

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Buổi 04 (Session 04)

Tên chủ đề: Pentesting Android Applications

GVHD: Ngô Đức Hoàng Sơn

Ngày báo cáo: 8/05/2024

Nhóm: 07 (ghi số thứ tự nhóm)

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.022.ATCL

STT	Họ và tên	MSSV	Email
1	Nguyễn Thị Kiều Trang	21520489	21520489@gm.uit.edu.vn
2	Trần Đình Huy	21522167	21522167@gm.uit.edu.vn
3	Dương Phú Cường	21521900	21521900@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Phân tích tĩnh (Static Analysis)	100%
2	Dịch ngược (Reverse Engineering)	100%
3	Phân tích động (Dynamic Analysis)	80%
4	Hooking với Frida	100%
5	Challenge CTF	64%

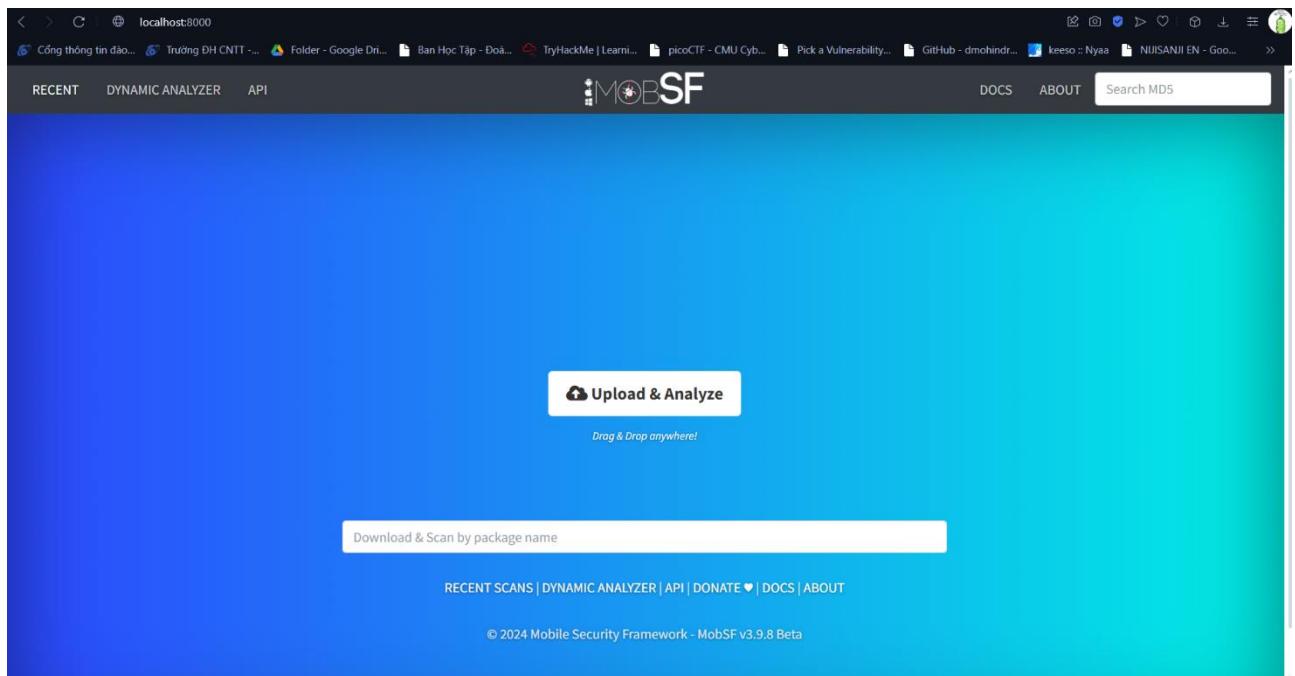
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

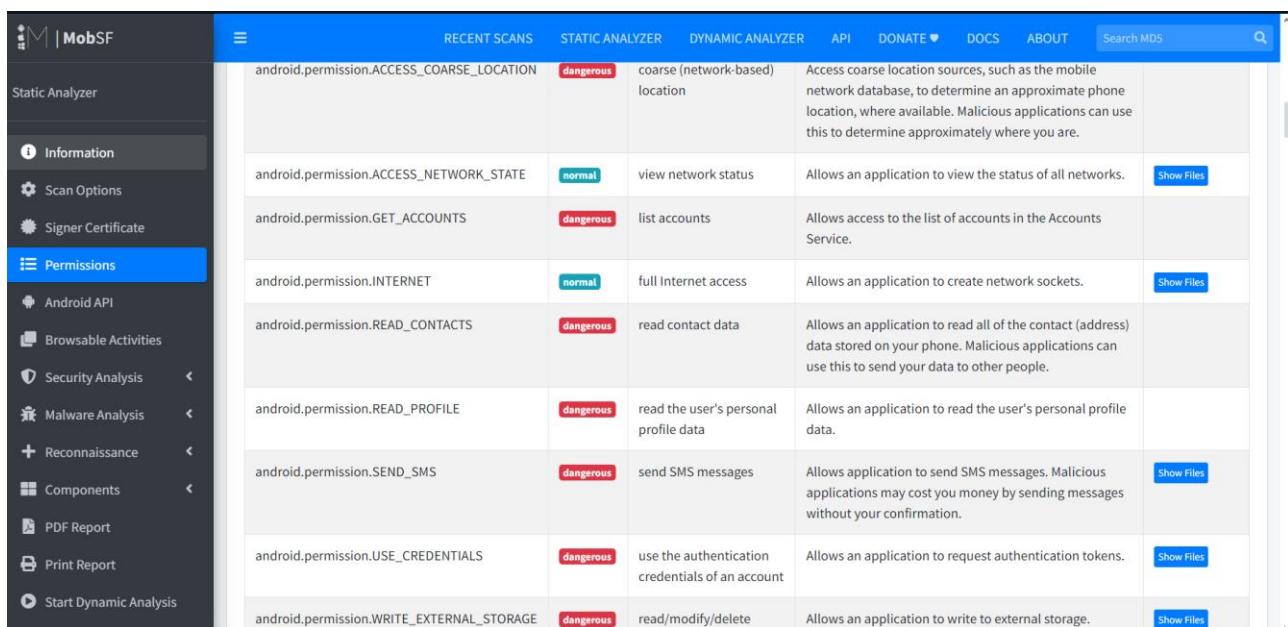
BÁO CÁO CHI TIẾT

1. Phân tích tĩnh (Static Analysis)

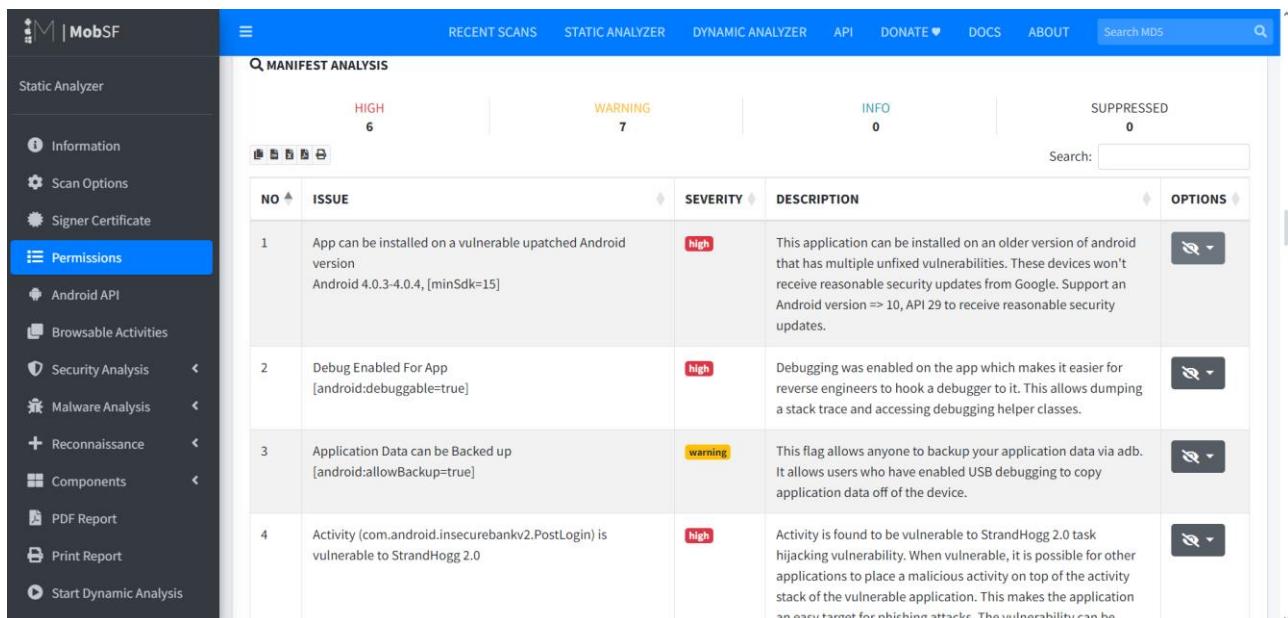
- Sau khi cài đặt và thiết lập môi trường của MobSF ta sẽ truy cập localhost:8000



- Tải lên hoặc kéo thả tập tin *InsecureBankv2.apk* MobSF để tiến hành phân tích tĩnh.



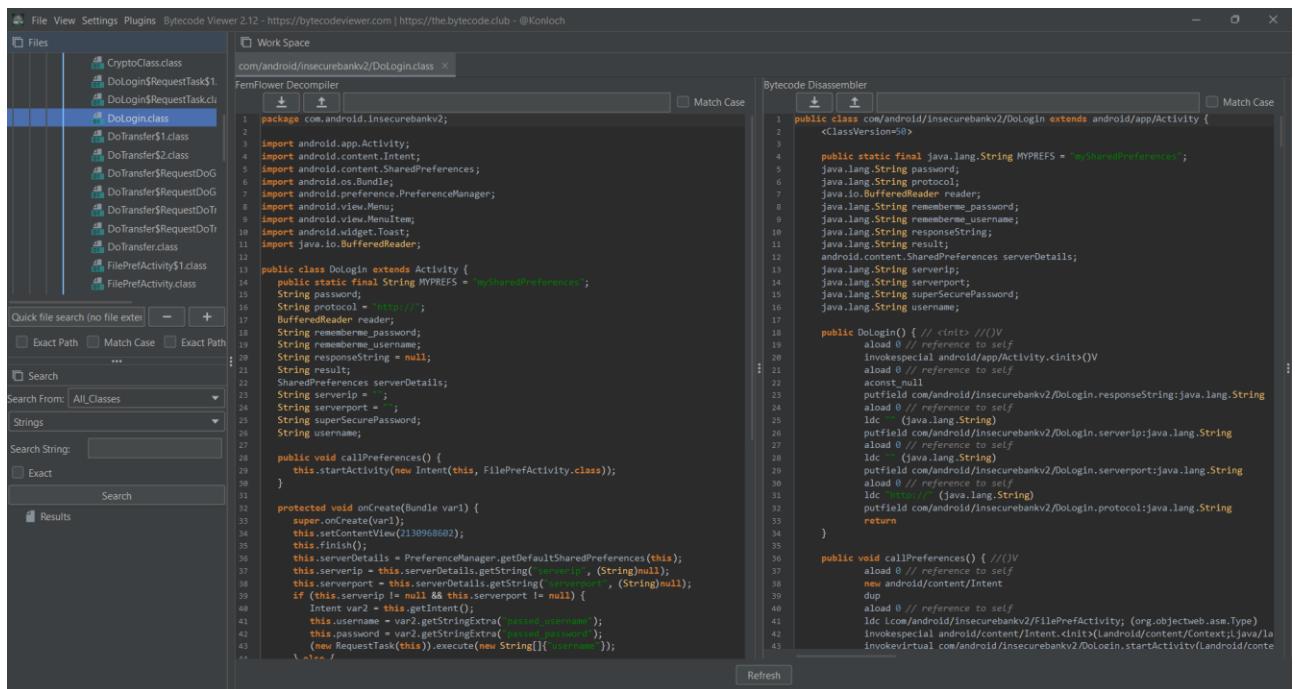
Permission	Risk Level	Description	Action
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks. Show Files
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets. Show Files
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.READ_PROFILE	dangerous	read the user's personal profile data	Allows an application to read the user's personal profile data.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation. Show Files
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens. Show Files
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete	Allows an application to write to external storage. Show Files



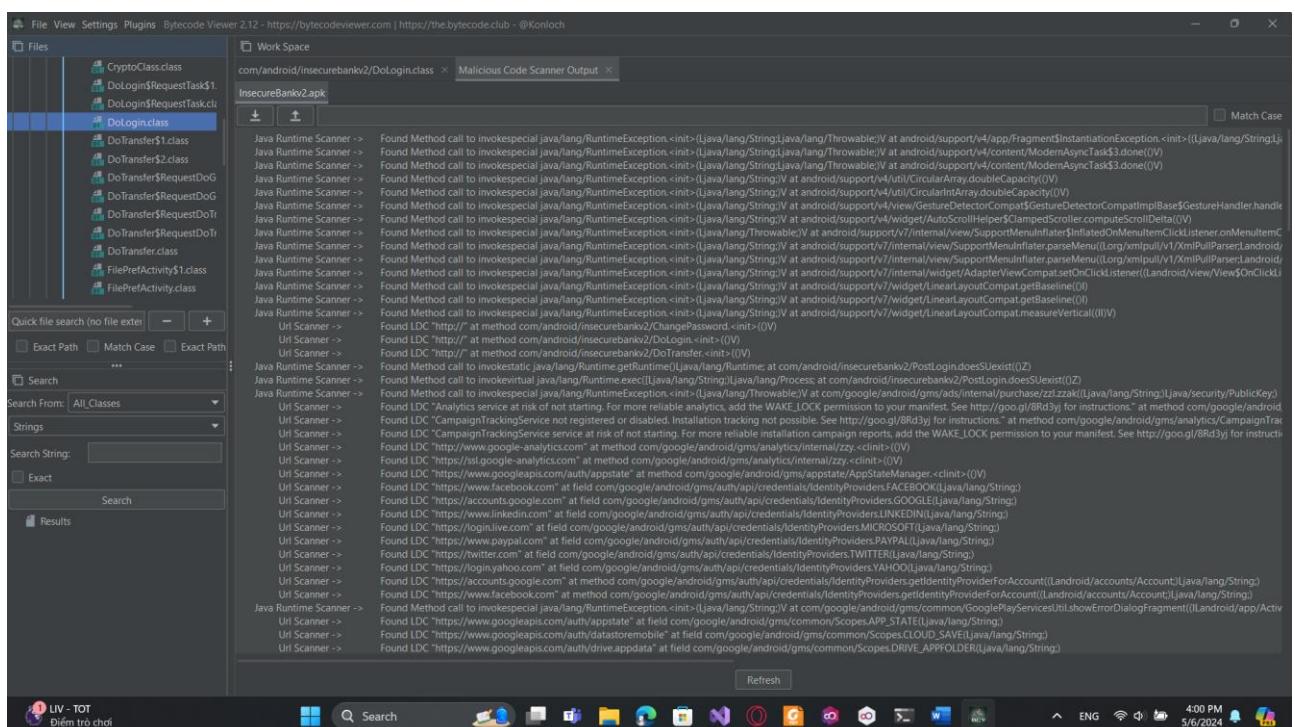
Severity	Count
HIGH	6
WARNING	7
INFO	0
SUPPRESSED	0

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable upatched Android version Android 4.0.3-4.0.4, [minSdk=15]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version >= 10, API 29 to receive reasonable security updates.	Edit
2	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.	Edit
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.	Edit
4	Activity (com.android.insecurebankv2.PostLogin) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be	Edit

- Ta thấy có một số vấn đề đã được hiển thị như SEND_SMS, USE_CREDENTIALS,...
- Một trong các bước quan trọng trong phân tích tĩnh là kiểm tra code. Để làm được việc này dùng ByteCode Viewer để xem code nhanh nha trong tập tin apk. Tải tập tin **Bytecode-Viewer-2.9.x.jar** từ <https://github.com/Konloch bytecode-viewer/releases>
- Kéo thả tập tin apk, ByteCode Viewer sẽ phân tích và hiển thị code.



- Sử dụng *Malicious Code Scanner* ở mục *Plugins* để quét các đoạn code có vẻ nguy hiểm.



`com/android/insecurebankv2/DoLogin$RequestTask.class`

```

181     protected void onPostExecute(Double var1) {
182     }
183
184     protected void onProgressUpdate(Integer... var1) {
185     }
186
187     public void postData(String var1) throws ClientProtocolException, IOException, JSONException, NoSuchAlgorithmException, NoSuchPaddingException, In
188     DefaultHttpClient var5 = new DefaultHttpClient();
189     HttpPost var4 = new HttpPost(this.this$0.protocol + this.this$0.serverip + ":" + this.this$0.serverport + "/login");
190     HttpPost var2 = new HttpPost(this.this$0.protocol + this.this$0.serverip + ":" + this.this$0.serverport + "/devlogin");
191     ArrayList var3 = new ArrayList(2);
192     var3.add(new BasicNameValuePair("username", this.this$0.username));
193     var3.add(new BasicNameValuePair("password", this.this$0.password));
194     var4.setEntity(new UrlEncodedFormEntity(var3));
195     var6 = var5.execute(var4);
196
197     if (this.this$0.username.equals("devadmin")) {
198         var6.setEntity(new UrlEncodedFormEntity(var3));
199         var6 = var5.execute(var2);
200     } else {
201         var4.setEntity(new UrlEncodedFormEntity(var3));
202         var6 = var5.execute(var4);
203     }
204
205     InputStream var7 = var6.getEntity().getContent();
206     this.this$0.result = this.convertStreamToString(var7);
207     this.this$0.result = this.this$0.result.replace("\r", " ");
208     if (this.this$0.result != null) {
209         Intent var8;
210         if (this.this$0.result.indexOf("connect_credentials") != -1) {
211             Log.d("Successful login!", " " + account + " " + this.this$0.username + ":" + this.this$0.password);
212             this.saveCreds(this.this$0.username, this.this$0.password);
213             this.trackUserLogins();
214             var8 = new Intent(this.this$0.getApplicationContext(), PostLogin.class);
215             var8.putExtra("name", this.this$0.username);
216             this.this$0.startActivity(var8);
217         } else {
218             var8 = new Intent(this.this$0.getApplicationContext(), WrongLogin.class);
219             this.this$0.startActivity(var8);
220         }
221     }
222 }

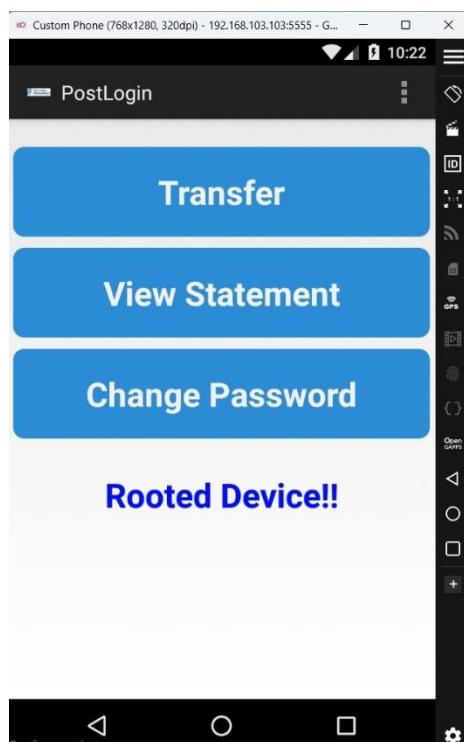
```

Yêu cầu 1 Phân tích và chỉ ra điểm bất thường của đoạn code trên?

- Đầu tiên ta có thể thấy trong đoạn mã sử dụngHttpPost để post các request đăng nhập. Do phương thức HTTP không có mã hóa nên nếu bắt được gói thì username và password có thể bị đọc được.
- Và nếu ta nhập username là devadmin thì có thể login thẳng mà không cần tới password.

Yêu cầu 2 Chỉ ra rằng dữ liệu lưu trữ có an toàn hay không?

- Đầu tiên ta sẽ thử đăng nhập vào chương trình để lưu thông tin.



- Tiếp đến vào command shell của điện thoại ảo di chuyển vào /data/data/com.android.insecurebankv2/databases
- Sử dụng lệnh sqlite3 mydb để tiến hành kiểm tra mydb. Trong database liệt kê tất cả các table hiện có, ở đây ta thấy có 2 table là android_metadata và names, ta sẽ cho hiển thị toàn bộ các thông tin có trong 2 table đó.

```
PS C:\Users\kieut> adb shell
genymotion:/ # cd /data/data/com.android.insecurebankv2/databases
genymotion:/data/data/com.android.insecurebankv2/databases # sqlite3 mydb
SQLite version 3.18.2 2017-07-21 07:56:09
Enter ".help" for usage hints.
sqlite> .database
main: /data/data/com.android.insecurebankv2/databases/mydb
sqlite> .table
android_metadata  names
sqlite> select * from names
...> ;
1|dinesh
2|jack
3|devadmin
sqlite> select * from android_metadata
...> ;
en_US
sqlite> |
```

- Kết quả chỉ hiển thị các username ở dưới dạng plain text.

Yêu cầu 3 Kiểm tra xem thông tin nhạy cảm có lưu lại trên thiết bị hay không? Một số từ khóa: deviceId, userId, imei, deviceSerialNumber, devicePrint, phone, XDSN, mdn, IMSI, uuid...

- Dùng adb shell để vào command shell của điện thoại ảo sau đó di chuyển đến /data/data/com.android.insecurebankv2.
- Chạy cấu trúc lệnh grep -r "string-to-find" \$(find), trong đó là những từ khóa gợi ý trong nội dung yêu cầu 3.
- Trong phần này thì ta không tìm được thông tin nhạy cảm nào cả.

```
Windows PowerShell
genymotion:/data/data/com.android.insecurebankv2 # grep -r "deviceId" $(find)
grep: ./cache/WebView/Crash: No such file or directory
grep: Reports: No such file or directory
grep: Cache: No such file or directory
grep: ./cache/org.chromium.android_webview/Code: No such file or directory
grep: Cache/js: No such file or directory
grep: ./cache/org.chromium.android_webview/Code: No such file or directory
grep: Cache/js/index: No such file or directory
grep: ./cache/org.chromium.android_webview/Code: No such file or directory
grep: Cache/js/index-dir: No such file or directory
grep: ./cache/org.chromium.android_webview/Code: No such file or directory
grep: Cache/js/index-dir/the-real-index: No such file or directory
grep: ./app_webview/Web: No such file or directory
grep: Data: No such file or directory
grep: ./app_webview/Web: No such file or directory
grep: Data-journal: No such file or directory
2|genymotion:/data/data/com.android.insecurebankv2 # grep -r "user" $(find)
./app_webview/pref_store>{"user_experience_metrics":{"low_entropy_source3":6406}}
grep: ./cache/WebView/Crash: No such file or directory
grep: Reports: No such file or directory
grep: Cache: No such file or directory
grep: ./cache/org.chromium.android_webview/Code: No such file or directory
grep: Cache/js: No such file or directory
grep: ./cache/org.chromium.android_webview/Code: No such file or directory
grep: Cache/js/index: No such file or directory
grep: ./cache/org.chromium.android_webview/Code: No such file or directory
grep: Cache/hs/index-dir: No such file or directory
grep: ./cache/org.chromium.android_webview/Code: No such file or directory
grep: Cache/hs/index-dir/the-real-index: No such file or directory
./app_webview/pref_store{"user_experience_metrics":{"low_entropy_source3":6406}}
grep: ./app_webview/Web: No such file or directory
grep: Data: No such file or directory
grep: ./app_webview/Web: No such file or directory
grep: Data-journal: No such file or directory
./app_webview/pref_store{"user_experience_metrics":{"low_entropy_source3":6406}}
2|genymotion:/data/data/com.android.insecurebankv2 # grep -r "userId" $(find)
grep: ./cache/WebView/Crash: No such file or directory
grep: Reports: No such file or directory
grep: Cache: No such file or directory
```

Yêu cầu 4 Theo bạn thư mục sao lưu chứa thông tin nào cần mã hoá, chỉ ra.

