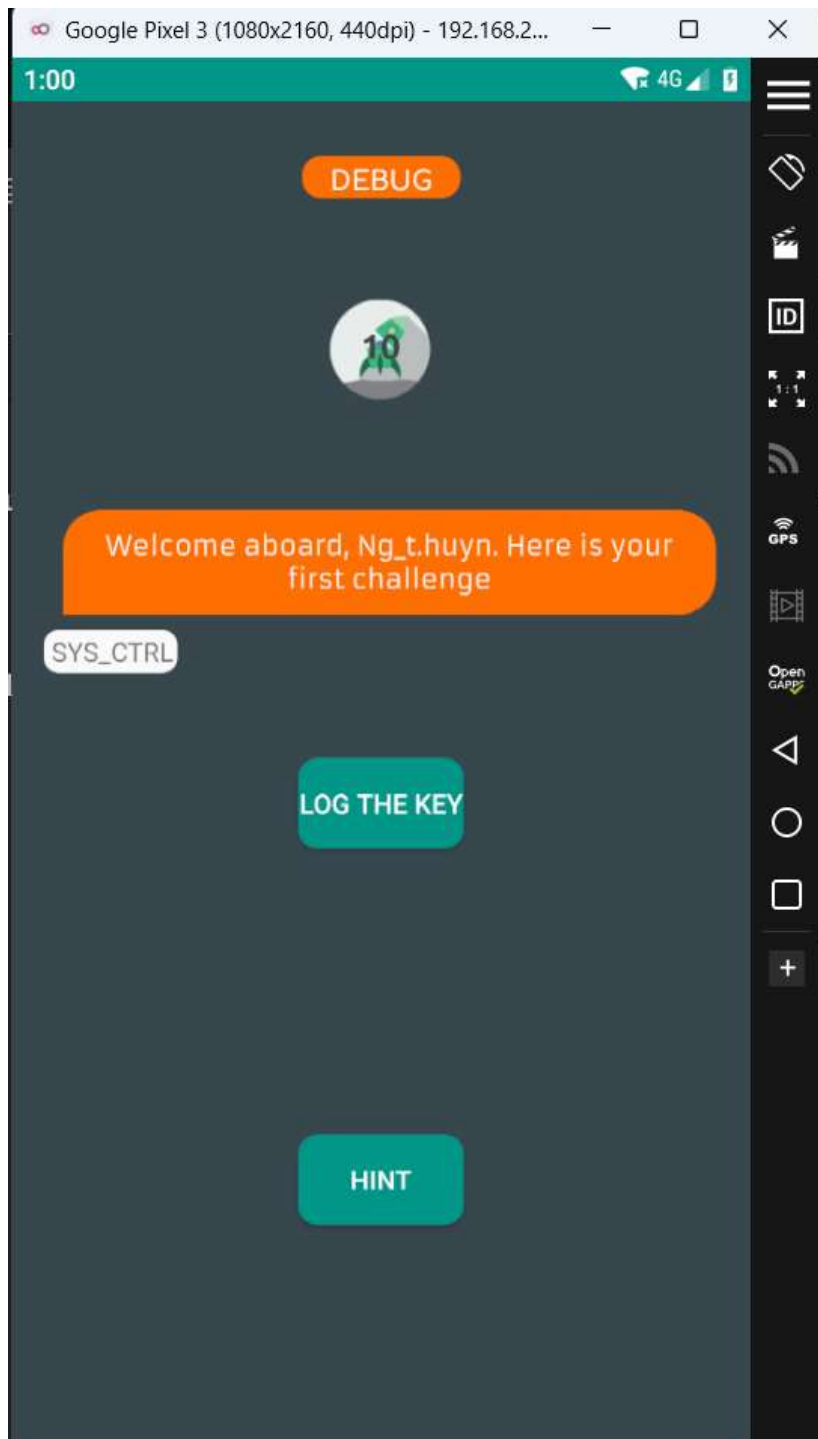


## 1. Level1



Theo hint của đề bài thì ta sẽ dùng lệnh  
Adb shell ps

```

root      2339      2      0      0 worker_thread      0 S [kworker/1:2]
u0_a72    2369    222  853140  78672 ep_poll      f011abb9 S com.google.android.partnersetup
root      2422      2      0      0 worker_thread      0 S [kworker/3:2]
u0_a83    2428    222  900876  116668 ep_poll      f011abb9 S com.google.android.tts
u0_a75    2478    222  846924  70284 ep_poll      f011abb9 S com.google.android.carriersetup
u0_a54    2498    222  851780  74456 ep_poll      f011abb9 S com.android.quicksearchbox
u0_a11    2523    222  856520  75744 ep_poll      f011abb9 S com.android.cellbroadcastreceiver
u0_a64    2549    222  860256  85260 ep_poll      f011abb9 S com.android.email
u0_a4     2664    222  851040  80188 ep_poll      f011abb9 S android.process.media
u0_a79    2914    222  925464  131784 ep_poll      f011abb9 S com.android.vending:instant_app_installer
u0_a79    2931    222  917192  133992 ep_poll      f011abb9 S com.android.vending:quick_launch
u0_a28    3091    222  928332  124212 ep_poll      f011abb9 S com.revo.evabs
root      3172    244    7560    2796 0      f2863bb9 R ps

```

Nó sẽ hiện ra như thế này

Sao đó ta đọc PID của nó

```

root      3172    244    7560    2796 0      f2863bb9 R ps

C:\Program Files\Genymobile\Genymotion\tools>adb logcat --pid=3091
----- beginning of main
05-20 00:56:53.226 3091 3091 I Zygot : seccomp disabled by setenfor
05-20 00:56:53.227 3091 3091 I com.revo.evabs: Late-enabling -Xcheck:
05-20 00:56:53.281 3091 3091 W com.revo.evabs: Unexpected CPU variant
05-20 00:56:53.605 3091 3091 I com.revo.evabs: The ClassLoaderContext

```

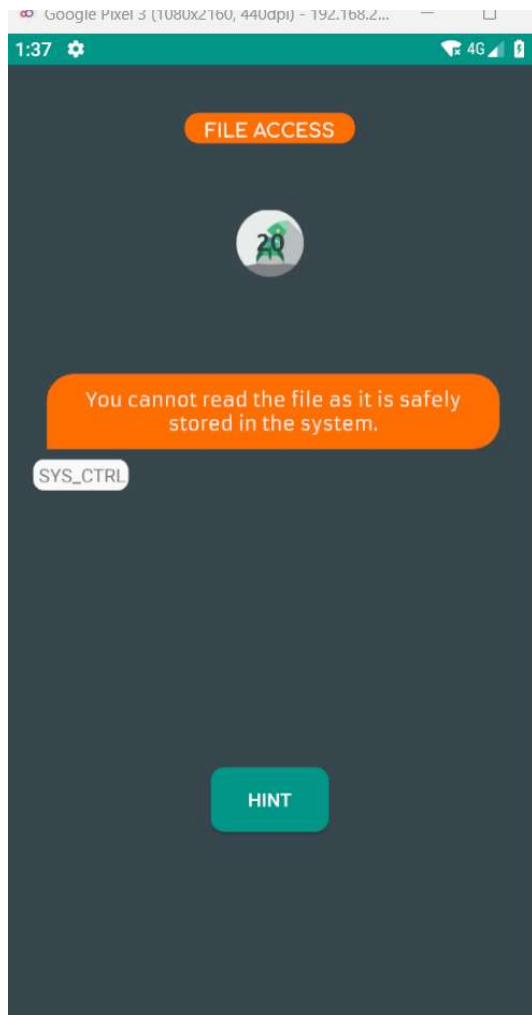
Đây là kết quả

```

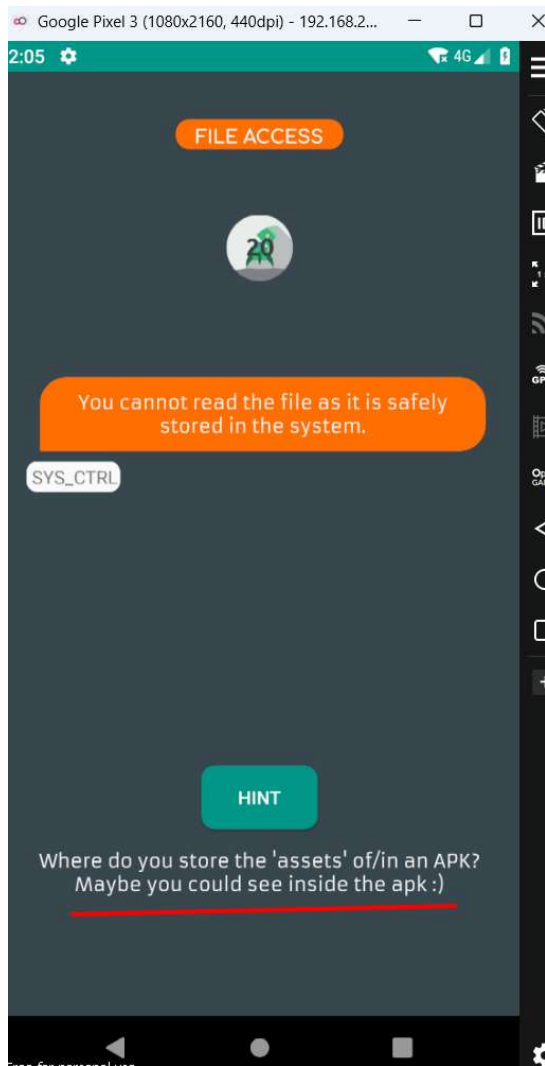
05-20 00:57:29.963 3091 3091 I Choreographer: Skipped 131 frames! The application may be doing too much work on i
ain thread.
05-20 00:57:30.005 3091 3110 I OpenGLRenderer: Davey! duration=2212ms; Flags=0, IntendedVsync=166771369673, Vsync=
54702919, OldestInputEvent=9223372036854775807, NewestInputEvent=0, HandleInputStart=168963273790, AnimationStart=16
342793, PerformTraversalsStart=168965163695, DrawStart=168965467923, SyncQueued=168970933702, SyncStart=168992615787
sueDrawCommandsStart=168992668028, SwapBuffers=168993314759, FrameCompleted=169005834227, DequeueBufferDuration=7640
QueueBufferDuration=332000,
05-20 00:57:30.059 3091 3110 I OpenGLRenderer: Davey! duration=2247ms; Flags=0, IntendedVsync=166771369673, Vsync=
54702919, OldestInputEvent=9223372036854775807, NewestInputEvent=0, HandleInputStart=168963273790, AnimationStart=16
342793, PerformTraversalsStart=168965163695, DrawStart=168992784524, SyncQueued=168992994606, SyncStart=169033461761
sueDrawCommandsStart=169033583564, SwapBuffers=169034258789, FrameCompleted=169059523732, DequeueBufferDuration=8740
QueueBufferDuration=994000,
05-20 00:57:31.765 3091 3091 W ActivityThread: handleWindowVisibility: no activity for token android.os.BinderProx
99c35
05-20 01:33:36.752 3091 3091 D ** SYS_CTRL **: EVABS{logging_info_never_safe}

