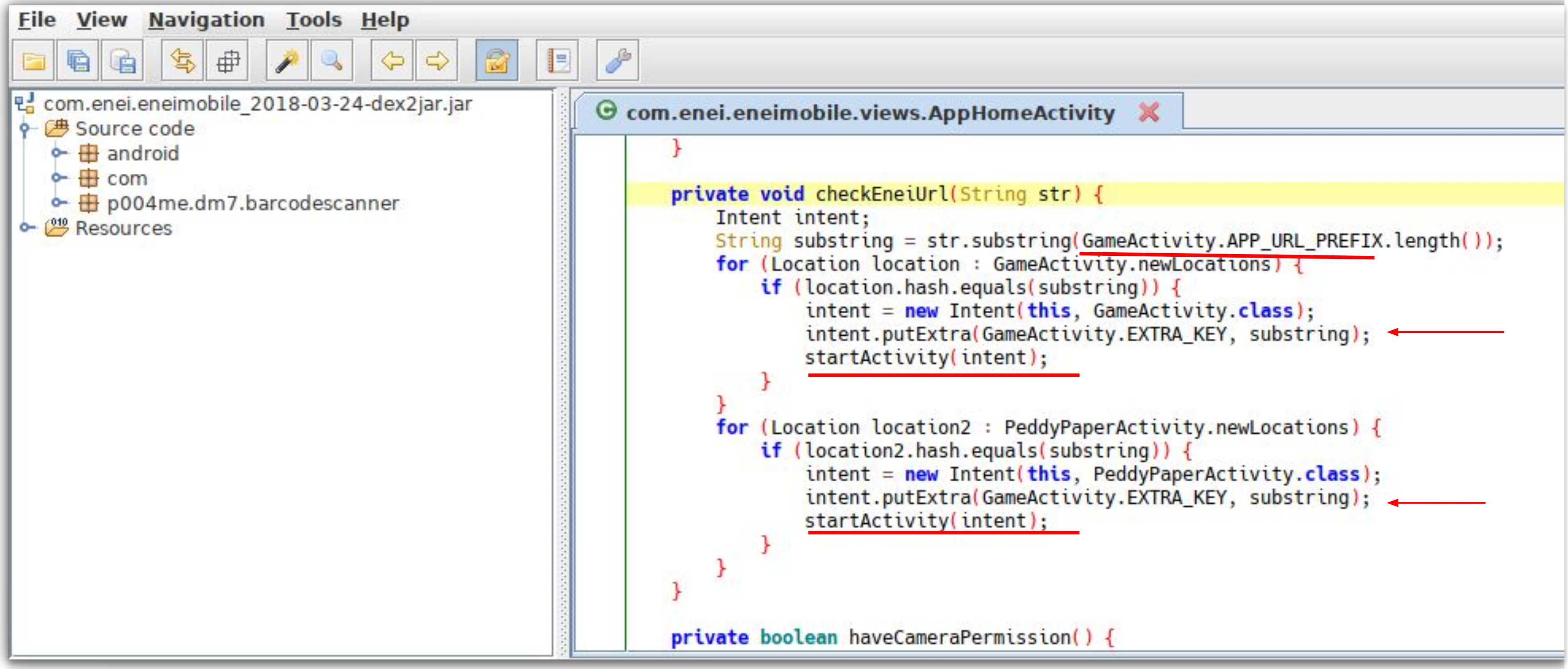
Jadx-GUI (1/5)- Search Intents



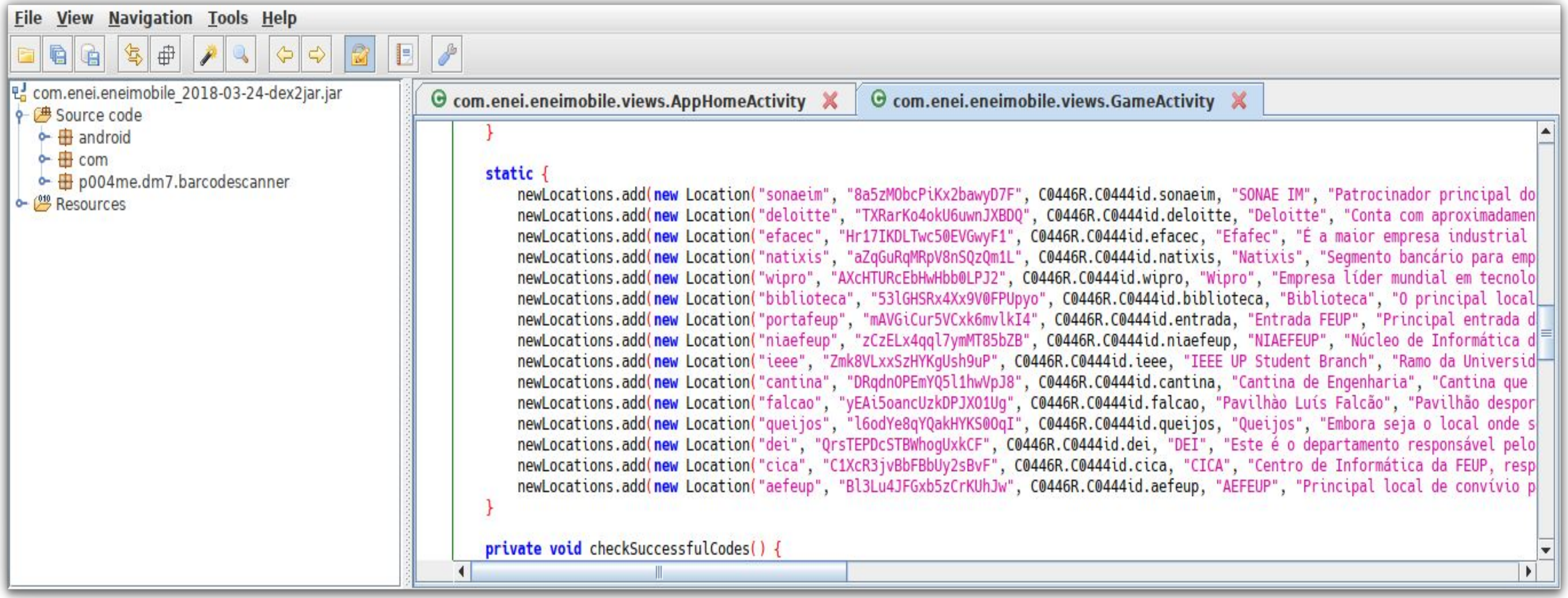
Jadx-GUI (2/5)- Code Analysis



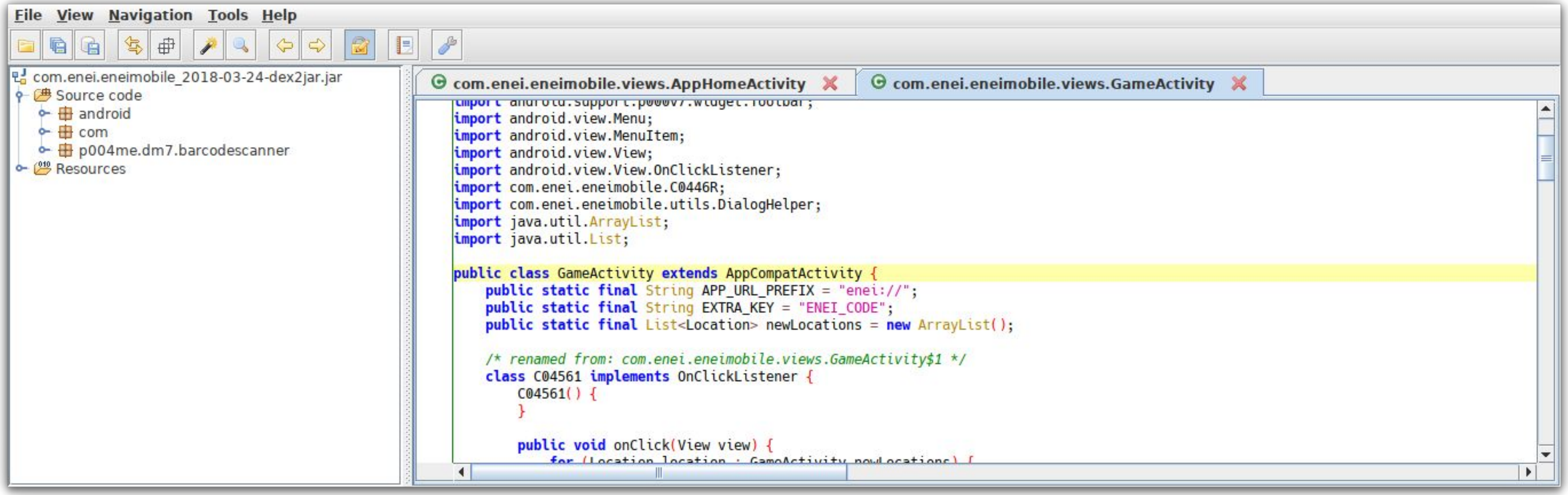
Jadx-GUI (3/5)- Code Analysis



Jadx-GUI (4/5)- Code Analysis

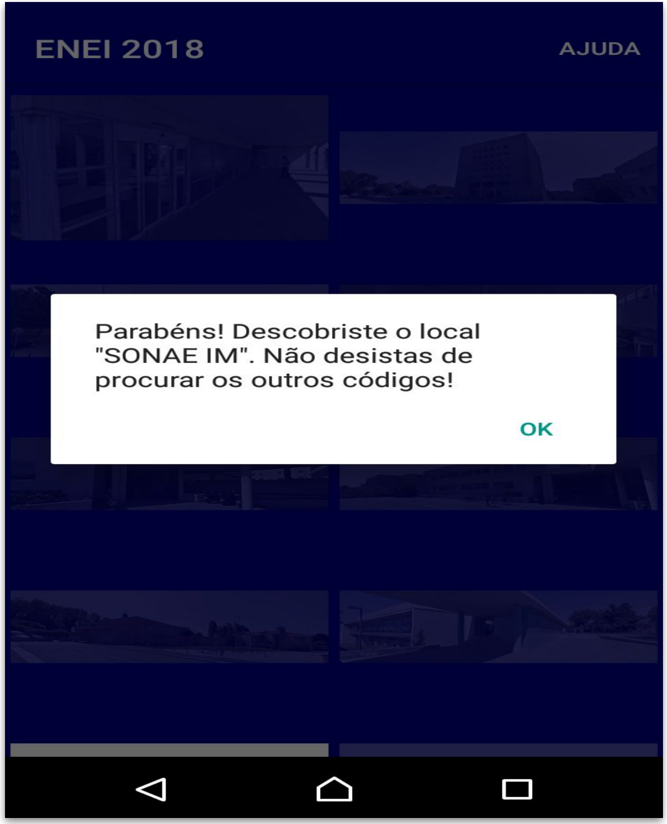


Jadx-GUI (5/5)- Code Analysis



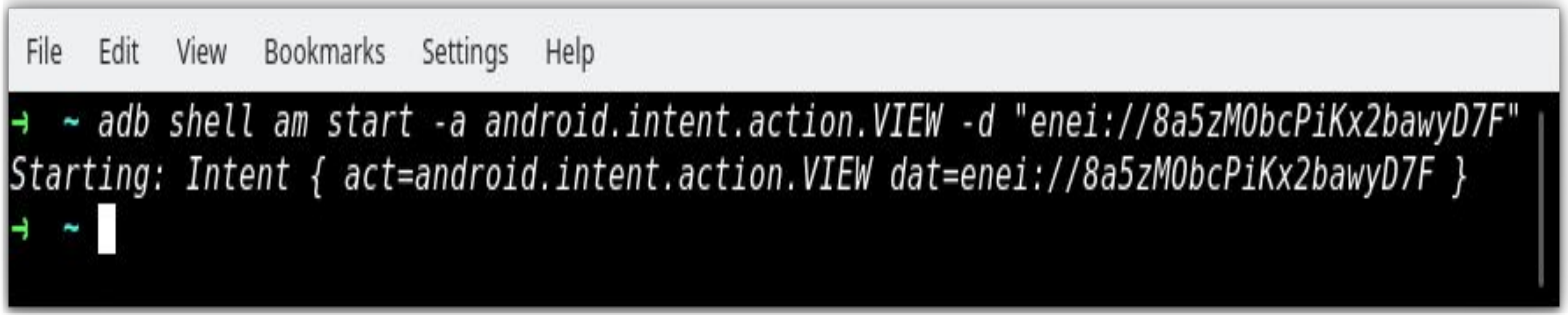
Exploit 1 - enei://8a5zMObcPiKx2bawyD7F

Solve 1


ENEI 2018
AJUDA
Parabéns! Descobriste o local "SONAE IM". Não desistas de procurar os outros códigos!
OK