- Đầu tiên đăng nhập với tài khoản người dùng bình thường sau đó sử dụng lệnh adb backup -apk -shared com.android.insecurebankv2 để backup dữ liệu

```
PS E:\3\bmweb\th\Lab4> 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...
```

- Chuyển đổi tập tin sao lưu qua định dạng có thể đọc được (cài gói qpdf)

```
trang@trang-virtual-machine:~$ cat backup.ab | (dd bs=24 count=0 skip=1; cat) | 
zlib-flate -uncompress > backup_compressed.tar
0+0 records in
0+0 records out
0 bytes copied, 0,000146494 s, 0,0 kB/s
```

Ta có đoạn dữ liệu được mã hoá, ta có thể thấy thông tin của user đã được mã hóa



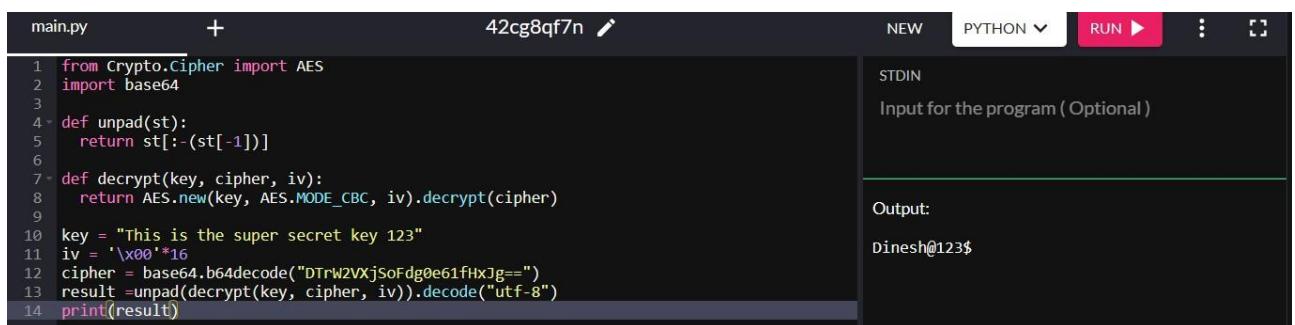
```

1 <?xml version='1.0' encoding='utf-8' standalone='yes' ?>
2 <map>
3   <string name="superSecurePassword">DTrW2VXjSoFdg0e61fHxJg==
4   </string>
5   <string name="EncryptedUsername">ZGluZXNo
6   </string>
7 </map>

```

Yêu cầu 5 Viết chương trình giải mã đoạn dữ liệu mã hoá (python3 chảng hạn...)

- Đề bài cũng đã cung cấp cho ta một đoạn mã java dùng thuật toán AES-256 với mode CBC và đệm PKCS5Padding để mã hóa kèm theo đó là key và iv dùng để giải mã.
- Từ đó ta có thể viết một chương trình Python dùng để giải mã. Chạy chương trình trên one compiler, kết quả trả về là mật khẩu của user dinesh.



```

from Crypto.Cipher import AES
import base64

def unpad(st):
    return st[:-st[-1]]

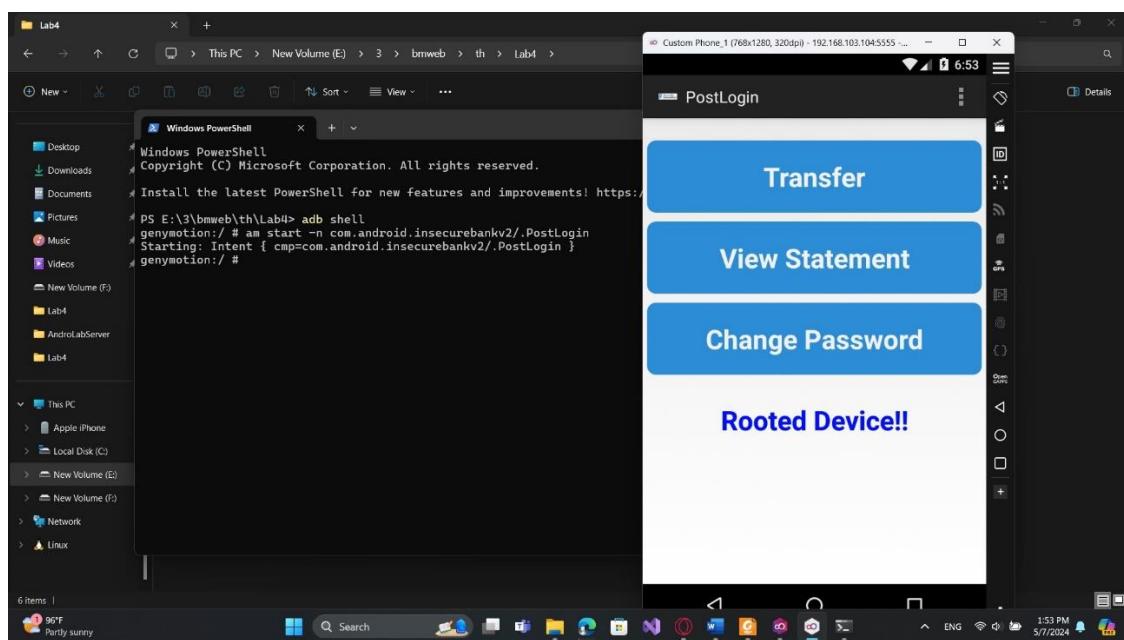
def decrypt(key, cipher, iv):
    return AES.new(key, AES.MODE_CBC, iv).decrypt(cipher)

key = "This is the super secret key 123"
iv = '\x00'*16
cipher = base64.b64decode("DTrW2VXjSoFdg0e61fHxJg==")
result = unpad(decrypt(key, cipher, iv)).decode("utf-8")
print(result)

```

Activity Hijacking

- Gọi Activity Manager (am): là lệnh gọi các lệnh của hệ thống; ví dụ chạy Activity, dừng một tiến trình, sửa đổi các thuộc tính...
- Thủ gọi activity PostLogin, dùng lệnh sau:
am start -n com.android.insecurebankv2/.PostLogin



2. Dịch ngược (Reverse Engineering)

- Đầu tiên ta sẽ sử dụng apktool để dịch ngược chương trình.

```
PS E:\3\bmweb\th\Lab4> apktool d InsecureBankv2.apk
I: Using Apktool 2.9.3 on InsecureBankv2.apk
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: C:\Users\kieut\AppData\Local\apktool\framework\1.apk
I: Decoding values */* XMLs...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

- Ta sẽ truy cập vào InsecureBankv2/smali/com/android/insecurebankv2/PostLogin.smali để sửa đổi tập tin. Thay đổi nhánh else để in ra Rooted Device

```
E: > 3 > bmweb > th > Lab4 > InsecureBankv2 > smali > com > android > insecurebankv2 > PostLogin.smali
422 .method showRootStatus()V
446
447     .line 88
448     .local v0, "isrooted":Z
449     :goto_0
450     if-ne v0, v1, :cond_2
451
452     .line 90
453     iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;->root_status:Landroid/widget/TextView;
454
455     const-string v2, "Rooted Device!!" [Red Box]
456
457     invoke-virtual {v1, v2}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V
458
459     .line 96
460     :goto_1
461     return-void
462
463     .line 87
464     .end local v0    # "isrooted":Z
465     :cond_1
466     const/4 v0, 0x0
467
468     goto :goto_0
469
470     .line 94
471     .restart local v0    # "isrooted":Z
472     :cond_2
473     iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;->root_status:Landroid/widget/TextView;
474
475     const-string v2, "Rooted Device!!" [Red Box]
476
477     invoke-virtual {v1, v2}, Landroid/widget/TextView;->setText(Ljava/lang/CharSequence;)V
478
479     goto :goto_1
480 .end method
```

- Sử dụng apktool để vá lại file apk

```
PS E:\3\bmweb\th\Lab4> apktool b InsecureBankv2 -o InsecureBankv2_1.apk
I: Using Apktool 2.9.3
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: InsecureBankv2_1.apk
```

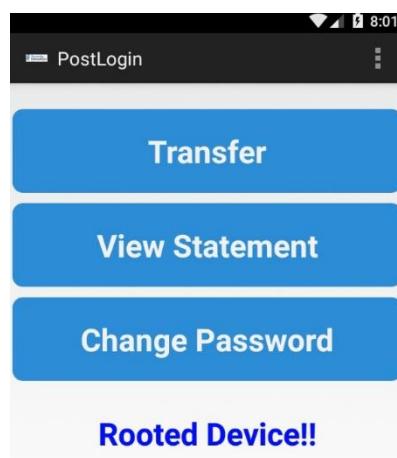
- Android yêu cầu các tập tin APK đều phải được ký bằng một chứng chỉ trước khi được phép cài đặt trên thiết bị. Sau khi chỉnh sửa, tập tin APK sẽ không còn toàn vẹn như ban đầu nên cần phải được ký lại.
- Vì vậy ta cần tạo key và kí

```
PS C:\Users\kieut> keytool -genkeypair -v -keystore E:\3\bmweb\th\Lab4\key.keystore -alias InsecureBankv2_1 -keyalg RSA
-keystore 2048 -validity 1000
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?
What is the name of your organizational unit?
What is the name of your organization?
What is the name of your City or Locality?
What is the name of your State or Province?
What is the two-letter country code for this unit?
Is CN=trang nguyen, OU=UIT, O=Group 06, L=HCM, ST=HCM, C=123 correct?
[no]: yes
Generating 2,048 bit RSA key pair and self-signed certificate (SHA384withRSA) with a validity of 1,000 days
    for: CN=trang nguyen, OU=UIT, O=Group 06, L=HCM, ST=HCM, C=123
[Storing E:\3\bmweb\th\Lab4\key.keystore]
```

```
PS C:\Program Files\Java\jdk-22\bin> jarsigner -keystore "E:\3\bmweb\th\Lab4\key.keystore" -storepass "E:\3\bmweb\th\Lab4\InsecureBankv2_1.apk" InsecureBankv2_1
jar signed.

Warning:
The signer's certificate is self-signed.
```

- Sau khi hoàn thành quá trình kí và tạo key ta sẽ cài đặt lại chương trình và kiểm tra.



3. Phân tích động (Dynamic Analysis)

- Địa chỉ IP của điện thoại ảo.

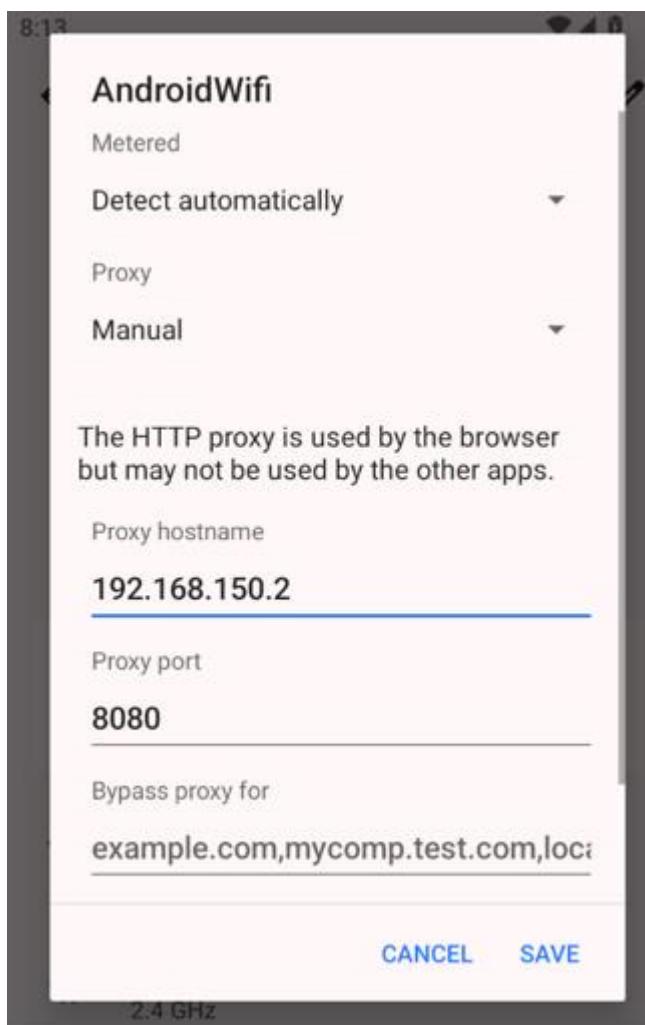
```
PS C:\Users\cuong> adb devices
List of devices attached
192.168.150.105:5555    device
```

- Tạo proxy cho điện thoại ảo.

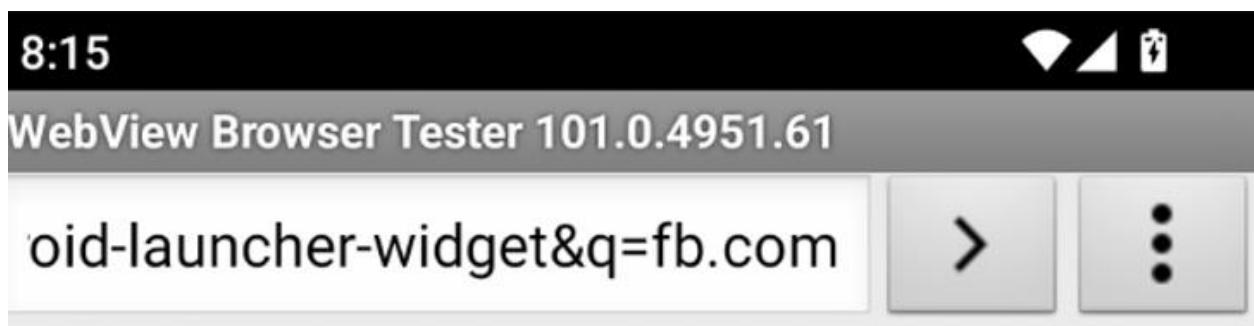
The screenshot shows the 'Add a new proxy listener' dialog in Burp Suite. The 'Binding' tab is active. The 'Bind to port:' field contains '8080'. The 'Bind to address:' section has three options: 'Loopback only' (radio button), 'All interfaces' (radio button), and 'Specific address:' (radio button, selected) with the value '192.168.150.2'. A note below says 'These settings control how Burp binds the proxy listener.'

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols	Support HTTP/2
	127.0.0.1:8080			Per-host	Default	✓
✓	192.168.150.2:80...			Per-host	Default	✓

- Cấu hình thông tin proxy điện thoại ảo.



- Truy cập thử trang fb.com.



- Ta thấy proxy đã được cấu hình thành công.

Request to http://fb.com:80 [157.240.217.35]

Forward	Drop	Intercept is on	Action	Open browser
---------	------	------------------------	--------	--------------

Pretty Raw Hex

```

1 GET / HTTP/1.1
2 Host: fb.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Linux; Android 13; Phone Build/TQCB.230505.005.A1; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/101.0.4951.61 Mobile Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 X-Requested-With: org.chromium.webview_shell
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: close
10

```

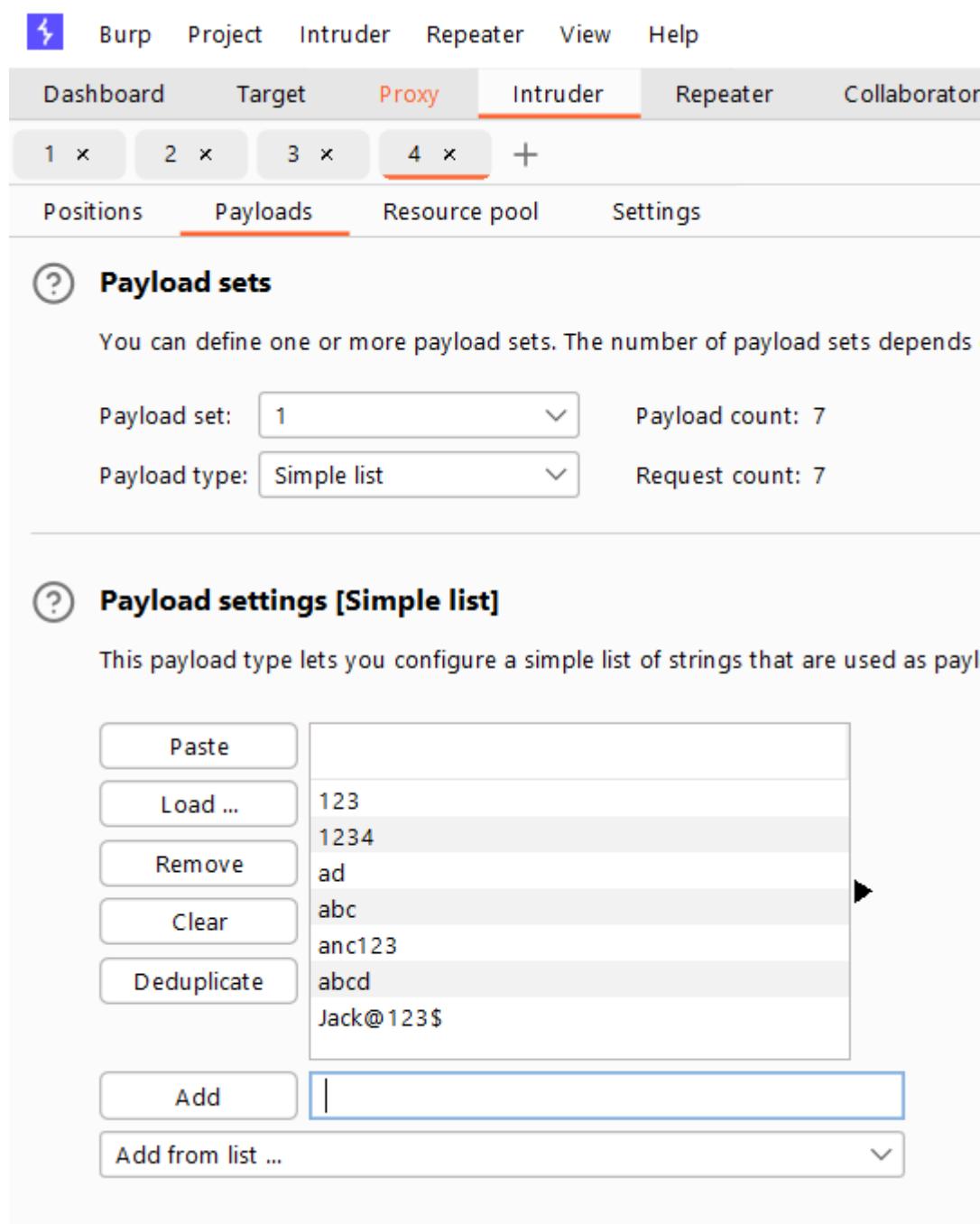
- Tại tab intruder, ta đánh dấu phần nội dung trường password.

Target: <http://10.0.2.2:8888>

```

1 POST /devlogin HTTP/1.1
2 Content-Length: 32
3 Content-Type: application/x-www-form-urlencoded
4 Host: 10.0.2.2:8888
5 Connection: close
6 User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)
7
8 username=jack&password=$11111$|
```

- Tại phần payload ta thêm các mật khẩu để tiến hành tấn công vét cạn.



The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. Under the 'Payloads' tab, there are four payload sets labeled 1 through 4. Set 1 is currently selected. The configuration for set 1 shows a payload count of 7 and a request count of 7, both using a simple list type. The payload list contains the following entries:

- 123
- 1234
- ad
- abc
- anc123
- abcd
- Jack@123\$

An 'Add' button is available to add more entries to the list.

- Kết quả sau khi tấn công vét cạn.

Request	Payload	Status code	Error	Timeout	Length
1	123		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	1234		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	ad		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	abc		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	anc123		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	abcd		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Jack@123\$		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

- Phần History hiển thị lịch sử của các request được gửi từ điện thoại ảo.

480 http://10.0.2.2:8888 POST /login ✓

Request

Pretty Raw Hex

```

1 POST /login HTTP/1.1
2 Content-Length: 36
3 Content-Type: application/x-www-form-urlencoded
4 Host: 10.0.2.2:8888
5 Connection: close
6 User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)
7
8 username=jack&password=Jack%40123%24

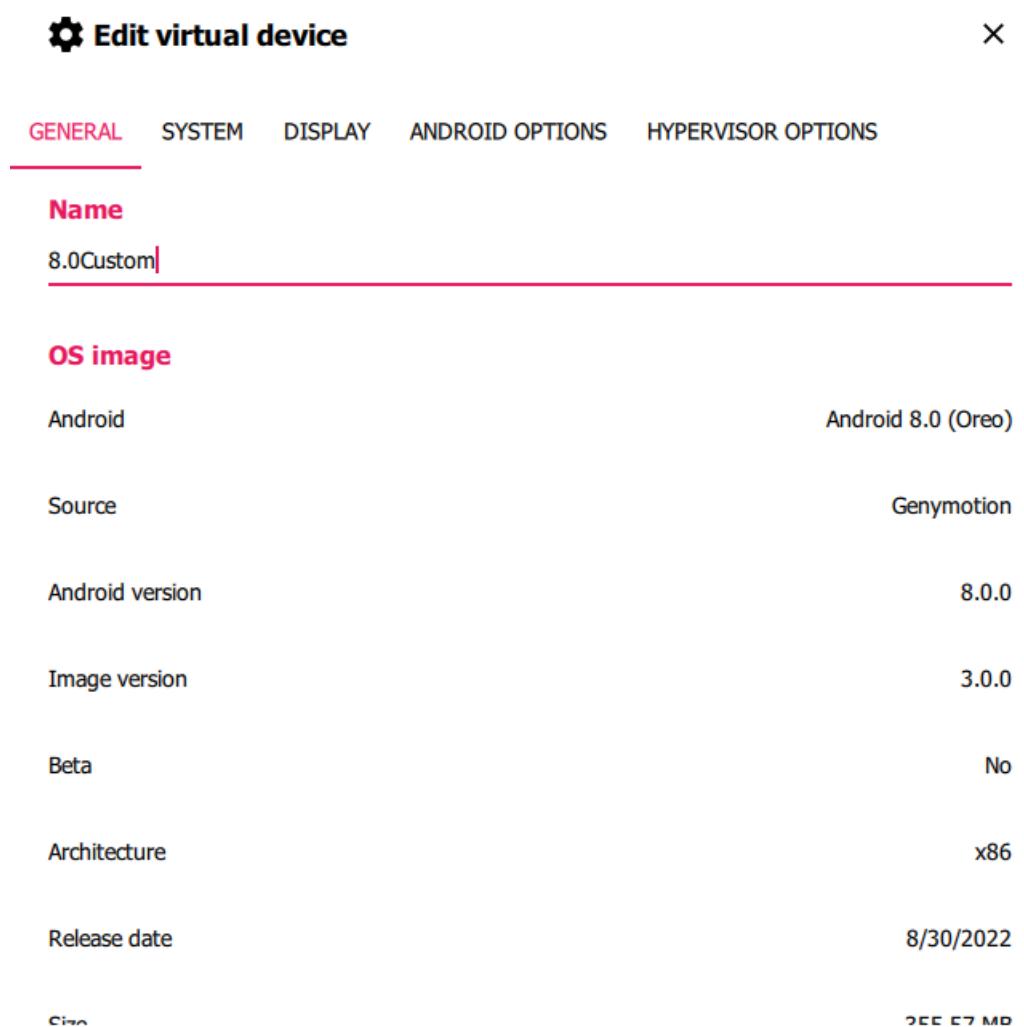
```

4. Hooking với Frida:

- Cài đặt Frida tool.

