



CTF MAKER	Kyle B3nac
CTF NAME	Injured_Android
CTF PLATFORM	ANDROID

الأدوات :

- APKTOOL
- DEX2JAR
- JD-GUI
- ARTK

المعلومات :

- عكس تطبيق الاندرويد
- تحليل [androidmanifest.xml](#)
- استغلال ثغره [PendingIntent](#)
- انشاء تطبيق لاستغلال الثغره

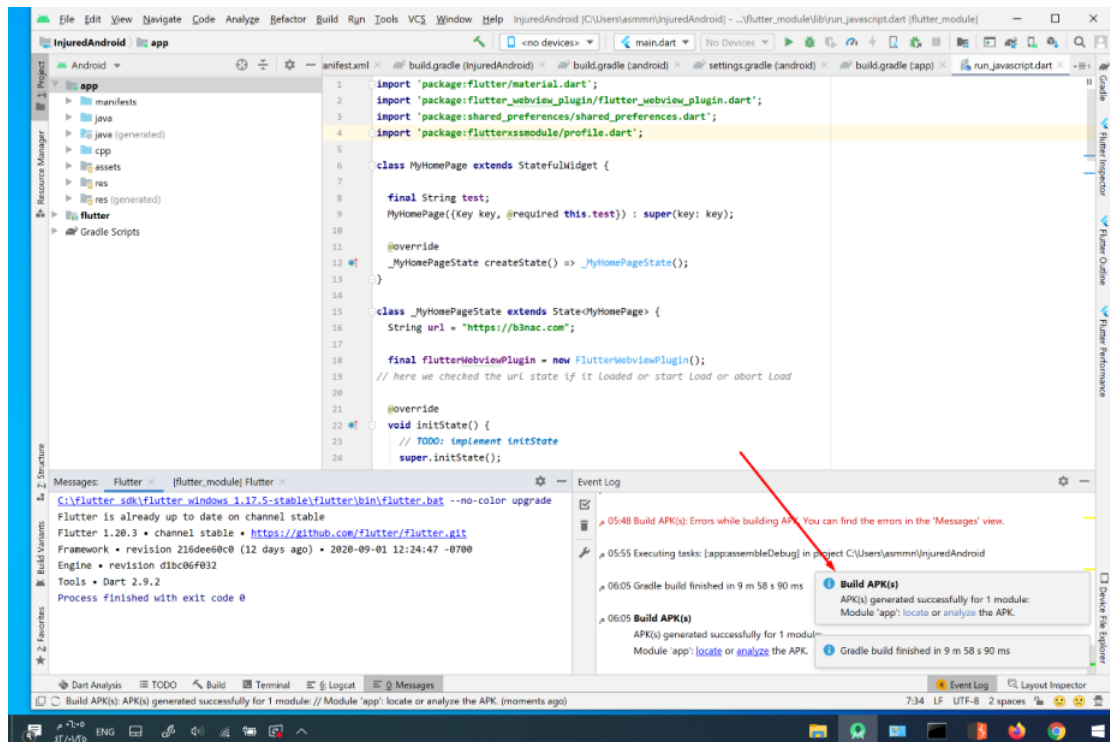
تنوية :

ال CTF فيه اكثر من فلاق واكثر من ثغره ولكن المتطرق له هو ال **PendingIntent** وتكلمت عنها بالمختصر في قناة ال mobile-pentest

● البداية :