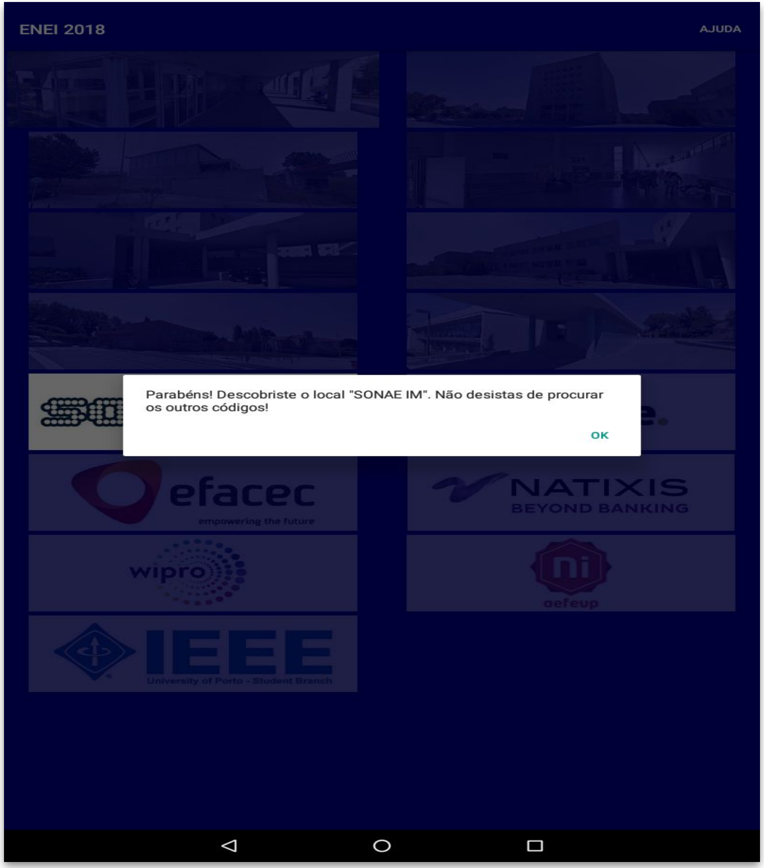

ENEI 2018
AJUDA
SONAE IM
Deloitte.
efacec
empowering the future
NATIXIS
BEYOND BANKING
wipro
ni
aefeup
IEEE
University of Porto - Student Branch

Exploit 2 - Stealth

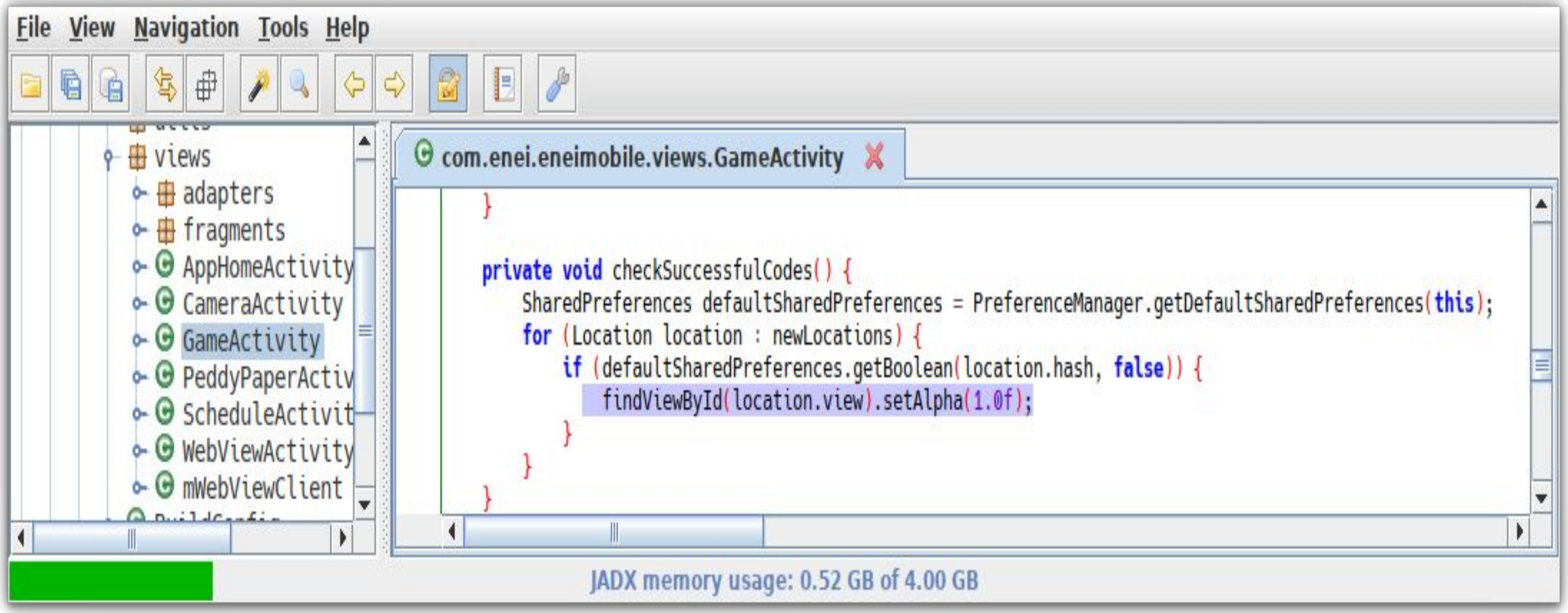


adb shell am start -a android.intent.action.VIEW -d "enei://8a5zMObcPiKx2bawyD7F"

Solve 2


ENEI 2018
AJUDA
Parabéns! Descobriste o local "SONAE IM". Não desistas de procurar os outros códigos!
OK
efacec
empowering the future
NATIXIS
BEYOND BANKING
wipro
ni
aefeup
IEEE
University of Porto - Student Branch