```
C:\Users\cuong>pip3 install frida-tools
Collecting frida-tools
  Downloading frida-tools-12.3.0.tar.gz (200 kB)
    200.5/200.5 kB 715.3 kB/s eta 0:00
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Installing backend dependencies ... done
  Preparing metadata (pyproject.toml) ... done
Requirement already satisfied: colorama<1.0.0,>=0.2.7 in c:\users\cuong\appdata\local\packages (from frida-tools) (0.4.6)
Collecting frida<17.0.0,>=16.0.9 (from frida-tools)
  Downloading frida-16.2.1-cp37-abi3-win_amd64.whl.metadata (2.1 kB)
Collecting prompt-toolkit<4.0.0,>=2.0.0 (from frida-tools)
  Downloading prompt_toolkit-3.0.43-py3-none-any.whl.metadata (6.5 kB)
Collecting pygments<3.0.0,>=2.0.2 (from frida-tools)
  Downloading pygments-2.18.0-py3-none-any.whl.metadata (2.5 kB)
Collecting wcwidth (from prompt-toolkit<4.0.0,>=2.0.0->frida-tools)
  Downloading wcwidth-0.2.13-py2.py3-none-any.whl.metadata (14 kB)
  Downloading frida-16.2.1-cp37-abi3-win_amd64.whl (32.7 MB)
    32.7/32.7 MB 14.6 MB/s eta 0:00:00
```

- Ở đây ta thấy kiến trúc điện thoại là x86.



- Do đó ta cần tải Frida-server tương ứng.

frida-server-16.2.1-android-x86.xz

15.1 MB

Feb 17

- Cài đặt Frida-server ở điện thoại ảo.

```
PS C:\Users\cuong\Downloads> adb push frida-server-16.2.1-android-x86 /data/local/tmp/frida-server
frida-server-16.2.1-android-x86: 1 file pushed. 102.0 MB/s (51807740 bytes in 0.484s)
PS C:\Users\cuong\Downloads> adb shell
genymotion:/ # chmod +x frida-server
chmod: frida-server: No such file or directory
1|genymotion:/ # cd /data/local/tmp/
genymotion:/data/local/tmp # chmod +x frida-server
genymotion:/data/local/tmp # ./frida-server &
[1] 1900
```

- Cài đặt thành công.

```
PS C:\Users\cuong> frida-ps -U
  PID  Name
----- 
 1436  Calendar
  952  Clock
 1505  Email
 1602  Messaging
  997  Phone
 1364  Search
  788  Settings
 1797  Superuser
  238  adbd
 1852  android.ext.services
  468  android.hardware.camera.provider@2.4-service
  469  android.hardware.configstore@1.0-service
  232  android.hardware.gnss@1.0-service
  470  android.hardware.graphicsallocator@2.0-service
  169  android.hardware.keymaster@3.0-service
  471  android.hardware.sensors@1.0-service
  472  android.hardware.wifi@1.0-service
```

Yêu cầu 7 Hoàn thiện đoạn code trên và demo.

- Đoạn script hook1.py

```

import frida
import time

device = frida.get_usb_device()
pid = device.spawn("com.android.insecurebankv2")
device.resume(pid)

time.sleep(1)
session=device.attach(pid)

hook_script=""""
Java.perform
(
    function()
    {
        console.log("Inside the hook_script");
        classPostLogin = Java.use('com.android.insecurebankv2.PostLogin');
        classPostLogin.doesSuperuserApkExist.implementation = function()
        {
            return true;
        };
    }
);
"""

script=session.create_script(hook_script)
script.load()

input('...?')

```

- Ở đây ta sẽ ghi đè method doesSuperuserApkExist() bằng cách sử dụng implementation.

```

classPostLogin.doesSuperuserApkExist.implementation = function()
{
    return true;
};

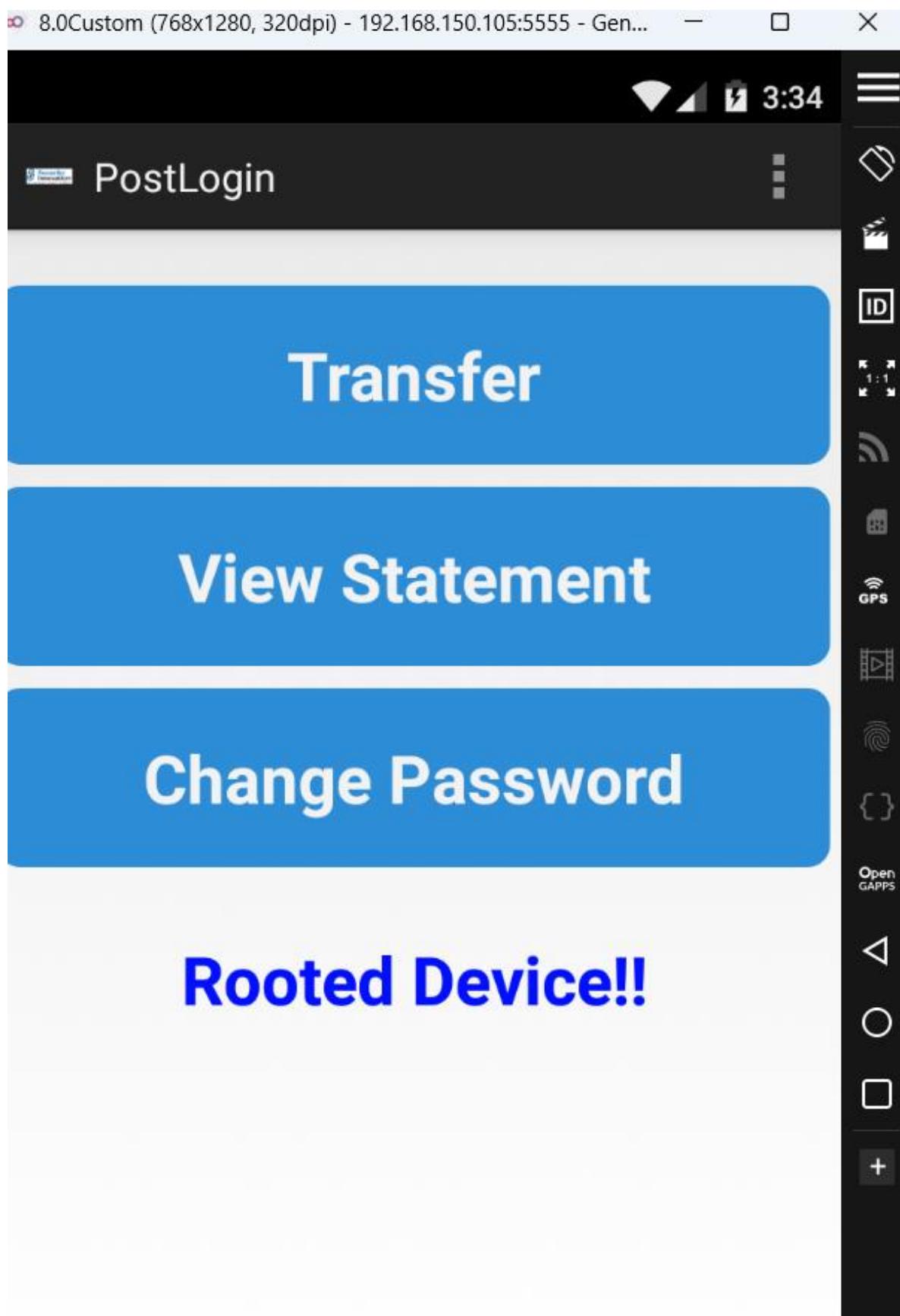
```

- Khi doesSuperuserApkExist() == true thì root detected.

```
void showRootStatus() {  
    boolean var1;  
    if (!this.doesSuperuserApkExist("/system/app/Superuser.apk") && !this.doesSUexist()) {  
        var1 = false;  
    } else {  
        var1 = true;  
    }  
  
    if (var1) {  
        this.root_status.setText("Rooted Device!!");  
    } else {  
        this.root_status.setText("Device not Rooted!!");  
    }  
}
```

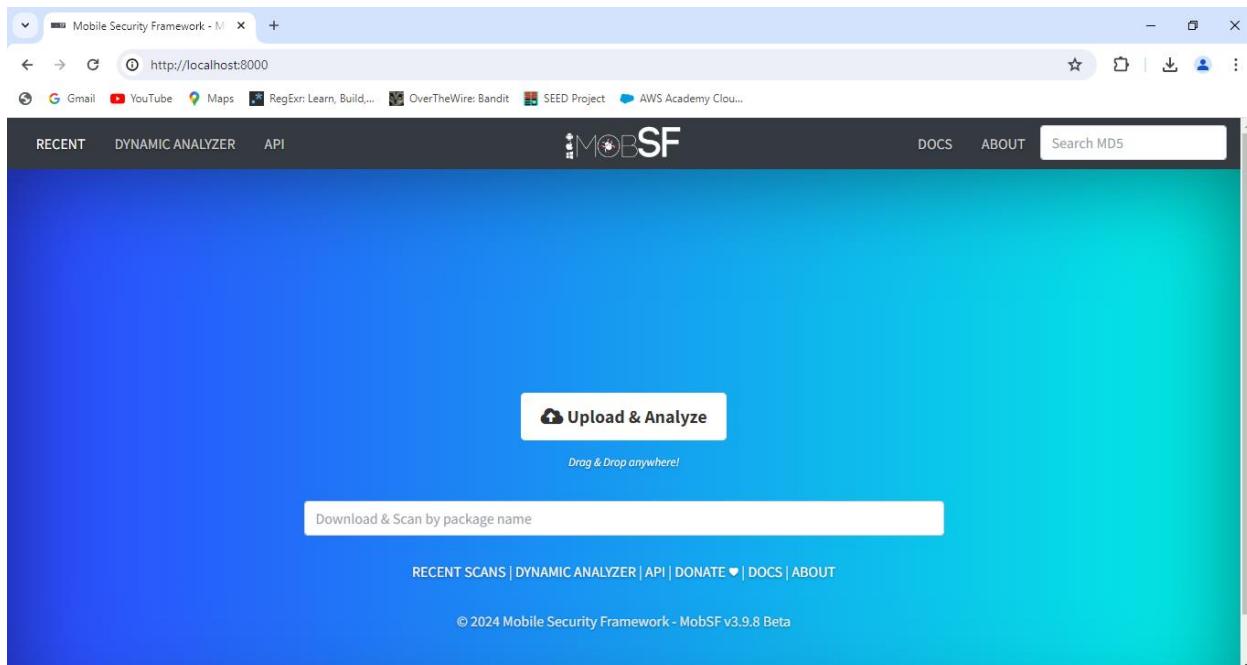
```
PS C:\Users\cuong\Downloads> python hook1.py  
Inside the hook_script  
...?|
```

- Kết quả cho thấy ta root device thành công.



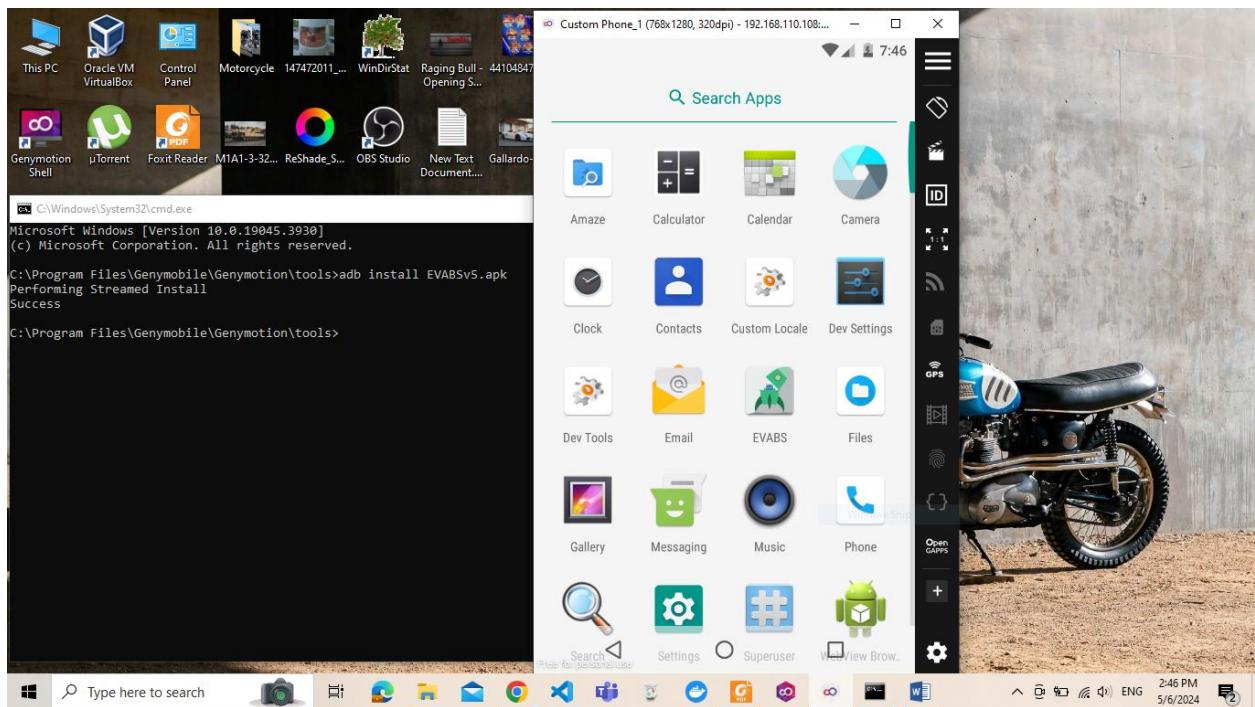
D. CHALLENGES CTF (BÀI TẬP BẢO MẬT ỨNG DỤNG)

Thiết lập môi trường

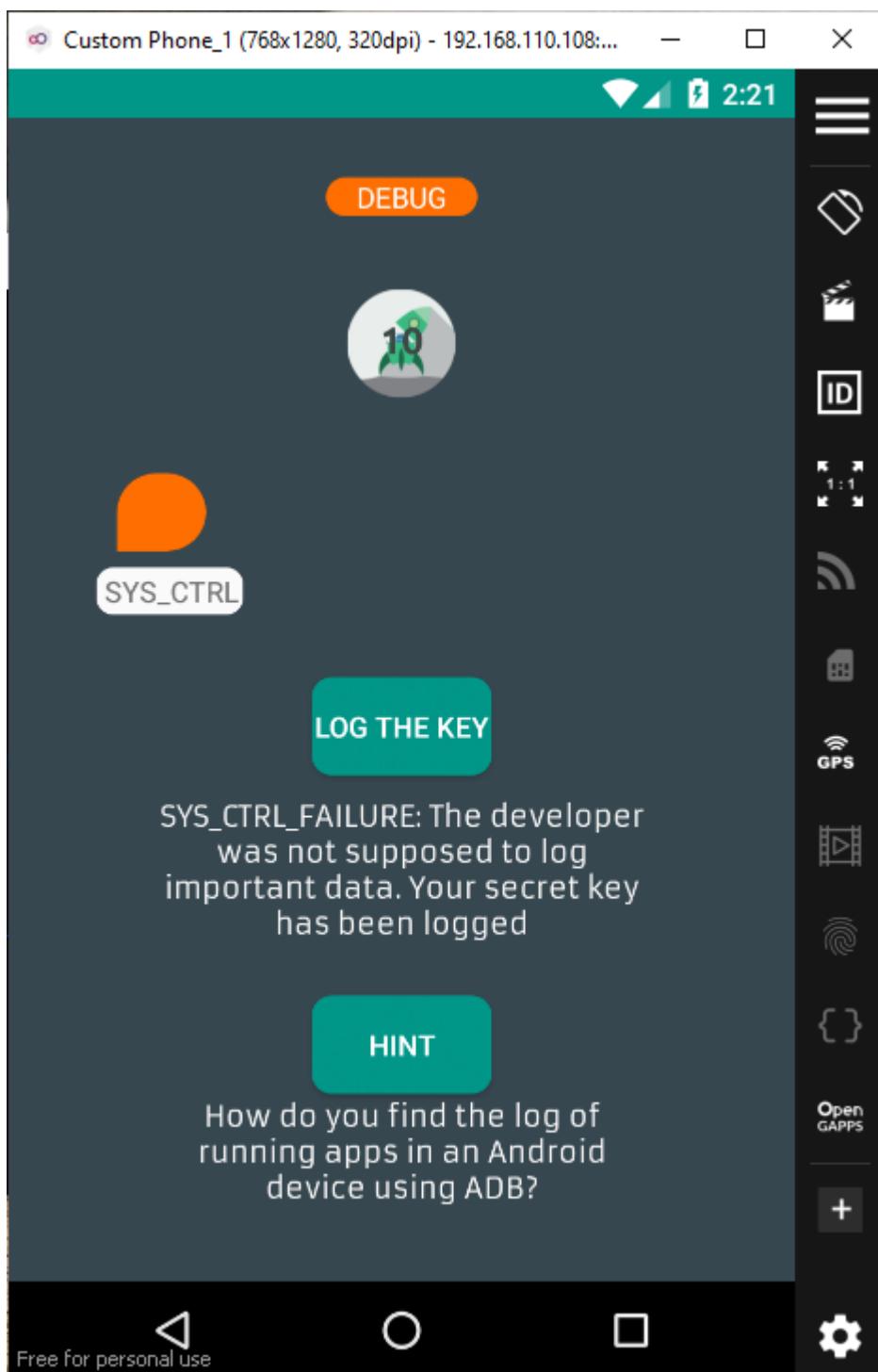


CHALLENGES CTF

EV ABS



Flag1:



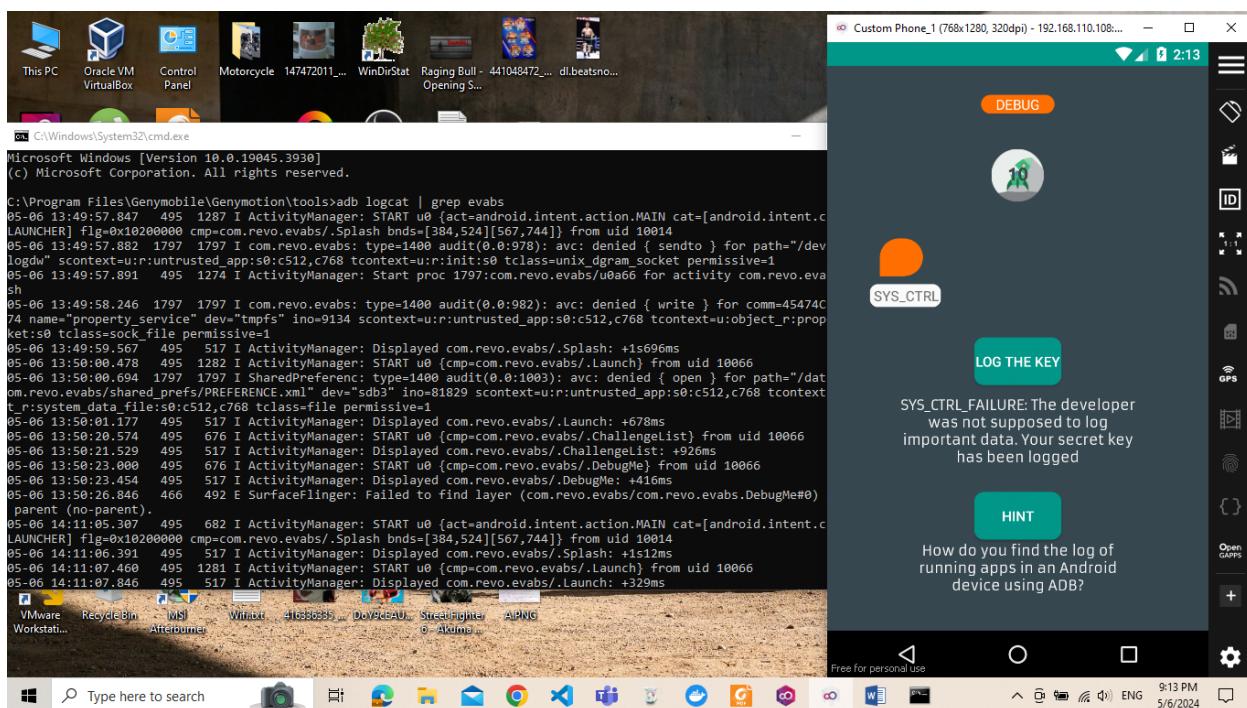
Tiến hành xem log của chương trình

```
C:\Windows\System32\cmd.exe - adb logcat
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\Genymobile\Genymotion\tools>adb install EVABSV5.apk
Performing Streamed Install
Success

C:\Program Files\Genymobile\Genymotion\tools>adb logcat
----- beginning of system
05-06 07:35:12.779 159 159 I void    : Void 3.0 (the awakening) firing up
05-06 07:35:12.779 159 159 V void    : Detected support for: ext4 vfat
05-06 07:35:12.785 159 159 I void    : [libfs_mgr]fs_mngr_read_fstab_dt(): failed to read fstab from dt
05-06 07:35:12.795 159 172 I void    : e4crypt_initialize_global_de
05-06 07:35:12.795 159 172 I void    : Creating new key
05-06 07:35:12.800 159 172 D void    : Creating key that doesn't need auth token
05-06 07:35:12.803 159 172 D void    : Created key /data/unencrypted/key
05-06 07:35:12.803 159 172 D void    : Added key 1010257162 (ext4:7fc5a61ddedfdaf5) to keyring 671894807 in process 159
05-06 07:35:12.858 159 172 D void    : e4crypt_init_user0
05-06 07:35:12.858 159 172 D void    : Preparing: /data/misc/vold/user_keys
05-06 07:35:12.858 159 172 D void    : Preparing: /data/misc/vold/user_keys/ce
05-06 07:35:12.858 159 172 D void    : Preparing: /data/misc/vold/user_keys/de
05-06 07:35:12.858 159 172 D void    : Preparing: /data/misc/vold/user_keys/ce/0
05-06 07:35:12.858 159 172 D void    : Skipping non-key .
05-06 07:35:12.858 159 172 D void    : Skipping non-key ..
05-06 07:35:12.861 159 172 D void    : Creating key that doesn't need auth token
05-06 07:35:12.863 159 172 D void    : Created key /data/misc/vold/user_keys/ce/0/current
05-06 07:35:12.867 159 172 D void    : Creating key that doesn't need auth token
05-06 07:35:12.872 159 172 D void    : Created key /data/misc/vold/user_keys/de/0
05-06 07:35:12.873 159 172 D void    : Added key 26902 (ext4:6c0c1d38fa584250) to keyring 671894807 in process 159
```

Ta thấy được tiến trình chạy lên bằng lệnh grep evabs

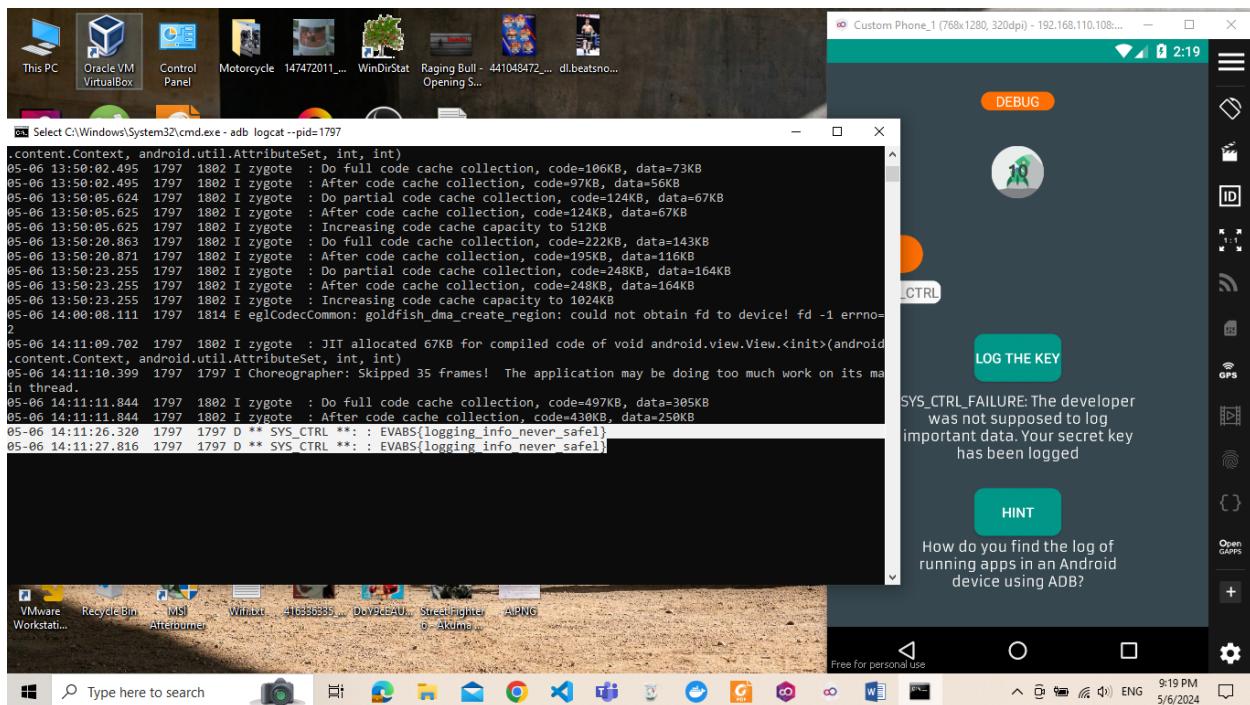


