

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật Web và Ứng dụng
Tên chủ đề: Lab 4 – Android Pentesting
GVHD: Ngô Đức Hoàng Sơn

Nhóm:

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.021.ANTT.1

STT	Họ và tên	MSSV	Email
1	Vũ Tuấn Sơn	21521389	21521389@gm.uit.edu.vn
2	Bùi Đức Anh Tú	21522735	21522735@gm.uit.edu.vn
3	Lê Huy Hiệp	21522067	21522067@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Yêu cầu 1	90%	1 - 3
2	Yêu cầu 2	50%	3 - 5
3
Điểm tự đánh giá			?/10

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

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

Đoạn code thực hiện việc kiểm tra đăng nhập thông qua HTTP. Các thông tin này được thực hiện bởi phương thức POST và gửi đi các thông tin đăng nhập bao gồm username và password.

```
public void postData(String var1) throws ClientProtocolException, IOException, JSONException, InvalidKeyException, NoSuchAlgorithmException {
    DefaultHttpClient var2 = new DefaultHttpClient();
    HttpPost var4 = new HttpPost(this.this$0.protocol + this.this$0.serverip + ":" + this.this$0.serverport + "/login");
    HttpPost var3 = new HttpPost(this.this$0.protocol + this.this$0.serverip + ":" + this.this$0.serverport + "/devlogin");
    ArrayList var5 = new ArrayList(2);
    var5.add(new BasicNameValuePair("username", this.this$0.username));
    var5.add(new BasicNameValuePair("password", this.this$0.password));
    HttpResponse var6;
    if (this.this$0.username.equals("devadmin")) {
        var3.setEntity(new UrlEncodedFormEntity(var5));
        var6 = var2.execute(var3);
    } else {
        var4.setEntity(new UrlEncodedFormEntity(var5));
        var6 = var2.execute(var4);
    }

    InputStream var7 = var6.getEntity().getContent();
    this.this$0.result = this.convertStreamToString(var7);
    this.this$0.result = this.this$0.result.replace("\n", "");
    if (this.this$0.result != null) {
        Intent var8;
        if (this.this$0.result.indexOf("Correct Credentials") != -1) {
            Log.d("Successful login:", "account:" + this.this$0.username + ":" + this.this$0.password);
            this.saveCreds(this.this$0.username, this.this$0.password);
            this.trackUserLogins();
            var8 = new Intent(this.this$0.getApplicationContext(), PostLogin.class);
            var8.putExtra("username", this.this$0.username);
            this.this$0.startActivity(var8);
        } else {
            var8 = new Intent(this.this$0.getApplicationContext(), WrongLogin.class);
            this.this$0.startActivity(var8);
        }
    }
}
```

Nhìn vào đoạn code được khoanh, ta có thể dễ dàng nhận ra ngay đoạn code này đã để lộ username để đăng nhập là devadmin.

Ngoài ra, đoạn code này còn không thực hiện các biện pháp bảo mật sau:

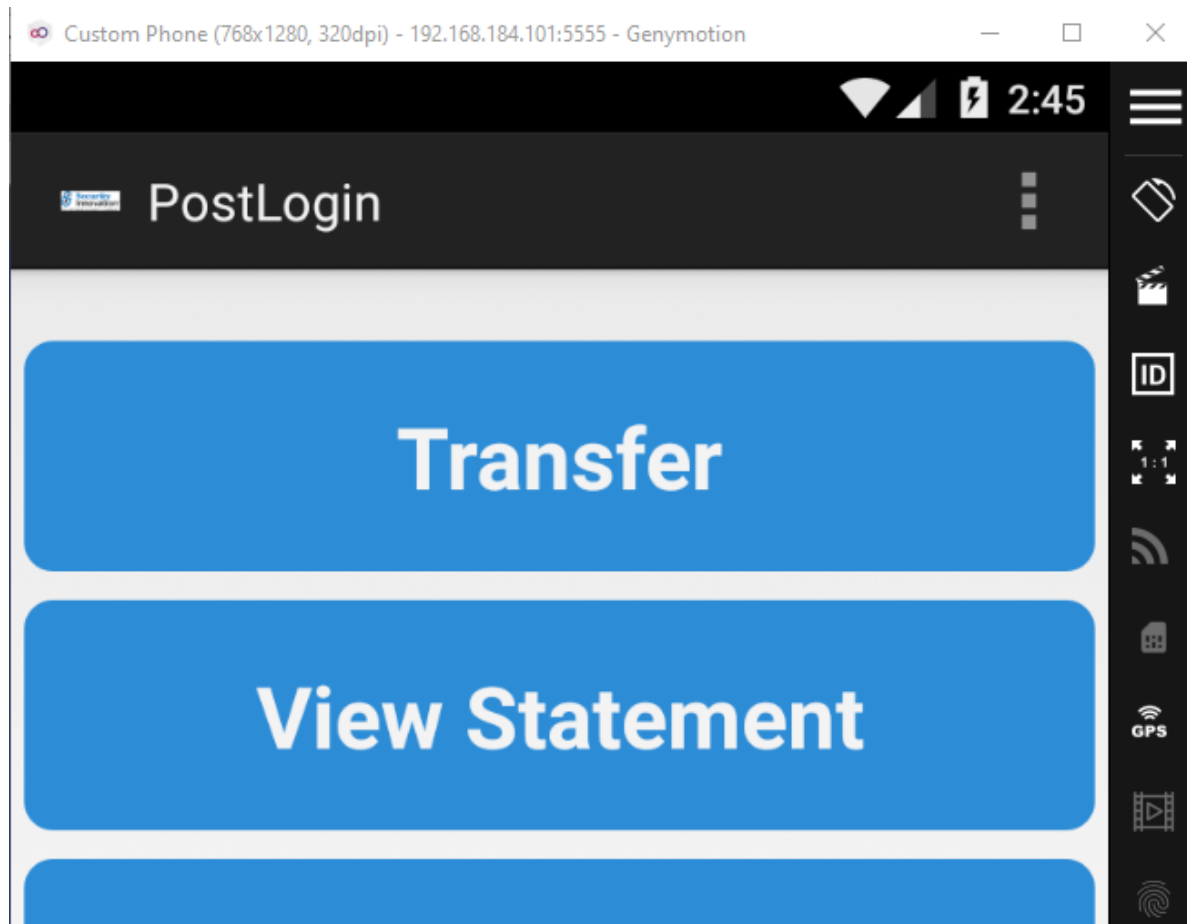
- Mã hóa các dữ liệu thông tin đăng nhập của người dùng trước khi gửi đi.
- Không có các biện pháp filter input để tránh việc bị dính các lỗ hổng như XSS, Injection, ...
- Không có các biện pháp hạn chế số lần login.
- Không sử dụng giao thức HTTPS thay thế cho HTTP.

Như vậy, các thông tin đăng nhập sẽ dễ dàng bị lộ và bị khai thác bởi những người có mục đích xấu.

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

Để kiểm tra dữ liệu có được an toàn hay không, ta cần login vào thiết bị và kiểm tra các thông tin của dữ liệu thông qua shell.

Tiến hành đăng nhập với tài khoản dinash/Dinash@123\$:



Bên shell của thiết bị android, tiến hành kiểm tra dữ liệu trong database:

```
sqlite> .database
main:
sqlite> .tables
sqlite> ^C^C^C1|genymotion:/data/data/com.android.insecurebankv2/databases #
130|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> .tables
android_metadata  names
sqlite> select * from names
...> ;
1|dinesh
```

Có thể thấy dữ liệu nằm hoàn toàn ở dạng plaintext và không được mã hóa.

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...

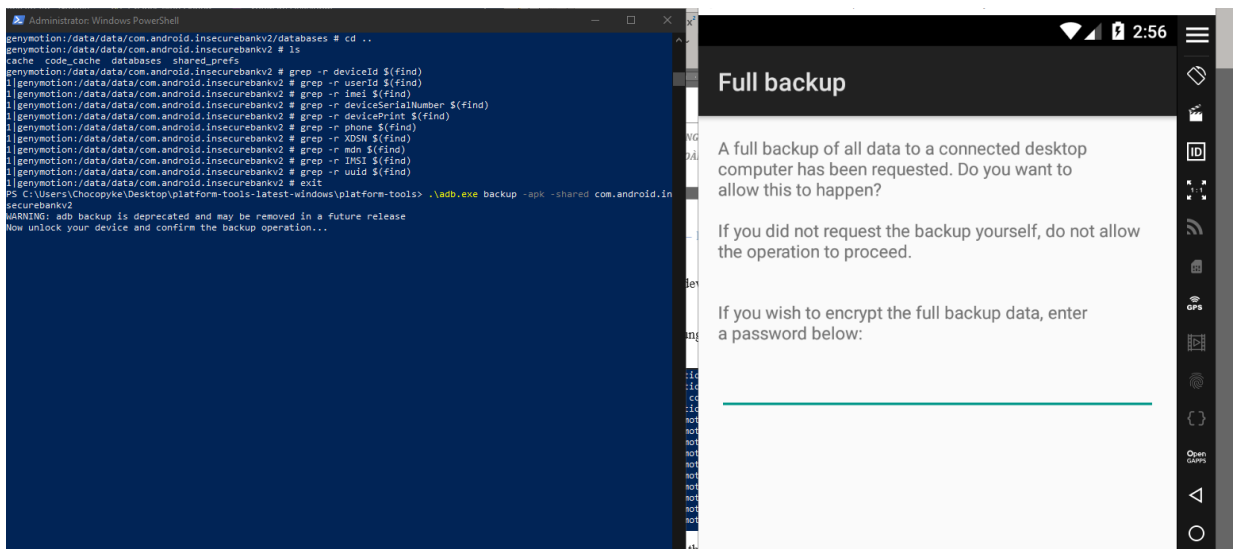
Thử dùng lệnh grep theo cấu trúc và các từ khóa đã cho để tìm kiếm các thông tin nhạy cảm:

```
genymotion:/data/data/com.android.insecurebankv2/databases # cd ..
genymotion:/data/data/com.android.insecurebankv2 # ls
cache code_cache databases shared_prefs
genymotion:/data/data/com.android.insecurebankv2 # grep -r deviceId $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r userId $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r imei $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r deviceSerialNumber $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r devicePrint $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r phone $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r XDSN $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r mdn $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r IMSI $(find)
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r uuid $(find)
1|genymotion:/data/data/com.android.insecurebankv2 #
```

Có thể thấy, không có thông tin nhạy cảm nào được lưu lại.

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

Tiến hành backup dữ liệu:



File backup đã được tạo:

AdbWinApi.dll	3/20/2024 4:42 PM	Application exten...	106 KB
AdbWinUsbApi.dll	3/20/2024 4:42 PM	Application exten...	72 KB
backup.ab	5/28/2024 10:01 AM	AB File	2,804 KB
etc1tool.exe	3/20/2024 4:42 PM	Application	429 KB
fastboot.exe	3/20/2024 4:42 PM	Application	1,765 KB

Giải nén để đọc thông tin backup:

```
(kali㉿kali)-[~/Desktop]
$ 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, 0.000136141 s, 0.0 kB/s

(kali㉿kali)-[~/Desktop]
$ tar -xf backup_compressed.tar
```

Lấy được một vài thông tin của máy, bao gồm cả database:

```
(kali㉿kali)-[~/Desktop/apps/com.android.insecurebankv2]
$ cd sp

(kali㉿kali)-[~/Desktop/apps/com.android.insecurebankv2/sp]
$ ls
com.android.insecurebankv2_preferences.xml  mySharedPreferences.xml

(kali㉿kali)-[~/Desktop/apps/com.android.insecurebankv2/sp]
$ cat com.android.insecurebankv2_preferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="serverport">8888</string>
  <string name="serverip">10.0.3.2</string>
</map>
```

```
(kali㉿kali)-[~/Desktop/apps/com.android.insecurebankv2]
$ cd db

(kali㉿kali)-[~/Desktop/apps/com.android.insecurebankv2/db]
$ ls
mydb  mydb-journal

(kali㉿kali)-[~/Desktop/apps/com.android.insecurebankv2/db]
$ sqlite3 mydb
SQLite version 3.45.1 2024-01-30 16:01:20
Enter ".help" for usage hints.
sqlite> .database
main: /home/kali/Desktop/apps/com.android.insecurebankv2/db/mydb r/w
sqlite> .tables
android_metadata  names
sqlite> select * from names
... > ;
1|dinesh
sqlite>
```

Có thể thấy, thư mục database là thư mục nhất định phải được mã hóa để có thể bảo vệ an toàn cho dữ liệu của người dùng.