Exploit 3 - Analysing



Exploit 3 - Patching

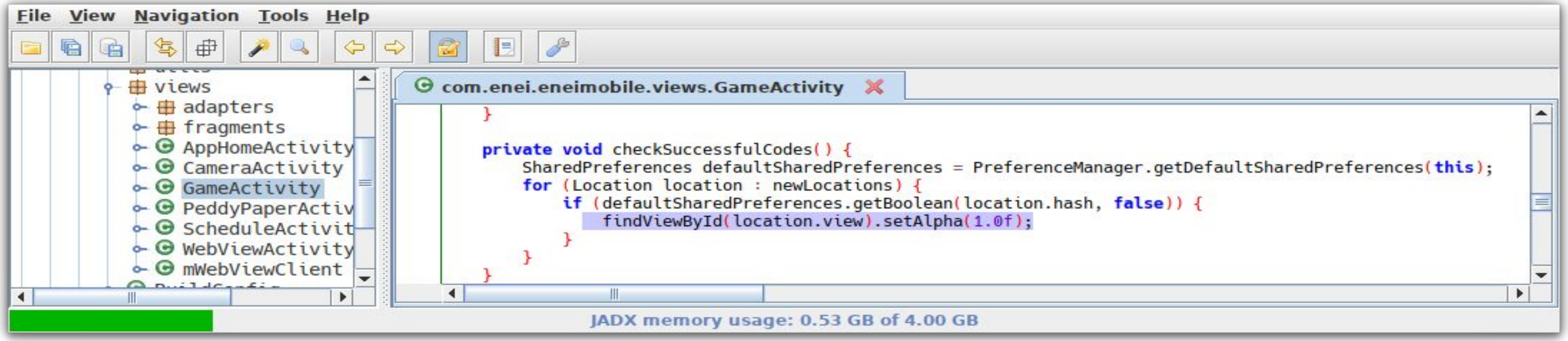
```
    move-result-object v2

    :cond_0
    :goto_0
    invoke-interface {v2}, Ljava/util/Iterator;->hasNext()Z

    move-result v3

    if-eqz v3, :cond_1

    invoke-interface {v2}, Ljava/util/Iterator;->next()Ljava/lang/Object;

    move-result-object v0

    check-cast v0, Lcom/enei/eneimobile/views/GameActivity$Location;

    .line 140
    .local v0, "location":Lcom/enei/eneimobile/views/GameActivity$Location;
    iget-object v3, v0, Lcom/enei/eneimobile/views/GameActivity$Location;->hash:Ljava/lang/String;

    const/4 v4, 0x0

    invoke-interface {v1, v3, v4}, Landroid/content/SharedPreferences;->getBoolean(Ljava/lang/
String;Z)Z

    move-result v3

    #if-eqz v3, :cond_0

    .line 141
    iget v3, v0, Lcom/enei/eneimobile/views/GameActivity$Location;->view:I

    invoke-virtual {p0, v3}, Lcom/enei/eneimobile/views/GameActivity;->findViewById(I)Landroid/view/
View;
```

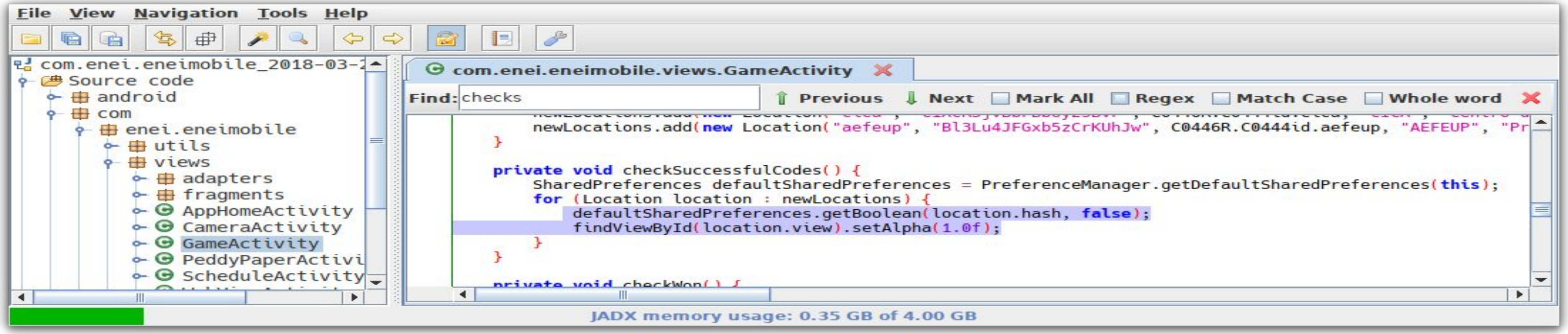
Exploit 3 - Recompile

File Edit View Bookmarks Settings Help

```
➜  oposeczadas apktool b com.enei.eneimobile_2018-03-24
I: Using Apktool 2.3.4
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
S: WARNING: Could not write to (/home/anon/.local/share/apktool/framework), using /tmp i
nstead...
S: Please be aware this is a volatile directory and frameworks could go missing, please
utilize --frame-path if the default storage directory is unavailable
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
➜  oposeczadas
```

Exploit 3 - Compare





Exploit 3 - Sign && Install

File Edit View Bookmarks Settings Help

```
➜  dist sign_apk com.enei.eneimobile_2018-03-24.apk
jar signed.

Warning:
The signer's certificate is self-signed.
➜  dist adb install com.enei.eneimobile_2018-03-24.apk
Success
➜  dist
```

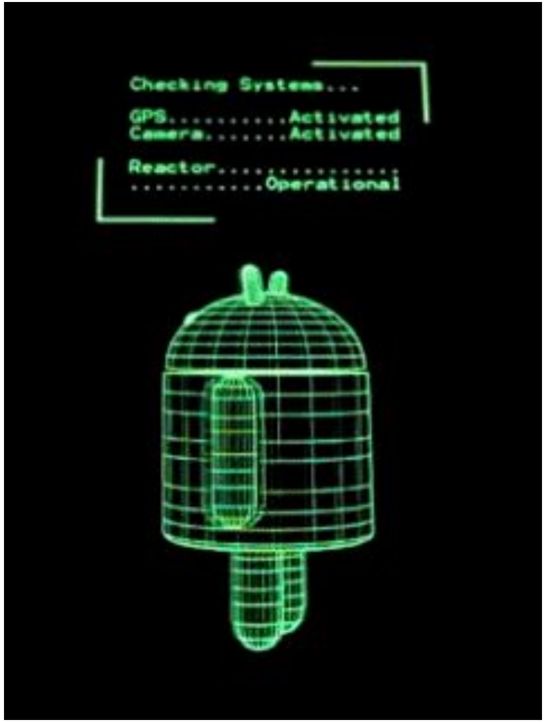
Solve 3

ENEI 2018
AJUDA
SONAE IM
Deloitte.
efacec
empowering the future
NATIXIS
BEYOND BANKING
wipro
ni
aefeup
IEEE
University of Porto - Student Branch

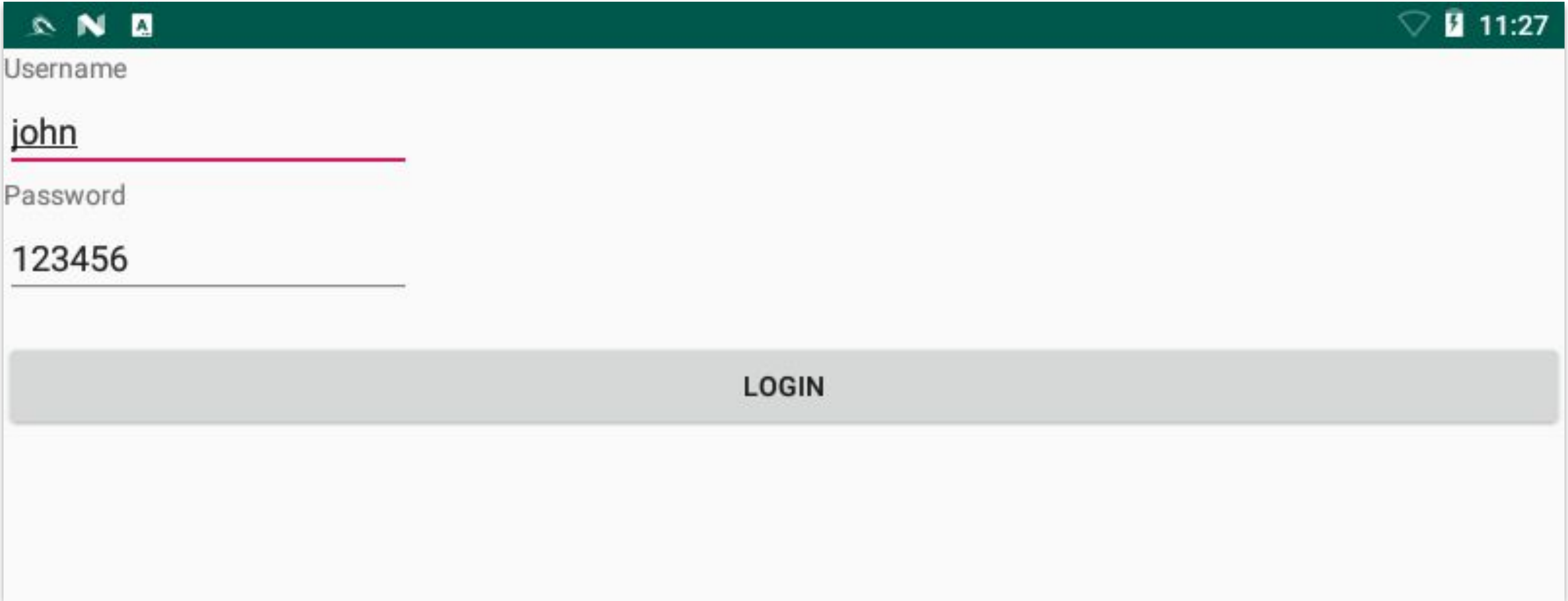
Practical - Vuln App

Ways to obtain APKs:

