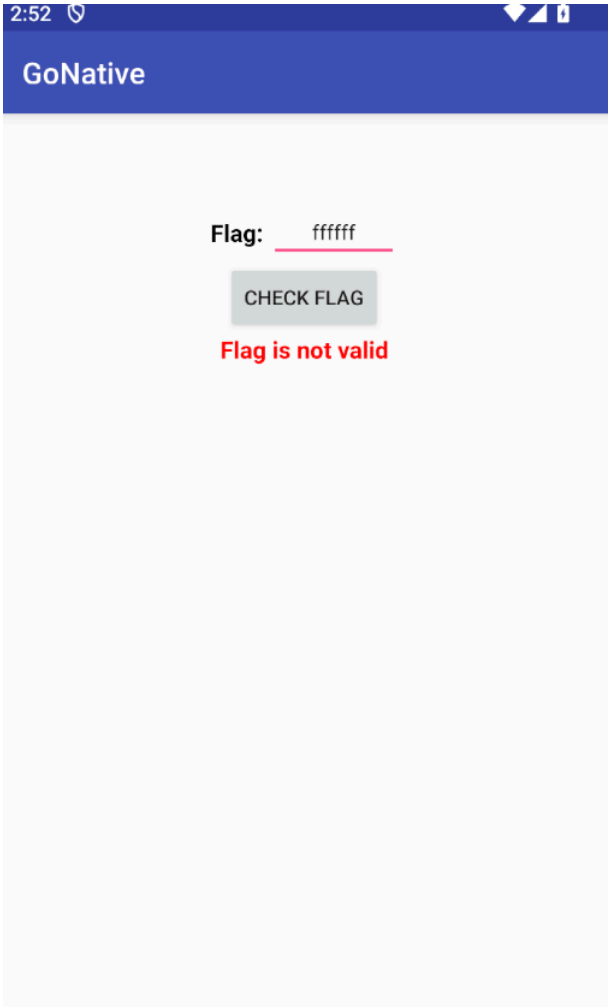
4-GoinNative - reverse engineering

هنا هو عايز يعرف ايه Flag



1- Check the ManiFest.xml If contain any activity

بس هو في MainActivity فقط فمش هنستفاد منه بحاجة

```xml
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="1"
    android:versionName="1.0"
    package="com.mobisec.gonative">
    <uses-sdk
        android:minSdkVersion="23"
        android:targetSdkVersion="23"/>
    <application
        android:theme="@style/AppTheme"
        android:label="@string/app_name"
        android:icon="@mipmap/ic_launcher"
        android:allowBackup="true"
        android:supportsRtl="true"
        android:roundIcon="@mipmap/ic_launcher_round"
        android:appComponentFactory="android.support.v4.app.CoreComponentFactory">
        <activity android:name="com.mobisec.gonative.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

2- Check checkFlag file

FlagChecker | AndroidManifest.xml

```java
package com.mobisec.gonative;

/* loaded from: classes.dex */
class FlagChecker {
    private static native boolean helloFromTheOtherSide(String str, int i);

    FlagChecker() {
    }

    static {
        System.loadLibrary("native-lib");
    }

    public static boolean checkFlag(String str) {
        String[] split = str.split("-");
        if (split.length != 2 || !split[0].startsWith("MOBISEC{") || !split[1].endsWith("}")) {
            return false;
        }
        String replace = split[0].replace("MOBISEC{", BuildConfig.FLAVOR);
        String replace2 = split[1].replace("}", BuildConfig.FLAVOR);
        if (replace2.matches("^[0-9]*$") && replace2.length() == 6) {
            return helloFromTheOtherSide(replace, Integer.parseInt(replace2));
        }
        return false;
    }
}
```

هنشوف ده بقي خطوة خطوة

1-check flag function

دي فانكشن بتاخد string الل هو flag وب**تحوله من string to array باستخدام split وبتشيل -** وبعد كده بتشوف ان arrray يحتوي علي قيمتين وان اول قيمة هي تبدا ب MOBISEC{ وان القيمة التانية تنتهي ب }

str --> MOBISEC{XXXXX-XXXXXXXX}

split ---> ["MOBISEC{XXXXX", "XXXXXXX}"]

split[0] --> "MOBISEC{XXXXX"

split[1] --> "XXXXXXX}"

```
    public static boolean checkFlag(String str) {
        String[] split = str.split("-");
        if (split.length != 2 || !split[0].startsWith("MOBISEC{") ||
!split[1].endsWith("}")) {
            return false;
        }
```

2-check part2 on code

هنا اه بيعمل replace للجزء اللي في القيكة الاولي اللي هي MOBISEC{ ب القيمة دي BuildConfig.FLAVOR اللي لو شوفناها هنلاقيها عبارة عن "" وبيخش علي القيمة التانية برده بيعمل replace لل } ب BuildConfig.FLAVOR بعد كده بيروح للقيمة التانية بيقول ان هي عبارة عن 6 ارقام من 0-9 وبس

before replace

split[0] --> "MOBISEC{XXXXX"

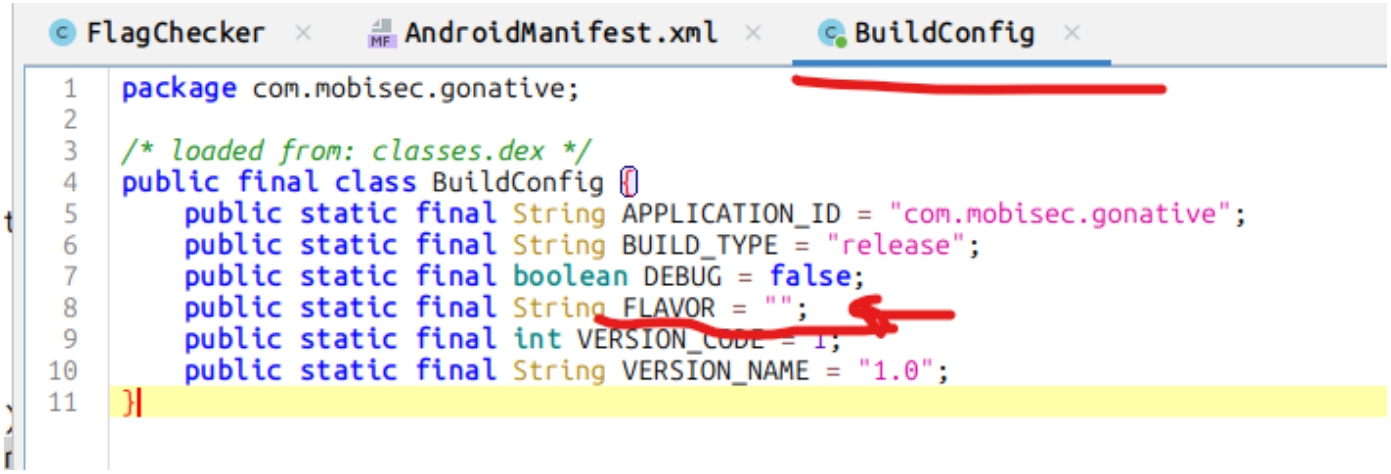
split[1] --> "XXXXXXX}"

after replace

split[0] --> "XXXXXXXXX"

split[1] --> "XXXXXX" --> [0-9]

```
        String replace = split[0].replace("MOBISEC{", BuildConfig.FLAVOR);
        String replace2 = split[1].replace("}", BuildConfig.FLAVOR);
        if (replace2.matches("^[0-9]*$") && replace2.length() == 6) {
            return helloFromTheOtherSide(replace,
Integer.parseInt(replace2));
        }
        return false;
    }
```



بس لحد هنا من هنعرف نجيب معلومة تاني وبكده ان مكنتش اعرف اعمل ايه حاولت افكر في اسم chellange هو goingnative اذهب للاصل قولت يبقي لازم اروح اشوف حاجة تانية وشوفت في الكود ان في library اللي هي native-lib فقولت اكيد لازم اشزفها ولكن مكنتش بتفتح معايا فكان لازم انزلاداة اللي هي Ghidra

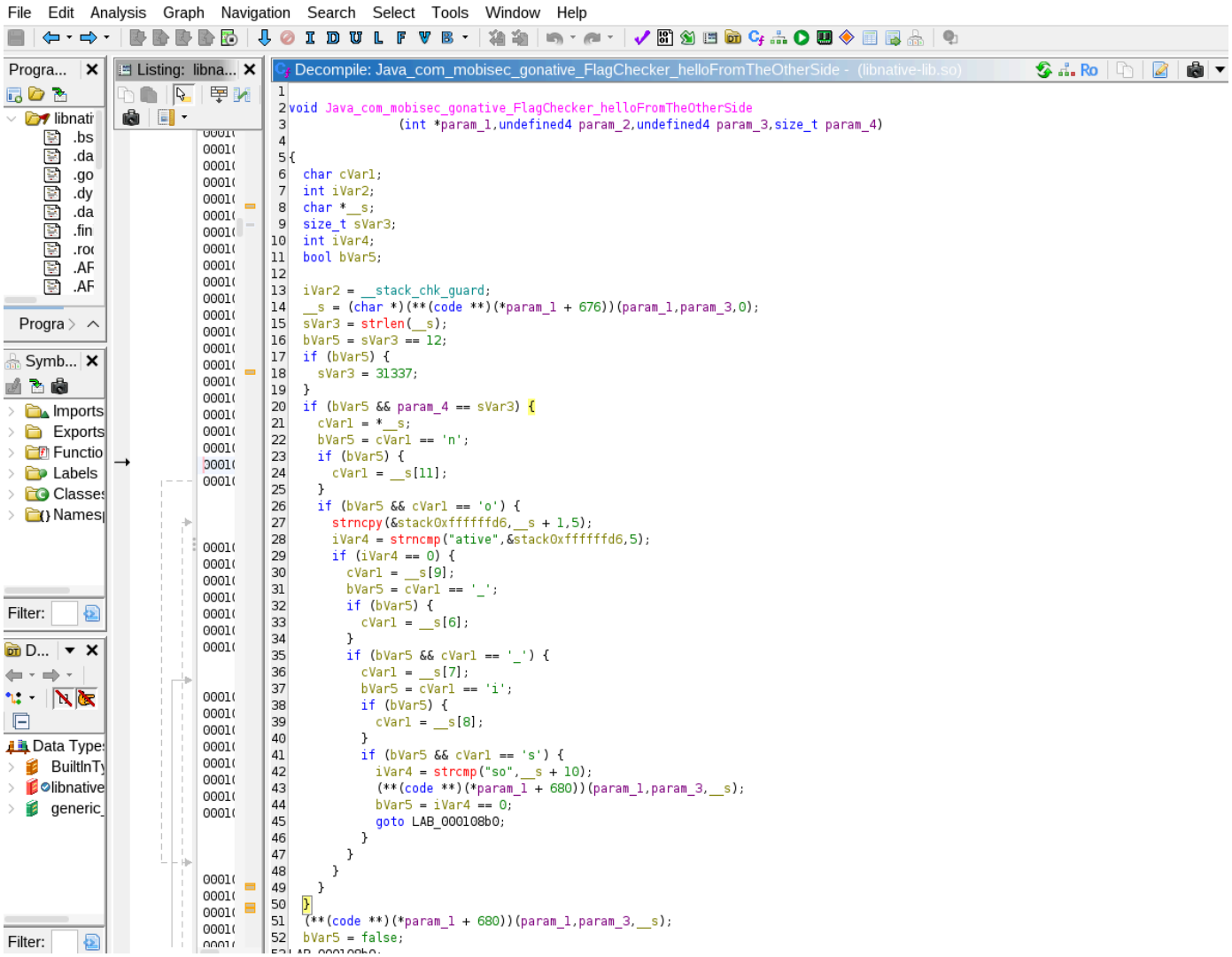
```
static {
        System.loadLibrary("native-lib");
    }
```

install ghidra : Ghidra Software Reverse Engineering Framework

```
-> wget
https://github.com/NationalSecurityAgency/ghidra/releases/download/Ghidra_11
.3.2_build/ghidra_11.3.2_PUBLIC_20250415.zip

-> unzip folder
-> ./tool
```

3- open library with hydra and library



هنا اهو ملف تعالي نشرح الكود اللي فيه

هنا اه بيعرف متغيرات عادي بعد كده في string اللي هو__ s ده هيبقي size بتاع 12 بعد كده هنلاقي ان في رقم 31337 وده غالبا بيبقي القيمة اللي في العنصر التاني اللي في array

sVar3 = strlen(__s); --> get the size of __s
bVar5 = sVar3 == 12; --> if size ==12 set bVar=1 else =0

```
char cVar1;
  int iVar2;
  char *__s;
  size_t sVar3;
  int iVar4;
  bool bVar5;

  iVar2 = __stack_chk_guard;
  __s = (char *)(**(code **)(*param_1 + 676))(param_1,param_3>
  sVar3 = strlen(__s);
  bVar5 = sVar3 == 12;
  if (bVar5) {
```

```
    sVar3 = 31337;
  }
```

هنا اه بيقول ان param_4 sVar331337 بعد كده السطر ده cVar1 = *__s; بيقول انه هيخزن اول قيمة في string وهنعرف ان هي n وبعد كده هيخلي cVar1=__s[11] --> index num 11

__s[0] = n

```
  if (bVar5 && param_4 == sVar3) {
    cVar1 = *__s;
    bVar5 = cVar1 == 'n';
    if (bVar5) {
      cVar1 = __s[11];
    }
```

هنا بيقول ان cVar1='o' يعني كده index number 11 =o بعد كده ده strncpy(&stack0xffffffd6,__s + 1,5); ان هياخد كوبي من copy from index 1 to index 5 and set on &stack0xffffffd6 بعد كده هتطلع القيمة هي دي ative وبعد كده بقي هيقول ان _ = index num 9 and 6

now :

__s[0] = n

__s[1-5]= ative

_s[6] =

_s[9] =

__s[11]=o

__s = "native_XX_Xo"

```
    if (bVar5 && cVar1 == 'o') {
      strncpy(&stack0xffffffd6,__s + 1,5);
      iVar4 = strncmp("ative",&stack0xffffffd6,5);
      if (iVar4 == 0) {
        cVar1 = __s[9];
        bVar5 = cVar1 == '_';
        if (bVar5) {
          cVar1 = __s[6];
        }
```

هنا اه cVar1 = __s[7]; bVar5 = cVar1 == 'i'; بيقول ان index num 7 = i وبعد كده هيقول ان index num 8 =s بعد كده iVar4 = strcmp("so",__s + 10); بيقول ان من اول index 10 هيبقي القيمة دي so

here :

__s[7]=i

__s[8]=s

__s[10,11]=so

```
        if (bVar5 && cVar1 == '_') {
          cVar1 = __s[7];
          bVar5 = cVar1 == 'i';
          if (bVar5) {
            cVar1 = __s[8];
          }
          if (bVar5 && cVar1 == 's') {
            iVar4 = strcmp("so",__s + 10);
            (**(code **)(*param_1 + 680))(param_1,param_3,__s>
            bVar5 = iVar4 == 0;
            goto LAB_000108b0;
          }
```

نجمع بقي كل ده

__s[0] = n

__s[1-5]= ative

_s[6] =

_s[9] =

__s[11]=o

__s[7]=i

__s[8]=s

__s[10,11]=so

__s="native_is_so"

كده بقي عرفنا العنصر الاول بتاع array وعرفنا العنصر التاني اللي هو فيه ارقام بس هما 5 ارقام وكده ناقص رقم ان معرفتش ايه هو الرقم ده بس حاولت بقي من 0 - 9 علي الرقم ده وطلع ان هو 0

now :

array[0]= "MOBISEC{native_is_so"

- between array[0] and array[1]

array[1]="031337}

now flag is MOBISEC{native_is_so-031337}

check flag in app

the flag is true