```
C:\Program Files\Genymobile\Genymotion\tools>adb logcat | grep evabs
05-06 13:49:57.847 495 1287 I ActivityManager: START u0 {act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] flg=0x10200000 cmp=com.revo.evabs/.Splash}
ash bnds=[384,524][567,744]} from uid 10014
context=u:r:init:s0 tclass=unix_dgram_socket permissive=1
05-06 13:49:57.883 1797 1797 I com.revo.evabs: type=1400 audit(0.0:978): avc: denied { sendto } for path="/dev/socket/logdw" scontext=u:r:untrusted_app:s0:c512,c768 t
context=u:::untrusted_app:s0:c512,c768 tcontext=u:object_r:property_socket:s0 tclass=sock_file permissive=1
05-06 13:49:58.246 1797 1797 I com.revo.evabs: type=1400 audit(0.0:982): avc: denied { write } for comm=45474C20496E6974 name="property_service" dev="tmpfs" ino=9134
scontext=u:::untrusted_app:s0:c512,c768 tcontext=u:object_r:property_socket:s0 tclass=sock_file permissive=1
05-06 13:49:58.567 495 517 I ActivityManager: Start proc 1797:com.revo.evabs/u0a66 for activity com.revo.evabs/.Splash
05-06 13:50:00.478 495 517 I ActivityManager: Displayed com.revo.evabs/.Splash: +1s696ms
05-06 13:50:00.694 1797 1797 I SharedPreference: type=1400 audit(0.0:1003): avc: denied { open } for path="/data/data/com.revo.evabs/shared_prefs/PREFERENCE.xml" dev="sdcard" ino=81829 scontext=u:::untrusted_app:s0:c512,c768 tcontext=u:object_r:system_data_file:s0:c512,c768 tclass=file permissive=1
05-06 13:50:01.177 495 517 I ActivityManager: Displayed com.revo.evabs/.Launch: +678ms
05-06 13:50:20.574 495 676 I ActivityManager: START u0 {cmp=com.revo.evabs/.ChallengeList} from uid 10066
05-06 13:50:21.529 495 517 I ActivityManager: Displayed com.revo.evabs/.ChallengeList: +926ms
05-06 13:50:23.000 495 676 I ActivityManager: START u0 {cmp=com.revo.evabs/.DebugMe} from uid 10066
05-06 13:50:23.456 495 517 I ActivityManager: Displayed com.revo.evabs/.DebugMe: +416ms
05-06 13:50:23.846 495 492 E SurfaceFlinger: Failed to find layer (com.revo.evabs/com.revo.evabs.DebugMe#0) in layer parent (no-parent).
05-06 14:11:05.307 495 682 I ActivityManager: START u0 {act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] flg=0x10200000 cmp=com.revo.evabs/.Splash}
ash bnds=[384,524][567,744]} from uid 10014
05-06 14:11:06.391 495 517 I ActivityManager: Displayed com.revo.evabs/.Splash: +1s12ms
05-06 14:11:07.466 495 1281 I ActivityManager: START u0 {cmp=com.revo.evabs/.Launch} from uid 10066
05-06 14:11:07.846 495 517 I ActivityManager: Displayed com.revo.evabs/.Launch: +329ms
05-06 14:11:09.442 495 813 I ActivityManager: START u0 {cmp=com.revo.evabs/.ChallengeList} from uid 10066
05-06 14:11:10.414 495 517 I ActivityManager: Displayed com.revo.evabs/.ChallengeList: +943ms
05-06 14:11:11.712 495 1287 I ActivityManager: START u0 {cmp=com.revo.evabs/.DebugMe} from uid 10066
05-06 14:11:12.036 495 517 I ActivityManager: Displayed com.revo.evabs/.DebugMe: +289ms
```

Tiếp tục tìm kiếm tiến trình với pid như vậy

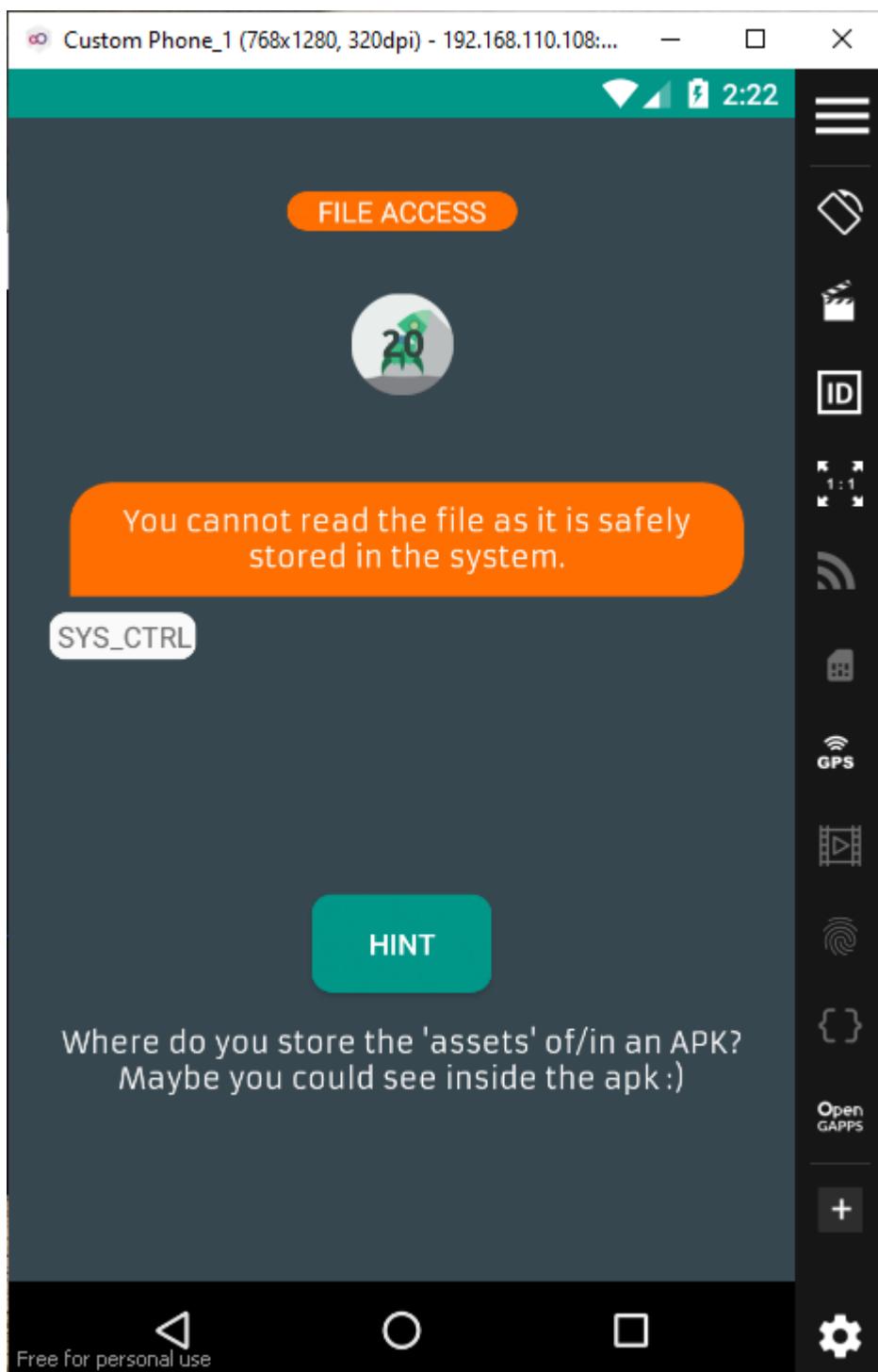
```
C:\Windows\System32\cmd.exe - adb logcat --pid=1797
- beginning of main
05-06 13:49:57.883 1797 1797 I com.revo.evabs: type=1400 audit(0.0:978): avc: denied { sendto } for path="/dev/socket/logdw" scontext=u:r:untrusted_app:s0:c512,c768 t
context=u:::untrusted_app:s0 tclass=unix_dgram_socket permissive=1
05-06 13:49:57.886 1797 1797 I zygote : Late-enabling Xcheck:jni
05-06 13:49:57.919 1797 1797 W zygote : Unexpected CPU variant for X86 using defaults: x86
05-06 13:49:57.966 1797 1797 I JNLP : type=1400 audit(0.0:980): avc: denied { connectto } for path=/006A6477782D36F6E74726F6C scontext=u:r:untrusted_app:s0:c512,c768 t
context=u:::untrusted_app:s0 tclass=unix_stream_socket permissive=1
05-06 13:49:58.246 1797 1797 I com.revo.evabs: type=1400 audit(0.0:982): avc: denied { write } for comm=45474C20496E6974 name="property_service" dev="tmpfs" ino=9134
scontext=u:::untrusted_app:s0:c512,c768 tcontext=u:object_r:property_socket:s0 tclass=sock_file permissive=1
05-06 13:49:58.250 1797 1812 I vndksupport: sphal namespace is not configured for this process. Loading /vendor/lib/egl/libGLES_emulation.so from the current namespace instead.
05-06 13:49:58.250 1797 1812 I vndksupport: sphal namespace is not configured for this process. Loading /vendor/lib/egl/libEGL_emulation.so from the current namespace instead.
05-06 13:49:58.252 1797 1812 I vndksupport: sphal namespace is not configured for this process. Loading /vendor/lib/egl/libGLESv1_CM_emulation.so from the current namespace instead.
05-06 13:49:58.262 1797 1812 I vndksupport: sphal namespace is not configured for this process. Loading /vendor/lib/egl/libGLESv2_emulation.so from the current namespace instead.
05-06 13:49:58.362 1797 1797 D FirebaseApp: com.google.firebaseio.iid.FirebaseInstanceId is not linked. Skipping initialization.
05-06 13:49:58.362 1797 1797 D FirebaseApp: com.google.firebaseio.crash.FirebaseCrash is not linked. Skipping initialization.
05-06 13:49:58.362 1797 1797 D FirebaseApp: com.google.android.gms.measurement.AppMeasurement is not linked. Skipping initialization.
05-06 13:49:58.362 1797 1797 I FirebaseInitProvider: FirebaseApp initialization successful
05-06 13:49:58.502 1797 1814 O OpenGLRenderer: HWUI GL Pipeline
05-06 13:49:58.586 1797 1797 I RenderThread: type=1400 audit(0.0:983): avc: denied { write } for name="local_opengl" dev="tmpfs" ino=11246 scontext=u:r:untrusted_app:s0:c512,c768 t
context=u:::untrusted_app:s0:object_r:socket_device:s0 tclass=sock_file permissive=1
05-06 13:49:58.586 1797 1797 I RenderThread: type=1400 audit(0.0:984): avc: denied { connectto } for path="/dev/socket/local_opengl" scontext=u:r:untrusted_app:s0:c512,c768 t
context=u:::untrusted_app:s0:object_r:socket_device:s0 tclass=sock_file permissive=1
05-06 13:49:58.588 1797 1814 D : HostConnection: get() New Host Connection established 0xe0824100, pid 1797, tid 1814
05-06 13:49:58.598 1797 1814 D : HostComposition ext ANDROID_EMU_host_composition_v1 ANDROID_EMU_host_composition_v2 ANDROID_EMU_async_unmap_buffer ANDROID_EMU_sync_buffer_data GL_OES_EGL_image_external_essl3 GL_OES_vertex_array_object GL_KHR_texture_compression_astc_ldr ANDROID_EMU_host_side_tracing ANDROID_EMU_async_frame_commands ANDROID_EMU_gles_max_version_3_1
05-06 13:49:58.598 1797 1814 W : Process pipe failed
05-06 13:49:58.714 1797 1814 I OpenGLRenderer: Initialized EGL, version 1.4
05-06 13:49:58.715 1797 1814 D OpenGLRenderer: Swap behavior 1
05-06 13:49:58.744 1797 1814 W OpenGLRenderer: Failed to choose config with EGL_SWAP_BEHAVIOR_PRESERVED, retrying without...
05-06 13:49:58.744 1797 1814 D OpenGLRenderer: Swap behavior 0
05-06 13:49:58.779 1797 1814 D EGL_emulation: eglCreateContext: 0xe08050c0: maj 3 min 1 rcv 4
05-06 13:49:59.209 1797 1814 I vndksupport: sphal namespace is not configured for this process. Loading /vendor/lib/hw/gralloc.vbox86.so from the current namespace instead.
05-06 13:49:59.209 1797 1814 D : createUnique: call
05-06 13:49:59.210 1797 1814 D : HostConnection: get() New Host Connection established 0xe0824370, pid 1797, tid 1814
05-06 13:49:59.216 1797 1814 D : HostComposition ext ANDROID_EMU_host_composition_v1 ANDROID_EMU_host_composition_v2 ANDROID_EMU_async_unmap_buffer ANDROID_EMU_sync_buffer_data GL_OES_EGL_image_external_essl3 GL_OES_vertex_array_object GL_KHR_texture_compression_astc_ldr ANDROID_EMU_host_side_tracing ANDROID_EMU_async_frame_commands ANDROID_EMU_gles_max_version_3_1
```

Ta thu được flag

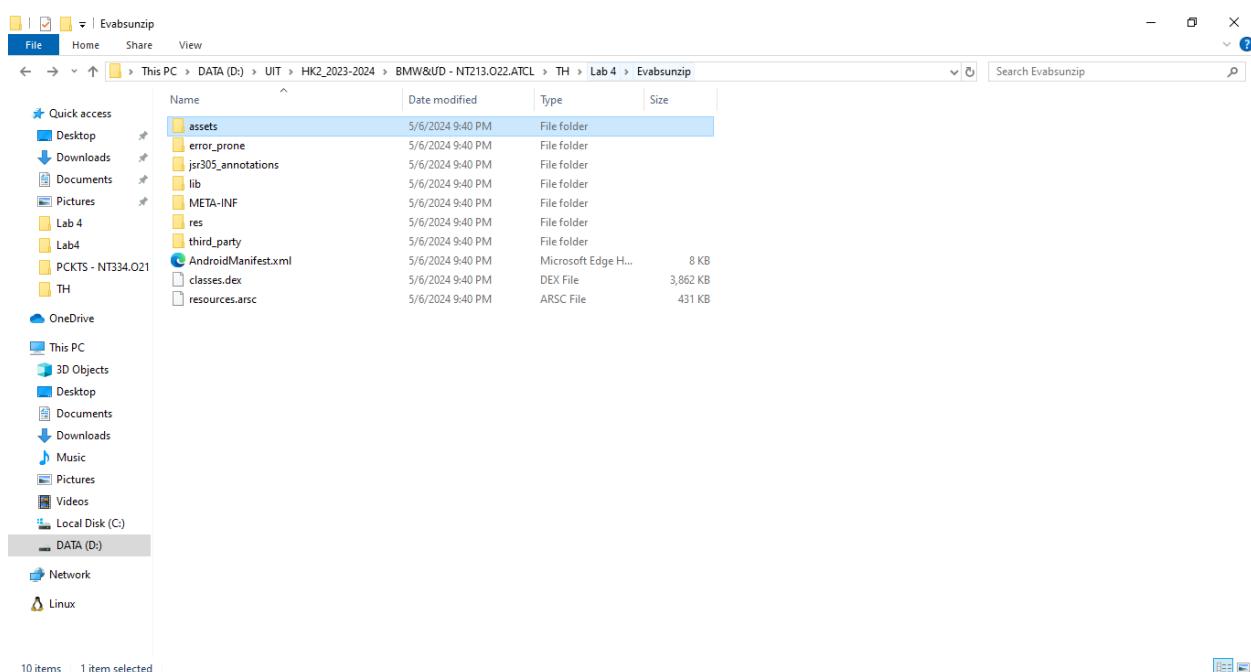


Flag: EVABS{logging_info_never_safel}

Flag2:



Ta thực hiện giải nén file apk



Tiến hành kiểm tra trong assets

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

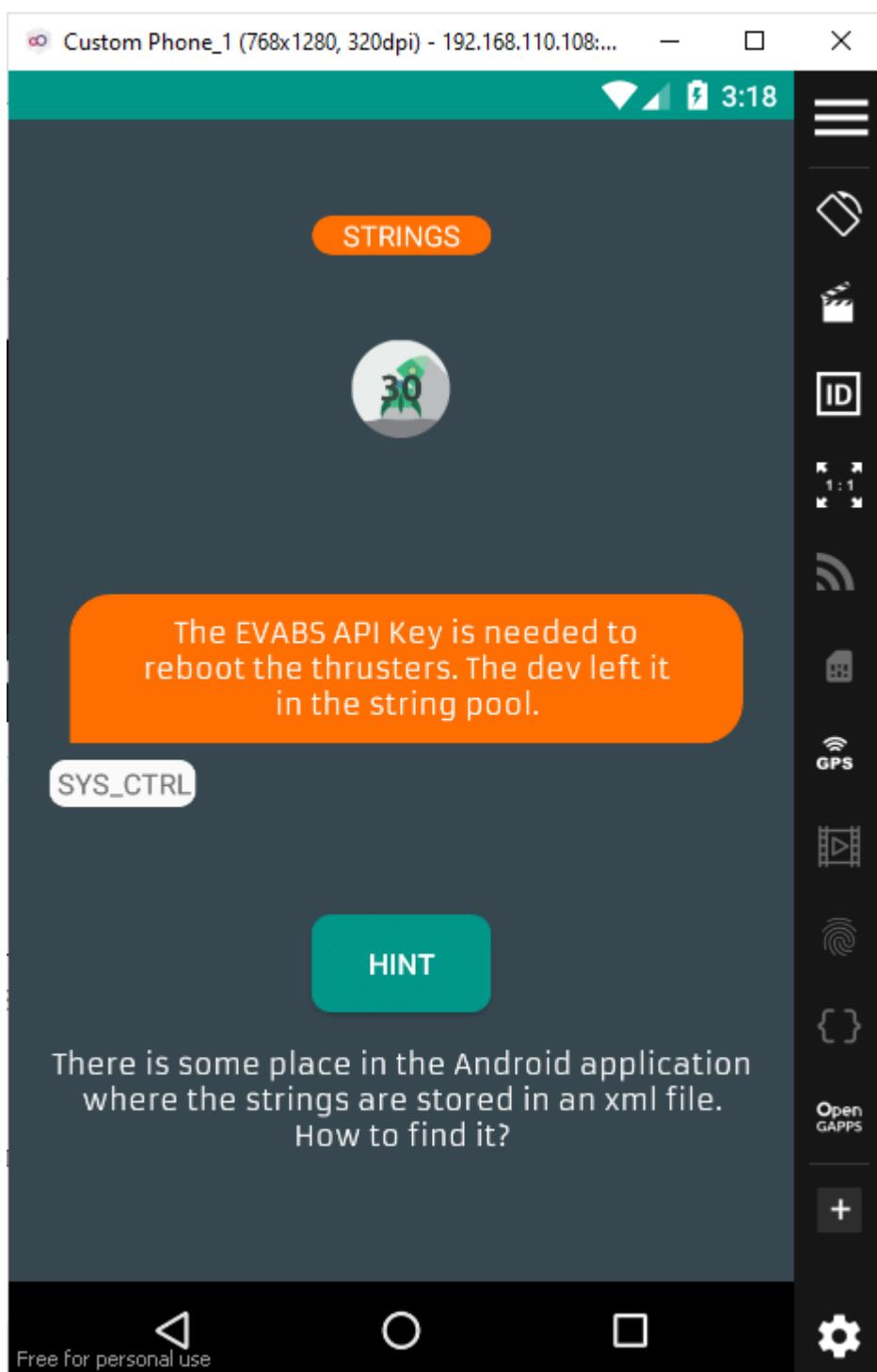
D:\UIT\HK2_2023-2024\BMW&UD - NT213.022.ATCL\TH\Lab 4\Evabsunzip\assets>ls
fonts secrets

D:\UIT\HK2_2023-2024\BMW&UD - NT213.022.ATCL\TH\Lab 4\Evabsunzip\assets>cat secrets
EVABS{fil3s_!n_ass3ts_ar3_eas!ly_hackabl3}
D:\UIT\HK2_2023-2024\BMW&UD - NT213.022.ATCL\TH\Lab 4\Evabsunzip\assets>
```

Ta thu được flag

Flag: EVABS{fil3s_!n_ass3ts_ar3_eas!ly_hackabl3}

Flag3:



Tiến hành cài đặt apktool

```

C:\Windows\System32\cmd.exe
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL\Desktop\apktool>apktool
Apktool 2.9.3 - a tool for reengineering Android apk files
with smali v3.0.3 and baksmali v3.0.3
Copyright 2010 Ryszard Wiśniewski <brut.alll@gmail.com>
Copyright 2010 Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
    -advance,--advanced      Print advanced information.
    -version,--version       Print the version.
usage: apktool if|install-framework [options] <framework.apk>
    -p,--frame-path <dir>   Store framework files into <dir>.
    -t,--tag <tag>          Tag frameworks using <tag>.
usage: apktool d[ecode] [options] <file_apk>
    -f,--force              Force delete destination directory.
    -o,--output <dir>       The name of folder that gets written. (default: apk.out)
    -p,--frame-path <dir>   Use framework files located in <dir>.
    -r,--no-res              Do not decode resources.
    -s,--no-src              Do not decode sources.
    -t,--frame-tag <tag>    Use framework files tagged by <tag>.
usage: apktool b[uild] [options] <app_path>
    -f,--force-all          Skip changes detection and build all files.
    -o,--output <dir>        The name of apk that gets written. (default: dist/name.apk)
    -p,--frame-path <dir>   Use framework files located in <dir>.

For additional info, see: https://apktool.org
For smali/baksmali info, see: https://github.com/google/smali

C:\Users\DELL\Desktop\apktool>
```