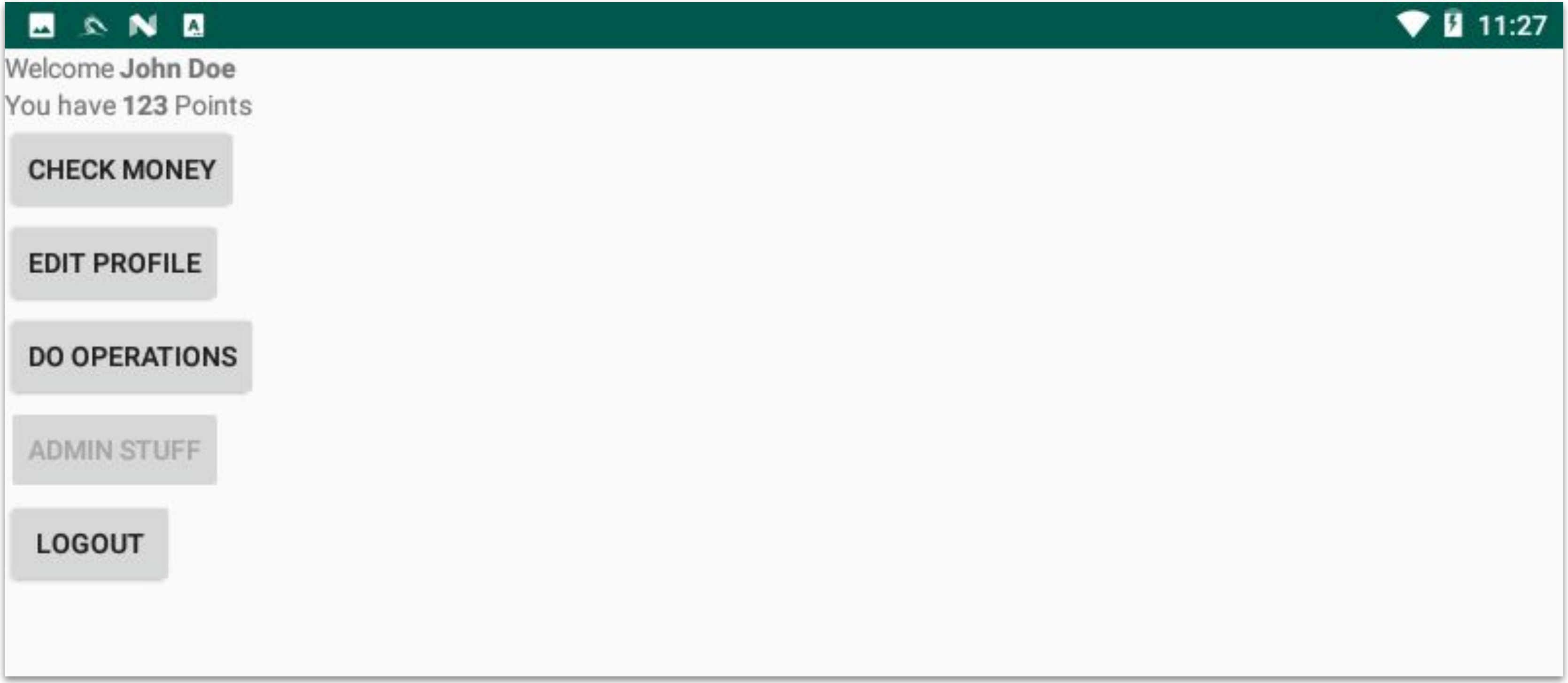
- Source:
  - https://github.com/zezadas/0xOPOSEC_0x73_VulnApp_Android
- Pull from android phone:
  - `$ adb shell pm list packages | grep -i vulnapp`
  - `$ adb shell pm path pt.oposec.vulnapp`
  - `$ adb pull /data/app/pt.oposec.vulnapp-1/base.apk`



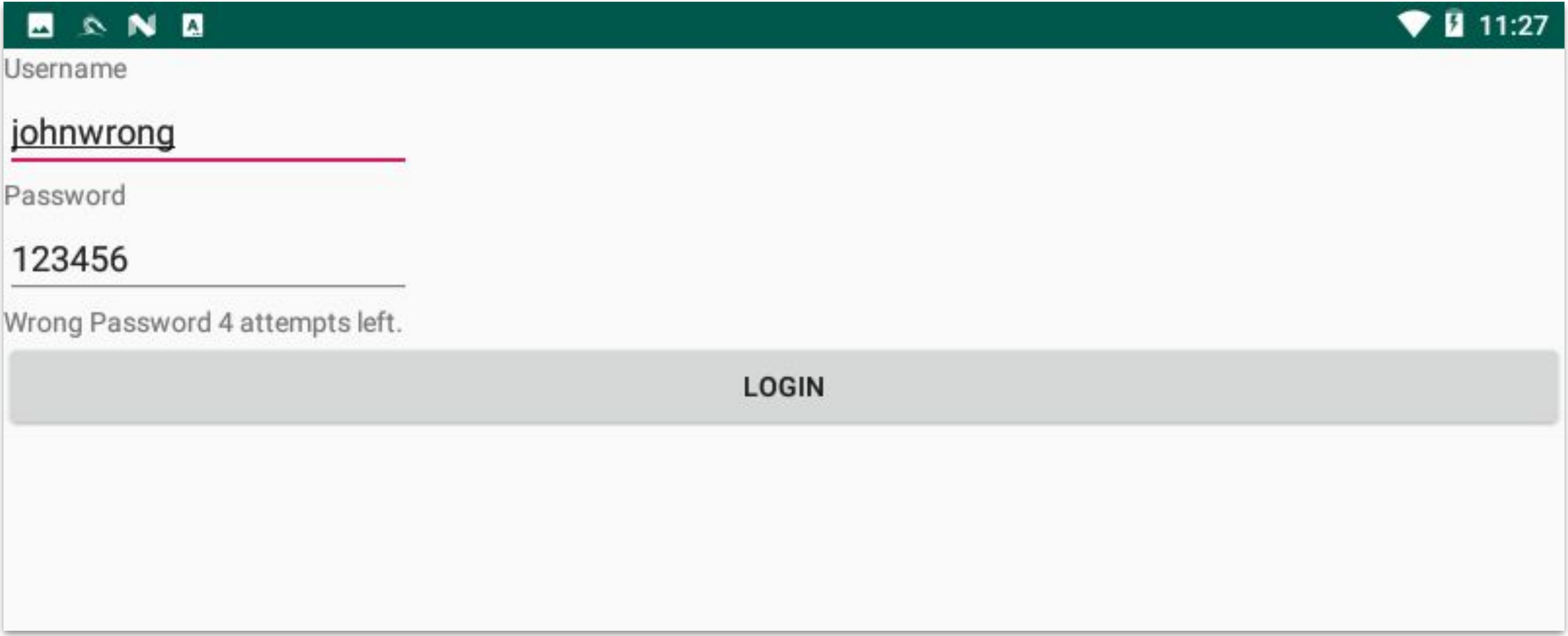
VulnApp



VulnApp - Valid User



VulnApp - Wrong User



VulnApp - AndroidManifest.xml

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents

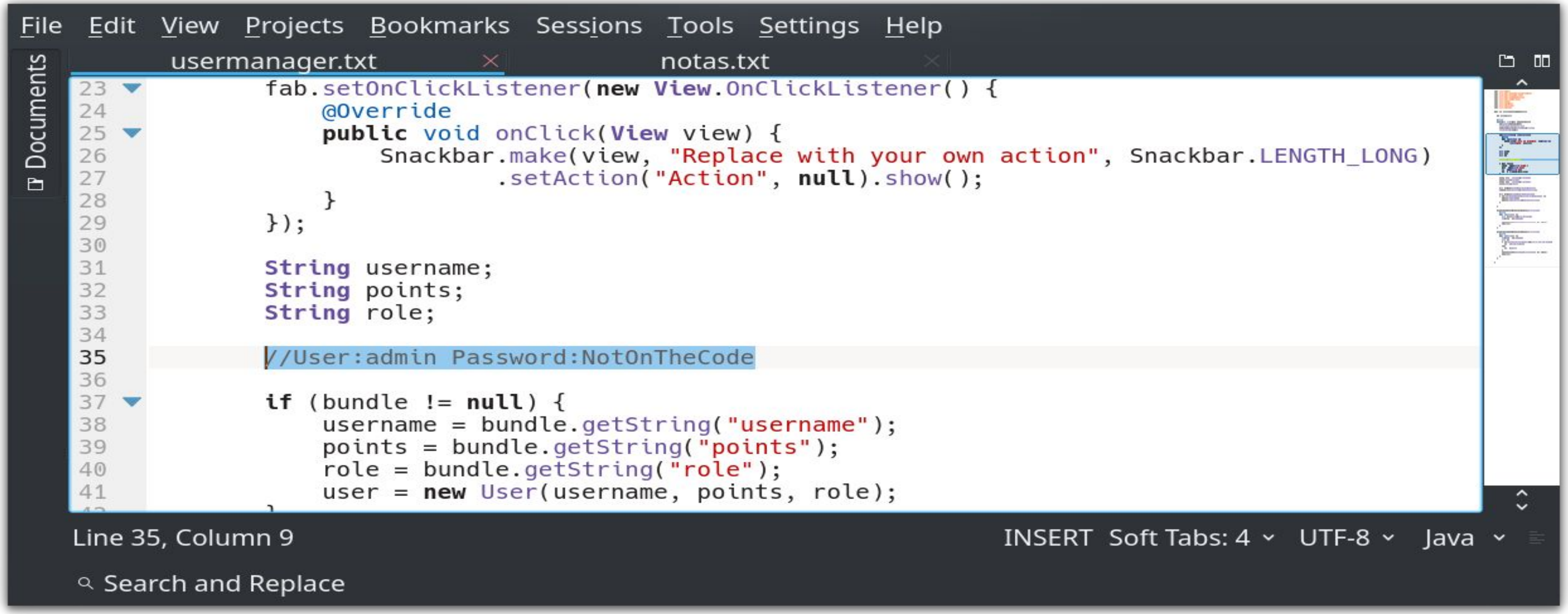
AndroidManifest.xml | notas.txt

```xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android"
android:compileSdkVersion="28" android:compileSdkVersionCodename="9" package="pt.oposec.vulnapp" platformBuildVersionCode="1"
platformBuildVersionName="1.0">
    <uses-permission android:name="android.permission.INTERNET"/>
    <application android:allowBackup="true" android:appComponentFactory="android.support.v4.app.CoreComponentFactory" android:debuggable="true"
    android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:roundIcon="@mipmap/ic_launcher_round" android:supportsRtl="true"
    android:testOnly="true" android:theme="@style/AppTheme">
        <activity android:label="@string/app_name" android:name="pt.oposec.vulnapp.MainActivity" android:theme="@style/AppTheme.NoActionBar">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:exported="true" android:label="@string/title_activity_user" android:name="pt.oposec.vulnapp.UserActivity"
        android:theme="@style/AppTheme.NoActionBar"/>
    </application>
</manifest>
```