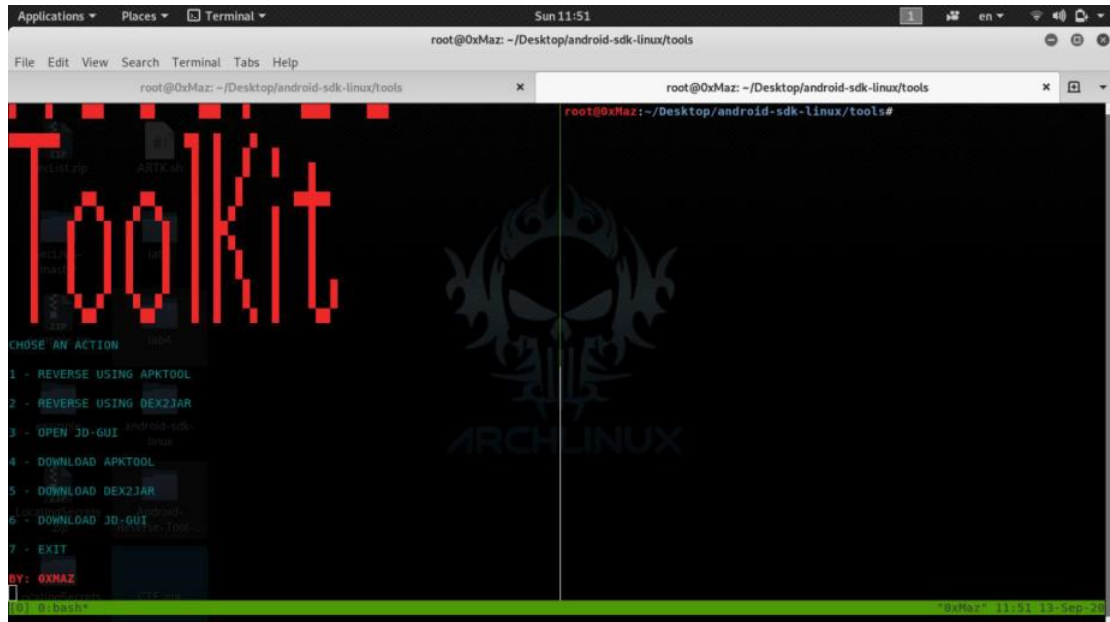
فالبداية مطور ال CTF حط السورس كود الخاص بالتطبيق ولازم انك تحل المشاكل وبعد كذا تسوي له كومبايل

Build from source Build steps in progress. The flutter module makes this slightly more complicated



• عكس التطبيق :

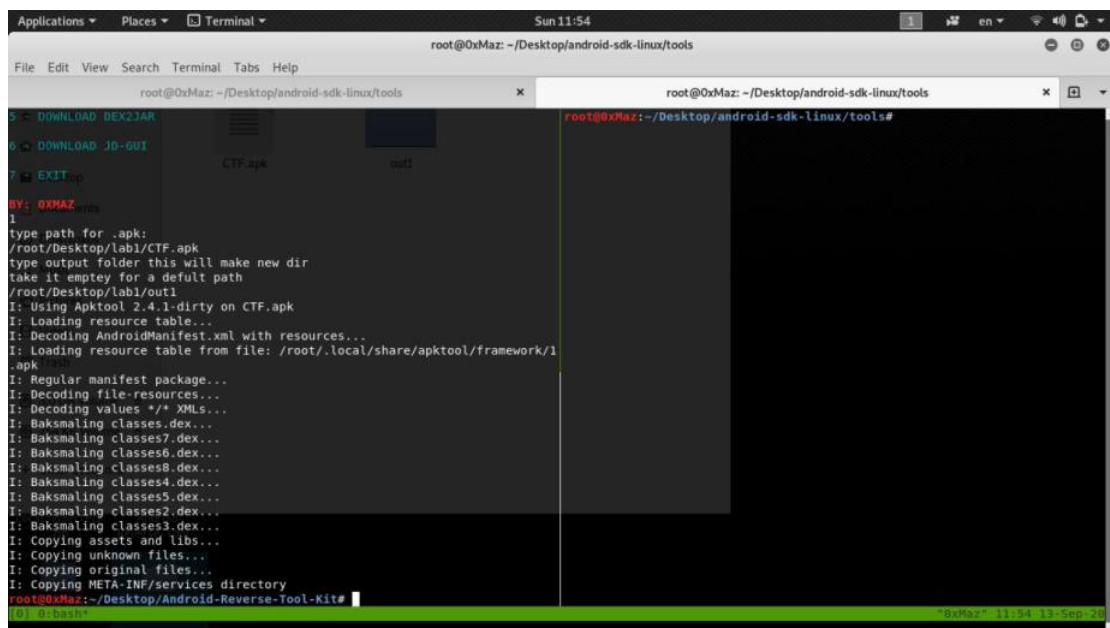
اول خطوه سويت ريفيرس للتطبيق :



```
root@0xMaz: ~/Desktop/android-sdk-linux/tools
root@0xMaz: ~/Desktop/android-sdk-linux/tools#

ToolKit

CHOOSE AN ACTION
1 - REVERSE USING APKTOOL
2 - REVERSE USING DEX2JAR
3 - OPEN JD-GUI
4 - DOWNLOAD APKTOOL
5 - DOWNLOAD DEX2JAR
6 - DOWNLOAD JD-GUI
7 - EXIT
BY: 0xMAZ
[0] 0:ibash*
```



```
root@0xMaz: ~/Desktop/android-sdk-linux/tools
root@0xMaz: ~/Desktop/android-sdk-linux/tools#

5 - DOWNLOAD DEX2JAR
6 - DOWNLOAD JD-GUI
7 - EXIT
BY: 0xMAZ
1
type path for .apk:
/root/Desktop/lab1/CTF.apk
type output folder this will make new dir
take it empty for a default path
/root/Desktop/lab1/out1
I: Using Apktool 2.4.1-dirty on CTF.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1
.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */*.xmls...
I: Baksmaling classes.dex...
I: Baksmaling classes7.dex...
I: Baksmaling classes6.dex...
I: Baksmaling classes8.dex...
I: Baksmaling classes4.dex...
I: Baksmaling classes5.dex...
I: Baksmaling classes2.dex...
I: Baksmaling classes3.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory
root@0xMaz: ~/Desktop/Android-Reverse-Tool-Kite
[0] 0:ibash*
```