Thực hiện decompile file

```

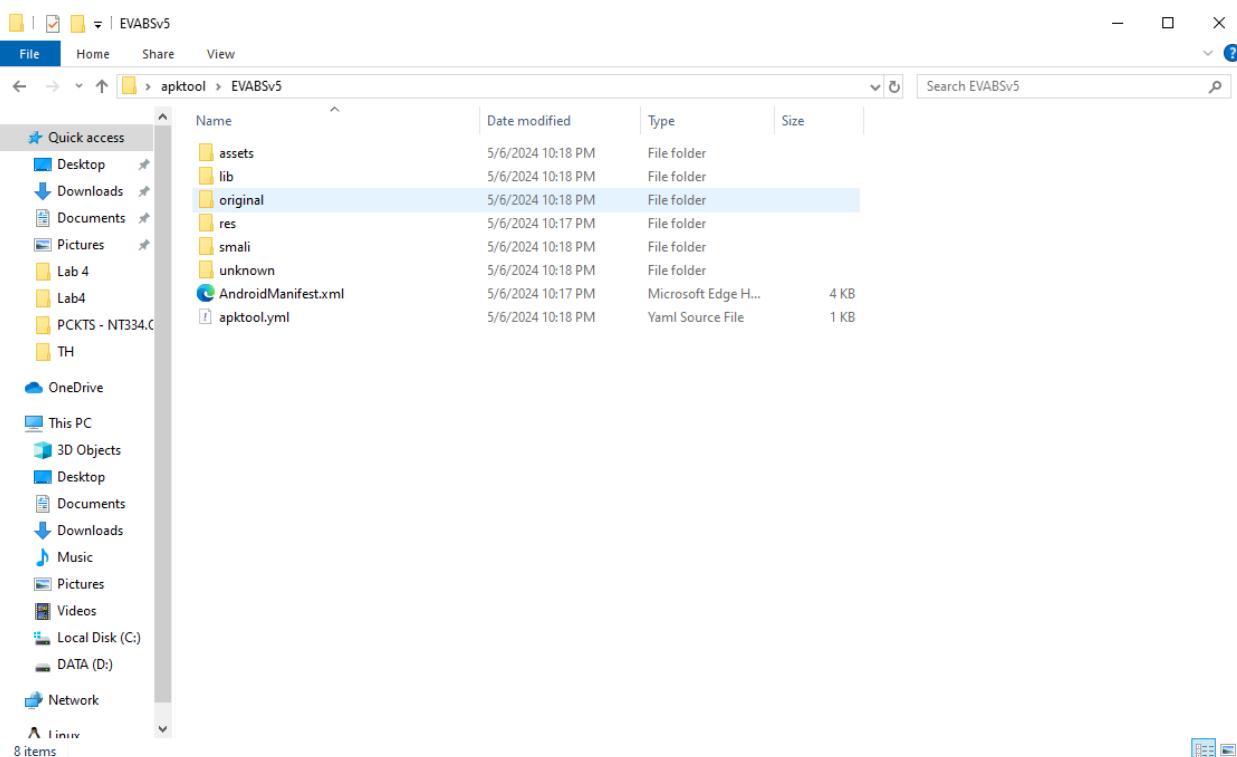
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL\Desktop\apktool>apktool if EVABSv5.apk
I: Framework installed to: C:\Users\DELL\AppData\Local\apktool\framework\127.apk

C:\Users\DELL\Desktop\apktool>apktool d EVABSv5.apk
I: Using Apktool 2.9.3 on EVABSv5.apk
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: C:\Users\DELL\AppData\Local\apktool\framework\1.apk
I: Decoding values /* XMLs...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

C:\Users\DELL\Desktop\apktool>
```

Ta thu được folder



Vào thư mục /res/values và kiểm tra các file strings

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Hien\Desktop\apktool\EVABSV5\res\values>cat strings.xml
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="abc_action_bar_home_description">Navigate home</string>
    <string name="abc_action_bar_home_description_format">%1$s, %2$s</string>
    <string name="abc_action_bar_home_subtitle_description_format">%1$s, %2$s, %3$s</string>
    <string name="abc_action_bar_up_description">Navigate up</string>
    <string name="abc_action_menu_overflow_description">More options</string>
    <string name="abc_action_mode_done">Done</string>
    <string name="abc_activity_chooser_view_see_all">See all</string>
    <string name="abc_activitychooserview_choose_application">Choose an app</string>
    <string name="abc_capital_off">OFF</string>
    <string name="abc_capital_on">ON</string>
    <string name="abc_font_family_body_1_material">sans-serif</string>
    <string name="abc_font_family_body_2_material">sans-serif-medium</string>
    <string name="abc_font_family_button_material">sans-serif-medium</string>
    <string name="abc_font_family_caption_material">sans-serif</string>
    <string name="abc_font_family_display_1_material">sans-serif</string>
    <string name="abc_font_family_display_2_material">sans-serif</string>
    <string name="abc_font_family_display_3_material">sans-serif</string>
    <string name="abc_font_family_display_4_material">sans-serif-light</string>
    <string name="abc_font_family_headline_material">sans-serif</string>
    <string name="abc_font_family_menu_material">sans-serif</string>
    <string name="abc_font_family_subhead_material">sans-serif</string>
    <string name="abc_font_family_title_material">sans-serif-medium</string>
    <string name="abc_search_hint">Search...</string>
    <string name="abc_searchview_description_clear">Clear query</string>
```

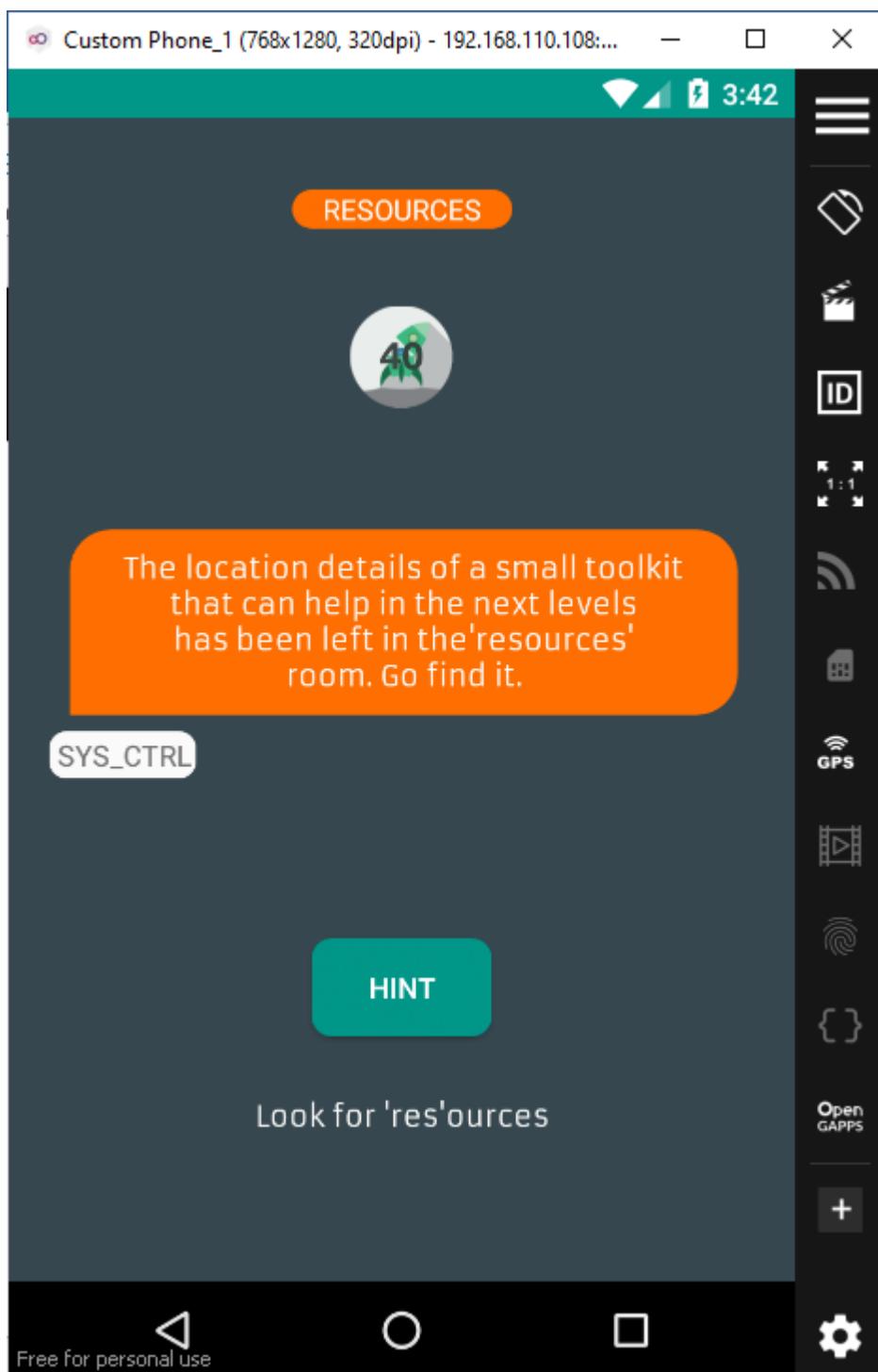
```
cmd Select C:\Windows\System32\cmd.exe
<string name="ob_header3">NO HIDDEN CHARGES OR FEES</string>
<string name="password_toggle_content_description">Toggle password visibility</string>
<string name="path_password_eye">M12,4.5C7,4.5 2.73,7.61 1,12c1.73,4.39 6,7.5 11,7.5s9.27,-3.11 11,-7.5c-1.73,-4.39
-6,-7.5 -11,-7.5zM12,17c-2.76,0 -5,-2.24 -5,-5s2.24,-5 5,-5.2.24 5,5 -2.24,5 -5,5zM12,9c-1.66,0 -3,1.34 -3,3s1.34,3 3,
3 3,-1.34 3,-3 -3,-3z</string>
<string name="path_password_eye_mask_strike_through">M2,4.27 L19.73,22 L22.27,19.46 L4.54,1.73 L4.54,1 L23,1 L23,23
L1,23 L1,4.27 Z</string>
<string name="path_password_eye_mask_visible">M2,4.27 L2,4.27 L4.54,1.73 L4.54,1.73 L4.54,1 L23,1 L23,23 L1,23 L1,4.
27 Z</string>
<string name="path_password_strike_through">M3.27,4.27 L19.74,20.74</string>
<string name="permission_rationale">"Contacts permissions are needed for providing email
completions."</string>
<string name="project_id">evabs-c0e8b</string>
<string name="prompt_email">Email</string>
<string name="prompt_password">Password (optional)</string>
<string name="search_menu_title">Search</string>
<string name="section_format">Hello World from section: %1$d</string>
<string name="status_bar_notification_info_overflow">999+</string>
<string name="the_evabs_api_key">EVABS{saf3ly_st0red_in_Strings?}</string>
<string name="title_activity_home">Home</string>
<string name="title_activity_launch">Launch</string>
<string name="title_activity_login">Sign in</string>
<string name="title_activity_splash">Splash</string>
<string name="title_activity_test">Test</string>
</resources>

C:\Users\Dell\Desktop\apktool\EVABSV5\res\values>
```

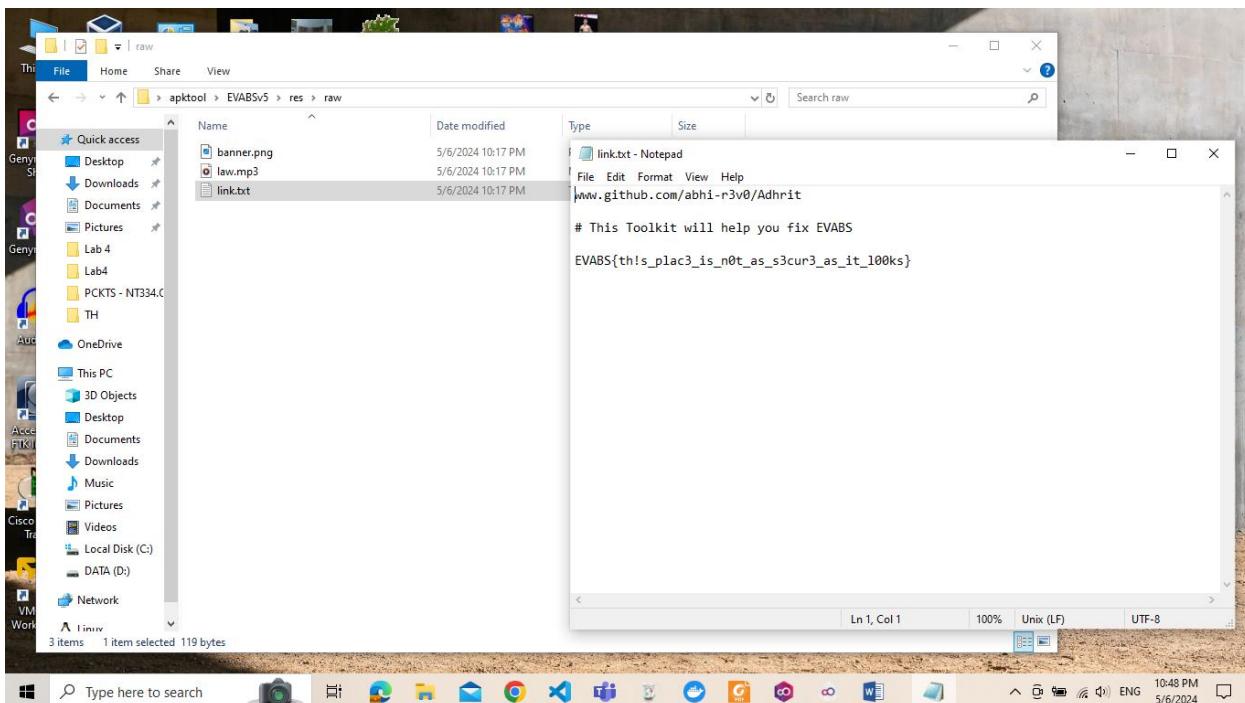
Ta thu được flag

Flag: EVABS{saf3ly_st0red_in_Strings?}

Flag4



Thông qua quá trình tìm kiếm trong /res, ta thu được flag



Flag: EVABS{th!s_plac3_is_n0t_as_s3cur3_as_it_l00ks}

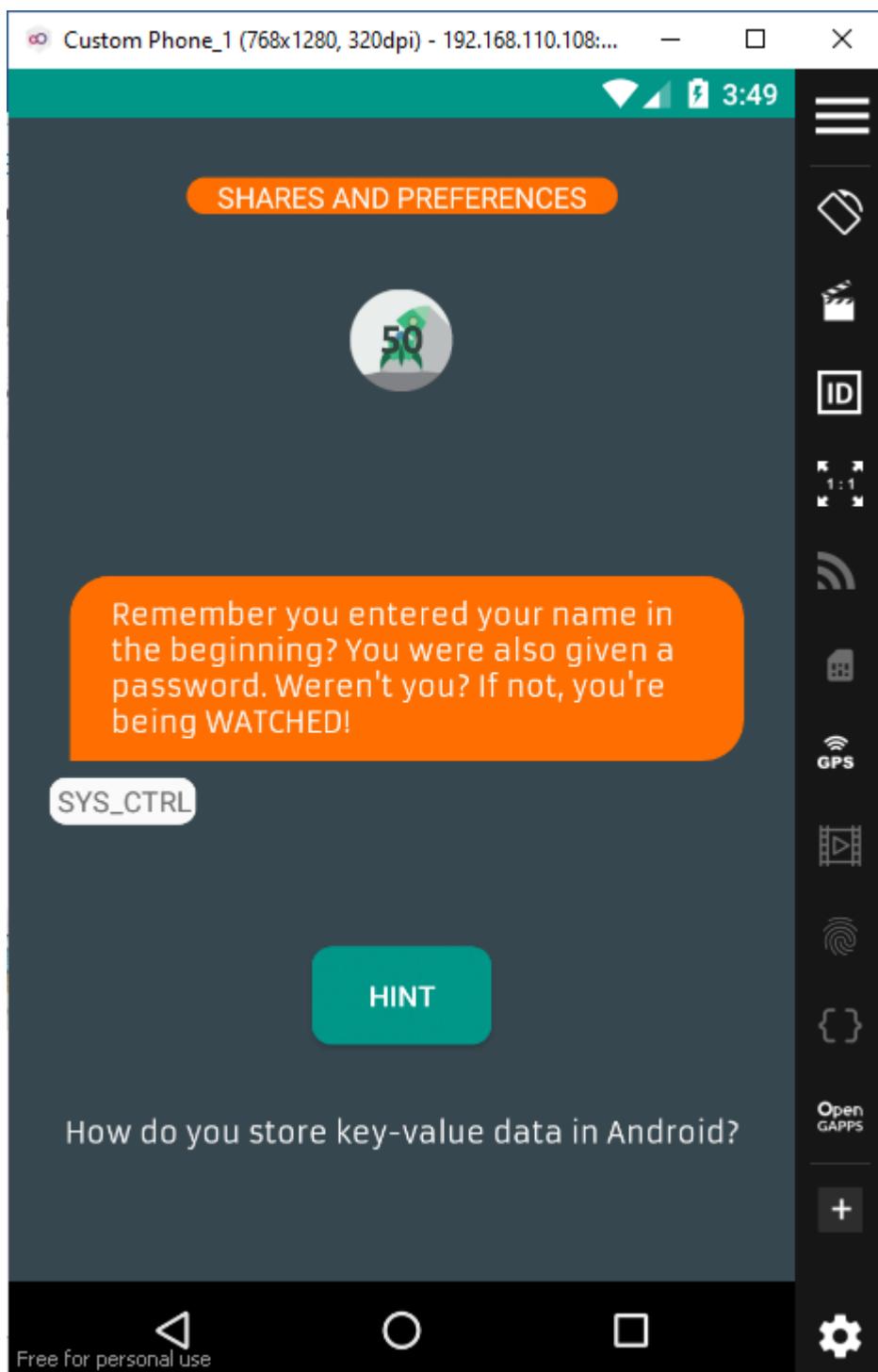
Ngoài ra ta còn thu được thêm 1 flag gợi ý

```
c:\ Select C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3938]
(c) Microsoft Corporation. All rights reserved.