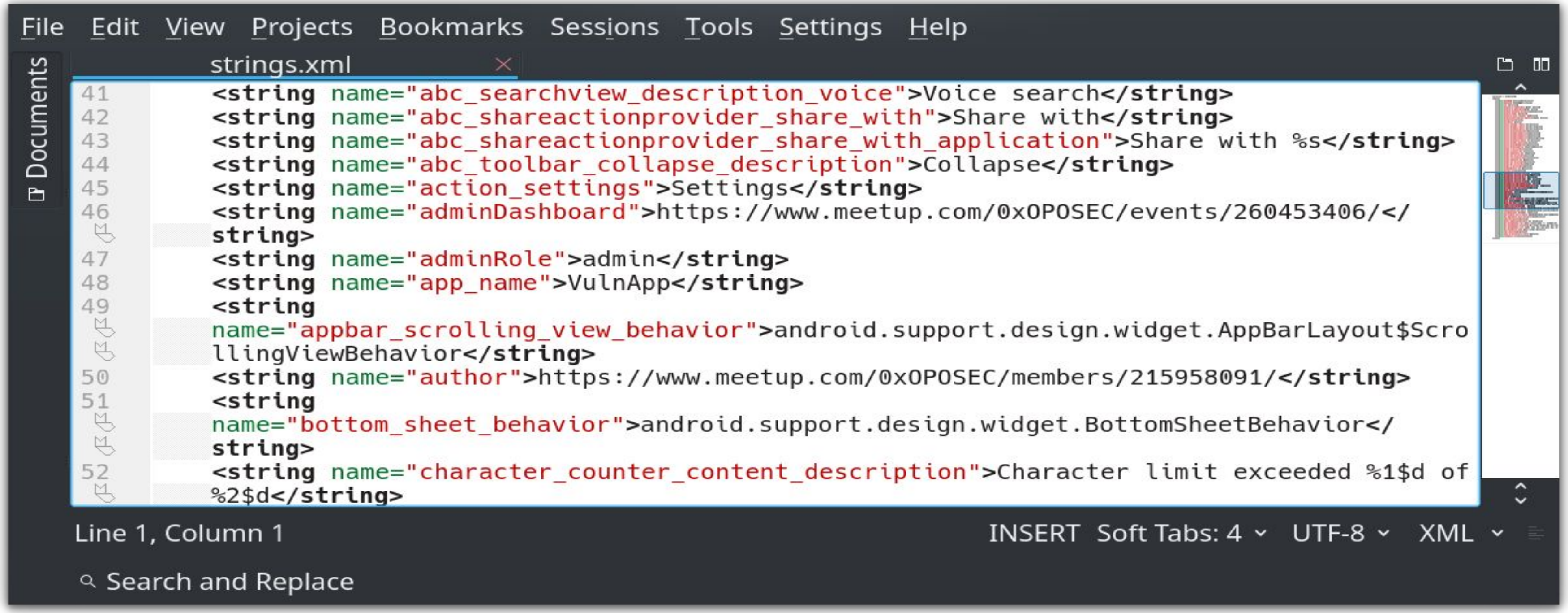
Line 12, Column 12 INSERT Soft Tabs: 4 UTF-8 XML