```

## 2. Level2



Ta xem hint



Ta xem trong thư mục đó và thấy

APK size: 7.9 MB, Download Size: 5.6 MB

Compare with previous APK...

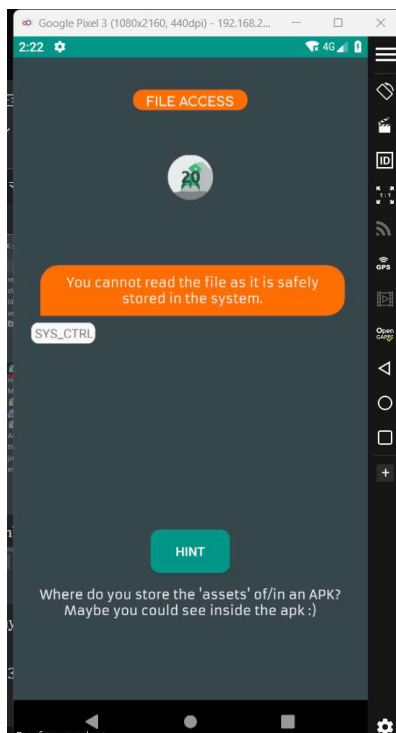
File	Raw File Size	Download Size	% of Total Download Si...
> res	5.1 MB	3.1 MB	58.1%
> classes.dex	1.7 MB	1.6 MB	29.2%
> lib	308.5 KB	283.6 KB	5.2%
> assets	280.2 KB	271 KB	4.9%
> fonts	280.1 KB	270.9 KB	4.9%
> SR.otf	130.6 KB	126.4 KB	2.3%
> ssb.otf	131 KB	126.1 KB	2.3%
> trench100free.otf	18.6 KB	18.4 KB	0.3%
> secrets	42 B	44 B	0%
> resources.arsc	430 KB	101.5 KB	1.8%
> META-INF	43 KB	38.9 KB	0.7%
> CERT.SF	21.1 KB	19.1 KB	0.3%
> MANIFEST.MF	20.9 KB	18.9 KB	0.3%
> CERT.RSA	1 KB	1 KB	0%
> AndroidManifest.xml	2.1 KB	2.1 KB	0%
> third_party	331 B	331 B	0%
> jsr305_annotations	104 B	104 B	0%
> error_prone	98 B	98 B	0%

Giờ thì đổi đuôi file thành zip và giải nén để đọc thông tin trong đó ra thôi

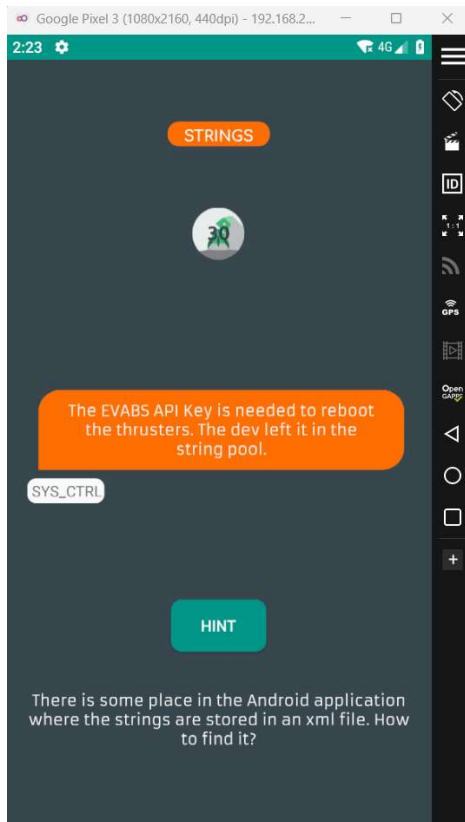
```
1 EVABS{fil3s_n_ass3ts_ar3_eas!ly_hackabl3}
```

Và đây là Flag

### 3. Level3



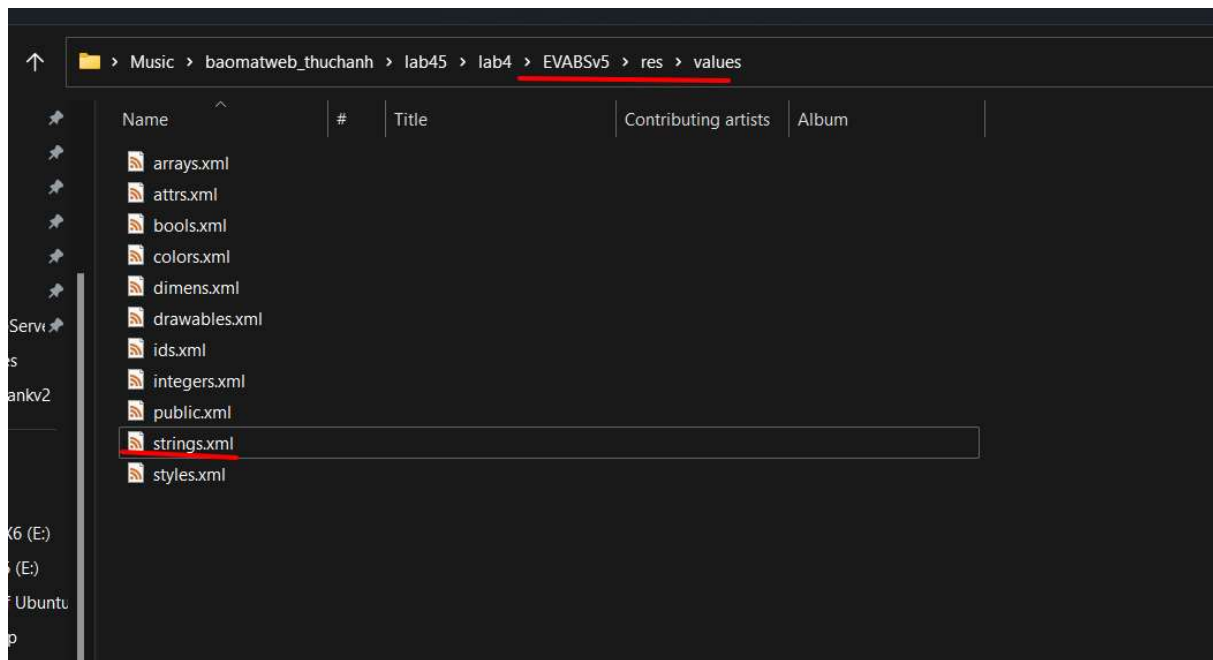
Đây là hint của đề bài



Sau khi tìm hiểu thì ta sẽ dùng apktool để tìm ra tất cả các file có đuôi là xml

```
C:\Users\Admin\Music\baomatweb_thuchanh\lab45\lab4>java -jar apktool_2.7.0.jar d EVABsv5.apk
I: Using Apktool 2.7.0 on EVABsv5.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\Admin\AppData\Local\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...
```