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

Dựa vào các thông tin đã cho và username/password đã được mã hóa trong file mySharedPreferences.xml, ta viết được chương trình như sau:

```
decrypt.py > ...
1 import sys
2 from Crypto.Cipher import AES
3 from Crypto.Util.Padding import unpad
4
5 # Define the key
6 key = b'This is the super secret key 123'
7
8 # Define the encrypted string (it is base64 encoded)
9 encrypted_string = 'DTrW2VXjSoFdq0e61fHxJg=='
10
11 # Decode the base64 string
12 encrypted_bytes = base64.b64decode(encrypted_string)
13
14 # Initialize the cipher with the key and a correct IV (16 bytes of zero)
15 iv = b'\x00' * 16
16 cipher = AES.new(key, AES.MODE_CBC, iv)
17
18 # Decrypt the data
19 decrypted_bytes = cipher.decrypt(encrypted_bytes)
20
21 # Unpad the decrypted bytes to get the original plaintext
22 decrypted_string = unpad(decrypted_bytes, AES.block_size)
23
24 # Convert bytes to string and print
25 print(decrypted_string.decode())
26
```

```
(kali㉿kali)-[~/Desktop]
└─$ python decrypt.py
Dinesh@123$
```

Kết quả thu được là mật khẩu của tài khoản dinesh.

Yêu cầu 6: Sinh viên điều chỉnh mã nguồn ứng dụng sao cho luôn hiển thị trạng thái “Rooted Device!!” với bất kỳ trạng thái nào của thiết bị.

Thực hiện theo hướng dẫn của bài lab và chỉnh leo quyền admin:

```
<string name="decline">Decline</string>
<string name="hello_world">Hello world!</string>
<string name="is_admin">yes</string>
<string name="login_screen_password">Password:</string>
<string name="login_screen_username">Username:</string>
```


Tạo lại file apk và thực hiện ký:

```
PS C:\Users\Chocopyke\Desktop\platform-tools-latest-windows\platform-tools> apktool b .\InsecureBankv2\ -o InsecureBankv3.apk
I: Using Apktool 2.9.3
I: Checking whether sources has changed...
I: Smaling small 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: InsecureBankv3.apk
Press any key to continue . . .
PS C:\Users\Chocopyke\Desktop\platform-tools-latest-windows\platform-tools>
```

```
(kali@kali)-[~/Desktop/lab/InsecureBank]
$ 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]:
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]: y
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]

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

(kali@kali)-[~/Desktop/lab/InsecureBank]
$
```

Thực hiện cài đặt lại file và lấy được quyền admin:

```
PS C:\Users\Chocopyke\Desktop\platform-tools-latest-windows\platform-tools> apktool b .\InsecureBankv2.apk -o InsecureBankv3.apk
I: Using Apktool 2.9.3
I: Checking whether sources has changed...
I: Smaling small 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: InsecureBankv3.apk
Press any key to continue . . .
PS C:\Users\Chocopyke\Desktop\platform-tools-latest-windows\platform-tools> adb.exe install .\InsecureBankv3.apk
Performing Streamed Install
adb: failed to install .\InsecureBankv3.apk: Failure [INSTALL_PARSE_FAILED_NO_CERTIFICATES: Failed to collect certificates from /data/app/vmdl1862158028.tmp/base.apk: Attempt to get length of null array]
PS C:\Users\Chocopyke\Desktop\platform-tools-latest-windows\platform-tools> adb.exe install .\InsecureBankv3.apk
Performing Streamed Install
Success
PS C:\Users\Chocopyke\Desktop\platform-tools-latest-windows\platform-tools>
```

Username

Password

Create User

Login

Autofill Credentials

Từ gợi ý của bài lab, ta nhận thấy tại label cond_2 sẽ in ra chuỗi “Device not Rooted!”. Như vậy ta chỉ cần chỉnh cho cond_2 này về vị trí “Rooted Device!!” để kết quả luôn trả về “Rooted Device!!”:

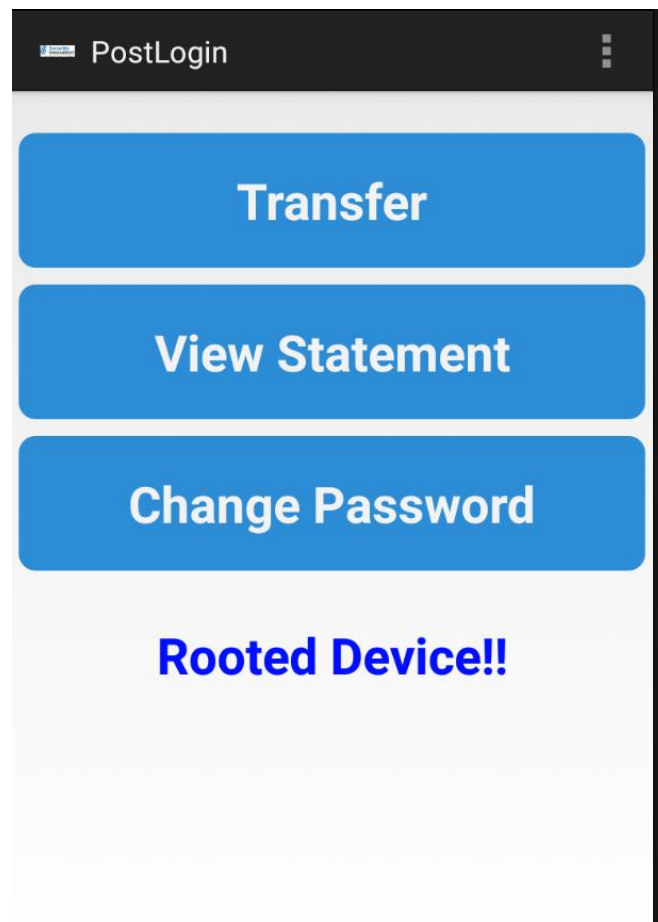
```
.line 88
.local v0, "isrooted":Z
:goto_0
if-ne v0, v1, :cond_2

.line 90
: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
```

Thực hiện lại các bước build, ký, cài đặt lại và chạy chương trình như trên. Kết quả thu được:



Yêu cầu 7: Hoàn thiện đoạn code trên và demo.

Cài đặt Frida trên máy tính:

```
C:\Users\Chocopyke>pip install frida
Defaulting to user installation because normal site-packages is not writeable
Collecting frida
  Downloading frida-16.2.5-cp37-ab13-win_amd64.whl.metadata (2.1 kB)
  Downloading frida-16.2.5-cp37-ab13-win_amd64.whl (33.0 MB)
    ----- 33.0/33.0 MB 114.3 kB/s eta 0:00:00
Installing collected packages: frida
Successfully installed frida-16.2.5

C:\Users\Chocopyke>pip install frida-tools
Defaulting to user installation because normal site-packages is not writeable
Collecting frida-tools
  Downloading frida-tools-12.4.2.tar.gz (345 kB)
    ----- 345.0/345.0 kB 1.0 MB/s eta 0:00:00
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\chocopyke\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from frida-tools) (0.4.6)
Requirement already satisfied: fridaclient<2.0.0,=>2.2 in c:\users\chocopyke\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from frida-tools) (10.2.5)
Collecting prompt_toolkit<4.0.0,=>2.0.0 (from frida-tools)
  Downloading prompt_toolkit-3.0.45-py3-none-any.whl.metadata (6.4 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-py3-none-any.whl.metadata (14 kB)
  Downloading prompt_toolkit-3.0.45-py3-none-any.whl (386 kB)
    ----- 386.0/386.0 kB 2.7 MB/s eta 0:00:00
  Downloading pygments-2.18.0-py3-none-any.whl (1.2 MB)
    ----- 1.2/1.2 MB 3.2 MB/s eta 0:00:00
  Downloading wcwidth-0.2.13-py3-none-any.whl (34 kB)
Building wheels for collected packages: frida-tools
  Building wheel for frida-tools (pyproject.toml) ... done
  Created wheel for frida-tools: filename=frida_tools-12.4.2-py3-none-any.whl size=209601 sha256=557a5097b9952a882ca7caca50c4cf8d2b534363f1804ac227bc88e0a23944
  Stored in directory: c:\users\chocopyke\appdata\local\pip\cache\wheels\eb\5e\05\44f1774268ebadd8fc813b1eb7dbdb96d8a61e25340224e2d
Successfully built frida-tools
Installing collected packages: wcwidth, pygments, prompt_toolkit, frida-tools
WARNING: The script pygmentize.exe is installed in 'C:\Users\Chocopyke\AppData\Local\Packages\PythonSoftwareFoundation.Python.3.12_qbz5n2kfra8p0\LocalCache\local-packages\Python312\Scripts' which is not on PATH.
Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
WARNING: The scripts frida-usb.exe, frida-compile.exe, frida-create.exe, frida-discover.exe, frida-kill.exe, frida-ls-devices.exe, frida-ls.exe, frida-ps.exe, frida-pull.exe, frida-push.exe, frida-rm.exe, frida-trace.exe and frida.exe are installed in 'C:\Users\Chocopyke\AppData\Local\Packages\PythonSoftwareFoundation.Python.3.12_qbz5n2kfra8p0\LocalCache\local-packages\Python312\Scripts' which is not on PATH.
Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed frida-tools-12.4.2 prompt_toolkit-3.0.45 pygments-2.18.0 wcwidth-0.2.13

C:\Users\Chocopyke>
```

Cài đặt Frida – server trên điện thoại ảo:

```
PS C:\Users\Chocopyke> cd C:\Users\Chocopyke\Desktop\platform-tools-latest-windows\platform-tools
PS C:\Users\Chocopyke\Desktop\platform-tools-latest-windows\platform-tools> .\adb.exe push .\frida-server-16.2.5-android-x86 /data/local/tmp/frida-server
.\frida-server-16.2.5-android-x86: 1 file pushed, 0 skipped. 195.0 MB/s (56528216 bytes in 0.276s)
PS C:\Users\Chocopyke\Desktop\platform-tools-latest-windows\platform-tools> .\adb.exe shell
genymotion:/ # cd /data/local/tmp/
genymotion:/data/local/tmp # ls
frida-server
genymotion:/data/local/tmp # chmod +x frida-server
genymotion:/data/local/tmp # ls
frida-server
genymotion:/data/local/tmp # ./frida-server &
[1] 5509
genymotion:/data/local/tmp # Unable to start: Error binding to address 127.0.0.1:27042: Address already in use

[1] + Done (5) ./frida-server
130|genymotion:/data/local/tmp # ./frida-server &
[1] 5518
```

Thực hiện code:

```
code lord.py x
code lord.py
1 import frida
2 import time
3 device = frida.get_usb_device()
4 pid = device.spawn("com.android.insecurebankv2")
5 device.resume(pid)
6 time.sleep(1)
7 session = device.attach(pid)
8 hook_script = """
9 Java.perform
10 (
11     function ()
12     {
13         console.log("In hook script");
14         var PostLogin = Java.use('com.android.insecurebankv2.PostLogin');
15         var doesSuperUserApkExist = PostLogin.doesSuperUserApkExist;
16         doesSuperUserApkExist.implementation = function (s)
17         {
18             console.log("Successful!");
19             return true;
20         }
21     }
22 )
23 """
24 script = session.create_script(hook_script)
25 script.load()
26 input('...?')
```

Ý tưởng: hook hàm doesSuperUserApkExist để giá trị nó trả về luôn bằng TRUE. Sử dụng Java.use() để ghi đè nội dung của phương thức này và khiến chương trình trả về rooted trong mọi trường hợp. Tuy nhiên, nhóm chưa thể chạy hiện thực được đoạn code do có quá nhiều lỗi phát sinh trong quá trình cài đặt.

```
PS C:\Users\Chocopyke> pip install frida-tools
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: frida-tools in c:\users\chocopyke\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (12.4.2)
Requirement already satisfied: colorama<1.0.0,>=0.2.7 in c:\users\chocopyke\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from frida-tools) (0.4.6)
Requirement already satisfied: frida<17.0.0,>=16.2.2 in c:\users\chocopyke\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from frida-tools) (16.2.5)
Requirement already satisfied: prompt-toolkit<4.0.0,>=2.0.0 in c:\users\chocopyke\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from frida-tools) (3.0.45)
Requirement already satisfied: pygments<3.0.0,>=2.0.2 in c:\users\chocopyke\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from frida-tools) (2.18.0)
Requirement already satisfied: wcwidth in c:\users\chocopyke\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from prompt-toolkit<4.0.0,>=2.0.0->frida-tools) (0.2.13)
PS C:\Users\Chocopyke> pip install frida
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: frida in c:\users\chocopyke\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (16.2.5)
PS C:\Users\Chocopyke> python
Python 3.12.3 (tags/v3.12.3:f6650f9, Apr 9 2024, 14:05:25) [MSC v.1938 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> frida-ps -U
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'frida' is not defined
>>> exit()
PS C:\Users\Chocopyke> frida-ps -U
frida-ps : The term 'frida-ps' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ frida-ps -U
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (frida-ps:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Chocopyke> cd C:\Users\Chocopyke\Desktop\platform-tools-latest-windows\platform-tools
```

Các package đã được cài đặt nhưng không thể tìm thấy khi thực thi. Do đó nhóm chưa thể hoàn thành task này.