Search and Replace

VulnApp - Information left inside APK

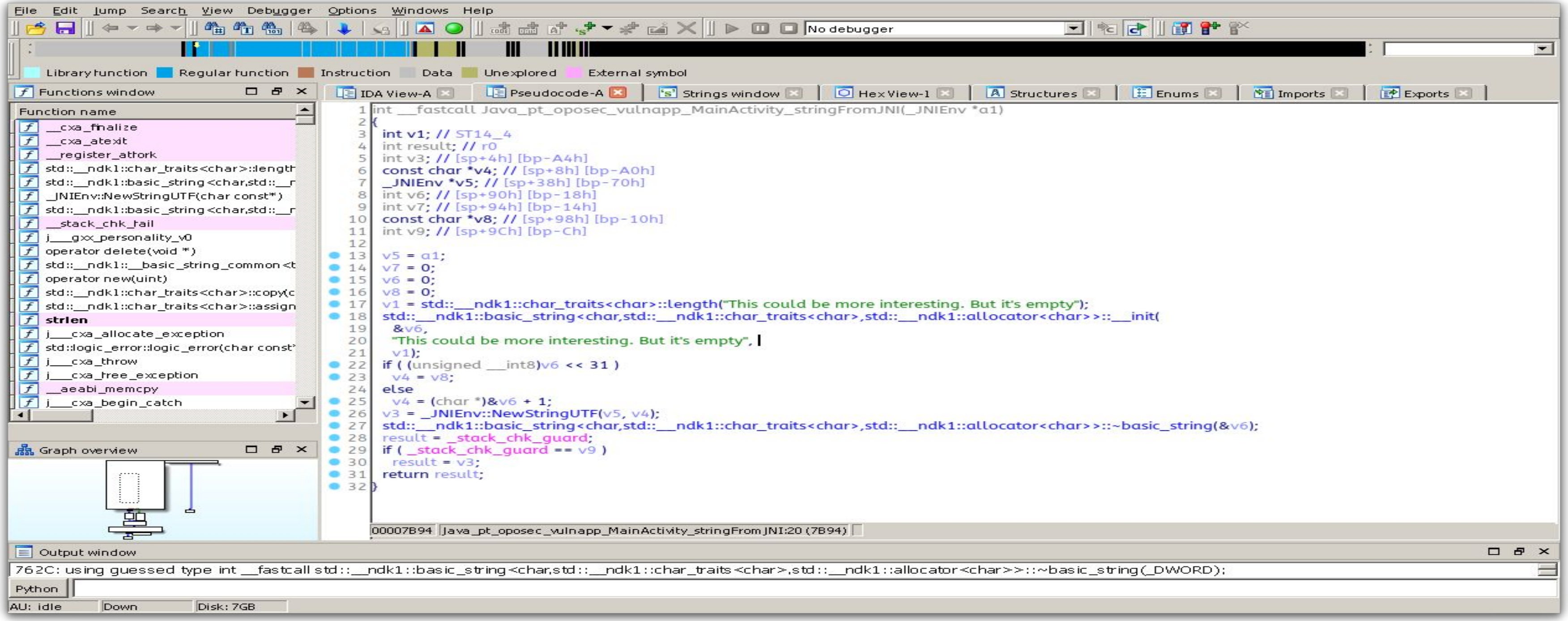


VulnApp - Information left inside APK

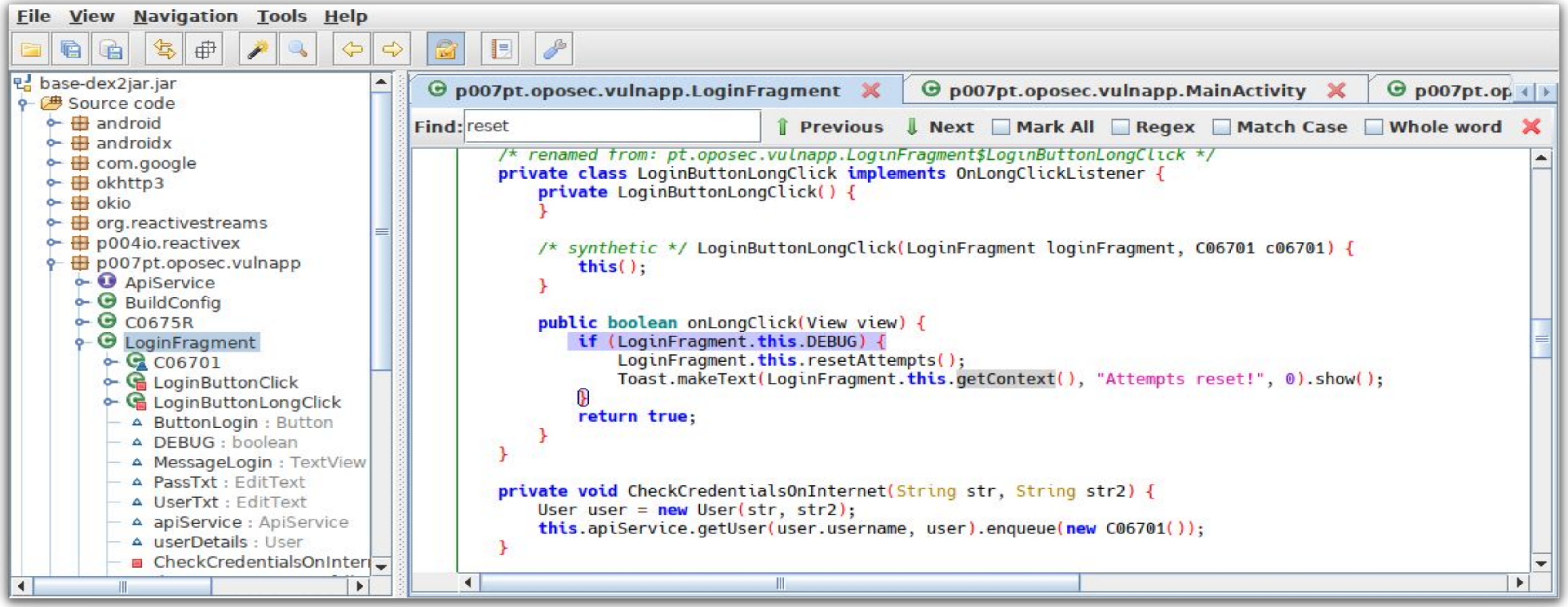



```xml
<string name="abc_searchview_description_voice">Voice search</string>
<string name="abc_shareactionprovider_share_with">Share with</string>
<string name="abc_shareactionprovider_share_with_application">Share with %s</string>
<string name="abc_toolbar_collapse_description">Collapse</string>
<string name="action_settings">Settings</string>
<string name="adminDashboard">https://www.meetup.com/0xOPOSEC/events/260453406/</string>
<string name="adminRole">admin</string>
<string name="app_name">VulnApp</string>
<string name="appbar_scrolling_view_behavior">android.support.design.widget.AppBarLayout$ScrollingViewBehavior</string>
<string name="author">https://www.meetup.com/0xOPOSEC/members/215958091/</string>
<string name="bottom_sheet_behavior">android.support.design.widget.BottomSheetBehavior</string>
<string name="character_counter_content_description">Character limit exceeded %1$d of %2$d</string>
```

VulnApp - Information left inside APK

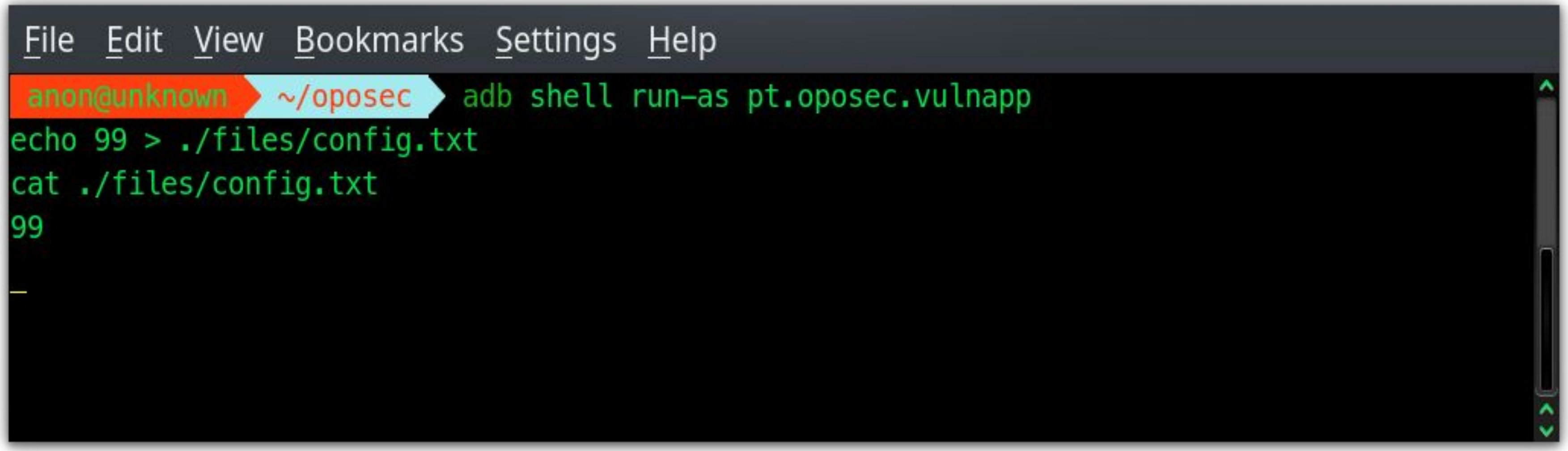


VulnApp - Dev features

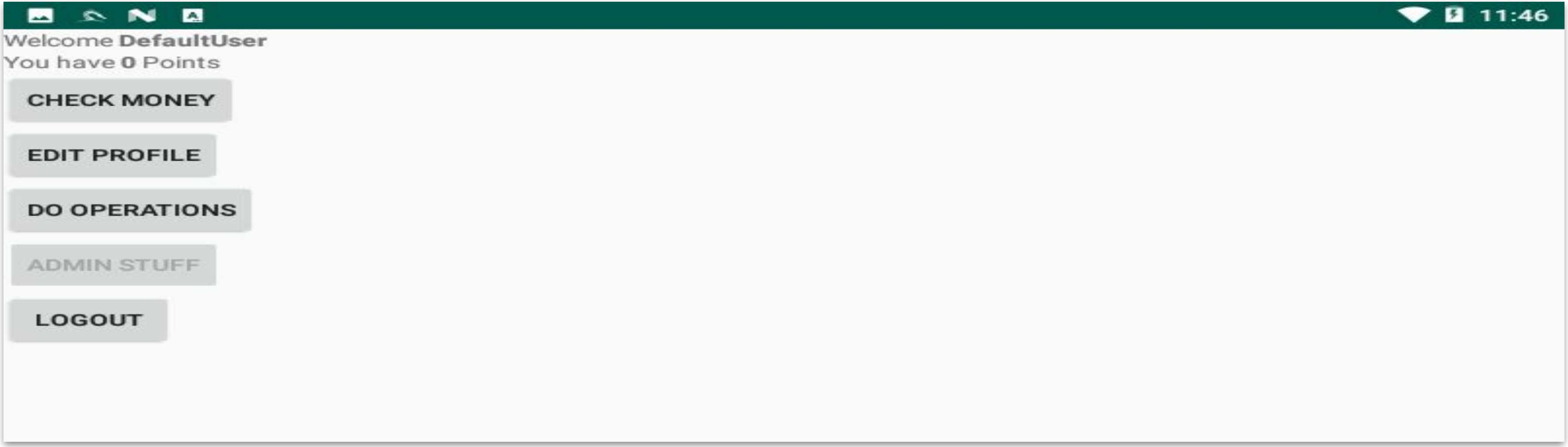


VulnApp - Debuggable Feature (1/2)

VulnApp - Debuggable Feature (2/2)



VulnApp - Exported Activity



adb shell am start -n pt.oposec.vulnapp/.UserActivity

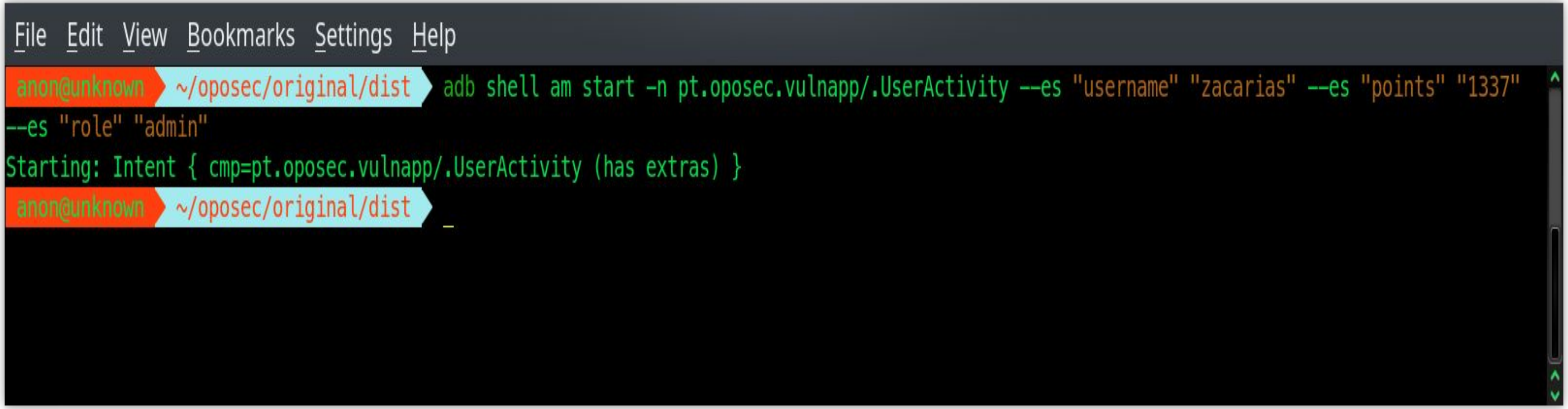
VulnApp - Backup/Restore Feature (1/2)

```
File  Edit  View  Bookmarks  Settings  Help
anon@unknown  ~/oposec  adb backup -f backup.ab pt.oposec.vulnapp
Now unlock your device and confirm the backup operation...
anon@unknown  ~/oposec  abe unpack backup.ab backup_opo.tar 123456
Calculated MK checksum (use UTF-8: true): 764D23C2736F81C0787764034E17492E27BDE03A3DDDF395A36B80B8A237A476
43% 53%
3584 bytes written to backup_opo.tar.
anon@unknown  ~/oposec  x backup_opo.tar
apps/pt.oposec.vulnapp/_manifest
apps/pt.oposec.vulnapp/f/config.txt
anon@unknown  ~/oposec  _
```