Đây là file được lưu trữ

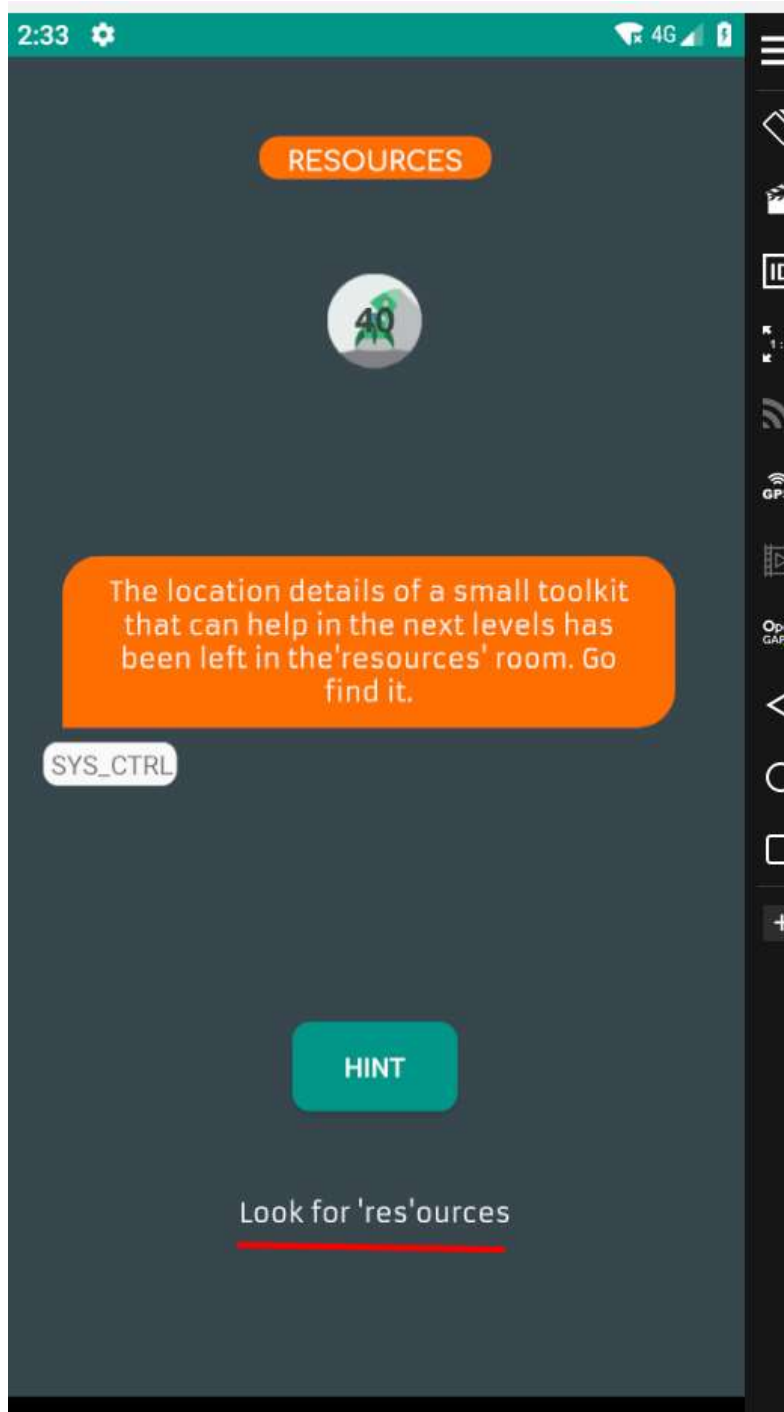


Đây là Flag được lưu trữ

```
strings.xml - X
C: > Users > Admin > Music > baomatweb_thuchanh > lab45 > lab4 > EVABSV5 > res > values > strings.xml > xml
81 <string name="ob_get_started">GET STARTED</string>
82 <string name="ob_header1">SIMPLE ABROAD CALLS</string>
83 <string name="ob_header2">FREE WONEP TO WONEP</string>
84 <string name="ob_header3">NO HIDDEN CHARGES OR FEES</string>
85 <string name="password_toggle_content_description">Toggle password visibility</string>
86 <string name="path_password_eye">M12,4.5C7,4.5 2.73,7.61 1,12c1.73,4.39 6,7.5 11,7.5</string>
87 <string name="path_password_eye_mask_strike_through">M2,4.27 L19.73,22 L22.27,19.46</string>
88 <string name="path_password_eye_mask_visible">M2,4.27 L2,4.27 L4.54,1.73 L4.54,1.73</string>
89 <string name="path_password_strike_through">M3.27,4.27 L19.74,20.74</string>
90 <string name="permission_rationale">"Contacts permissions are needed for providing c
91 completions."</string>
92 <string name="project_id">evabs-c0e8b</string>
93 <string name="prompt_email">Email</string>
94 <string name="prompt_password">Password (optional)</string>
95 <string name="search_menu_title">Search</string>
96 <string name="section_format">Hello World from section: %1$d</string>
97 <string name="status_bar_notification_info_overflow">999+</string>
98 <string name="the_evabs_api_key">EVABS{saf3ly st0red_in_strings?}</string>
99 <string name="title_activity_home">Home</string>
100 <string name="title_activity_launch">Launch</string>
101 <string name="title_activity_login">Sign in</string>
102 <string name="title_activity_splash">Splash</string>
103 <string name="title_activity_test">Test</string>
104 </resources>
105
```

#### 4. Level 4

Bài 4 khá đơn giản

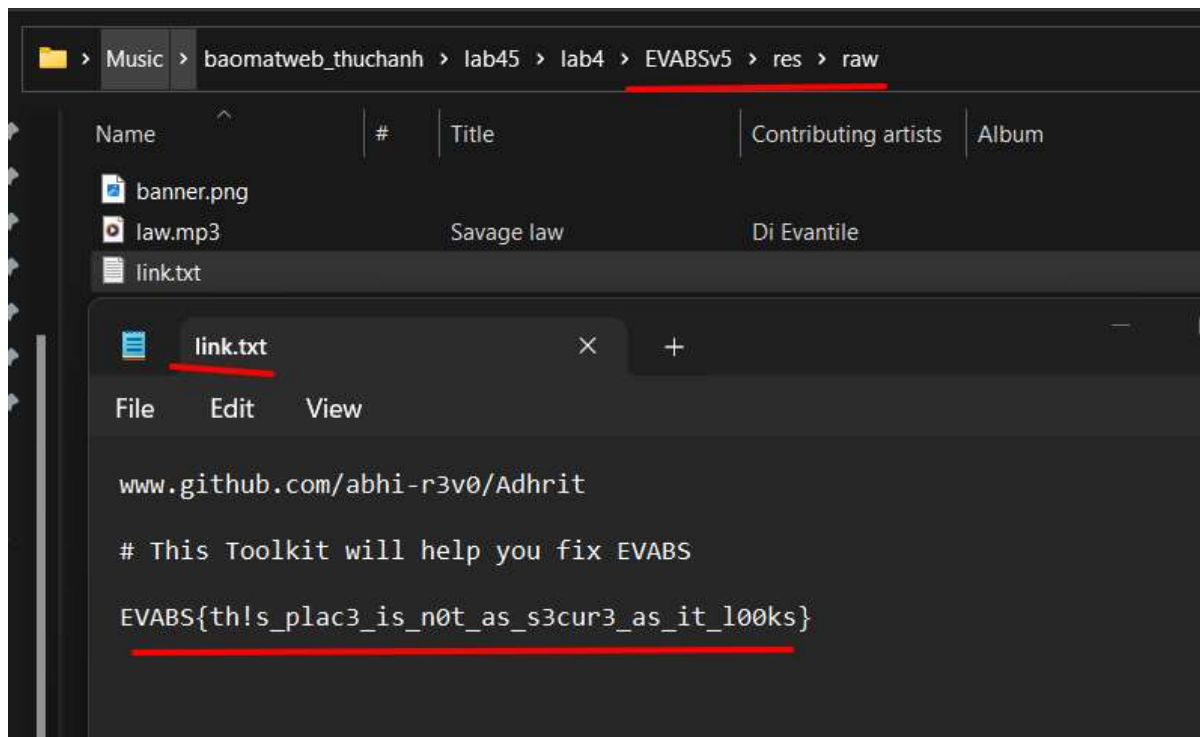


Đây là yêu cầu và hint

Như ở level 3 ta đã dùng apktool để tìm, giờ thì tìm thêm phần được lưu trữ link của app

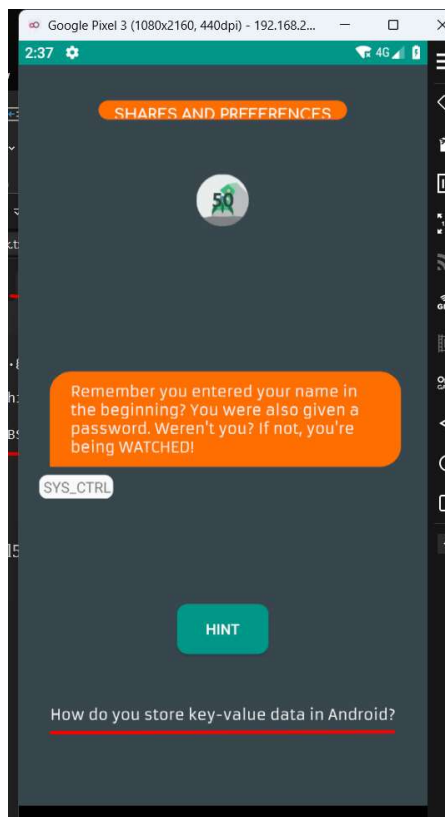
Đây là kết quả khi ta tìm ra





## 5. Level5

Đây là đề bài và gợi ý



Đầu tiên ta chạy adb shell để vào shell giống như terminal của linux

```
C:\Program Files\Genymobile\Genymotion\tools>adb shell
vbox86p:/ # |
```

Sau đó vào /data/data/com.revo.evabs/shared\_prefs

Để truy cập vào thư mục kho lưu trữ của phần mềm

```
C:\Program Files\Genymobile\Genymotion\tools>adb shell
vbox86p:/ # cd /data/data/com.revo.evabs/shared_prefs
vbox86p:/data/data/com.revo.evabs/shared_prefs # ls
DETAILS.xml PREFERENCE.xml
vbox86p:/data/data/com.revo.evabs/shared_prefs #
```

Do gợi ý của đề bài là nó nằm tại thư mục này

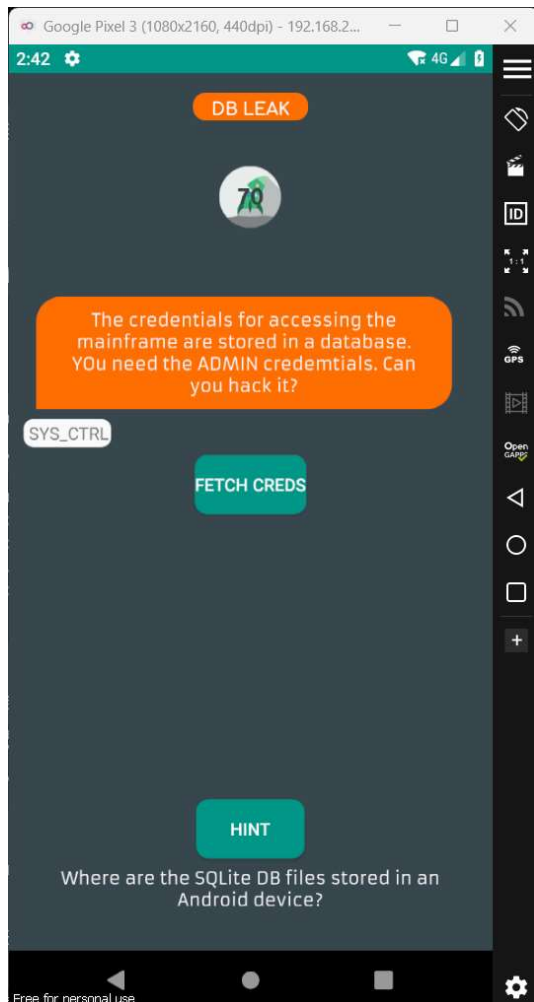
Vậy nên ta sẽ tìm trong 2 file này thì ta thấy file PREFERENCE.xml có chứa flag

```
DETAILS.xml PREFERENCE.xml
vbox86p:/data/data/com.revo.evabs/shared_prefs # cat PREFERENCE.xml | grep -r "EVABS" *
DETAILS.xml:    <string name="password">EVABS{shar3d_pr3fs_c0uld_be_c0mpromiz3ds}</string>
vbox86p:/data/data/com.revo.evabs/shared_prefs # |
```

Đây là kết quả

## 6. Level6

Đây là đề bài và gợi ý



Theo như yêu cầu thì ta vẫn nằm ở thư mục đó

Để đọc database của app

```
C:\Windows\System32\cmd.e  X  +  v
vbox86p:/data/data/com.revo.evabs # ls
cache code_cache databases lib shared_prefs
vbox86p:/data/data/com.revo.evabs #
```

Giờ thì chạy lệnh để đọc database

Xem có gì

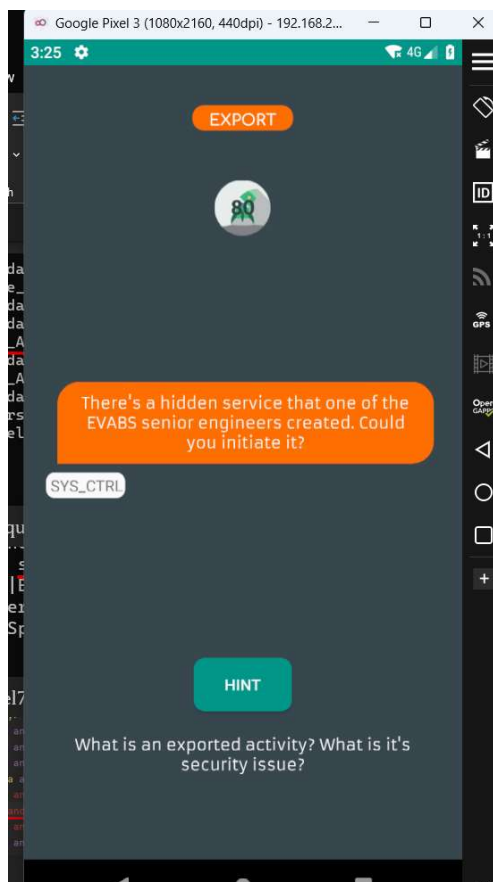
```
vbox86p:/data/data/com.revo.evabs # ls
cache code_cache databases lib shared_prefs
vbox86p:/data/data/com.revo.evabs # cd databases/
vbox86p:/data/data/com.revo.evabs/databases # ls
MAINFRAME_ACCESS MAINFRAME_ACCESS-shm MAINFRAME_ACCESS-wal
vbox86p:/data/data/com.revo.evabs/databases # sqlite3 M
MAINFRAME_ACCESS      MAINFRAME_ACCESS-shm      MAINFRAME_ACCESS-wal
vbox86p:/data/data/com.revo.evabs/databases # sqlite3 MAINFRAME_ACCESS
SQLite version 3.22.0 2019-09-03 18:36:11
Enter ".help" for usage hints.
sqlite>
```

Đây là kết quả

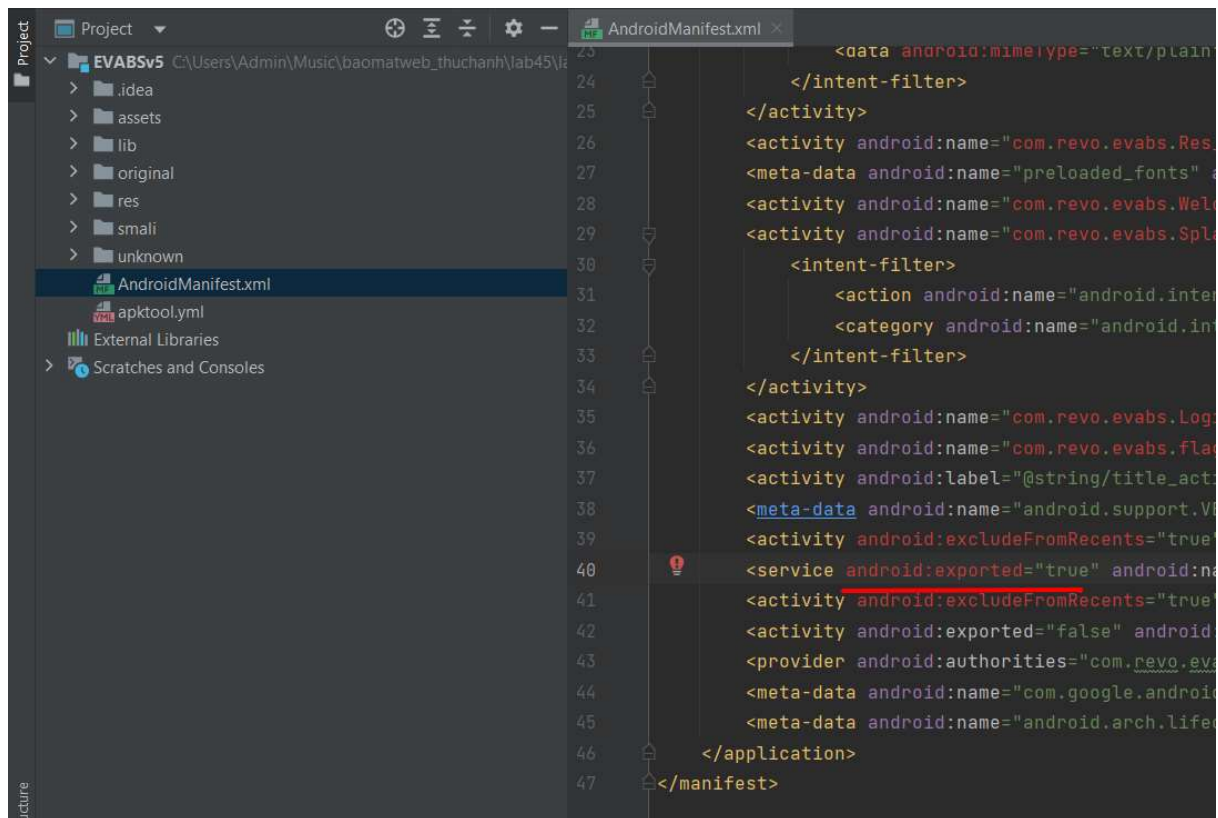
```
sqlite> select * from CREDs:
Dr.l33t|EVABS{sqlite_is_not_safe}E|ADMIN
Mr BufferOverflow|0xNotSecureSQLite_|STAFF
Ms HeapSpray|SQLite_exploit|USER
sqlite>
```

## 7. Level7

Đề bài và gợi ý



Khi ta mở file apk để đọc xem



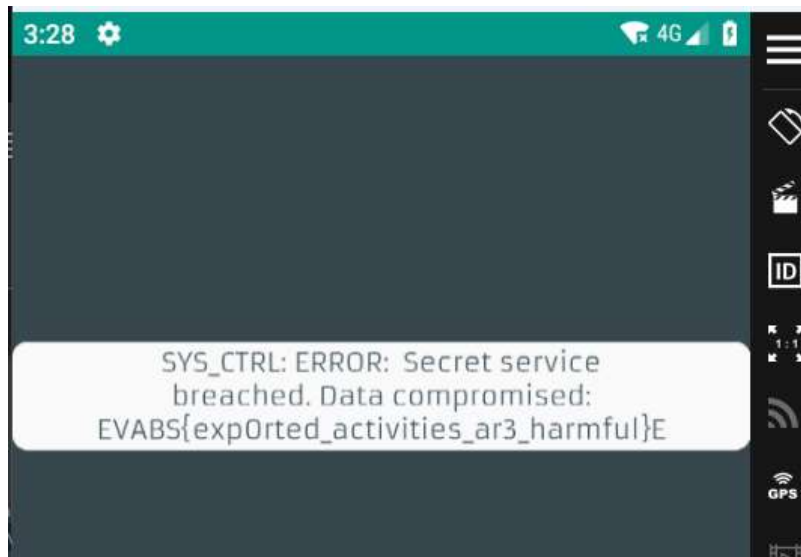
Thì thấy trường exported= "true"

Thì activity được kích hoạt bởi cách ứng dụng khác

Vì thế ta chạy shell như sau

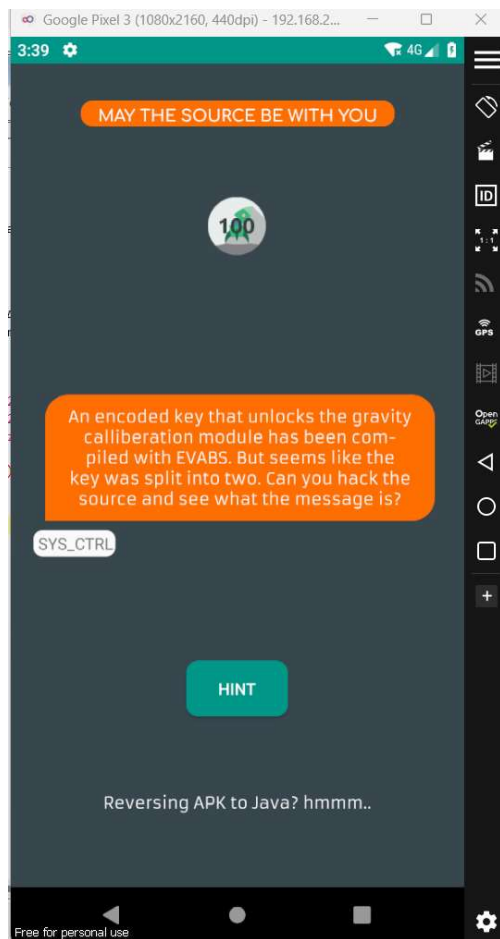
```
C:\Program Files\Genymobile\Genymotion\tools>adb shell am start -n com.revo.evabs/com.revo.evabs.ExportedActivity
Starting: Intent { cmp=com.revo.evabs/.ExportedActivity }
C:\Program Files\Genymobile\Genymotion\tools>
```

Thì đây là kết quả thu được

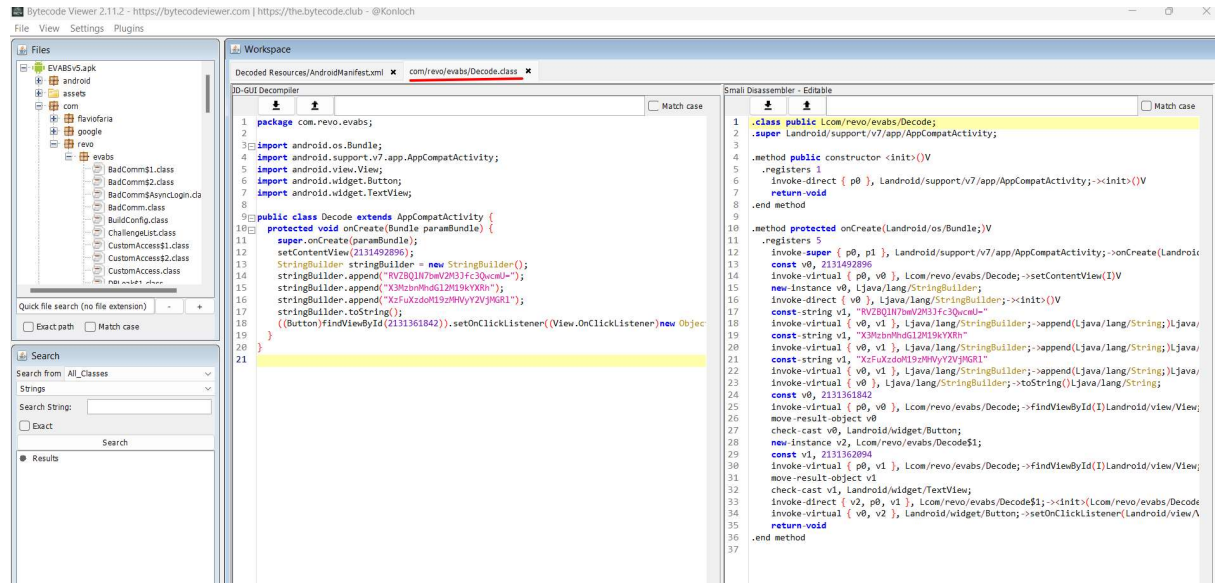


## 8. Level8

Đây là yêu cầu và gợi ý



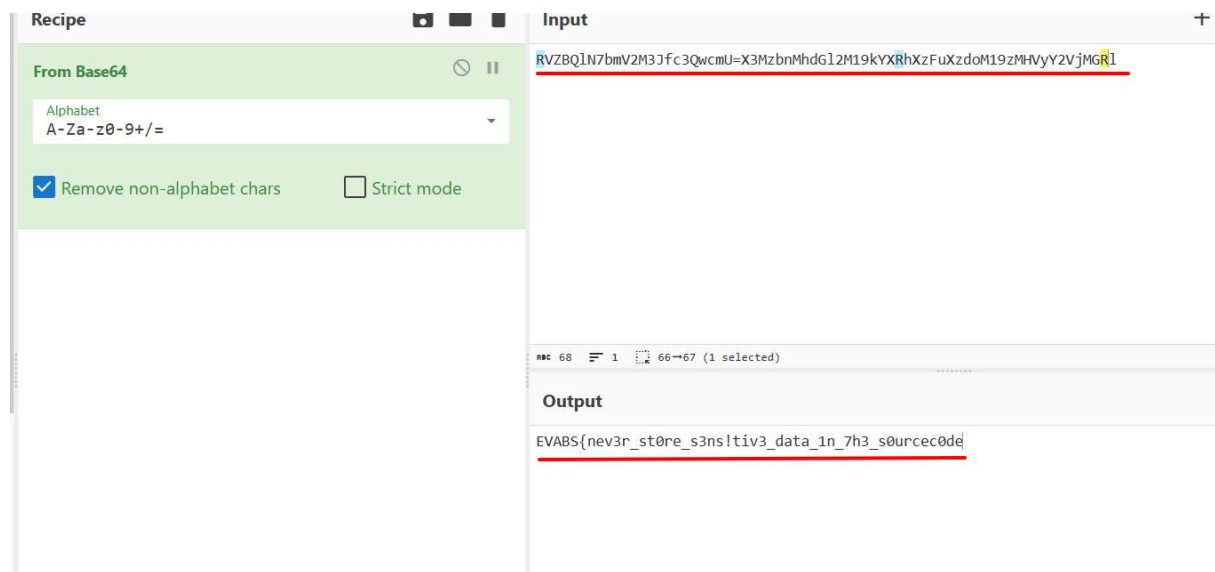
Do gợi ý kêu ta reversing APK to Java nên ta làm bằng tool Bytecode-viewer của java



Sau đó ta mở đến file decode.class

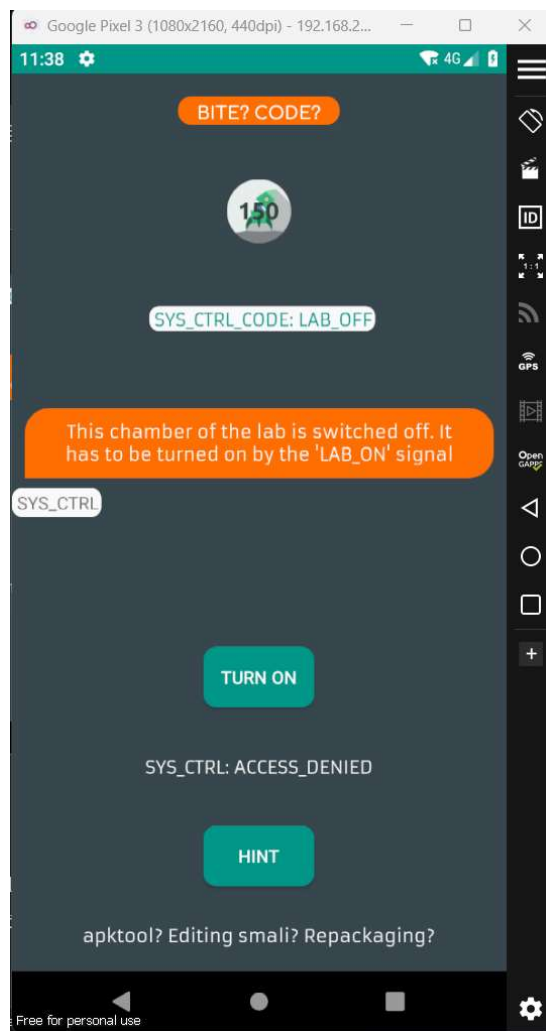
Và thấy có 3 dòng được mã hóa bằng base64

Và đây là kết quả



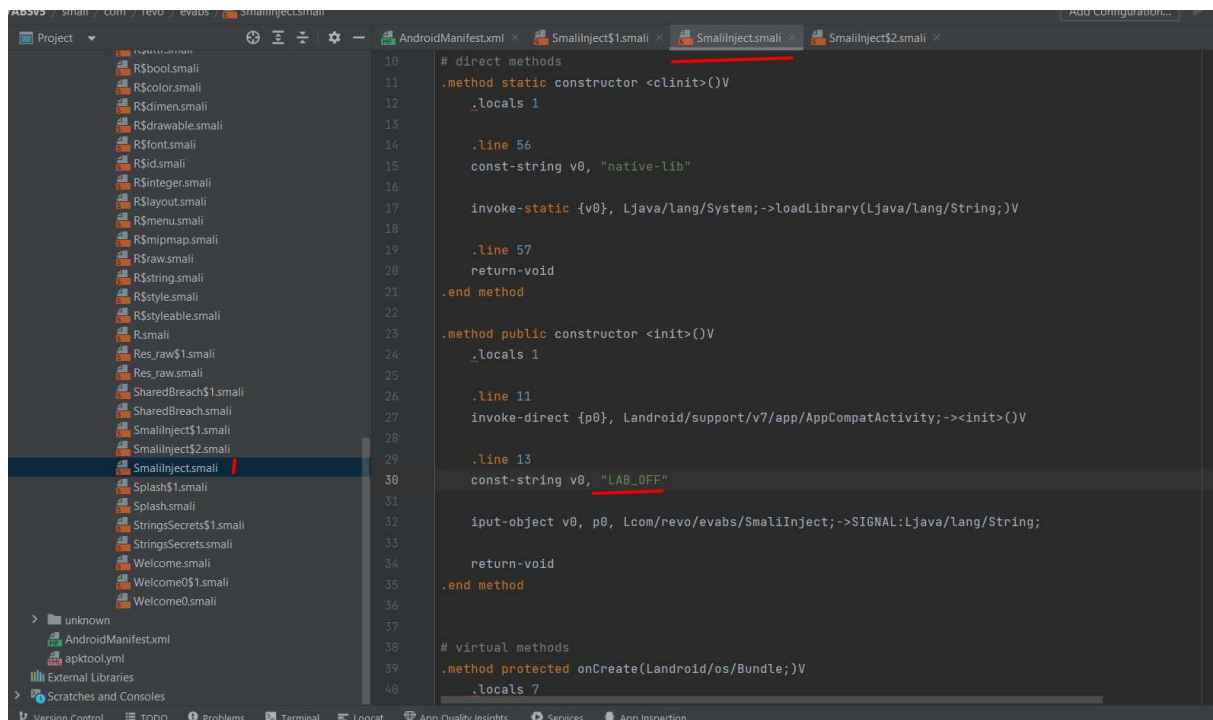
## 9. Level9

Đây là yêu cầu và gợi ý



Có vẻ ta phải dùng apktool để sửa lại code trong đó





Đây là chỗ ta cần sửa

Ta sẽ sửa thành “LAB\_ON”

Sau đó dùng smali để build lại thành file apk

```
C:\Users\Admin\Music\baomatweb_thuchanh\lab45\lab4>java -jar apktool_2.4.1.jar b EVABSv5
Error: Unable to access jarfile apktool_2.4.1.jar
```

```
C:\Users\Admin\Music\baomatweb_thuchanh\lab45\lab4>java -jar apktool_2.7.0.jar b EVABSv5
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: Copying libs... (/lib)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: EVABSv5\dist\EVABSv5.apk
C:\Users\Admin\Music\baomatweb_thuchanh\lab45\lab4>
```

Ta tạo chữ kí

```
C:\Windows\System32\cmd.exe
C:\Users\Admin\Music\baomatweb_thuchanh\lab45\lab4>keytool -genkeypair -v -keystore EVABSV5.keystore -alias publishingdoc -keyalg RSA -keysize 2048 -validity 10000
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: 1
What is the name of your organizational unit?
[Unknown]: 1
What is the name of your organization?
[Unknown]: 1
What is the name of your City or Locality?
[Unknown]: 1
What is the name of your State or Province?
[Unknown]: 1
What is the two-letter country code for this unit?
[Unknown]: 1
Is CN=1, OU=1, O=1, L=1, ST=1, C=1 correct?
[no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
for: CN=1, OU=1, O=1, L=1, ST=1, C=1
Enter key password for <publishingdoc>
(RETURN if same as keystore password):
Key password is too short - must be at least 6 characters
Enter key password for <publishingdoc>
(RETURN if same as keystore password):
Re-enter new password:
[Storing EVABSV5.keystore]
```

Sau đó ta kí vào file đó

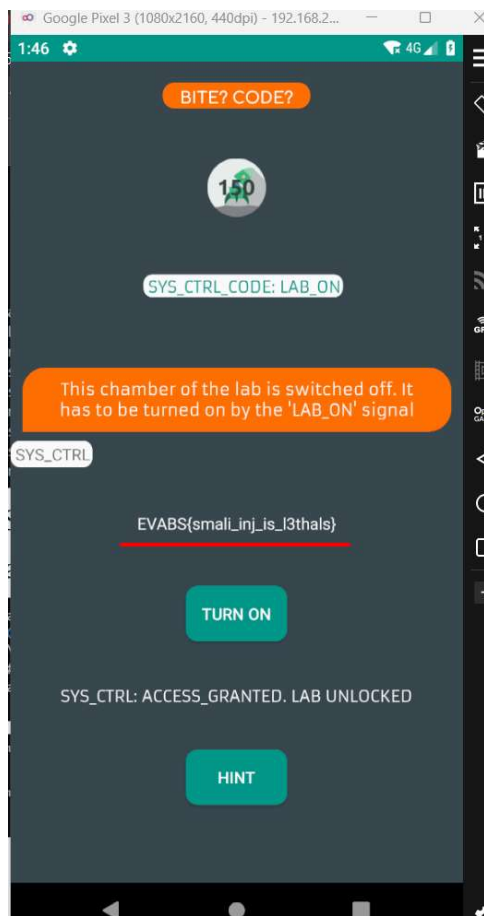
```
C:\Users\Admin\AppData\Local\Android\Sdk\build-tools\30.0.3>apksigner.bat sign --ks "C:\Users\Admin\Music\baomatweb_thuchanh\lab45\lab4\EVABSV5.keystore" C:\Users\Admin\Music\baomatweb_thuchanh\lab45\lab4\EVABSV5_2.apk
Keystore password for signer #1:
```

Sau đó ta cài lại phần mềm vào điện thoại

```
C:\Program Files\Genymobile\Genymotion\tools>adb install EVABSV5_2.apk
Performing Streamed Install
Success

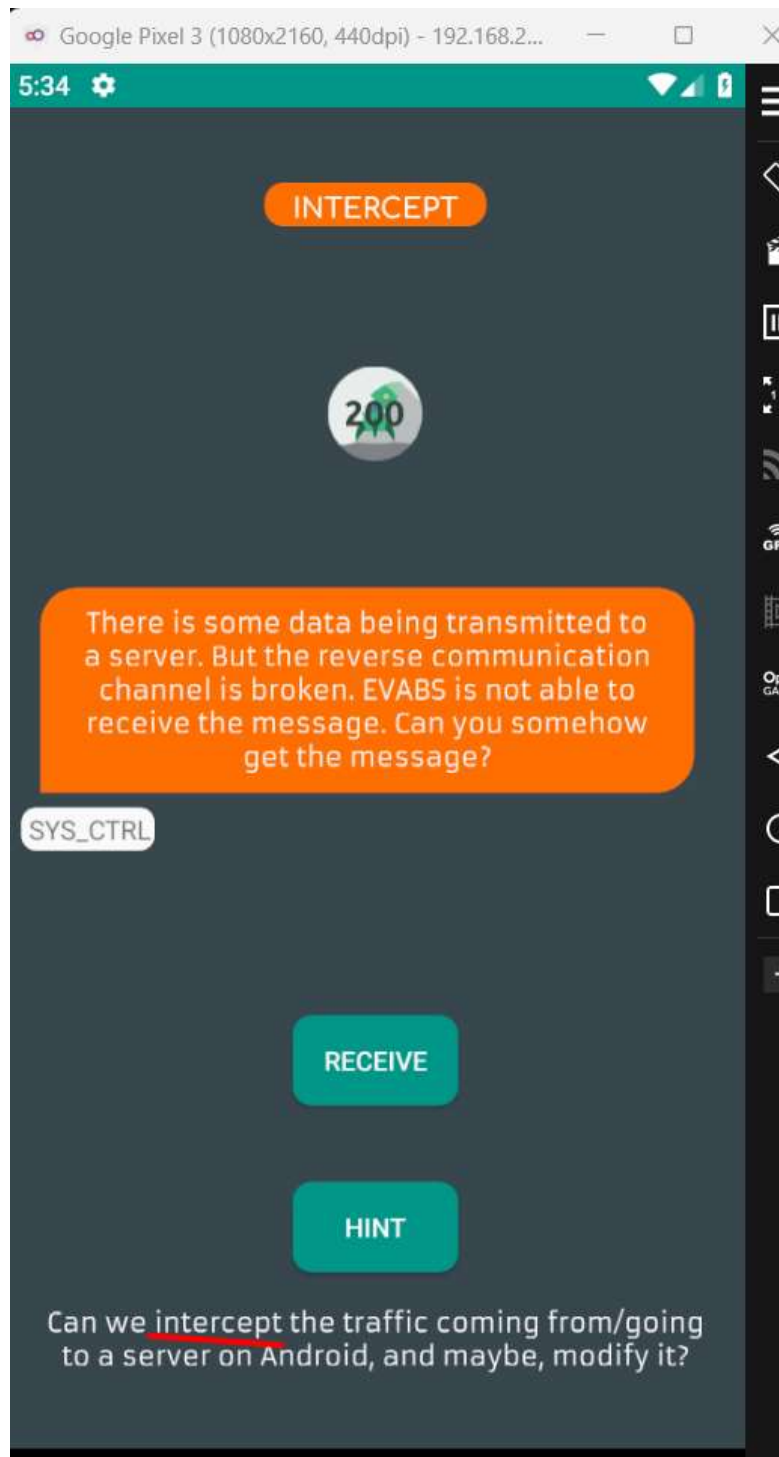
C:\Program Files\Genymobile\Genymotion\tools>|
```

Và đây là kết quả khi mở app lên

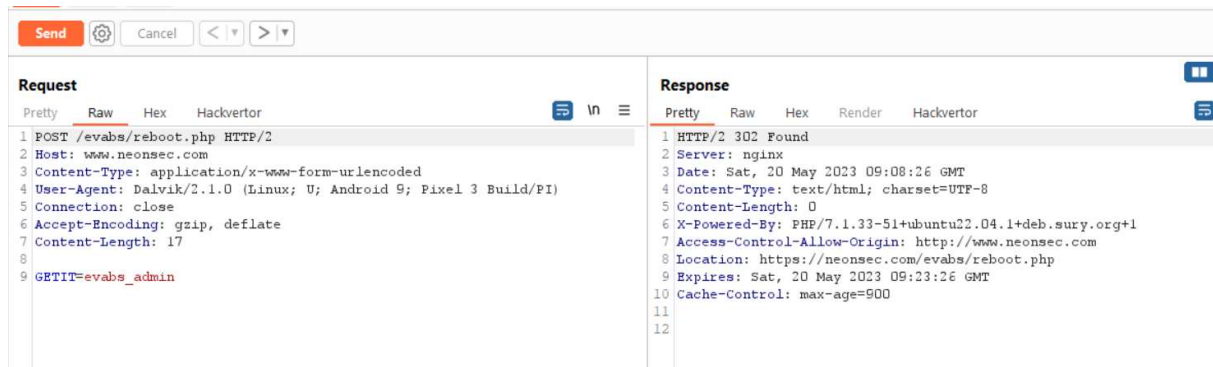


## 10.Level10

yêu cầu của đề bài và gợi ý



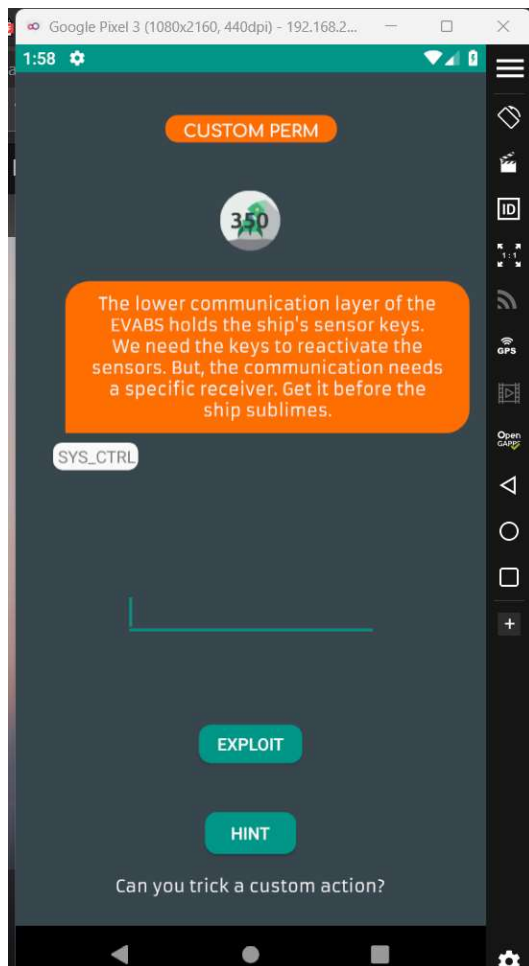
Lần này ta dùng burpsuite để bắt gói tin do app gửi đi



Nhưng không có gì cả  
Đọc đi đọc lại challenge  
Gửi đi gửi lại gói tin thì vẫn không thấy Flag

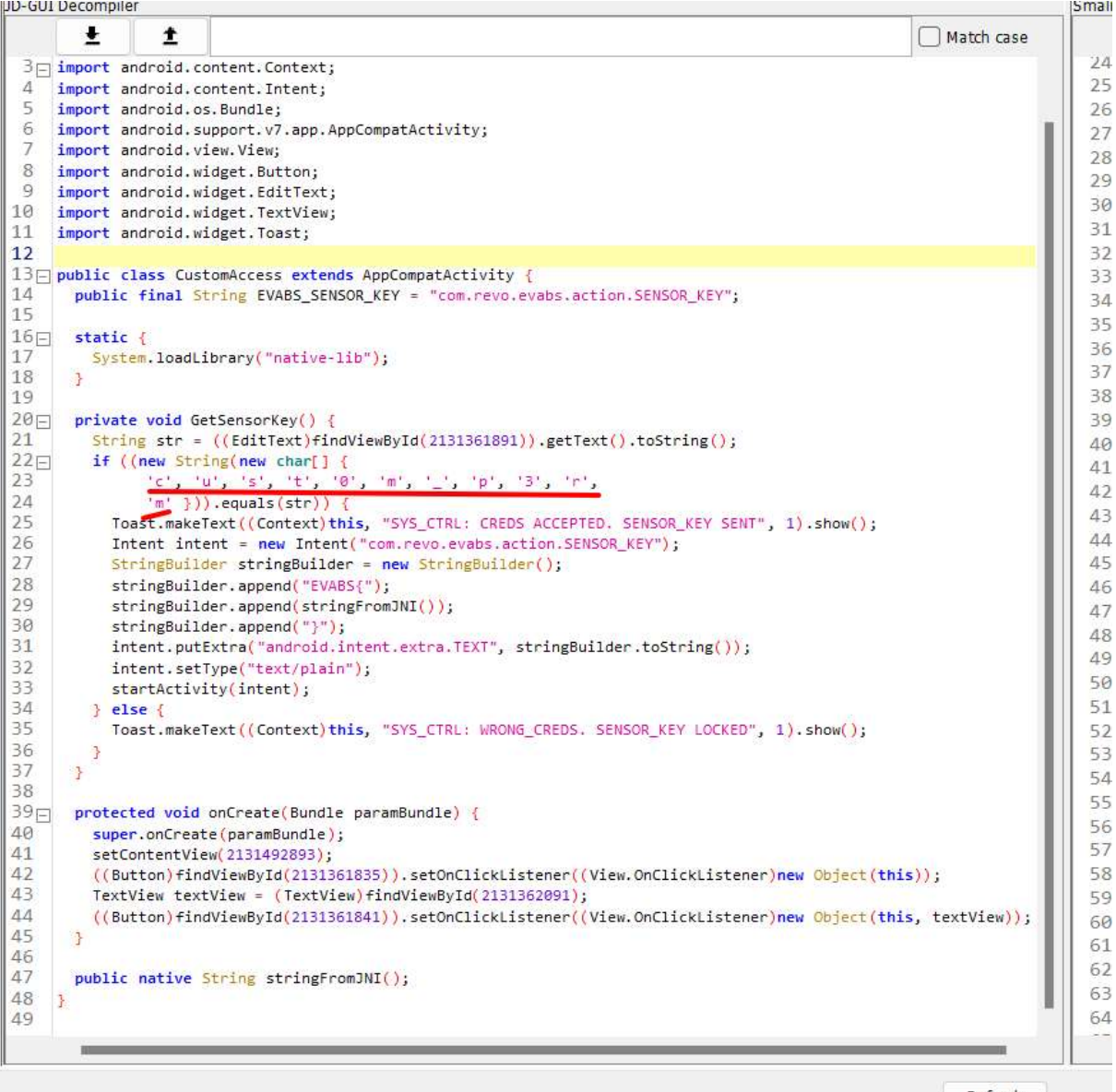
## 11.Level11

Đây là yêu cầu và gợi ý của đề bài



Dùng Bytecode\_viewer để đọc code của file apk

Khi ta nhập vào



```
JD-GUI Decompiler
import android.content.Context;
import android.content.Intent;
import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.TextView;
import android.widget.Toast;

public class CustomAccess extends AppCompatActivity {
    public final String EVABS_SENSOR_KEY = "com.revo.evabs.action.SENSOR_KEY";

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

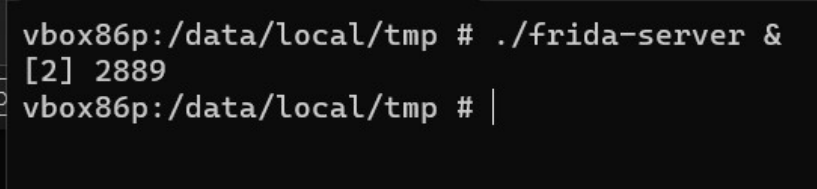
    private void GetSensorKey() {
        String str = ((EditText)findViewById(2131361891)).getText().toString();
        if ((new String(new char[] {
            'c', 'u', 's', 't', 'o', 'm', '_', 'p', '3', 'r',
            'm' })).equals(str)) {
            Toast.makeText((Context)this, "SYS_CTRL: CREDITS ACCEPTED. SENSOR_KEY SENT", 1).show();
            Intent intent = new Intent("com.revo.evabs.action.SENSOR_KEY");
            StringBuilder stringBuilder = new StringBuilder();
            stringBuilder.append("EVABS(");
            stringBuilder.append(stringFromJNI());
            stringBuilder.append(")");
            intent.putExtra("android.intent.extra.TEXT", stringBuilder.toString());
            intent.setType("text/plain");
            startActivity(intent);
        } else {
            Toast.makeText((Context)this, "SYS_CTRL: WRONG_CREDITS. SENSOR_KEY LOCKED", 1).show();
        }
    }

    protected void onCreate(Bundle paramBundle) {
        super.onCreate(paramBundle);
        setContentView(2131492893);
        ((Button)findViewById(2131361835)).setOnClickListener((View.OnClickListener)new Object(this));
        TextView textView = (TextView)findViewById(2131362091);
        ((Button)findViewById(2131361841)).setOnClickListener((View.OnClickListener)new Object(this, textView));
    }

    public native String stringFromJNI();
}
```

Phân tích thì thấy nhập cust0m\_p3rm thì sẽ đưa ra được Flag

Thì ta phân tích vào cài và chạy Frida-server trên điện thoại



```
vbox86p:/data/local/tmp # ./frida-server &
[2] 2889
vbox86p:/data/local/tmp # |
```

Sau đó viết shell\_hook để phân tích

```

1 import frida
2 import time
3 device = frida.get_usb_device()
4 pid = device.spawn("com.revo.evabs")
5 device.resume(pid)
6 session = device.attach(pid)
7 # Định nghĩa mã JavaScript để hook
8 js_code = """
9 Java.perform(function() {
10     console.log("[-] Starting hooks android.content.Intent.putExtra");
11
12     var intent = Java.use("android.content.Intent");
13
14     // Hook vào phương thức putExtra()
15     intent.putExtra.overload("java.lang.String", "java.lang.String").implementation = function(var_1, var_2) {
16         console.log("[+] Flag: " + var_2);
17
18         // Gọi lại phương thức gốc
19         this.putExtra(var_1, var_2);
20     };
21 });
22 """
23
24 # Kết nối đến thiết bị Android và ứng dụng cần hook
25
26 # Tải mã JavaScript và chạy
27 script = session.create_script(js_code)
28 script.load()
29
30 # Chờ cho tới khi ứng dụng kết thúc
31 input('...?')
32 session.detach()
33
34

```

Chạy shell và nhập kết quả phân tích lúc này và ta nhận được Flag

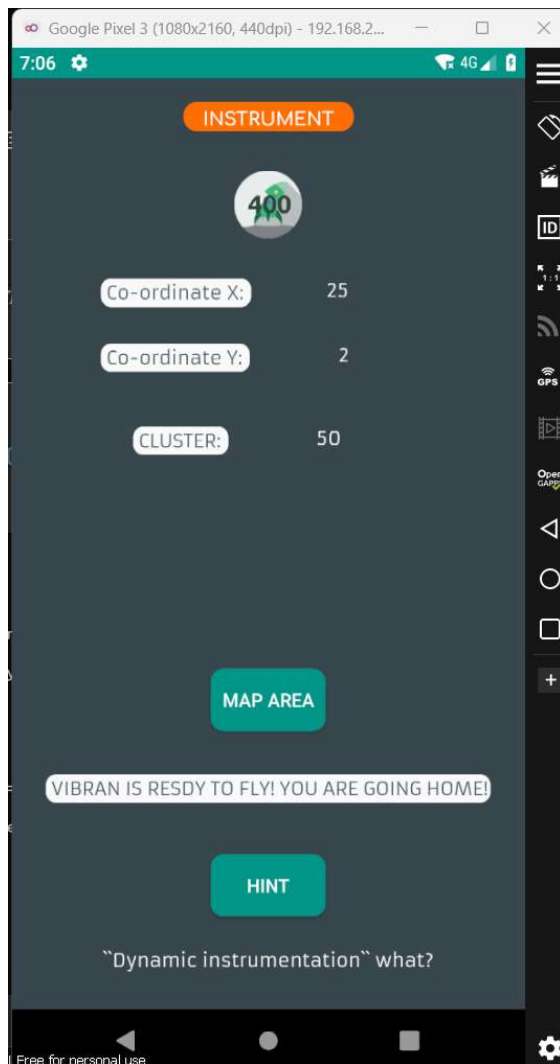
```

PS C:\Users\Admin\Desktop> python3 .\shellhook.py
[-] Starting hooks android.content.Intent.putExtra
...?[+] Flag: EVABS{always_verify_packag3sa}

```

## 12.Level12

Đây là yêu cầu và gợi ý của đề bài



Đầu tiên ta phân tích code bằng Bytecode\_viewer  
Tại frida1.class



```
com/revo/evabs/Frida1$1.class x com/revo/evabs/Launch$1.class x com/revo/eva
D-GUI Decompiler
1 import android.support.v7.app.AppCompatActivity;
2 import android.util.Log;
3 import android.view.View;
4 import android.widget.Button;
5 import android.widget.TextView;
6 import java.util.Random;
7
8 public class Frida1 extends AppCompatActivity implements View.OnClickListener {
9     int a = 25;
10     int b = 2;
11     int x;
12
13     static {
14         System.loadLibrary("native-lib");
15     }
16
17     public void onClick(View paramView) {
18         TextView textView4 = (TextView)findViewById(2131361996);
19         TextView textView3 = (TextView)findViewById(2131362132);
20         TextView textView2 = (TextView)findViewById(2131362134);
21         TextView textView1 = (TextView)findViewById(2131362142);
22         textView3.setText(String.valueOf(this.a));
23         textView2.setText(String.valueOf(this.b));
24         this.x = this.a * this.b;
25         int i = (new Random()).nextInt(70);
26         textView1.setText(String.valueOf(this.x));
27         if (this.x > i + 150) {
28             textView4.setText("VIBRAM IS REDSY TO FLY! YOU ARE GOING HOME!");
29             Log.d("CONGRATZ!", stringFromJNI());
30         } else {
31             textView4.setText("Co-ordinates Not Found!");
32         }
33     }
34
35     protected void onCreate(Bundle paramBundle) {
36         super.onCreate(paramBundle);
37         setContentView(2131492901);
38         ((Button)findViewById(2131361902)).setOnClickListener(this);
39         ((Button)findViewById(2131361844)).setOnClickListener((View.OnClickListener)new Object(this, (Te
40     }
41
42     public native String stringFromJNI();
43 }
```

Sau đó ta viết shell code để hook app

```

1  import frida
2  import time
3  device = frida.get_usb_device()
4  pid = device.spawn("com.revo.evabs")
5  device.resume(pid)
6  session = device.attach(pid)
7  # Định nghĩa mã JavaScript để hook
8  js_code = """
9  Java.perform(function () {
10     send("[-] Starting hooks java.util.Random.nextInt");
11     var random = Java.use("java.util.Random");
12     random.nextInt.overload("int").implementation = function(var_1) {
13         return -150;
14     };
15
16 });
17 """
18
19 # Kết nối đến thiết bị Android và ứng dụng cần hook
20
21 # Tải mã JavaScript và chạy
22 script = session.create_script(js_code)
23 script.load()
24
25 # Chờ cho tới khi ứng dụng kết thúc
26 input('...?')
27 session.detach()
28
29

```

Và rồi chạy Frida-server trên điện thoại

```

vbox86p:/data/local/tmp # ./frida-server &
[3] 3191

```

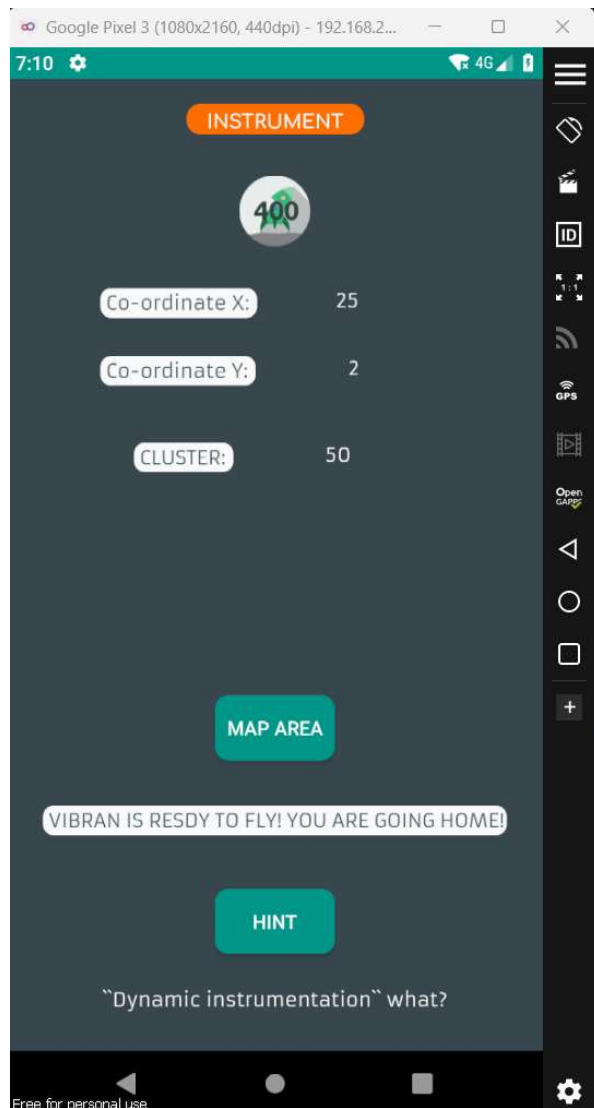
Và rồi chạy shell code ta vừa viết ở trên

```

● PS C:\Users\Admin\Desktop> python3 .\shellhook2.py
...?
○ PS C:\Users\Admin\Desktop> python3 .\shellhook2.py
...?

```

Và rồi chạy chạy phần mềm



Kết quả được đưa ra lại logcat

Đây là kết quả thu được

```
05-21 07:03:32.045 523 588 D gralloc_ranchu: gralloc_alloc: Creating ashmem region of size 9334784
05-21 07:03:32.057 523 588 E : open_verbose:32: Could not open '/dev/goldfish_pipe': No su
ry
05-21 07:03:32.251 487 512 I ActivityManager: Displayed com.revo.evabs/.Frida1: +570ms
05-21 07:03:32.577 525 525 I health@2.0-serv: type=1400 audit(0.0:1170): avc: denied { read } for
v="fuse" ino=8 scontext=u:r:hal_health_default:s0 tcontext=u:object_r:fuse:s0 tclass=file permissive=1
05-21 07:03:32.577 525 525 I health@2.0-serv: type=1400 audit(0.0:1171): avc: denied { open } for
ttery/BAT0/capacity" dev="fuse" ino=8 scontext=u:r:hal_health_default:s0 tcontext=u:object_r:fuse:s0 t
ive=1
05-21 07:03:34.190 3071 3071 D CONGRATZ!: EVABS{a_dynam1c_h00k}E
05-21 07:03:37.369 517 583 W genymotion_audio: Not supplying enough data to HAL, expected position
ote 1102320
05-21 07:03:47.929 218 218 I redis : type=1400 audit(0.0:1173): avc: denied { accept } for lport
:redis:s0 tcontext=u:r:redis:s0 tclass=tcp_socket permissive=1
05-21 07:03:47.929 218 218 I redis : type=1400 audit(0.0:1174): avc: denied { write } for name="
s" ino=11388 scontext=u:r:redis:s0 tcontext=u:object_r:fwmarkd_socket:s0 tclass=sock_file permissive=1
05-21 07:04:58.876 517 2662 W genymotion_audio: Not supplying enough data to HAL, expected position
ote 1102320
05-21 07:04:59.092 517 2662 W genymotion_audio: Not supplying enough data to HAL, expected position
ote 1111680
05-21 07:04:59.092 517 2662 W genymotion_audio: Not supplying enough data to HAL, expected position
ote 1111680
05-21 07:04:59.109 517 2662 W genymotion_audio: Not supplying enough data to HAL, expected position
ote 1112400
```

---