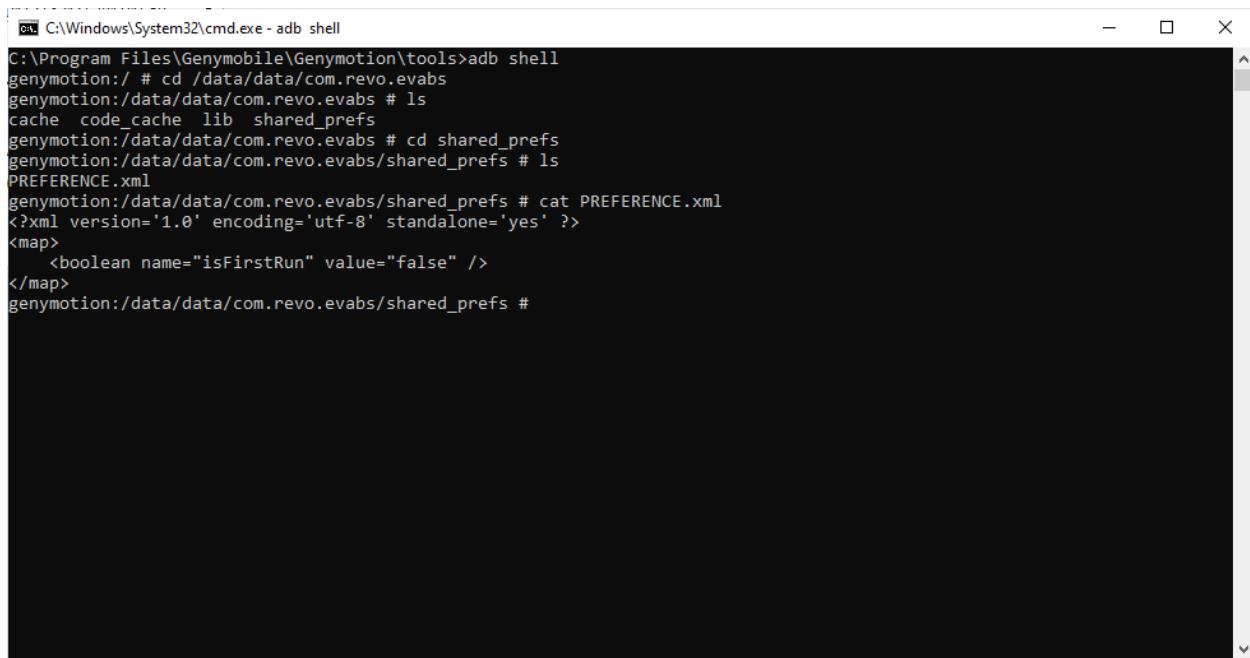
C:\Users\DeLL\Desktop\apktool\EVABSV5\res\layout-v17>cat activity_flagcheck.xml
<?xml version="1.0" encoding="utf-8"?>
<android.support.constraint.ConstraintLayout android:background="@color/colorPrimaryDark" android:layout_width="fill_parent" android:layout_height="fill_parent"
    xmlns:android="http://schemas.android.com/apk/res/android" xmlns:app="http://schemas.android.com/apk/res-auto">
    <TextView android:id="@+id/textView12" android:layout_width="102.0dp" android:layout_height="27.0dp" android:layout_marginLeft="8.0dp" android:layout_marginTop="8.0dp" android:layout_marginRight="8.0dp" android:layout_marginBottom="8.0dp" android:text="Flag Check" android:textAlignment="center" android:layout_marginStart="8.0dp" android:layout_marginEnd="8.0dp" app:layout_constraintEnd_toEndOf="parent" app:layout_constraintStart_toStartOf="parent" app:layout_constraintBottom_toTopOf="parent" app:layout_constraintVertical_bias="0.082" />
    <EditText android:textColor="@color/colorWhite" android:id="@+id/editTextflag" android:layout_width="wrap_content" android:layout_height="wrap_content" android:layout_marginLeft="8.0dp" android:layout_marginTop="8.0dp" android:layout_marginRight="8.0dp" android:layout_marginBottom="8.0dp" android:inputType="textPersonName" android:textAlignment="center" android:layout_marginStart="8.0dp" android:layout_marginEnd="8.0dp" app:layout_constraintBottom_toBottonOf="parent" app:layout_constraintEnd_toEndOf="parent" app:layout_constraintHorizontal_bias="0.503" app:layout_constraintStart_toStartOf="parent" app:layout_constraintVertical_bias="0.401" />
    <Button android:theme="@style/ButtonTheme" android:textColor="@color/colorWhite" android:gravity="center" android:id="@+id/buttonSubmit" android:background="#d9eaf7" android:layout_width="wrap_content" android:layout_height="wrap_content" android:layout_marginLeft="8.0dp" android:layout_marginTop="8.0dp" android:layout_marginRight="8.0dp" android:layout_marginBottom="8.0dp" android:text="SUBMIT" android:layout_marginStart="8.0dp" android:layout_marginEnd="8.0dp" app:layout_constraintEnd_toEndOf="parent" app:layout_constraintStart_toStartOf="parent" app:layout_constraintBottom_toTopOf="parent" app:layout_constraintVertical_bias="0.604" />
    <TextView android:id="@+id/textViewResult" android:layout_width="333.0dp" android:layout_height="27.0dp" android:layout_marginLeft="8.0dp" android:layout_marginTop="8.0dp" android:layout_marginRight="8.0dp" android:layout_marginBottom="8.0dp" android:text="" android:id="id/textViewResult" android:paddingLeft="10.0dp" android:paddingRight="10.0dp" android:layout_width="310.0dp" android:layout_height="24.0dp" android:layout_marginLeft="15.0dp" android:layout_marginRight="15.0dp" android:layout_marginBottom="36.0dp" android:text="NOTE: All flags are in the format EVABS{Some text here}." android:textAlignment="center" android:layout_marginStart="8.0dp" android:layout_marginEnd="8.0dp" app:layout_constraintBottom_toBottomOf="parent" app:layout_constraintEnd_toEndOf="parent" app:layout_constraintStart_toStartOf="parent" app:layout_constraintVertical_bias="0.902" />
    <TextView android:textSize="10.0dp" android:textColor="@color/colorWhite" android:autoLink="phone|web" android:id="@+id/textView25" android:paddingLeft="10.0dp" android:paddingRight="10.0dp" android:layout_width="105.0dp" android:layout_height="wrap_content" android:layout_marginLeft="15.0dp" android:layout_marginRight="15.0dp" android:layout_marginBottom="8.0dp" android:text="Alternatively, use https://neonsec.com/evabs/verify.php to access the web interface to submit flags." android:textAlignment="center" android:layout_marginStart="8.0dp" android:layout_marginEnd="8.0dp" app:layout_constraintEnd_toEndOf="parent" app:layout_constraintStart_toStartOf="parent" app:layout_constraintBottom_toBottomOf="parent" app:layout_constraintTop_toTopOf="parent" app:layout_constraintVertical_bias="0.984" />
</android.support.constraint.ConstraintLayout>
C:\Users\DeLL\Desktop\apktool\EVABSV5\res\layout-v17>
```

Flag: EVABS{s0me_t3xt_here}

Flag5

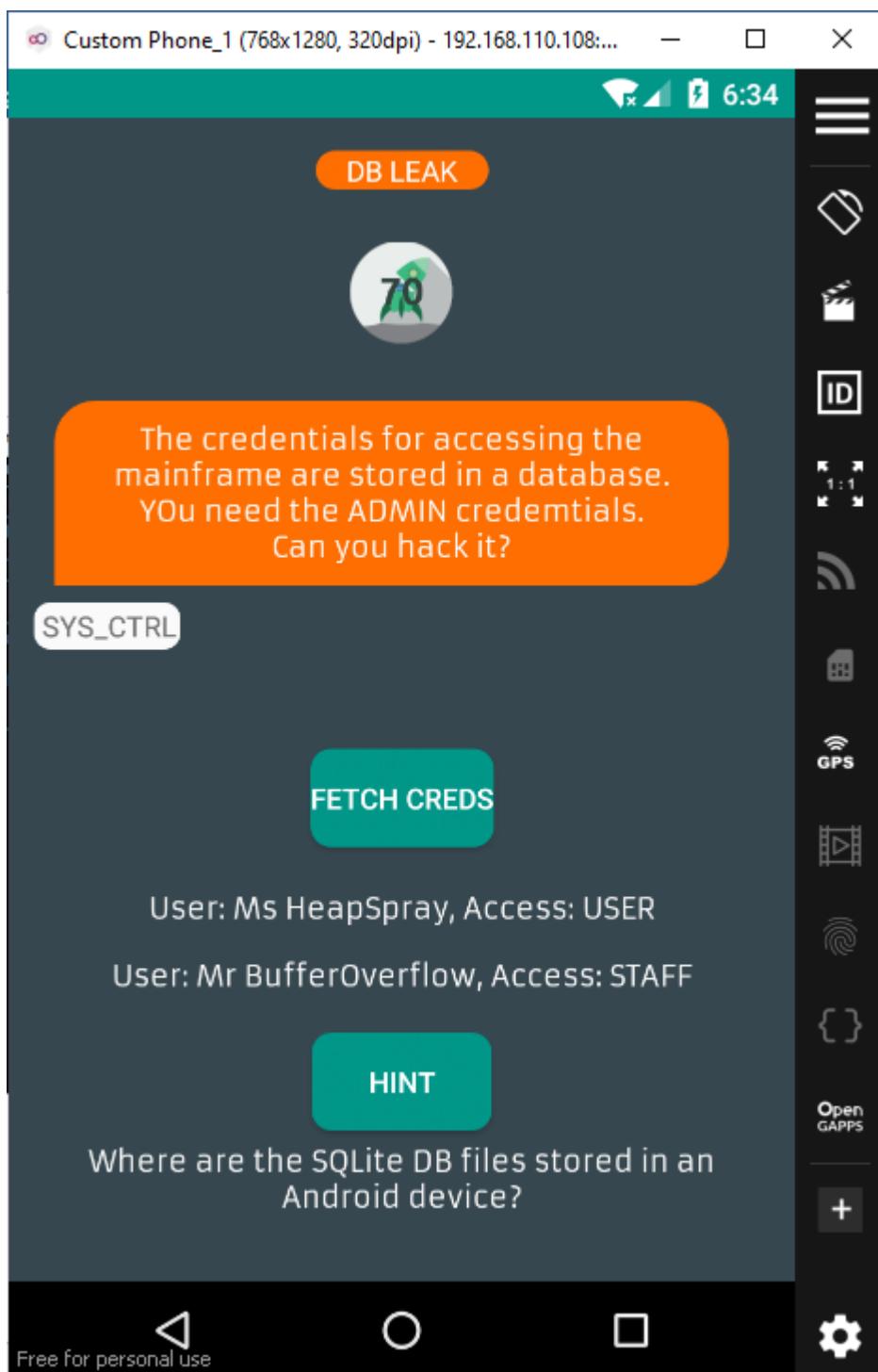


Theo gợi ý, ta vào folder shared_prefs

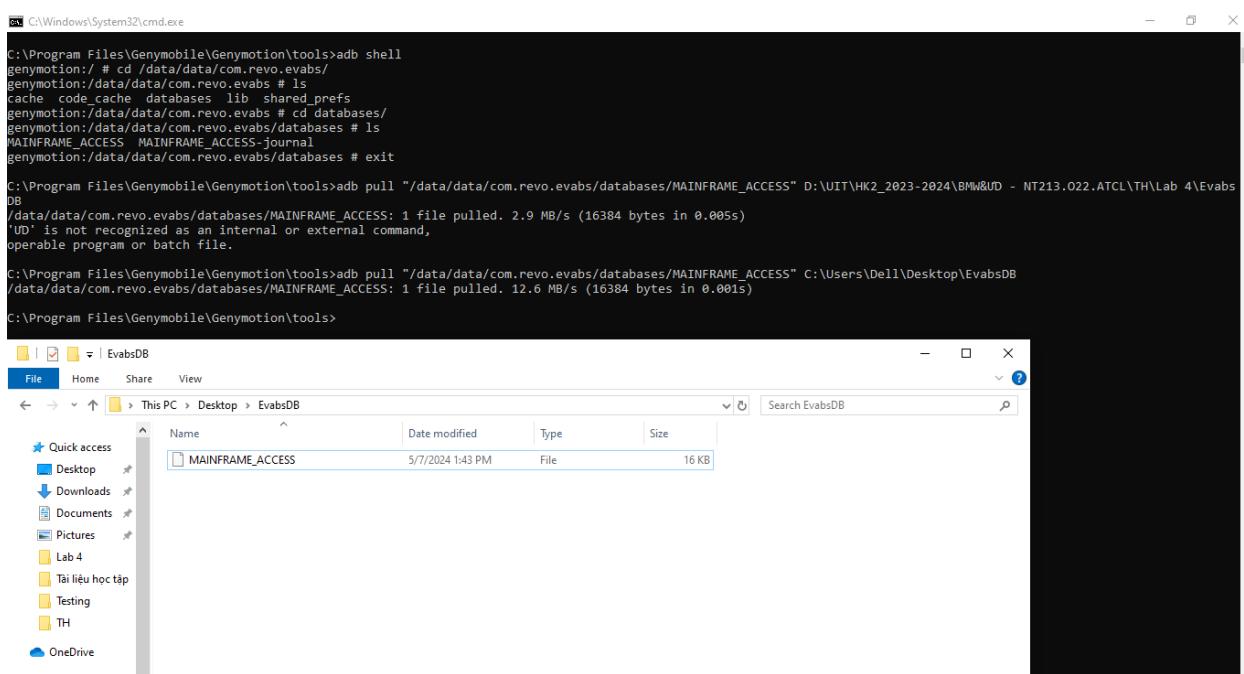


```
C:\Windows\System32\cmd.exe - adb shell
C:\Program Files\Genymobile\Genymotion\tools>adb shell
genymotion:/ # cd /data/data/com.revo.evabs
genymotion:/data/data/com.revo.evabs # ls
cache code_cache lib shared_prefs
genymotion:/data/data/com.revo.evabs # cd shared_prefs #
genymotion:/data/data/com.revo.evabs/shared_prefs # ls
PREFERENCE.xml
genymotion:/data/data/com.revo.evabs/shared_prefs # cat PREFERENCE.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <boolean name="isFirstRun" value="false" />
</map>
genymotion:/data/data/com.revo.evabs/shared_prefs #
```

Flag6



Tiến hành pull về máy



```
C:\Program Files\Genymobile\Genymotion\tools>adb shell
genymotion:/ # cd /data/data/com.revo.evabs/
genymotion:/data/data/com.revo.evabs # ls
cache  code  cache  databases  lib  shared_prefs
genymotion:/data/data/com.revo.evabs # cd databases/
genymotion:/data/data/com.revo.evabs/databases # ls
MAINFRAME_ACCESS  MAINFRAME_ACCESS-journal
genymotion:/data/data/com.revo.evabs/databases # exit

C:\Program Files\Genymobile\Genymotion\tools>adb pull "/data/data/com.revo.evabs/databases/MAINFRAME_ACCESS" D:\UIT\HK2_2023-2024\BMW&UD - NT213.022.ATCL\TH\Lab 4\EvabsDB
/data/data/com.revo.evabs/databases/MAINFRAME_ACCESS: 1 file pulled. 2.9 MB/s (16384 bytes in 0.005s)
'DU' is not recognized as an internal or external command,
operable program or batch file.

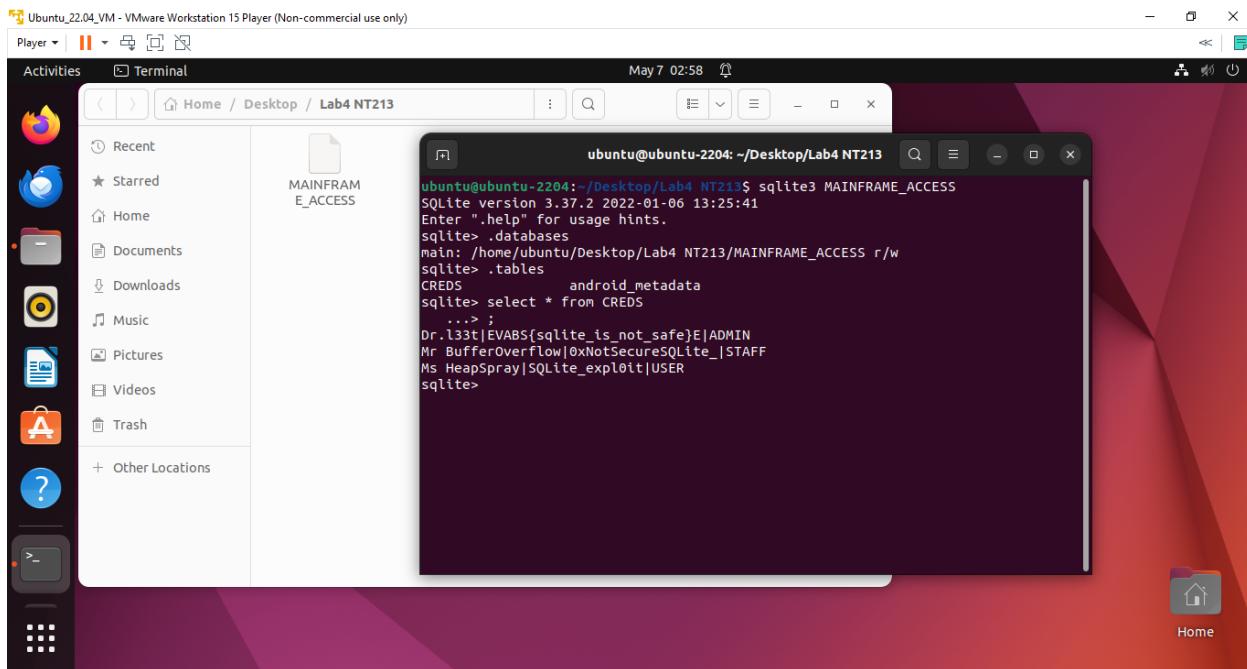
C:\Program Files\Genymobile\Genymotion\tools>
```

File Home Share View

< → This PC > Desktop > EvabsDB

Name	Date modified	Type	Size
MAINFRAME_ACCESS	5/7/2024 1:43 PM	File	16 KB

Sử dụng sqlite3 để kiểm tra file

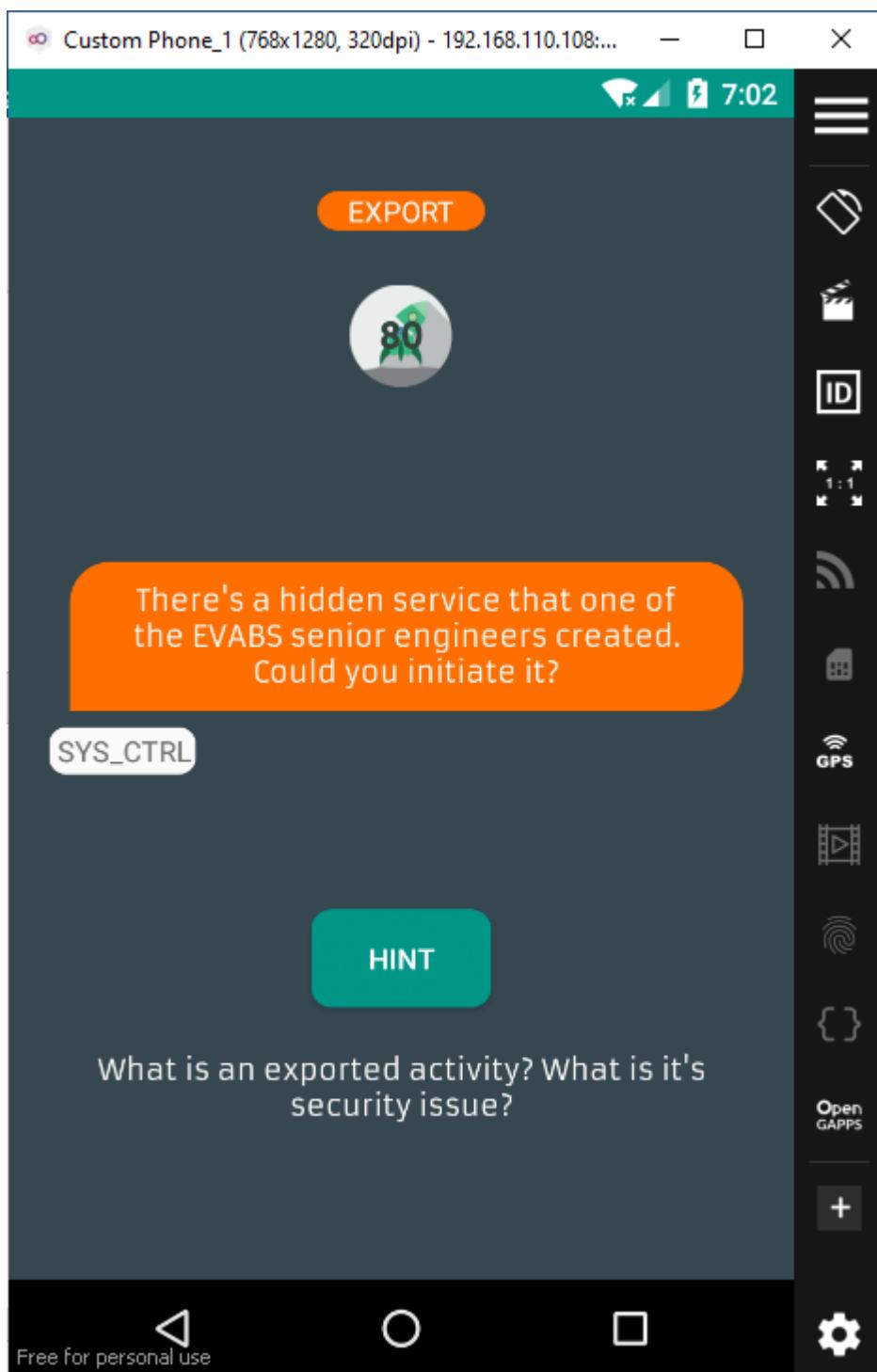