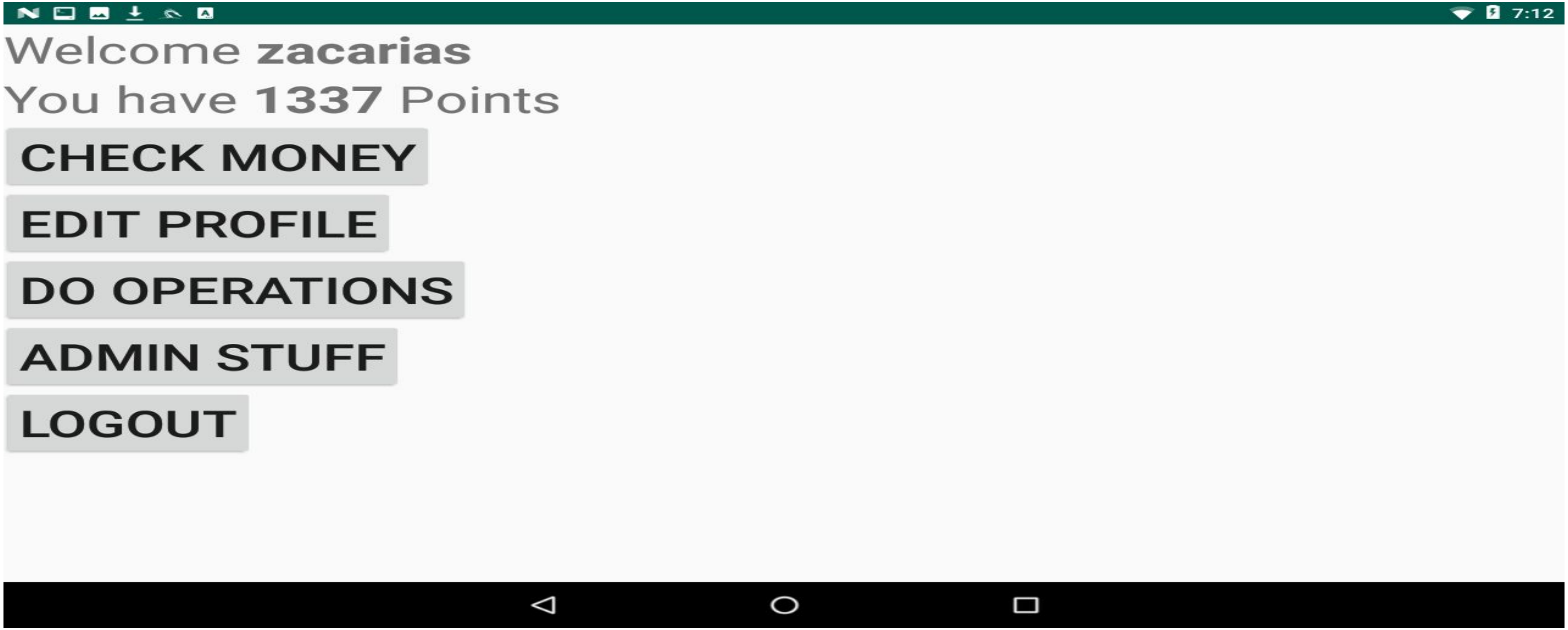
VulnApp - Backup/Restore Feature (2/2)

```
File  Edit  View  Bookmarks  Settings  Help
anon@unknown  ~/oposec  echo 99 > apps/pt.oposec.vulnapp/f/config.txt
anon@unknown  ~/oposec  tar -tf backup_opo.tar > backup_opo.list
anon@unknown  ~/oposec  cat backup_opo.list | grep pt.oposec.vulnapp > vulnapp.list
anon@unknown  ~/oposec  cat vulnapp.list | pax -wd > vulnapp.tar
anon@unknown  ~/oposec  abe pack vulnapp.tar vulnapp.ab 123456
10240 bytes written to vulnapp.ab.
anon@unknown  ~/oposec  adb restore vulnapp.ab
Now unlock your device and confirm the restore operation.
anon@unknown  ~/oposec  _
```

VulnApp - Exported Activity (1/2)



VulnApp - Exported Activity (2/2)



VulnApp - Patch & Recompile (1/2)

File Edit View Projects Bookmarks Sessions Tools Settings Help

Documents

LoginFragment...ngClick.smali

```

# virtual methods
.method public onLongClick(Landroid/view/View;)Z
    .locals 4
    .param p1, "v"    # Landroid/view/View;

    .line 238
    const-string v0, "I\'m a lazy dev, I leave debug features on my app"

    .line 239
    .local v0, "aaa":Ljava/lang/String;
    iget-object v1, p0, Lpt/oposec/vulnapp/LoginFragment$LoginButtonLongClick;->this$0:Lpt/oposec/vulnapp/LoginFragment;

    iget-boolean v1, v1, Lpt/oposec/vulnapp/LoginFragment;->DEBUG:Z

    #if-eqz v1, :cond_0

    .line 240
    iget-object v1, p0, Lpt/oposec/vulnapp/LoginFragment$LoginButtonLongClick;->this$0:Lpt/oposec/vulnapp/LoginFragment;

    invoke-static {v1}, Lpt/oposec/vulnapp/LoginFragment;->access$200(Lpt/oposec/vulnapp/LoginFragment;)V

    .line 241
    const-string v1, "Attempts reset!"

    .line 242
```

Line 62, Column 24

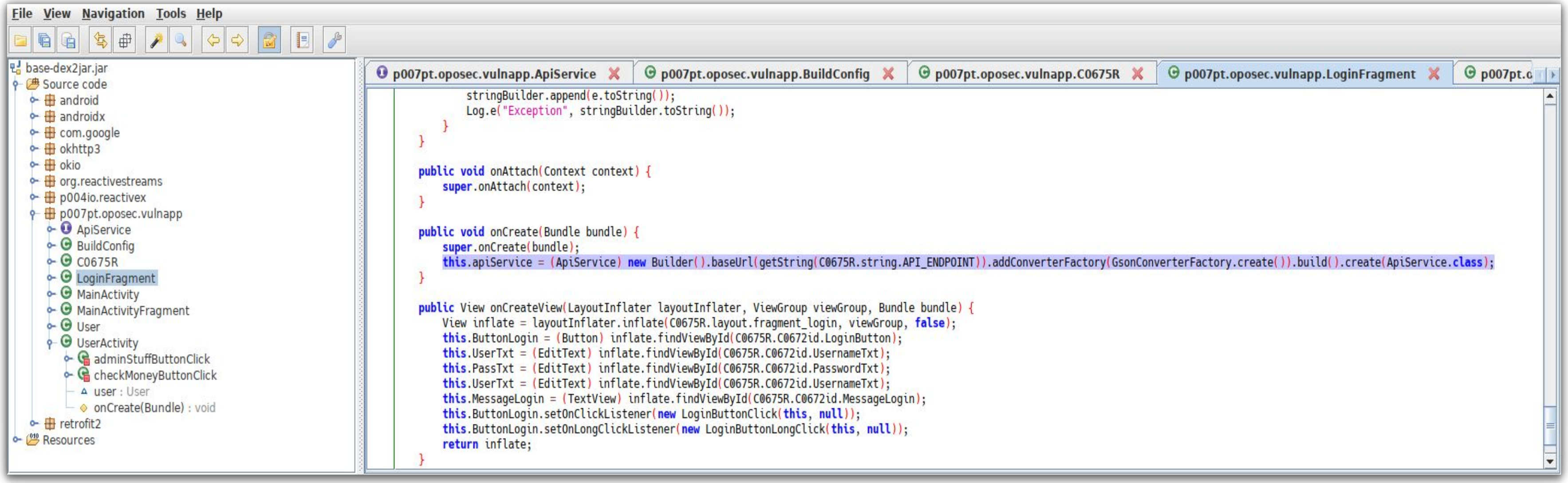
INSERT Soft Tabs: 4 UTF-8 Normal

Search and Replace

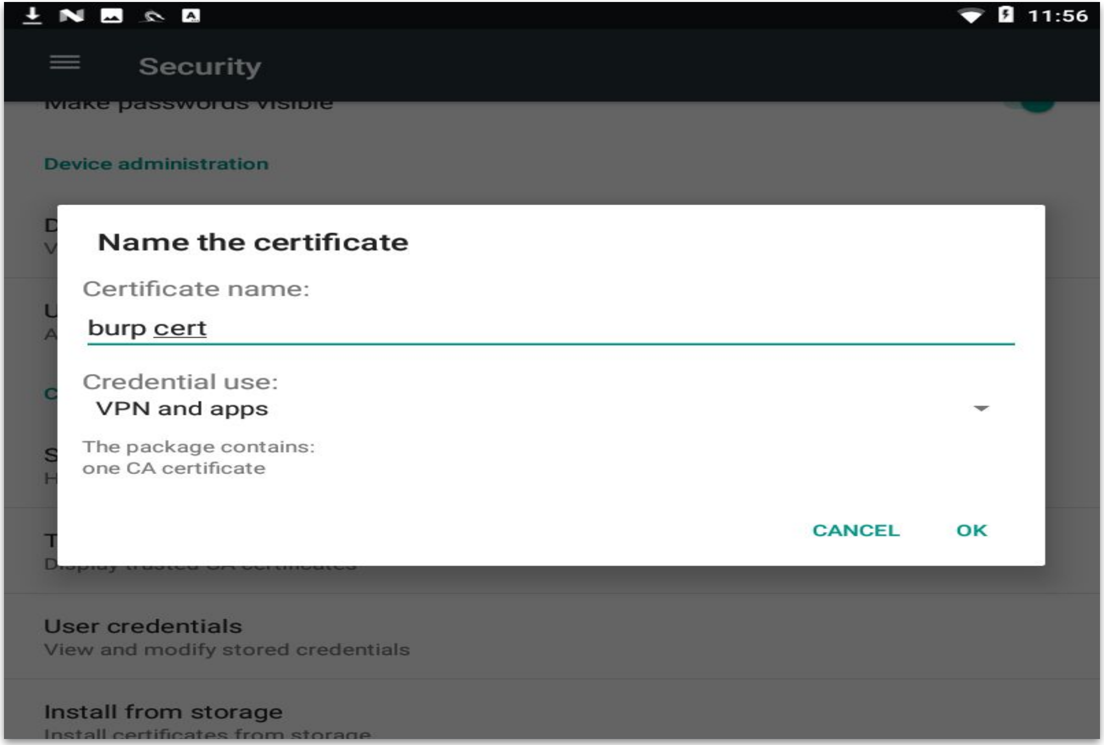
VulnApp - Patch & Recompile (2/2)

```
File  Edit  View  Bookmarks  Settings  Help
anon@unknown  ~/oposec  apktool b original
I: Using Apktool 2.3.4
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
anon@unknown  ~/oposec  cd original/dist
anon@unknown  ~/oposec/original/dist  assina original.apk
jar signed.

Warning:
The signer's certificate is self-signed.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to validate this jar after
the signer certificate's expiration date (2045-01-01) or after any future revocation date.
anon@unknown  ~/oposec/original/dist  adb install original.apk
Success
anon@unknown  ~/oposec/original/dist  _
```

VulnApp - No certificate Pinning



Traffic Interception - Install CA must have SDK < 23



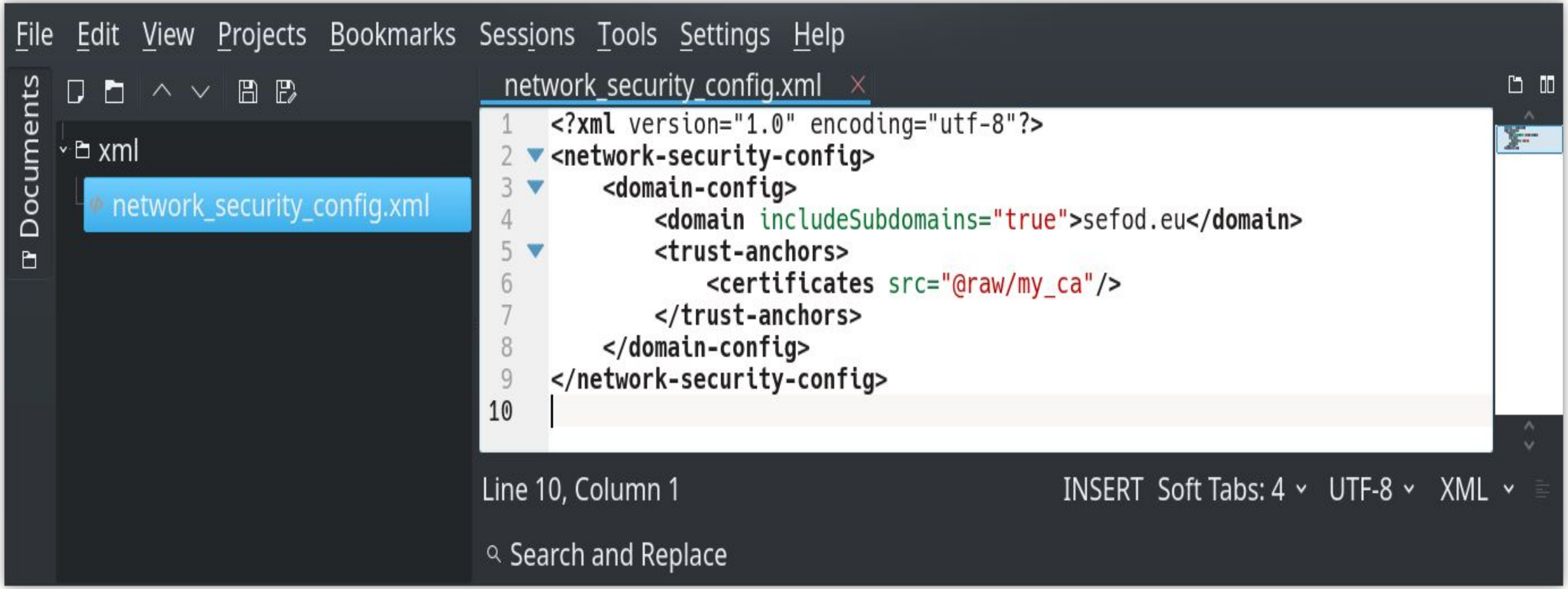
Traffic Interception - Install CA must have SDK >= 23 (1/4)

AndroidManifest.xml

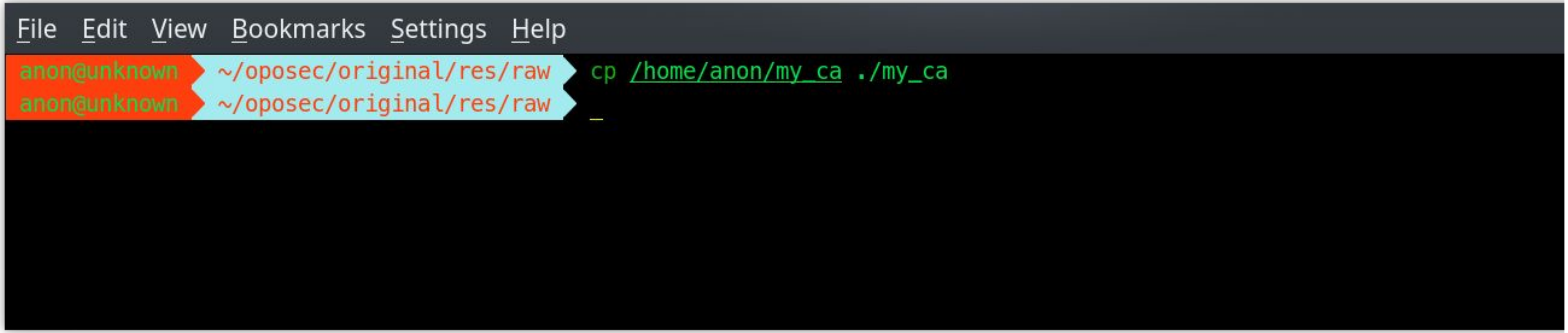
```xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android"
android:compileSdkVersion="28" android:compileSdkVersionCodename="9" package="pt.oposec.vulnapp" platformBuildVersionCode="1"
platformBuildVersionName="1.0">
    <uses-permission android:name="android.permission.INTERNET"/>
    <application android:networkSecurityConfig="@xml/network_security_config" android:allowBackup="true"
    android:appComponentFactory="android.support.v4.app.CoreComponentFactory" android:debuggable="true" android:icon="@mipmap/
    ic_launcher" android:label="@string/app_name" android:roundIcon="@mipmap/ic_launcher_round" android:supportsRtl="true"
    android:theme="@style/AppTheme">
        <activity android:label="@string/app_name" android:name="pt.oposec.vulnapp.MainActivity" android:theme="@style/
        AppTheme.NoActionBar">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:exported="true" android:label="@string/title_activity_user" android:name="pt.oposec.vulnapp.UserActivity"
        android:theme="@style/AppTheme.NoActionBar"/>
    </application>
</manifest>
```

Line 3, Column 18 INSERT Soft Tabs: 4 UTF-8 XML

Traffic Interception - Install CA must have SDK >= 23 (2/4)



Traffic Interception - Install CA must have SDK >= 23 (3/4)



Traffic Interception - Install CA must have SDK >= 23 (4/4)

```
File  Edit  View  Bookmarks  Settings  Help
anon@unknown  ~/oposec  apktool b original
I: Using Apktool 2.3.4
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
anon@unknown  ~/oposec  cd original/dist
anon@unknown  ~/oposec/original/dist  assina original.apk
jar signed.

Warning:
The signer's certificate is self-signed.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to validate this jar after
the signer certificate's expiration date (2045-01-01) or after any future revocation date.
anon@unknown  ~/oposec/original/dist  adb install original.apk
Success
anon@unknown  ~/oposec/original/dist  _
```

OWASP - Mobile Top 10 2016

- M1-Improper Platform Usage
- M2-Insecure Data Storage
- M3-Insecure Communication
- M4-Insecure Authentication
- M5-Insufficient Cryptography
- M6-Insecure Authorization
- M7-Poor Code Quality
- M8-Code Tampering
- M9-Reverse Engineering
- M10-Extraneous Functionality

OWASP
Open Web Application
Security Project

Other Resources

- Qark - https://github.com/linkedin/qark
- Drozer - https://github.com/mwrlabs/drozer
- Frida - https://github.com/frida/
- Android-security-awesome - https://github.com/ashishb/android-security-awesome
- OWASP ASVS - https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
- OWASP Mob Testing Guide - https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide

END