راح نبداً بملف ال androidmanifest.xml

```
GNU nano 5.2      AndroidManifest.xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:and>
  <uses-permission android:name="android.permission.ACCESS_NETWORK_STAT>
  <uses-permission android:name="android.permission.INTERNET"/>
  <uses-permission android:name="android.permission.WRITE_EXTERNAL STOR>
  <uses-permission android:name="android.permission.READ_PHONE STATE"/>
  <uses-permission android:name="android.permission.READ_EXTERNAL STORA>
  <application android:appComponentFactory="androidx.core.app.CoreCompo>
    <activity android:label="@string/title_activity_assembly" android>
    <activity android:configChanges="density|fontScale|keyboard|keybo>
    <activity android:label="@string/title_activity_rce" android:name>
      <intent-filter android:label="filter_view_flag11">
        <action android:name="android.intent.action.VIEW"/>
        <category android:name="android.intent.category.DEFAULT"/>
        <category android:name="android.intent.category.BROWSABLE>
        <data android:host="rce" android:scheme="flag13"/>
      </intent-filter>
    </activity>
    <activity android:name="b3nac.injuredandroid.SettingsActivity"/>
    <activity android:exported="true" android:label="@string/title_ad>
    <activity android:exported="true" android:name="b3nac.injuredandr>
    <activity android:label="@string/title_activity_flag_twelve_prote>
    <activity android:label="@string/title_activity_deep_link" android>
      <intent-filter android:label="filter_view_flag11">
        <action android:name="android.intent.action.VIEW"/>
        <category android:name="android.intent.category.DEFAULT"/>
        <category android:name="android.intent.category.BROWSABLE>
        <data android:scheme="flag11"/>
      </intent-filter>
      <intent-filter android:label="filter_view_flag11">
        <action android:name="android.intent.action.VIEW"/>

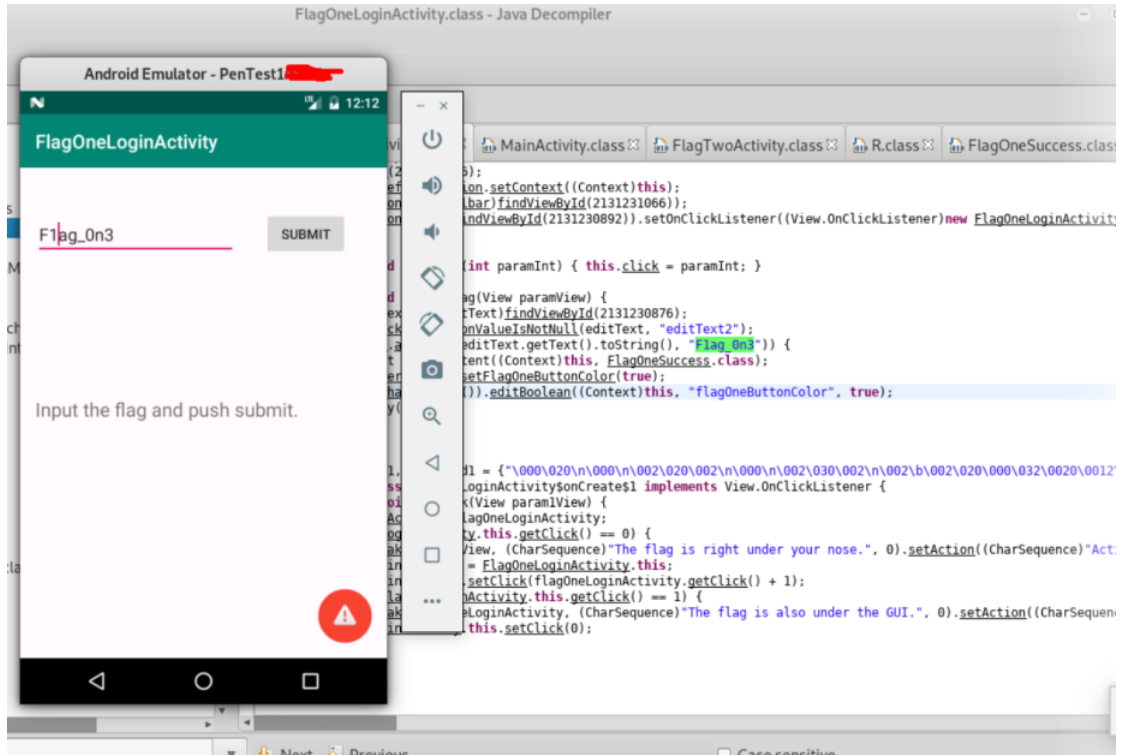
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify

"0xMaz" 11:59 13-Sep-20

بدايه حصلنا معلومه جميله وهو فلتر لل intent

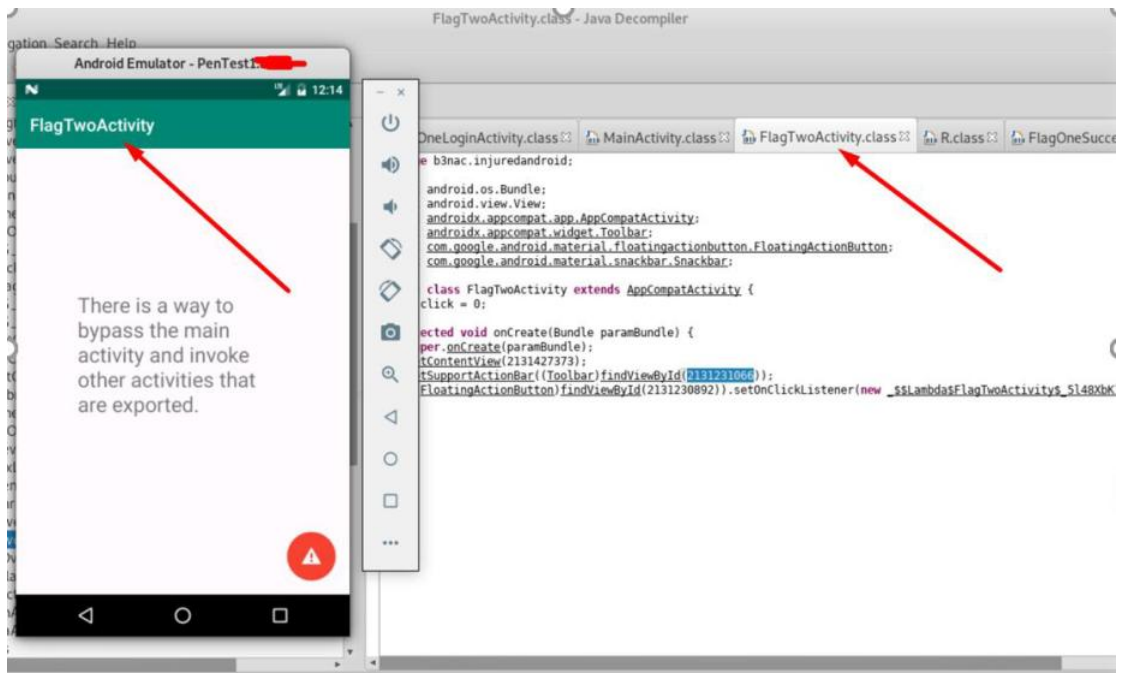
بعد كذا نستمر في التحليل وننتقل للكود



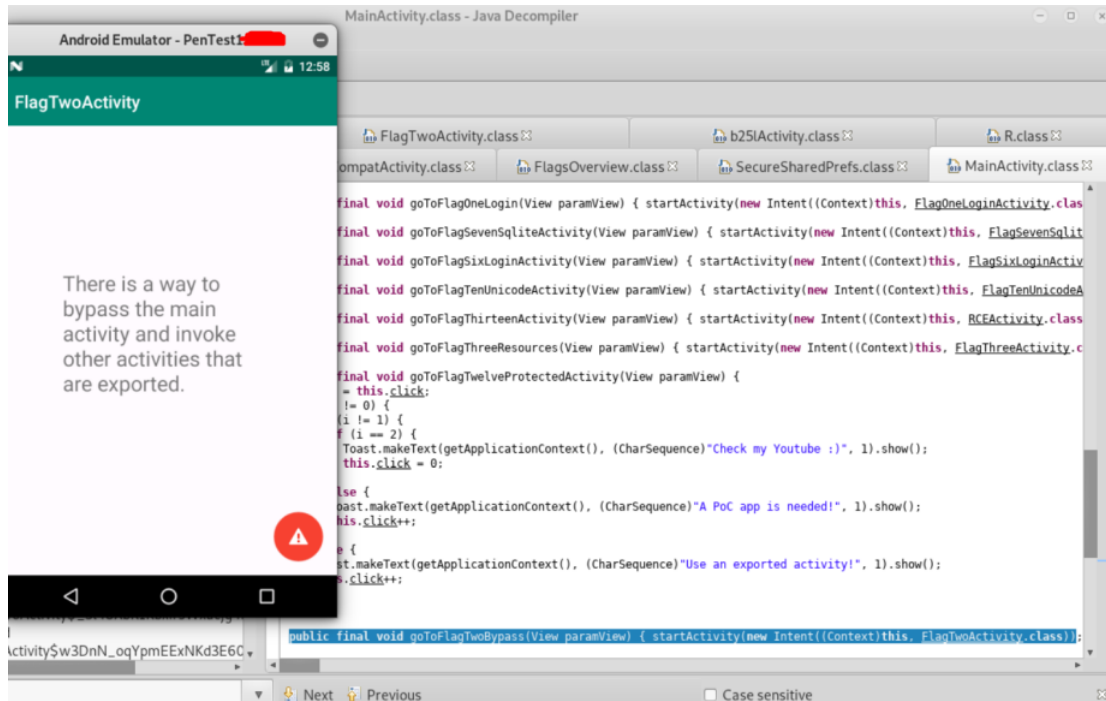
ضمن البحث حصلنا الفلاق للتحدي الأول (١)

ولكن مو هذا اللي يهمنى

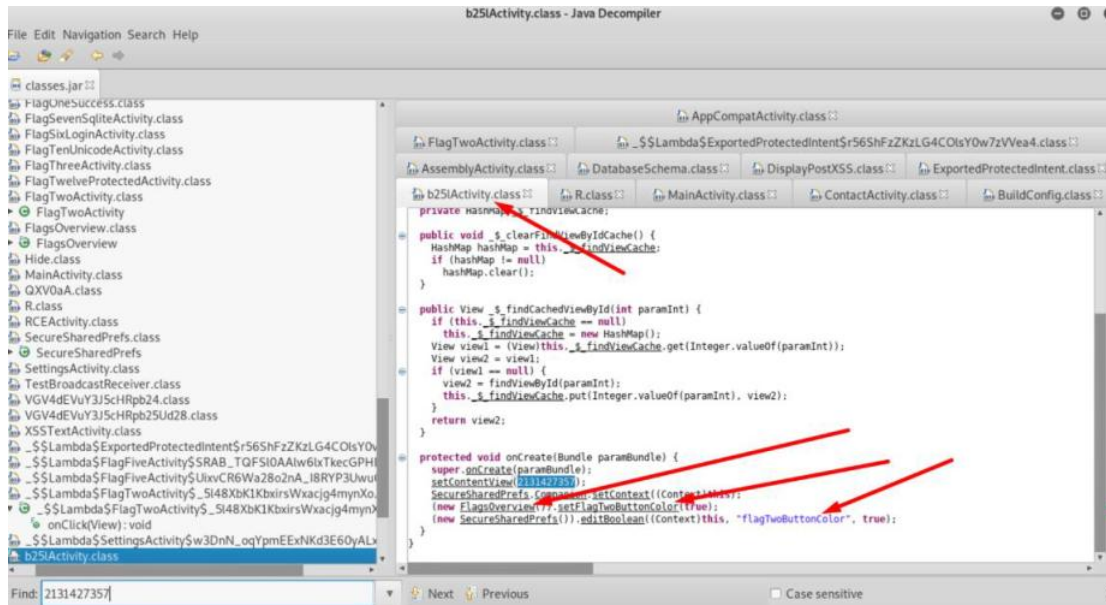
نستمر في التحليل ونتعمق اكثر



حصلنا الكلاس الخاص بالفلاق الثاني (وهو اللي يهمنى لانه متضمن للثغره)

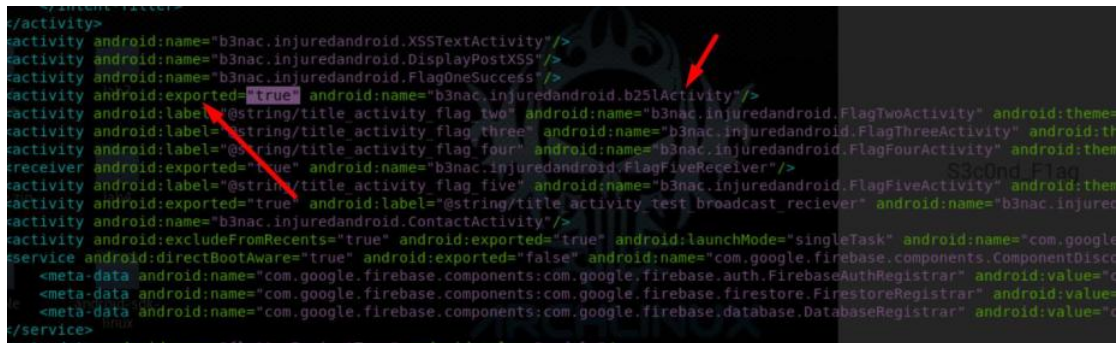


حصلنا كلاس وكانه راح يفيدنا ، نستمر برضه بالتحليل



برضه كلاس ثاني واسمه غريب ومرتب بالكلاس اوفر فيو ومنه مرتبط بفلاق 2 كلاس

نبحث عنه في androidmanifest.xml



```
<activity android:name="b3nac.injuredandroid.XSSTextActivity"/>
<activity android:name="b3nac.injuredandroid.DisplayPostXSS"/>
<activity android:name="b3nac.injuredandroid.FlagOneSuccess"/>
<activity android:exported="true" android:name="b3nac.injuredandroid.b25lActivity"/>
<activity android:label="@string/title_activity_flag_two" android:name="b3nac.injuredandroid.FlagTwoActivity" android:theme="@style/Theme.AppCompat.NoActionBar"/>
<activity android:label="@string/title_activity_flag_three" android:name="b3nac.injuredandroid.FlagThreeActivity" android:theme="@style/Theme.AppCompat.NoActionBar"/>
<activity android:label="@string/title_activity_flag_four" android:name="b3nac.injuredandroid.FlagFourActivity" android:theme="@style/Theme.AppCompat.NoActionBar"/>
<receiver android:exported="true" android:name="b3nac.injuredandroid.FlagFiveReceiver"/>
<activity android:label="@string/title_activity_flag_five" android:name="b3nac.injuredandroid.FlagFiveActivity" android:theme="@style/Theme.AppCompat.NoActionBar"/>
<activity android:exported="true" android:label="@string/title_activity_test_broadcast_reciever" android:name="b3nac.injuredandroid.TestBroadcastReceiver"/>
<activity android:name="b3nac.injuredandroid.ContactActivity"/>
<service android:directBootAware="true" android:exported="false" android:name="com.google.firebase.components.ComponentDiscoveryService" android:permission="android.permission.BIND_JOB_SERVICE">
    <meta-data android:name="com.google.firebase.components:com.google.firebase.auth.FirebaseAuthRegistrar" android:value="com.google.firebase.auth.FirebaseAuthRegistrar" />
    <meta-data android:name="com.google.firebase.components:com.google.firebase.firestore.FirestoreRegistrar" android:value="com.google.firebase.firestore.FirestoreRegistrar" />
    <meta-data android:name="com.google.firebase.components:com.google.firebase.database.DatabaseRegistrar" android:value="com.google.firebase.database.DatabaseRegistrar" />
</service>
```

نلاحظ اننا نقدر نسوي له exported

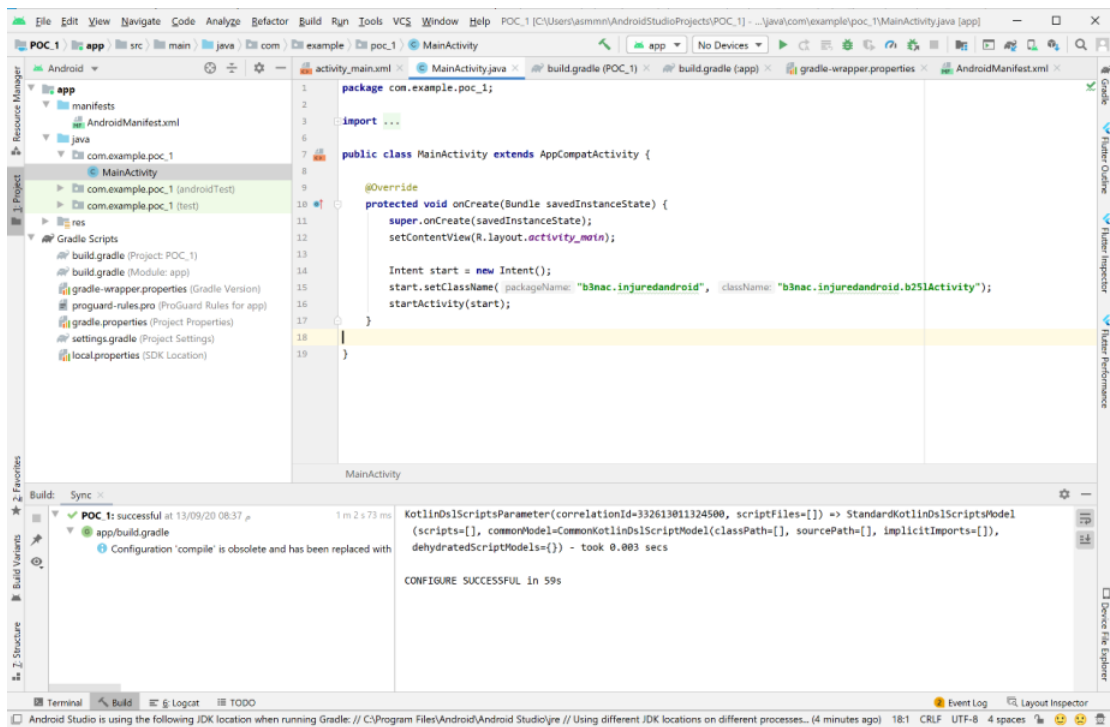
خلونا نشرحها ع السريع :

يسمونها ال content providers ومهمتها هي مشاركة ال structured data بين التطبيقات وعن طريقها تقدر تسمح للتطبيقات بالتواصل مع التطبيق الخاص بك عن طريق ال androidmanifest.xml زي ماحنا شايفين ان الكلاسb25 نقدر نسوي له اكسبورت لان موجود صلاحية

وموجود عندنا في AndroidManifest ثلاث انشطه او كلاسات نقدر نسوي لها exported وهو MainActivity وهو نقدر نسوي له exported افتراضيا لان فيه عامل تصفيه نيه intent filter وبرزه عندنا TestBroadcastReceiver و b25lActivity وهي exported عن طريق الصلاحيات الموجوده في AndroidManifest زي مو موضح في الصورة

• الاختراق :

نجي الحين للخطوة المهمة وهي استغلال ال pendingintent vulnerability راح اسوي كود يوضح ويفصل طريقه عمل الثغره بطريقه برمجيه



شرح مبسط للكود :

سويت intent اسمها start بعدها استدعيت البكج الخاص بالتطبيق وبعده الكلاس المصاب بالثغره، وبعد بكل بساطه سويت تشغيل لل intent اللي سويتها

فيديو لطريقه عمل الثغره وراح يوضح لكم اكثر :

[فتح الفيديو فالمتصفح](#)