```
ubuntu@ubuntu-2204: ~/Desktop/Lab4 NT213$ sqlite3 MAINFRAME_ACCESS
SQLite version 3.37.2 2022-01-06 13:25:41
Enter ".help" for usage hints.
sqlite> .databases
main: /home/ubuntu/Desktop/Lab4 NT213/MAINFRAME_ACCESS r/w
sqlite> .tables
CREDS  android_metadata
sqlite> select * from CREDS
...>;
Dr.l33t|EVABS{sqlite_is_not_safe}E|ADMIN
Mr BufferOverflow|0xNotSecureSQLite_|STAFF
Ms HeapSpray|SQLite_expl0it|USER
sqlite>
```

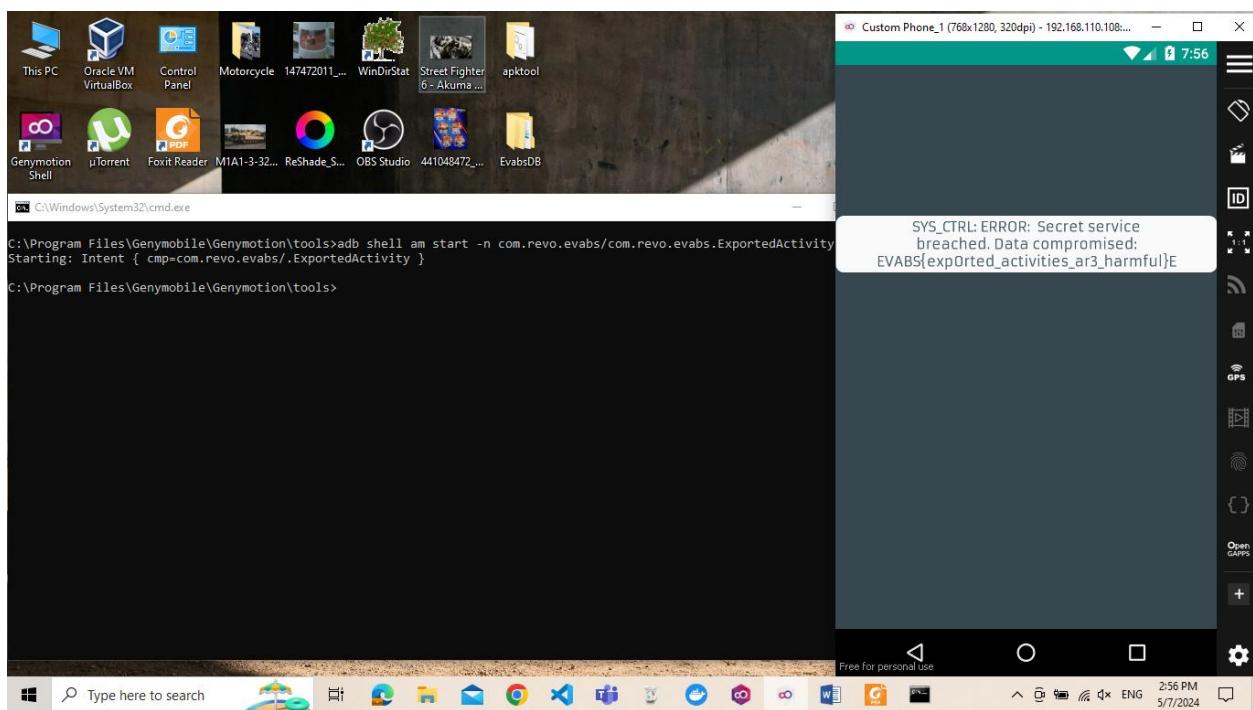
Ta thu được flag

Flag: EVABS{sqlite_is_not_safe}

Flag?



Tùy gợi ý



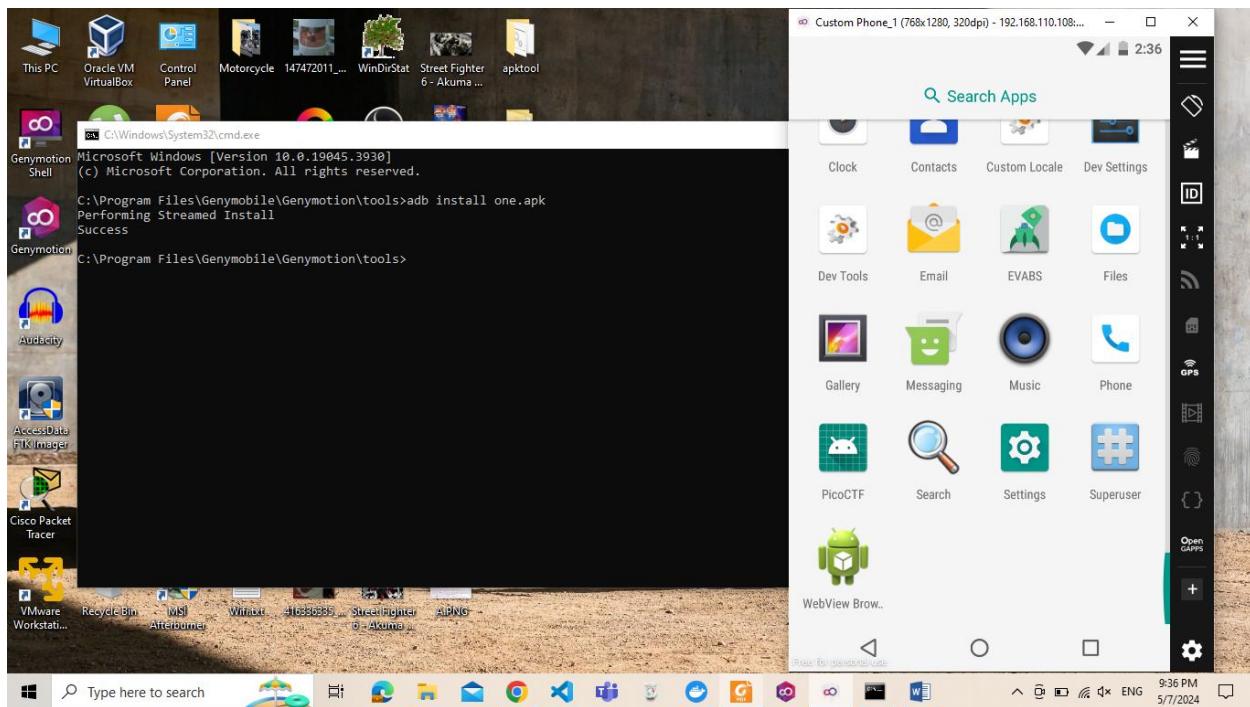
Ta thu được flag

Flag: EVABS{exported_activities_ar3_harmful}

Flag8

picoCTF

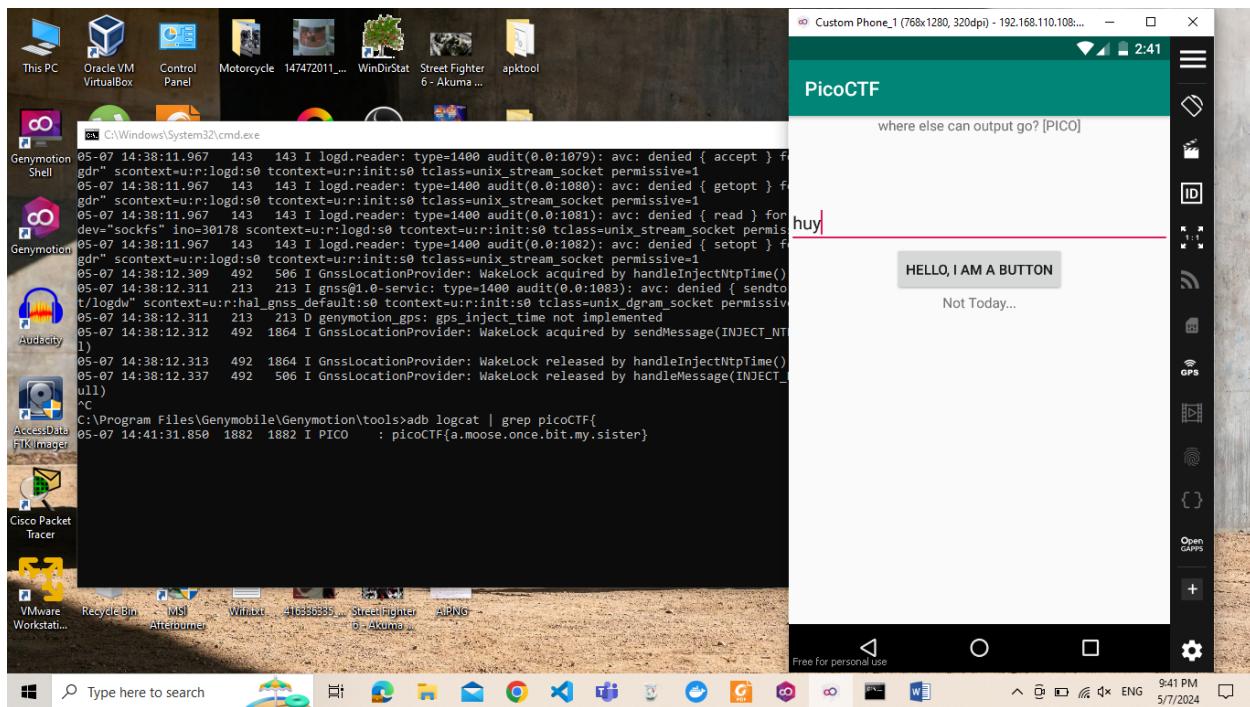
Flag1



Kiểm tra log của chương trình

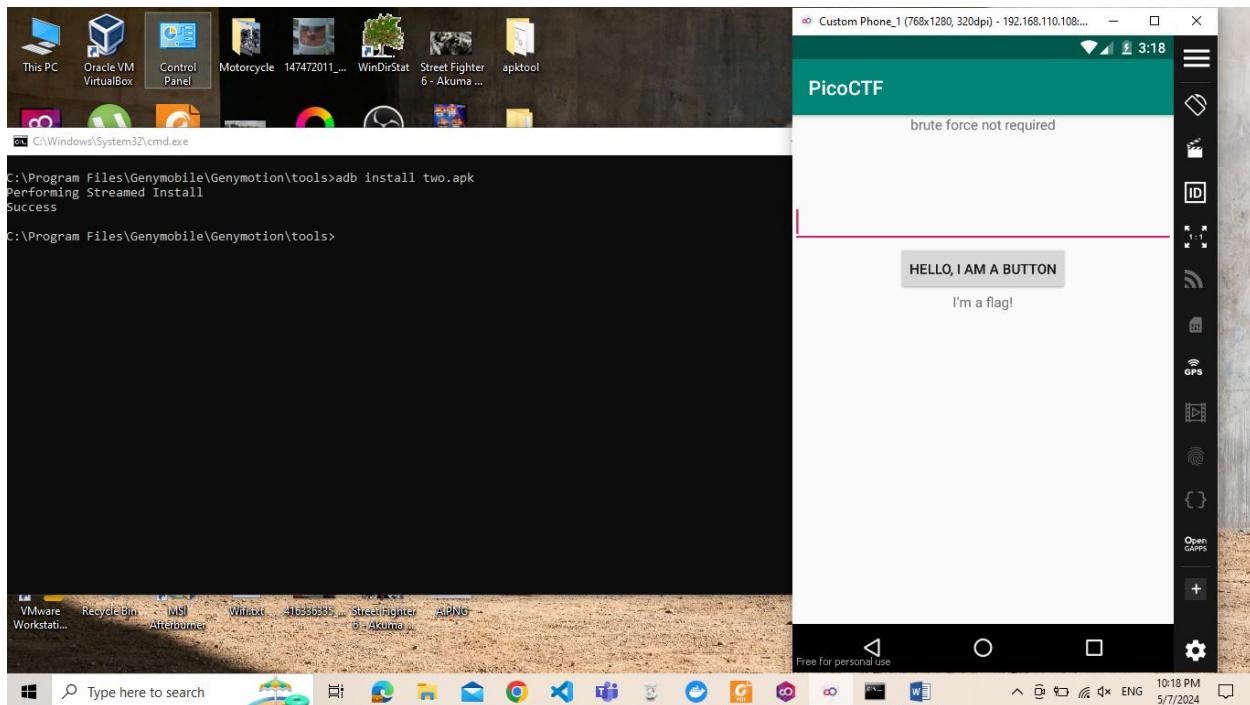
```
C:\Windows\System32\cmd.exe
C:\Program Files\Genymobile\Genymotion\tools>adb logcat
...
beginning of main
05-07 14:32:25.660 143 143 W audited : type=2000 audit(0.0:1): initialized
05-07 14:32:26.435 143 143 I audited : type=103 audit(0.0:2): policy loaded auid=4294967295 ses=4294967295
05-07 14:32:26.443 1 1 I init : type=1400 audit(0.0:3): avc: denied { read write } for path="/dev/console" dev="rootfs" ino=7899 scontext=u:r:init:s0 tcontext=u:object_r:rootfs:s0 tclass=chr_file permissive=1
05-07 14:32:26.443 1 1 I init : type=1400 audit(0.0:4): avc: denied { execute_no_trans } for path="/init" dev="rootfs" ino=7911 scontext=u:r:init:s0 tcontext=u:object_r:init_exec:s0 tclass=file permissive=1
05-07 14:32:26.651 124 124 I init : type=1400 audit(0.0:5): avc: denied { setattr } for path="/dev/console" dev="rootfs" ino=7899 scontext=u:r:init:s0 tcontext=u:object_r:rootfs:s0 tclass=chr_file permissive=1
05-07 14:32:26.651 124 124 I ueventd : type=1400 audit(0.0:6): avc: denied { ioctl } for path="/dev/console" dev="rootfs" ino=7899 ioclcmd=5401 scontext=u:r:init:s0 tcontext=u:object_r:ueventd:s0 tclass=chr_file permissive=1
05-07 14:32:26.651 124 124 I ueventd : type=1400 audit(0.0:7): avc: denied { create } for scontext=u:r:init:s0 tcontext=u:r:init:s0 tclass=netlink_kobject_uevent_socket permissive=1
05-07 14:32:26.695 124 124 I ueventd : type=1400 audit(0.0:8): avc: denied { setopt } for scontext=u:r:init:s0 tcontext=u:r:init:s0 tclass=netlink_kobject_uevent_socket permissive=1
05-07 14:32:26.695 124 124 I ueventd : type=1400 audit(0.0:9): avc: denied { bind } for scontext=u:r:init:s0 tcontext=u:r:init:s0 tclass=netlink_kobject_uevent_socket permissive=1
05-07 14:32:26.695 124 124 I ueventd : type=1400 audit(0.0:10): avc: denied { read } for scontext=u:r:init:s0 tcontext=u:r:init:s0 tclass=netlink_kobject_uevent_socket permissive=1
05-07 14:32:29.873 0 144 I SELinux : SELinux: Loaded service_contexts from:
05-07 14:32:29.877 0 144 I SELinux : /plat_service_contexts
05-07 14:32:29.877 0 144 I SELinux : /nonplat_service_contexts
05-07 14:32:29.899 0 146 I SELinux : SELinux: Loaded service contexts from:
05-07 14:32:29.899 0 146 I SELinux : /vndservice_contexts
05-07 14:32:30.175 145 145 I hwservicemanager: type=1400 audit(0.0:78): avc: denied { sendto } for path="/dev/socket/logdw" scontext=u:r:hwservicemanager:s0 tcontext=u:r:init:s0 tclass=unix_dgram_socket permissive=1
05-07 14:32:30.177 145 145 E hwservicemanager: BINDER_SET_INHERIT_FIFO_PRIO failed with error -1
05-07 14:32:30.219 155 155 I init.genymotion: type=1400 audit(0.0:79): avc: denied { setattr } for path="/system/bin/sh" dev="sda6" ino=568 scontext=u:r:vbox86-setup:s0 tcontext=u:object_r:shell_exec:s0 tclass=file permissive=1
05-07 14:32:30.219 155 155 I init.genymotion: type=1400 audit(0.0:80): avc: denied { read } for path="/system/bin/sh" dev="sda6" ino=568 scontext=u:r:vbox86-setup:s0 tcontext=u:object_r:shell_exec:s0 tclass=file permissive=1
05-07 14:32:30.239 159 159 I init.genymotion: type=1400 audit(0.0:81): avc: denied { setattr } for path="/system/bin/toybox" dev="sda6" ino=608 scontext=u:r:vbox86-setup:s0 tcontext=u:object_r:toolbox_exec:s0 tclass=file permissive=1
05-07 14:32:30.239 157 157 I void : type=1400 audit(0.0:82): avc: denied { read write } for path="socket:[9438]" dev="sockfs" ino=9438 scontext=u:r:vold:s0 tcontext=u:object_r:stream_socket permissive=1
05-07 14:32:30.239 159 159 I init.genymotion: type=1400 audit(0.0:83): avc: denied { execute } for name="toybox" dev="sda6" ino=608 scontext=u:r:vbox86-setup:s0 tcontext=u:object_r:toolbox_exec:s0 tclass=file permissive=1
05-07 14:32:30.239 159 159 I init.genymotion: type=1400 audit(0.0:84): avc: denied { read open } for path="/system/bin/toybox" dev="sda6" ino=608 scontext=u:r:vbox86-setup:s0 tcontext=u:object_r:toolbox_exec:s0 tclass=file permissive=1
05-07 14:32:30.239 159 159 I init.genymotion: type=1400 audit(0.0:85): avc: denied { execute_no_trans } for path="/system/bin/toybox" dev="sda6" ino=608 scontext=u:r:vbox86-setup:s0 tcontext=u:object_r:toolbox_exec:s0 tclass=file permissive=1
05-07 14:32:30.355 156 156 I android.hardware: type=1400 audit(0.0:86): avc: denied { sendto } for path="/dev/socket/Lab4.docx-Word_ext:ur:hal_keymaster_default:s0 tcontext=u:object_r:socket_permit:s0 tclass=unix_stream_socket permissive=1
```

Tiến hành tìm flag

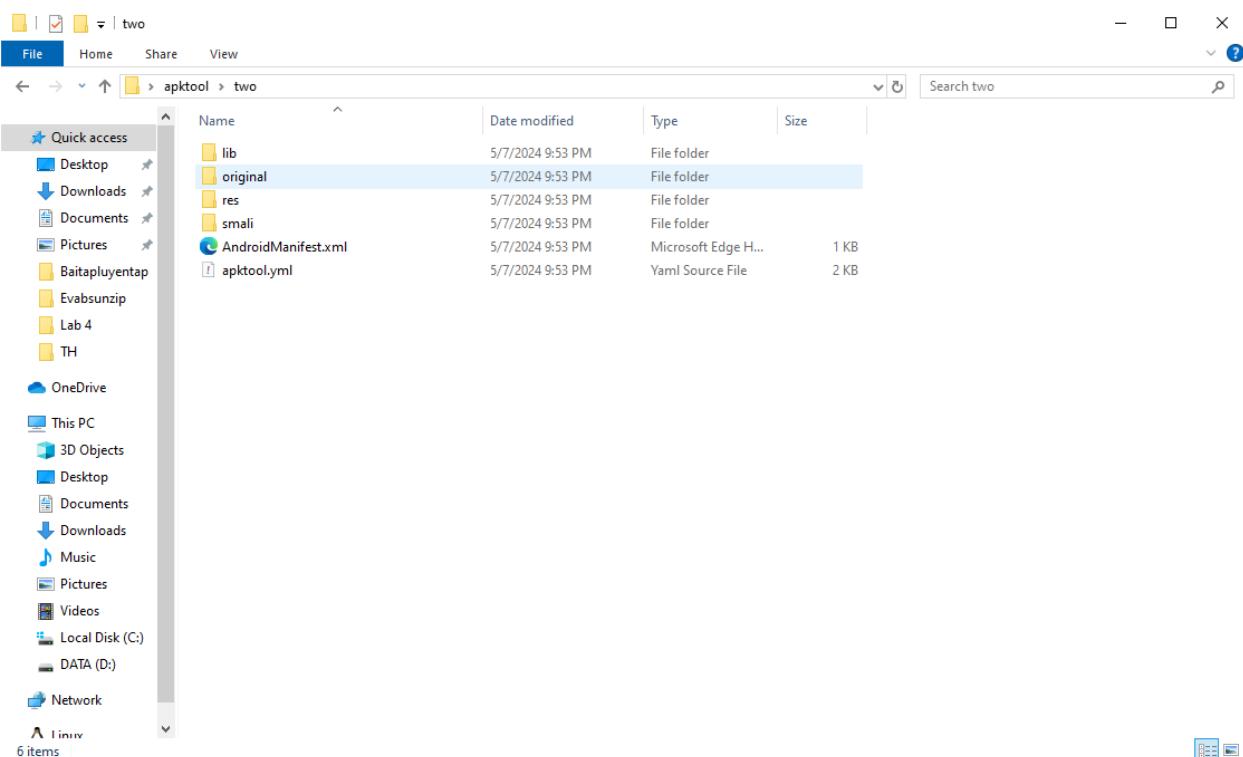


Flag: picoCTF{a.moose.once.bit.my.sister}

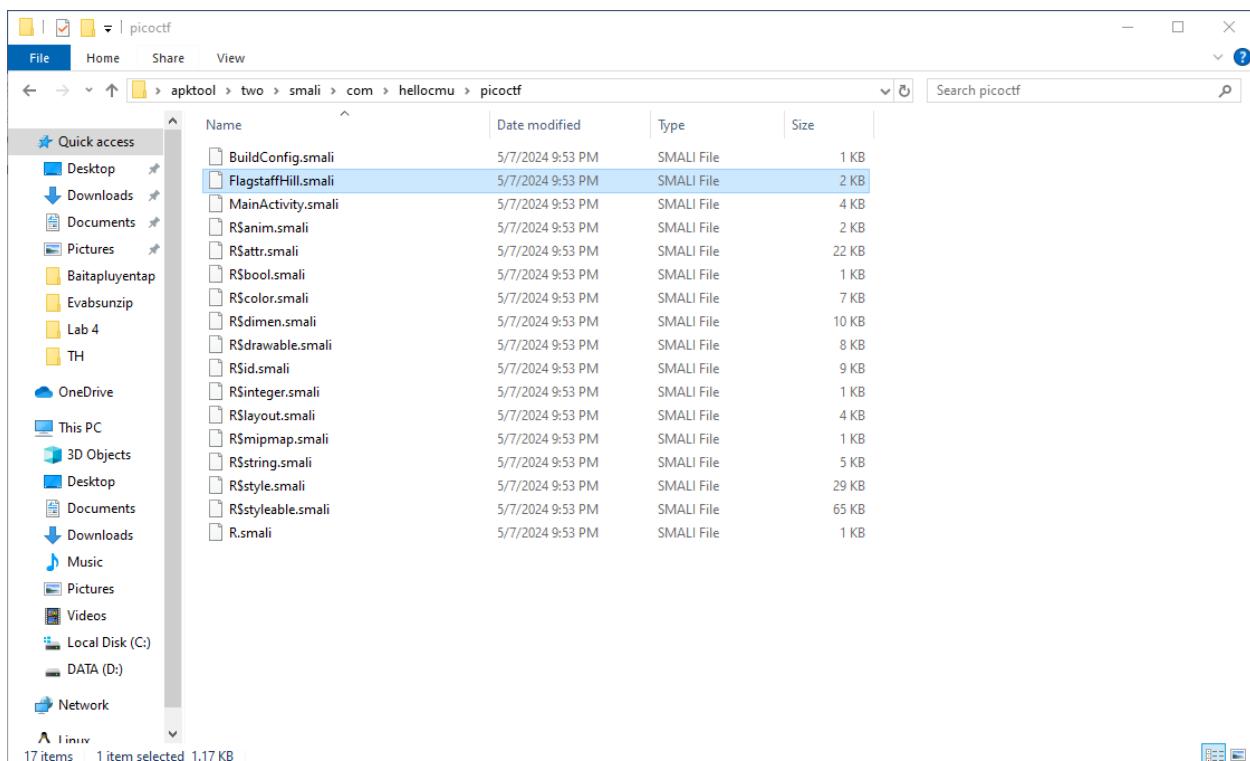
Flag2



Tiến hành decompile file



Ta kiểm tra thử FlagstaffHill.smali



Ta thấy được thông tin

```

FlagstaffHill.smali
C: > Users > Dell > Desktop > apktool > two > smali > com > hellocmu > picocft > FlagstaffHill.smali
1   .class public Lcom/hellocmu/picocft/FlagstaffHill;
2   .super Ljava/lang/Object;
3   .source "FlagstaffHill.java"
4
5
6   # direct methods
7   .method public constructor <init>()
8   {
9       .locals 0
10      .line 6
11      invoke-direct {p0}, Ljava/lang/Object;-><init>()
12
13      return-void
14     .end method
15
16   .method public static native fenugreek(Ljava/lang/String;)Ljava/lang/String;
17   .end method
18
19   .method public static getFlag(Ljava/lang/String;Landroid/content/Context;)Ljava/lang/String;
20   {
21       .locals 2
22       .param p0, "input"    # Ljava/lang/String;
23       .param p1, "ctx"      # Landroid/content/Context;
24
25       .line 11
26       const v0, 0x7f0b002f
27
28       invoke-virtual {p1, v0}, Landroid/content/Context;->getString(I)Ljava/lang/String;
29
30       move-result-object v0
31
32       .line 12

```

Ln 25, Col 25 (10 selected) Spaces: 4 UTF-8 CRLF Plain Text

Giá trị: 0x7f0b002f

Tiến hành tìm kiếm giá trị ở file chứa

```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3930]
(c) Microsoft Corporation. All rights reserved.

C:\Users\...\\Desktop\apktool\two\res\values>cat public.xml
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <public type="anim" name="abc_fade_in" id="0x7f010000" />
    <public type="anim" name="abc_fade_out" id="0x7f010001" />
    <public type="anim" name="abc_grow_fade_in_from_bottom" id="0x7f010002" />
    <public type="anim" name="abc_popup_enter" id="0x7f010003" />
    <public type="anim" name="abc_popup_exit" id="0x7f010004" />
    <public type="anim" name="abc_shrink_fade_out_from_bottom" id="0x7f010005" />
    <public type="anim" name="abc_slide_in_bottom" id="0x7f010006" />
    <public type="anim" name="abc_slide_in_top" id="0x7f010007" />
    <public type="anim" name="abc_slide_out_bottom" id="0x7f010008" />
    <public type="anim" name="abc_slide_out_top" id="0x7f010009" />
    <public type="anim" name="abc_tooltip_enter" id="0x7f01000a" />
    <public type="anim" name="abc_tooltip_exit" id="0x7f01000b" />
    <public type="attr" name=" actionBarDivider" id="0x7f020000" />
    <public type="attr" name=" actionBarItemBackground" id="0x7f020001" />
    <public type="attr" name=" actionBarPopupTheme" id="0x7f020002" />
    <public type="attr" name=" actionBarSize" id="0x7f020003" />
    <public type="attr" name=" actionBarSplitStyle" id="0x7f020004" />
    <public type="attr" name=" actionBarStyle" id="0x7f020005" />
    <public type="attr" name=" actionBarTabBarStyle" id="0x7f020006" />
    <public type="attr" name=" actionBarTabStyle" id="0x7f020007" />
    <public type="attr" name=" actionBarTabTextStyle" id="0x7f020008" />
    <public type="attr" name=" actionBarTheme" id="0x7f020009" />
    <public type="attr" name=" actionBarWidgetTheme" id="0x7f02000a" />
    <public type="attr" name=" actionBarStyle" id="0x7f02000b" />

```

```

<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="abc_menu_space_shortcut_label" id="0x7f0b001b" />
    <string name="abc_menu_sym_shortcut_label" id="0x7f0b001c" />
    <string name="abc_prepend_shortcut_label" id="0x7f0b001d" />
    <string name="abc_search_hint" id="0x7f0b001e" />
    <string name="abc_searchview_description_clear" id="0x7f0b001f" />
    <string name="abc_searchview_description_query" id="0x7f0b0020" />
    <string name="abc_searchview_description_searh" id="0x7f0b0021" />
    <string name="abc_searchview_description_submit" id="0x7f0b0022" />
    <string name="abc_searchview_description_voice" id="0x7f0b0023" />
    <string name="abc_shareactionprovider_share_with" id="0x7f0b0024" />
    <string name="abc_shareactionprovider_share_with_application" id="0x7f0b0025" />
    <string name="abc_toolbarCollapse_description" id="0x7f0b0026" />
    <string name="app_name" id="0x7f0b0027" />
    <string name="bat" id="0x7f0b0028" />
    <string name="bear" id="0x7f0b0029" />
    <string name="cottentail" id="0x7f0b002a" />
    <string name="gopher" id="0x7f0b002b" />
    <string name="hint" id="0x7f0b002c" />
    <string name="manatee" id="0x7f0b002d" />
    <string name="myotis" id="0x7f0b002e" />
    <string name="password" id="0x7f0b002f" />
    <string name="porcupine" id="0x7f0b0030" />
    <string name="porpoise" id="0x7f0b0031" />
    <string name="search_menu_title" id="0x7f0b0032" />
    <string name="skunk" id="0x7f0b0033" />
    <string name="status_bar_notification_info_overflow" id="0x7f0b0034" />
    <string name="vole" id="0x7f0b0035" />
    <style name="AlertDialog.AppCompat" id="0x7f0c0000" />
    <style name="AlertDialog.AppCompat.Light" id="0x7f0c0001" />
    <style name="Animation.AppCompat.Dialog" id="0x7f0c0002" />

```

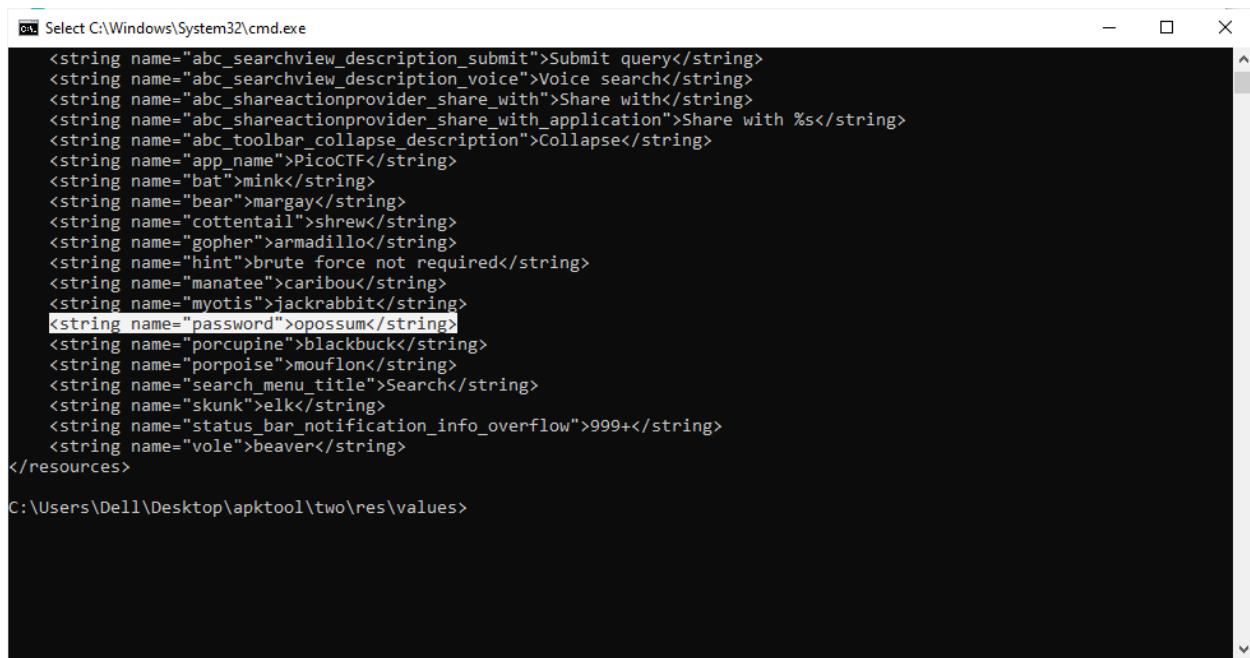
Ta thấy giá trị liên quan với thông tin name password

Đây là dữ liệu string, do đó ta tiếp tục tìm kiếm ở file strings.xml

```

C:\Users\Hien\Downloads\apktool\apktool\2.3.0\res\values>cat strings.xml
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="abc_action_bar_home_description">Navigate home</string>
    <string name="abc_action_bar_up_description">Navigate up</string>
    <string name="abc_action_menu_overflow_description">More options</string>
    <string name="abc_action_mode_done">Done</string>
    <string name="abc_activity_chooser_view_se_all">See all</string>
    <string name="abc_activitychooserview_choose_application">Choose an app</string>
    <string name="abc_capital_off">OFF</string>
    <string name="abc_capital_on">ON</string>
    <string name="abc_font_family_body_1_material">sans-serif</string>
    <string name="abc_font_family_body_2_material">sans-serif-medium</string>
    <string name="abc_font_family_button_material">sans-serif-medium</string>
    <string name="abc_font_family_caption_material">sans-serif</string>
    <string name="abc_font_family_display_1_material">sans-serif</string>
    <string name="abc_font_family_display_2_material">sans-serif</string>
    <string name="abc_font_family_display_3_material">sans-serif</string>
    <string name="abc_font_family_display_4_material">sans-serif-light</string>
    <string name="abc_font_family_headline_material">sans-serif</string>
    <string name="abc_font_family_menu_material">sans-serif</string>
    <string name="abc_font_family_subhead_material">sans-serif</string>
    <string name="abc_font_family_title_material">sans-serif-medium</string>
    <string name="abc_menu_alt_shortcut_label">Alt+</string>
    <string name="abc_menu_ctrl_shortcut_label">Ctrl+</string>
    <string name="abc_menu_delete_shortcut_label">delete</string>
    <string name="abc_menu_enter_shortcut_label">enter</string>

```

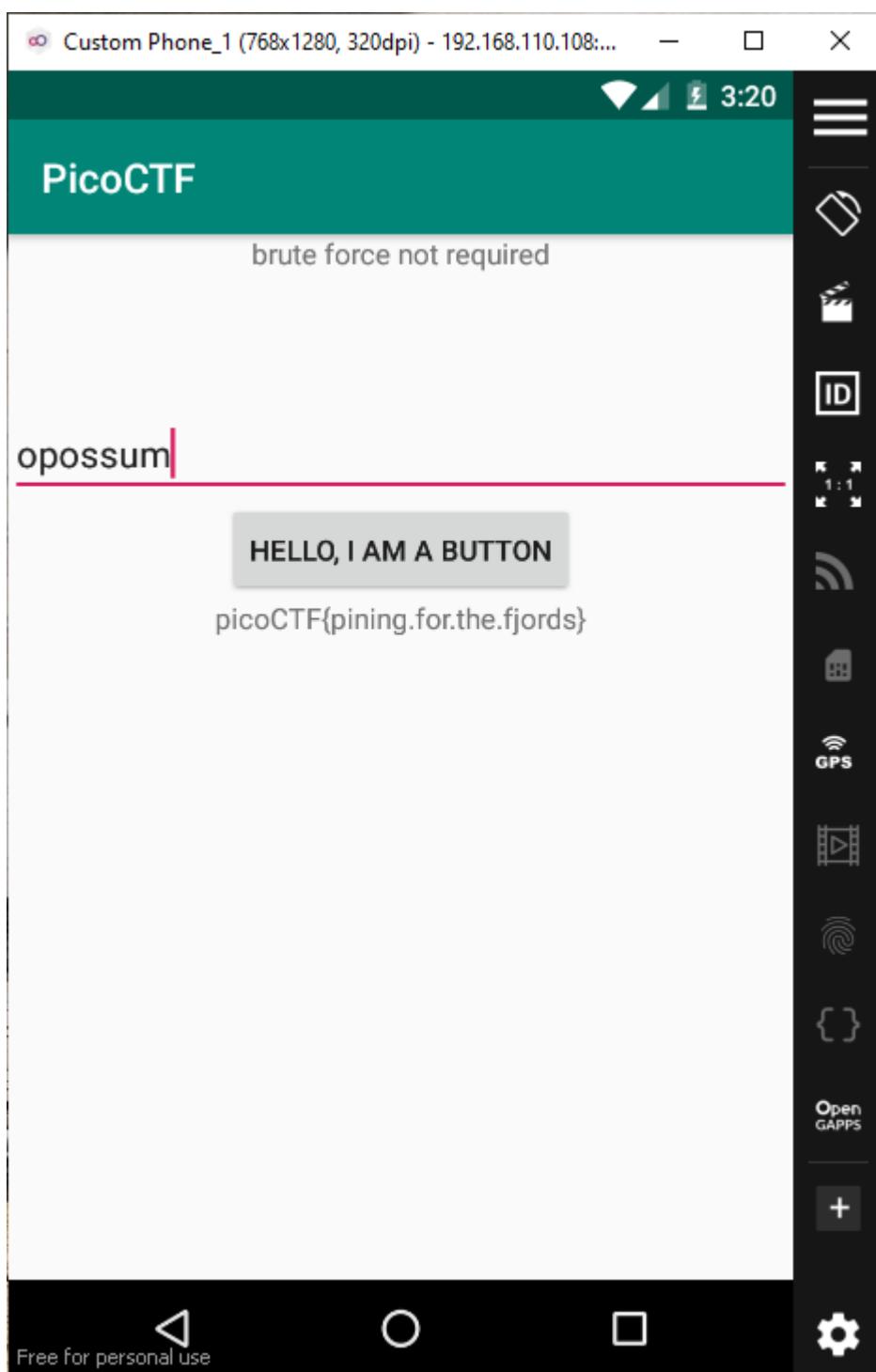


The screenshot shows a terminal window with the title "Select C:\Windows\System32\cmd.exe". The window displays the contents of an XML file, likely a resources file from an Android application. The file contains several string definitions, such as "Submit query", "Voice search", "Share with", "Share with %s", "Collapse", "PicoCTF", "mink", "margay", "shrew", "armadillo", "brute force not required", "caribou", "jackrabbit", "opossum", "blackbuck", "mouflon", "Search", "skunk", "elk", "999+", and "beaver". The file is named "values.xml" and is located at "C:\Users\...apktool\two\res\values".

Ta thu được password

Password: opossum

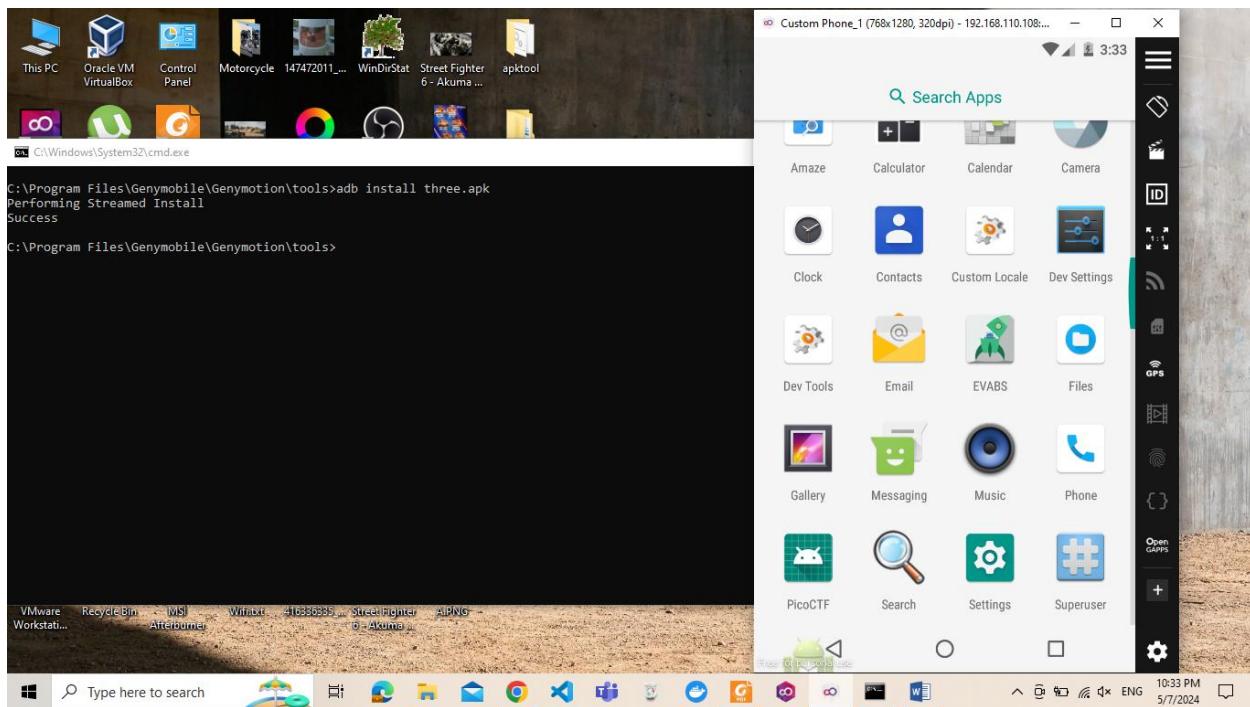
Nhập thử password



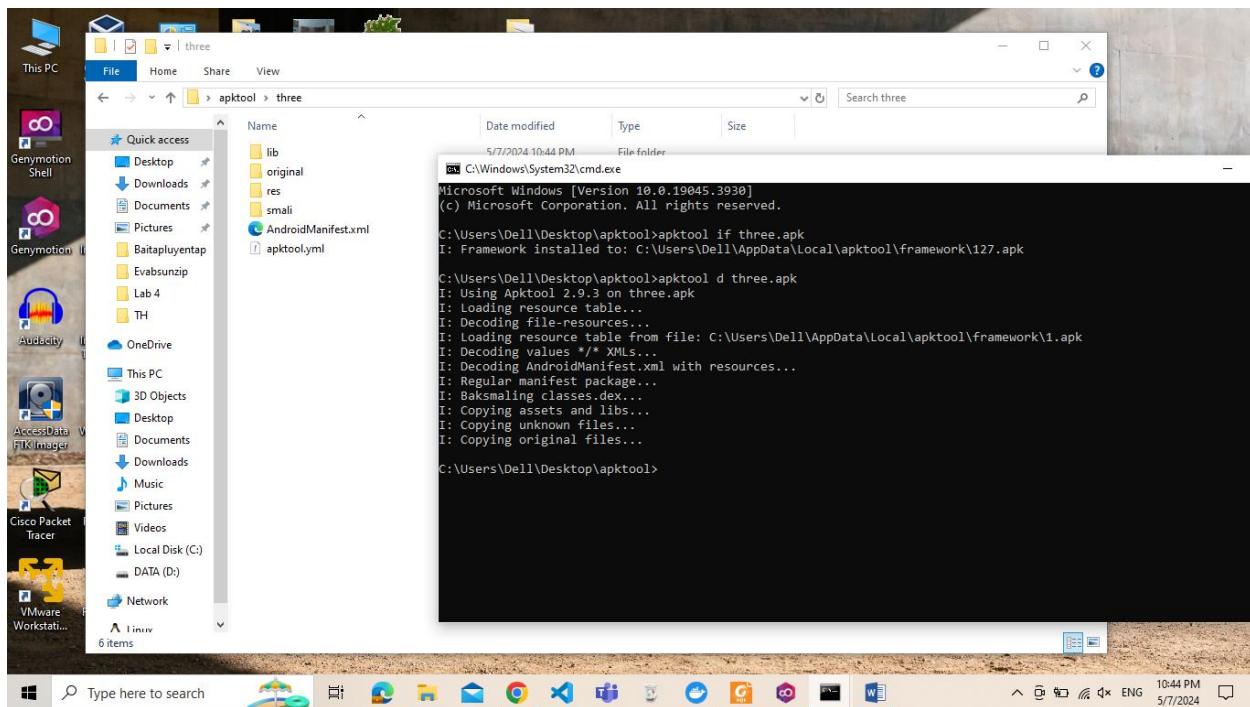
Ta thu được flag

Flag: picoCTF{pining.for.the.fjords}

Flag3



Tiến hành decompile file



Ta kiểm tra thử FlagstaffHill.smali

```

File Edit Selection View Go Run ...
Search
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
FlagstaffHill.smali X
C: > Users > Dell > Desktop > apktool > three > smali > com > hellocmu > picoctf > FlagstaffHill.smali
1 .class public Lcom/hellocmu/picoctf/FlagstaffHill;
2 .super Ljava/lang/Object;
3 .source "FlagstaffHill.java"
4
5
6 # direct methods
7 .method public constructor <init>()
8     .locals 0
9
10    .line 6
11    invoke-direct {p0}, Ljava/lang/Object;-><init>()
12
13    return-void
14 .end method
15
16 .method public static getFlag(Ljava/lang/String;Landroid/content/Context;)Ljava/lang/String;
17     .locals 10
18     .param p0, "input" # Ljava/lang/String;
19     .param p1, "ctx"   # Landroid/content/Context;
20
21     .line 11
22     const/4 v0, 0x6
23
24     new-array v0, v0, [Ljava/lang/String;
25
26     .line 12
27     .local v0, "witches":[Ljava/lang/String;
28     const/4 v1, 0x8
29
30     const-string v2, "weatherwax"
31

```

You have Windows Subsystem for Linux (WSL) installed on your system. Do you want to install the recommended 'WSL' extension from Microsoft for it?

Install Show Recommendations

Ta thử tạo lại file FlagtaffHill.java từ thông tin trên

```

File Edit Selection View Go Run ...
Search
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
FlagstaffHill.java X
C: > Users > Dell > Desktop > FlagstaffHill.java
1 package com.hellocmu.picoctf;
2
3 import android.content.Context;
4
5 public class FlagstaffHill {
6     public static String getFlag(String input, Context ctx) {
7         String[] witches = new String[]{"weatherwax", "ogg", "garlick", "nitt", "aching", "dismass"};
8
9         int first = 3;
10        int second = 0;
11        int third = first / first + second;
12        int fourth = third + third - second;
13        int fifth = first + fourth;
14        int sixth = fifth + second - third;
15
16        String password = witches[fifth] + "." + witches[third] + "." + witches[second] + "."
17            + witches[sixth] + "." + witches[first] + "." + witches[fourth];
18
19        if (input.equals(password)) {
20            return sesame(input);
21        } else {
22            return "NOPE";
23        }
24    }
25
26    public static String sesame(String input) {
27        // Implementation of sesame method
28        return input; // Replace with actual implementation
29    }
30

```

Do you want to install the recommended 'Extension Pack for Java' extension from Microsoft for the Java language?

Install Show Recommendations

Ta nhận thấy cách làm trên không ra được kết quả
Sử dụng công cụ Jadx

```

package com.hellocmu.picotf;

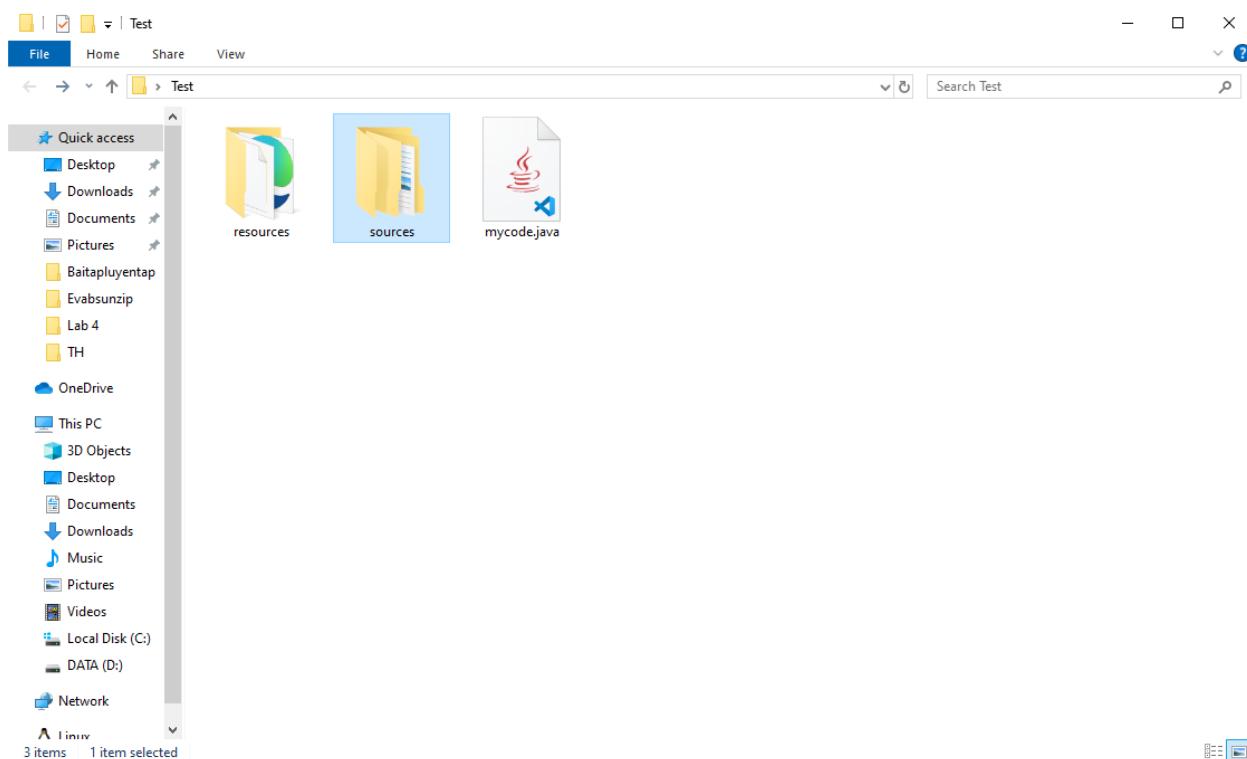
import android.content.Context;

/* Loaded from: classes.dex */
public class FlagstaffHill {
    public static native String sesame(String str);

    public static String getFlag(String input, Context ctx) {
        String[] witches = {"weatherwax", "ogg", "garlick", "nitt", "aching", "dismass"};
        int second = 3 - 3;
        int third = (3 / 3) + second;
        int fourth = (third + third) - second;
        int fifth = 3 + fourth;
        int sixth = (fifth + second) - third;
        String password = "" .concat(witches[fifth]).concat(".").concat(witches[third]).concat(".").concat(witches[fifth]).concat(".");
        return input.equals(password) ? sesame(input) : "NOPE";
    }
}

```

Ta down code về



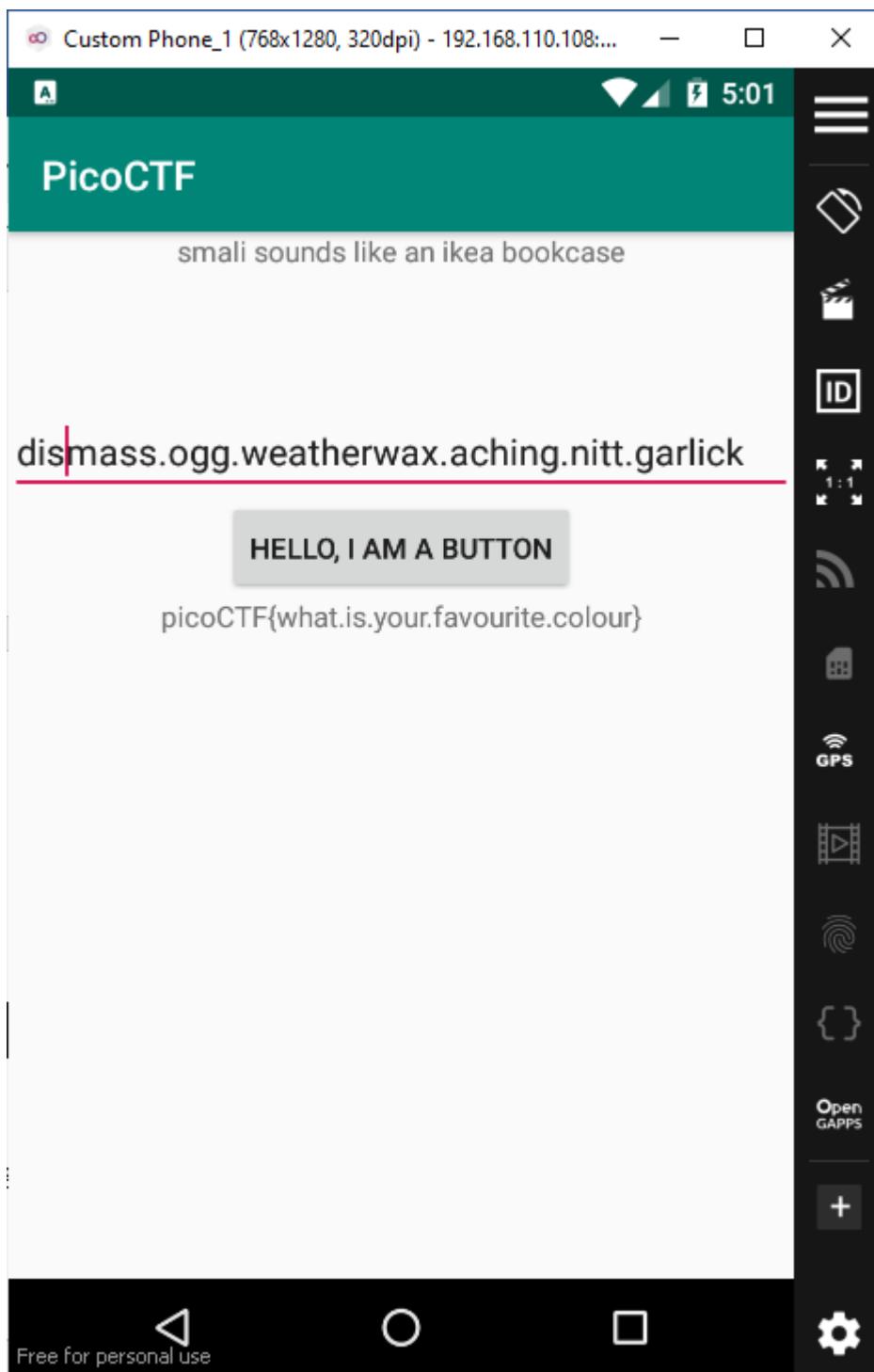
Tới đây, để chạy mycode.java cần thiết lập môi trường

Sau khi chạy thành công, thu được password

password: dismass.ogg.weatherwax.aching.nitt.garlick

password: dismiss.ogg.weatherwax.aching.nitt.garlick

Nhập password vào



Ta thu được flag

Flag: picoCTF{what.is.your.favourite.colour}

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.DOCX** và **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)** – cỡ **chữ 13**. **Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

Ví dụ: [NT101.K11.ATCL]-Session1_Group3.

- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài Lab.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT