

BÁO CÁO BÀI TẬP

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Buổi 04 (Session 04)

Tên chủ đề: Android pentest app

GV: Nghi Hoàng Khoa

Ngày báo cáo: 11/5/2023

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT101.N21.ANTN

STT	Họ và tên	MSSV	Email
1	Võ Anh Kiệt	20520605	20520605@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Kịch bản 1 đến 6	100%	
2	Kịch bản 7	0%	
3			
4			
5			

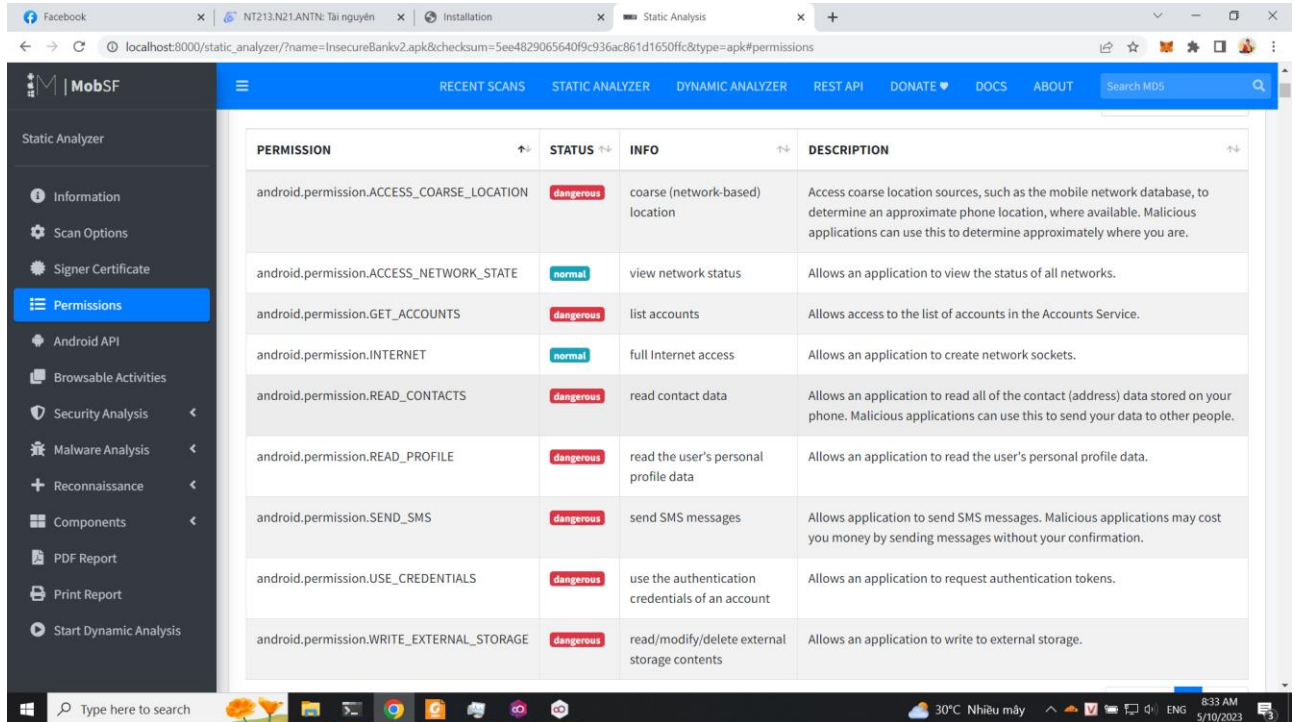
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

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

BÁO CÁO CHI TIẾT

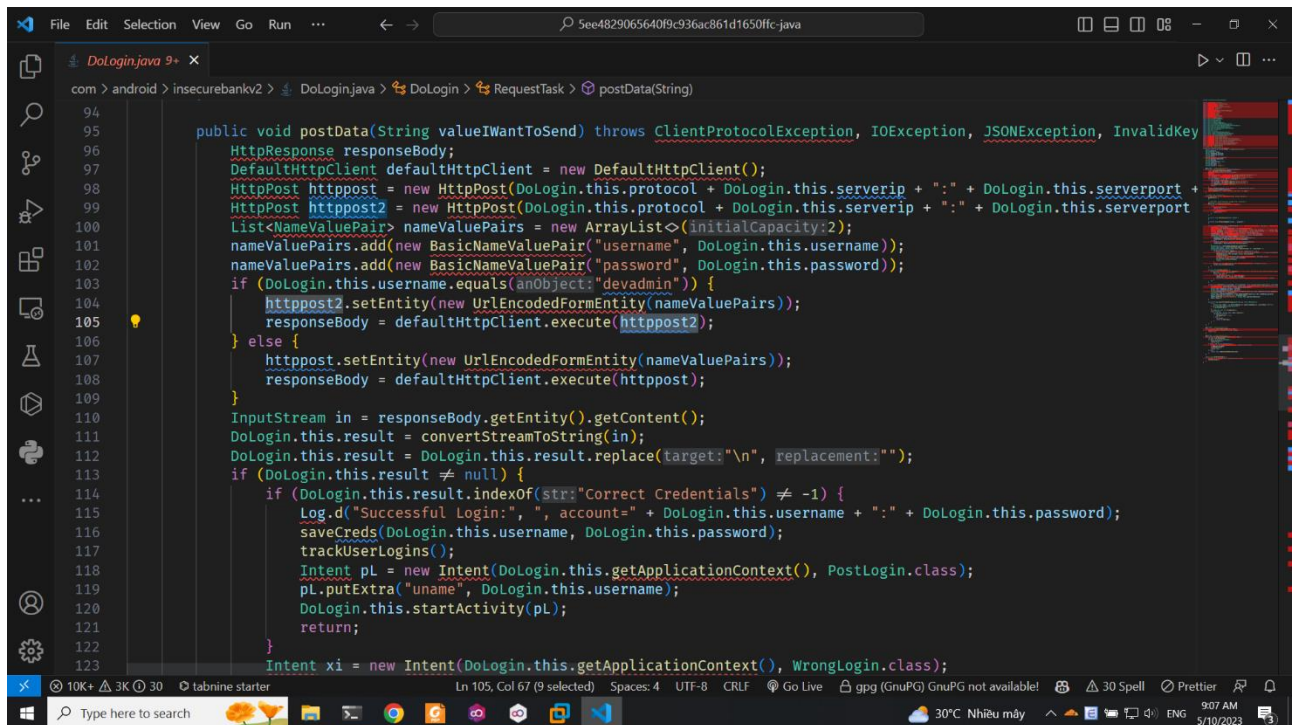
1. Kịch bản 01

Đầu tiên chạy chương trình phân tích code



Ta thấy có một số vấn đề đã được hiển thị như SEND_SMS, USE_CREDENTIAL,...

Tiếp tục ta sẽ thực hiện việc tải code java về và thực hiện phân tích kỹ



```
com > android > insecurebankv2 > DoLogin.java > DoLogin > RequestTask > postData(String)
94
95
96 public void postData(String valueIWantToSend) throws ClientProtocolException, IOException, JSONException, InvalidKey
97 {
98     DefaultHttpClient defaultHttpClient = new DefaultHttpClient();
99     HttpPost httpPost = new HttpPost(DoLogin.this.protocol + DoLogin.this.serverip + ":" + DoLogin.this.serverport +
100     HttpPost httpPost2 = new HttpPost(DoLogin.this.protocol + DoLogin.this.serverip + ":" + DoLogin.this.serverport
101     List<NameValuePair> nameValuePairs = new ArrayList<>(initialCapacity:2);
102     nameValuePairs.add(new BasicNameValuePair("username", DoLogin.this.username));
103     nameValuePairs.add(new BasicNameValuePair("password", DoLogin.this.password));
104     if (DoLogin.this.username.equals("devadmin")) {
105         httpPost2.setEntity(new UrlEncodedFormEntity(nameValuePairs));
106         responseBody = defaultHttpClient.execute(httpPost2);
107     } else {
108         httpPost.setEntity(new UrlEncodedFormEntity(nameValuePairs));
109         responseBody = defaultHttpClient.execute(httpPost);
110     }
111     InputStream in = responseBody.getEntity().getContent();
112     DoLogin.this.result = convertStreamToString(in);
113     DoLogin.this.result = DoLogin.this.result.replace(target:"\n", replacement:"");
114     if (DoLogin.this.result != null) {
115         if (DoLogin.this.result.indexOf(Str:"Correct Credentials") != -1) {
116             Log.d("Successful Login:", " ", account=" + DoLogin.this.username + ":" + DoLogin.this.password);
117             saveCreds(DoLogin.this.username, DoLogin.this.password);
118             trackUserLogins();
119             Intent pl = new Intent(DoLogin.this.getApplicationContext(), PostLogin.class);
120             pl.putExtra("uname", DoLogin.this.username);
121             DoLogin.this.startActivity(pl);
122             return;
123         }
124     }
125     Intent xi = new Intent(DoLogin.this.getApplicationContext(), WrongLogin.class);
126 }
```

Ở phần này ta thấy code đang thực hiện việc đăng nhập qua http protocol. Đầu tiên là sẽ khởi tạo các đối tượng sau đó lấy thông tin đăng nhập được thực hiện bởi http post. Tiếp tục thực hiện đến kết nối máy chủ bằng kết nối http và gửi thông tin login bao gồm username và password. Sau đó server sẽ trả kết quả về và kiểm tra xem cho phép đăng nhập hay không.

Hạn chế:

Để lộ thông tin đăng nhập là devadmin

Không thực hiện mã hoá dữ liệu thông tin đăng nhập

Không lọc đầu vào

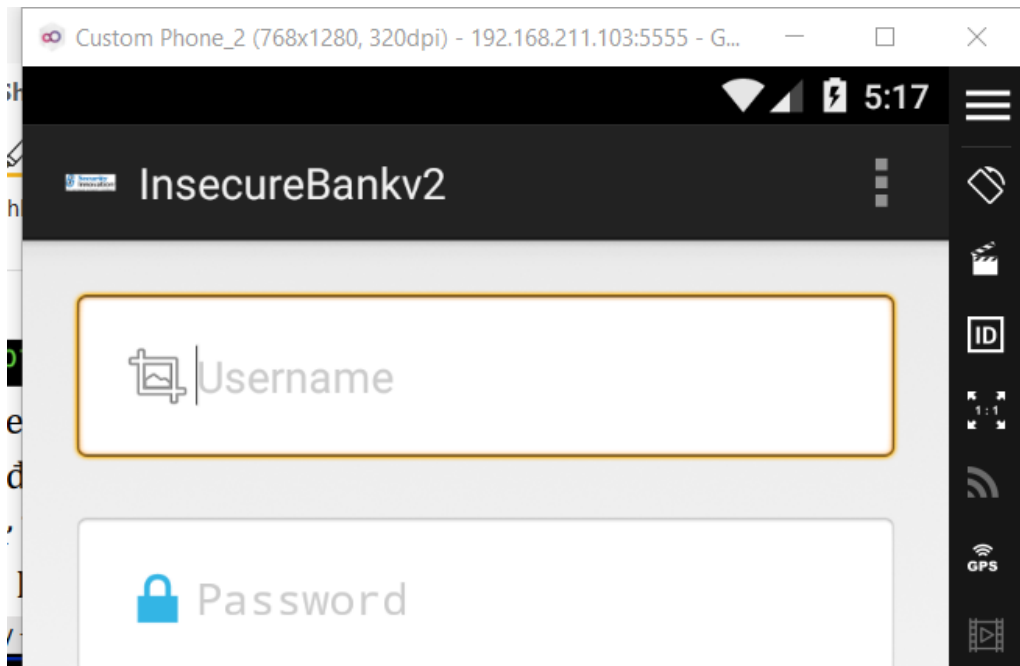
Không giới hạn số lần login

Không sử dụng những thư viện, class được cập nhật cải tiến

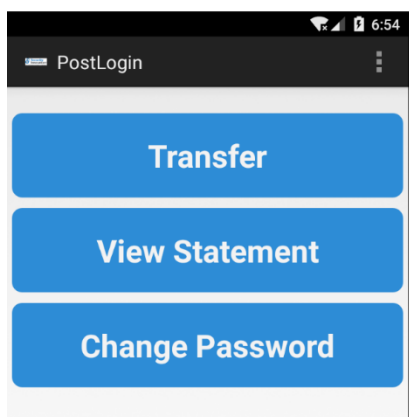
Không sử dụng https thay http

2. Yêu cầu 2

Ta sẽ thực hiện login và connect vào thiết bị sau đó sử dụng shell



Sau khi đã login vào



Connect shell tới thiết bị

```
PowerShell
mydb          mydb-journal
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
```

Tiếp tục thực hiện truy vấn và gọi tables thông tin ra

```

sqlite> .tables
android_metadata  names
sqlite> select * from names
...> ;
1|dinesh

```

Ở đây ta thấy việc lưu trữ dữ liệu không an toàn do dữ liệu được lưu hoàn toàn ở dạng plaintext chứ không được mã hoá

3. Yêu cầu 3

Ở thông tin tiếp theo thì ta thấy được rằng là những thông tin nhạy cảm được tìm kiếm với grep thì kết quả trả về là không thấy một thông tin nào đáng ngờ cả

```

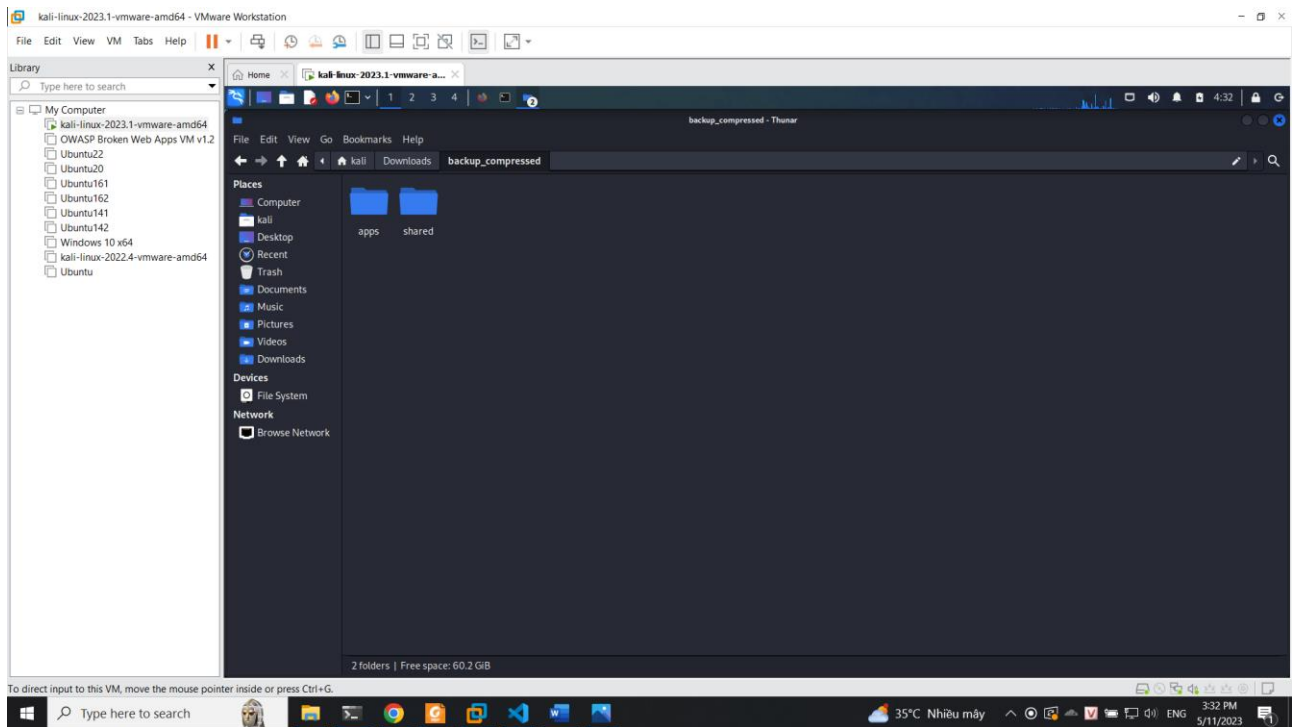
PowerShell
genymotion:/data/data/com.android.insecurebankv2 # grep -r <string-to-find> ${find}
/system/bin/sh: can't open string-to-find: No such file or directory
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r <user> ${find}
/system/bin/sh: can't open user: No such file or directory
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r <cache> ${find}
/system/bin/sh: can't create .
./cache
./code_cache
./databases
./databases/mydb
./databases/mydb-journal
./shared_prefs
./shared_prefs/com.android.insecurebankv2_preferences.xml
./shared_prefs/mySharedPreferences.xml: No such file or directory
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r <deviceId> ${find}
/system/bin/sh: can't open deviceId: No such file or directory
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r <userId> ${find}
/system/bin/sh: can't open userId: No such file or directory
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r <imei> ${find}
/system/bin/sh: can't open imei: No such file or directory
1|genymotion:/data/data/com.android.insecurebankv2 # cd cache
genymotion:/data/data/com.android.insecurebankv2/cache # ls
genymotion:/data/data/com.android.insecurebankv2/cache # ls -la
total 16
drwxrwx--x 2 u0_a66 u0_a66 .cache 4096 2023-05-10 01:26 .
drwxr-x--x 6 u0_a66 u0_a66 4096 2023-05-10 01:38 ..
genymotion:/data/data/com.android.insecurebankv2/cache # cd ..
genymotion:/data/data/com.android.insecurebankv2 # grep -r <deviceSerialNumber> ${find}
/system/bin/sh: can't open deviceSerialNumber: No such file or directory
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r <devicePrint> ${find}
/system/bin/sh: can't open devicePrint: No such file or directory
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r <phone> ${find}
/system/bin/sh: can't open phone: No such file or directory
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r <XDSN> ${find}
/system/bin/sh: can't open XDSN: No such file or directory
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r <IMSI> ${find}
/system/bin/sh: can't open IMSI: No such file or directory
1|genymotion:/data/data/com.android.insecurebankv2 # grep -r <IMSI> ${find}
/system/bin/sh: can't open IMSI: No such file or directory
1|genymotion:/data/data/com.android.insecurebankv2 #

```

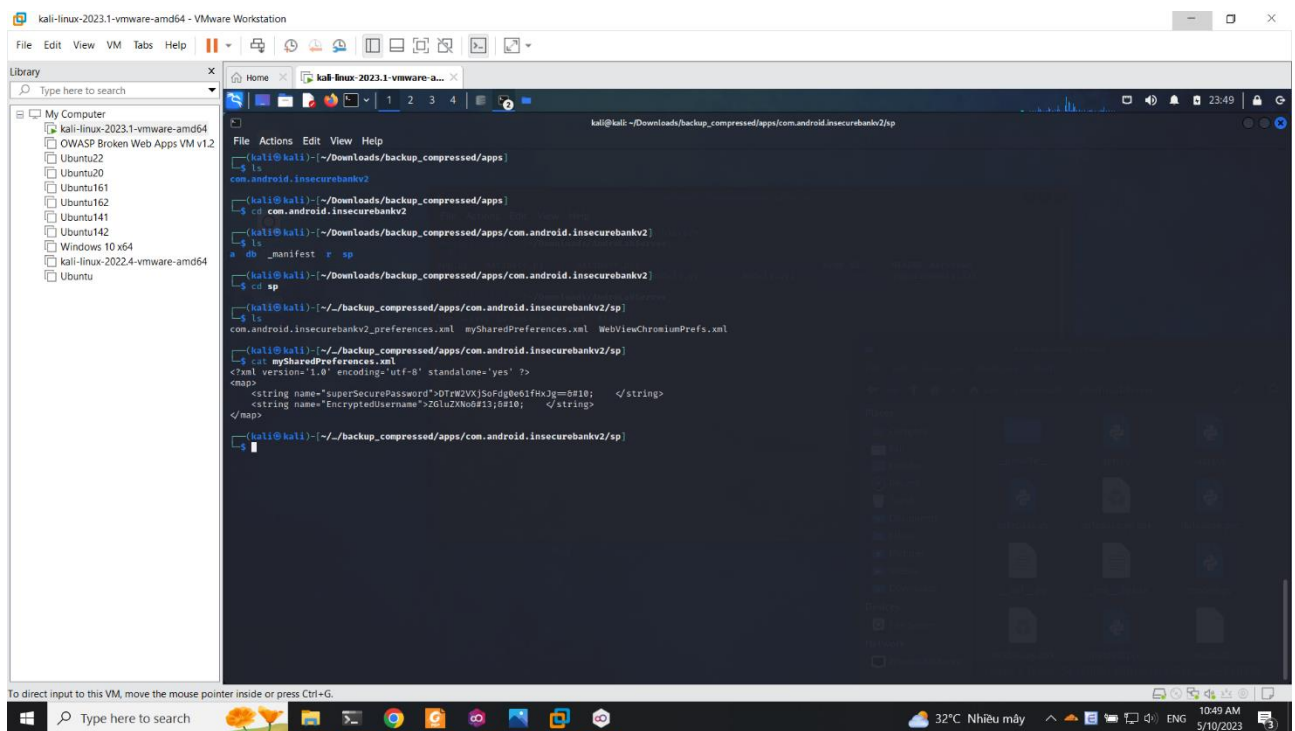
Có thể là ở trong phần này không có gì để tìm kiếm những thông tin nhạy cảm

4. Yêu cầu 4

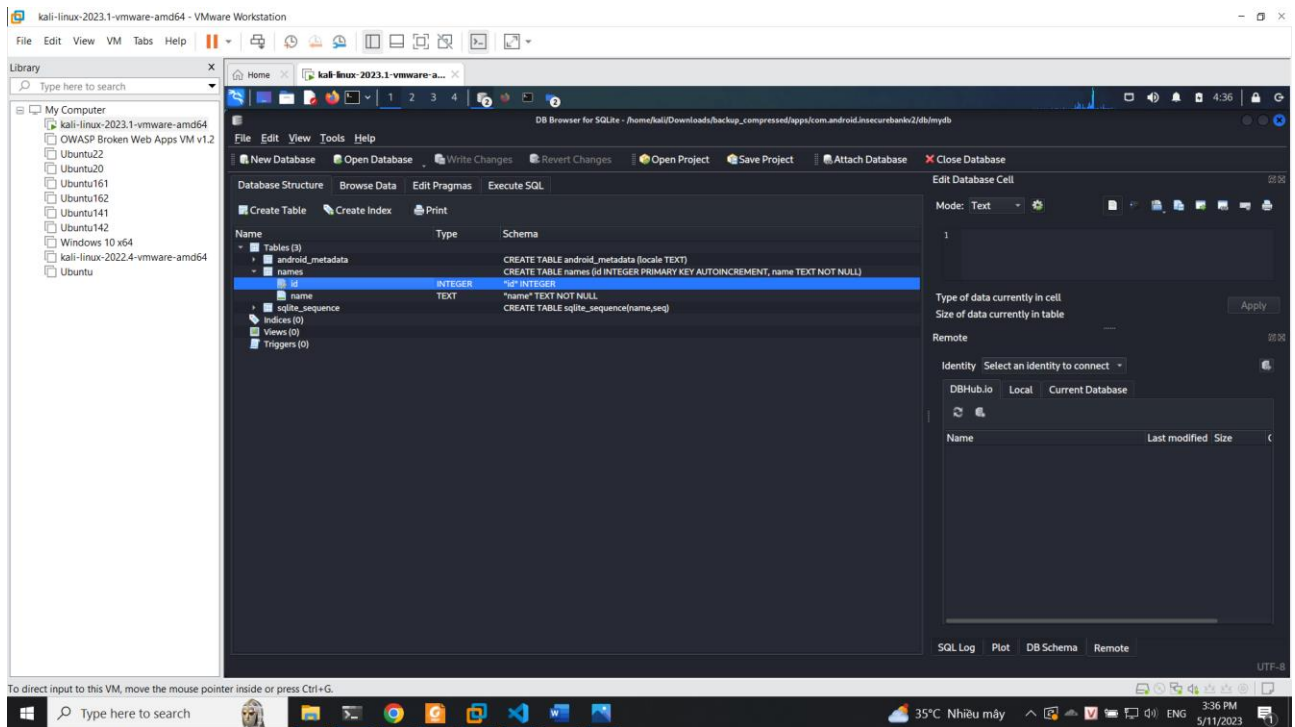
Tiếp tục quá trình ta sẽ thực hiện việc sao lưu thông tin, tạo nén và giải nén



Sau khi hoàn thành ta sẽ có file backup trên, thực hiện kiểm tra thì ta thấy có được một số thông tin được mã hoá

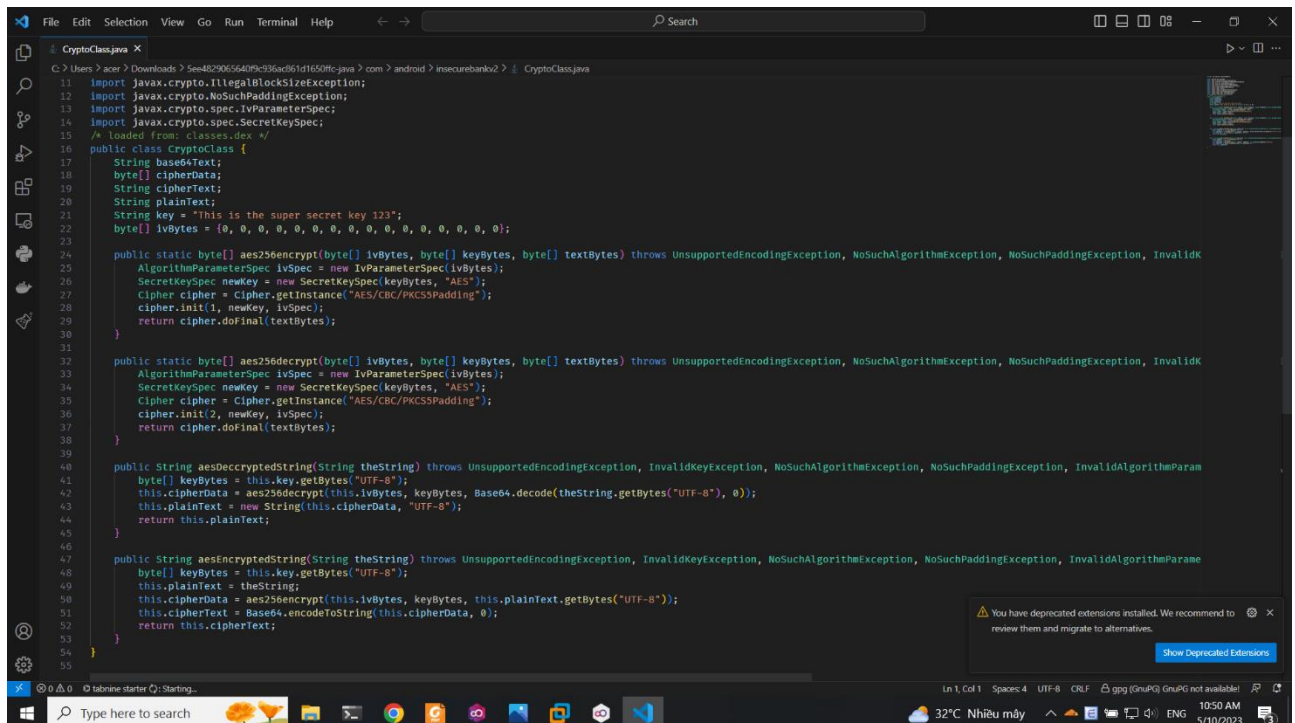


Và một số thông tin liên quan đến database

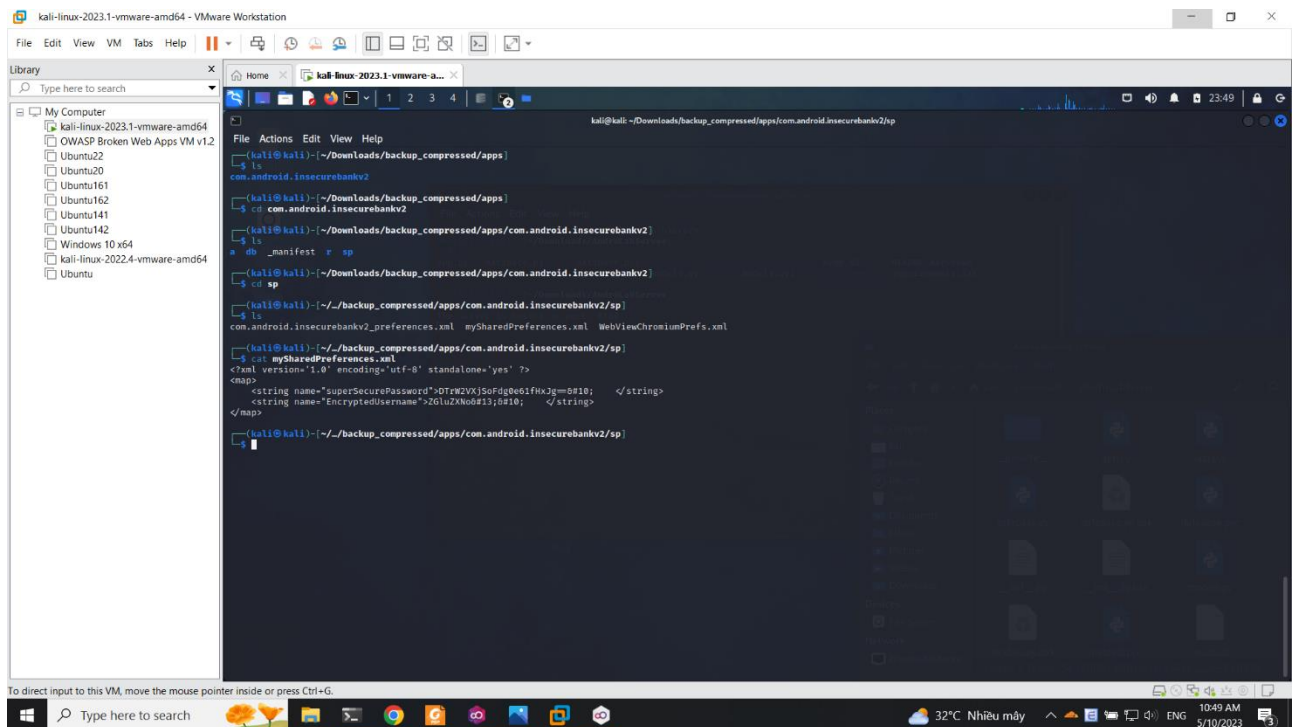


5. Yêu cầu 5

Tiếp tục tìm kiếm thông tin liên quan đến cơ chế mã hoá thì ta thấy được mã hoá đang sử dụng là aes cbc, với key là This is the super secret key 123 và iv như hình

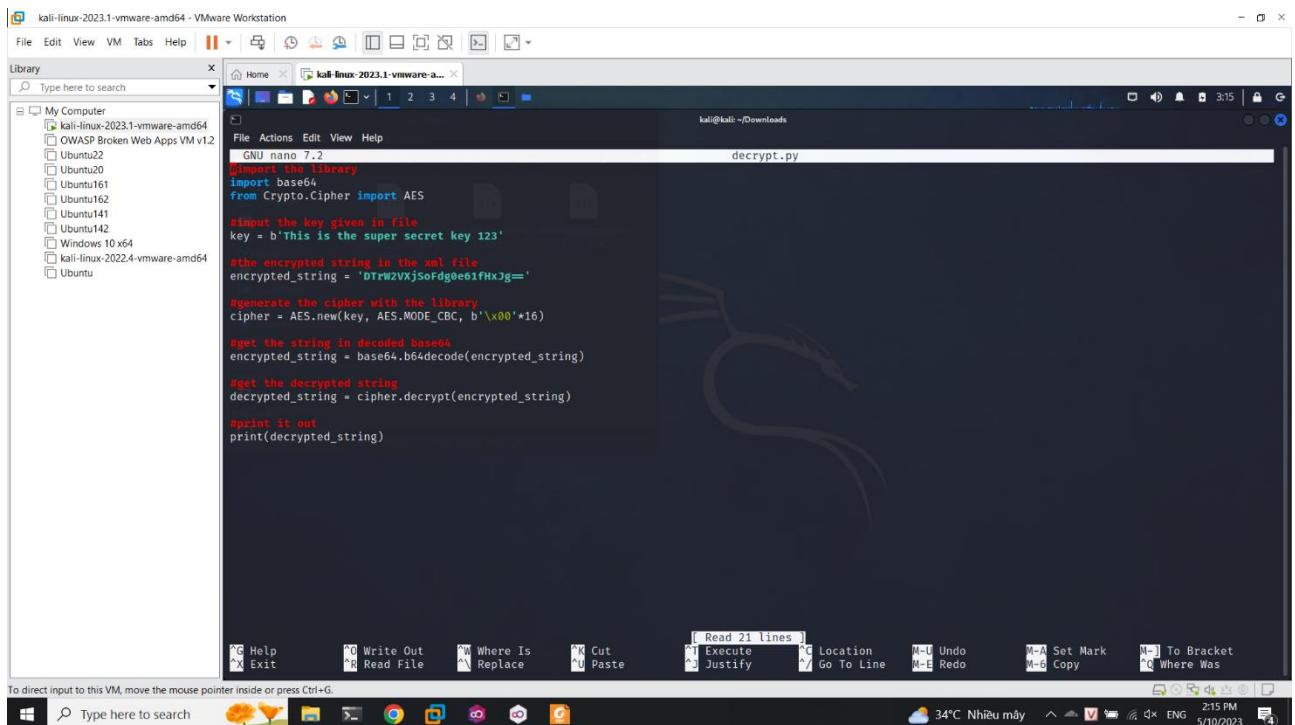


Đồng thời như bên trên ta cũng thấy được các thông tin mã hoá

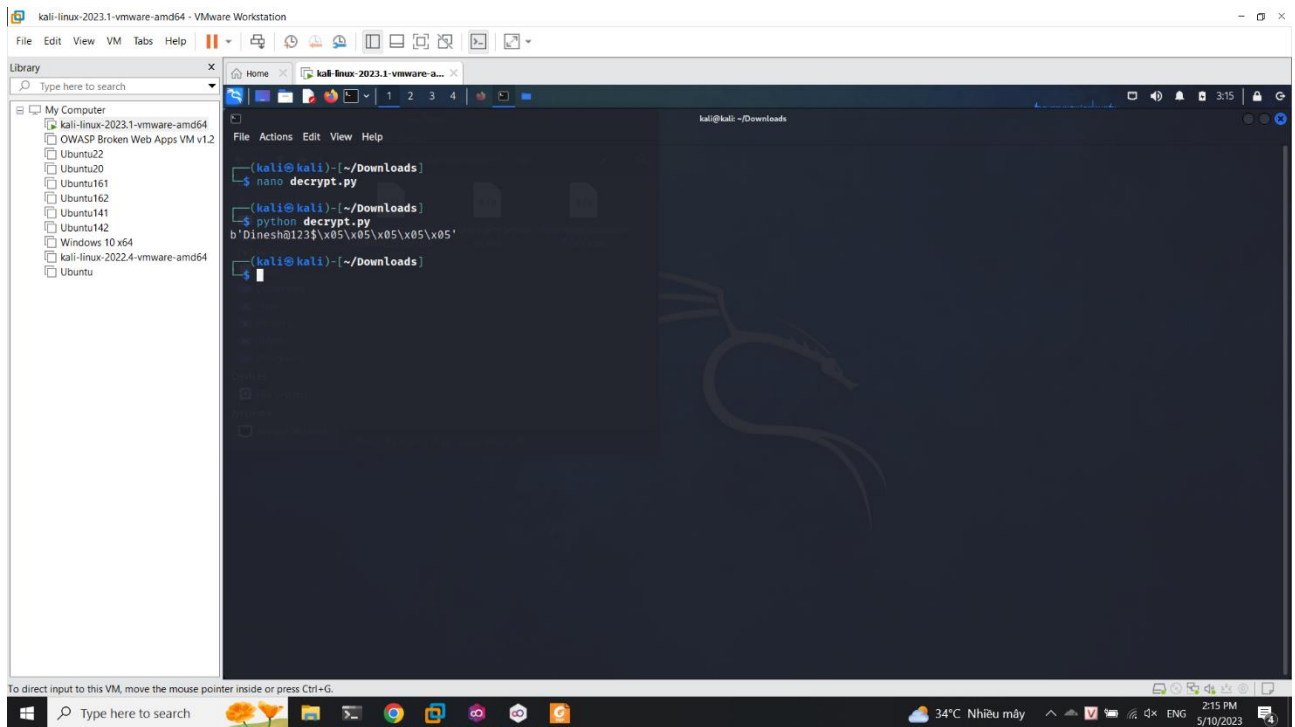


Thực hiện code python để lấy thông tin và giải mã

Với chương trình này ta sẽ thực hiện import các thư viện mật mã, truyền các tham số key và string mã hoá, tạo ra cipher bằng thư viện aes và cuối cùng thực hiện quá trình giải mã và xuất kết quả ra màn hình



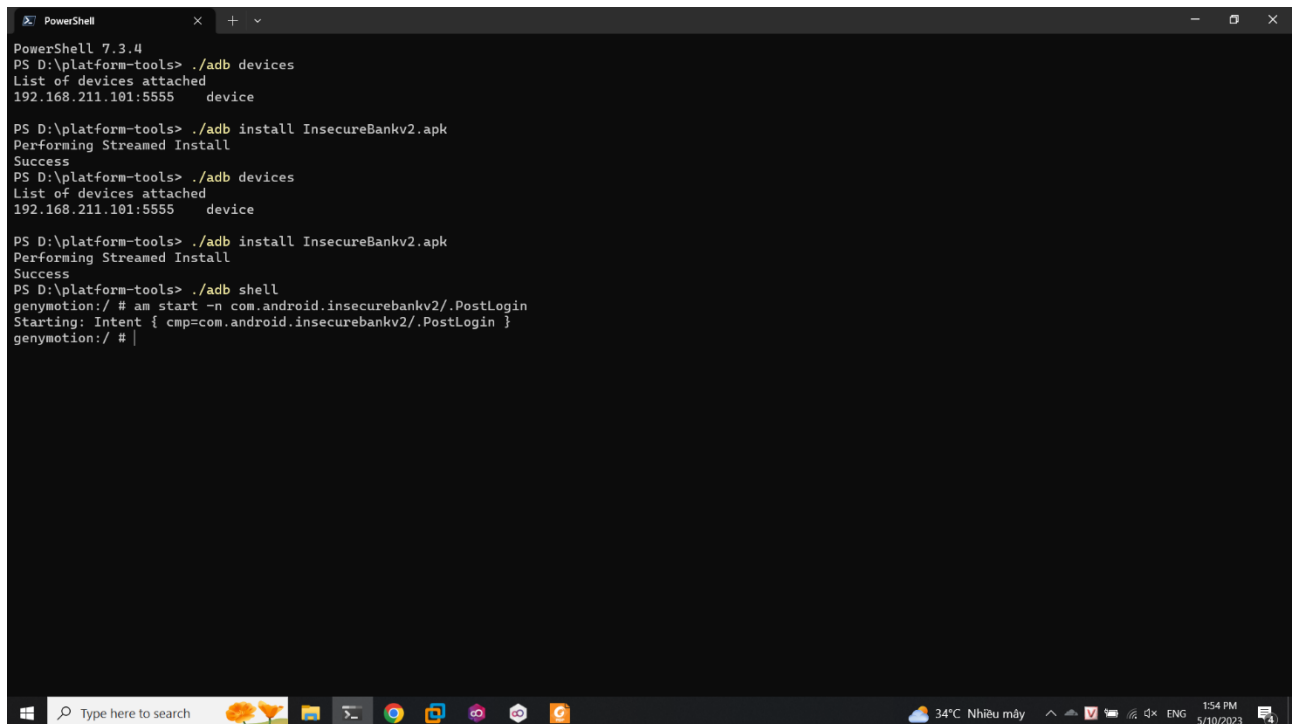
Sau khi chạy chương trình thì ta có kết quả



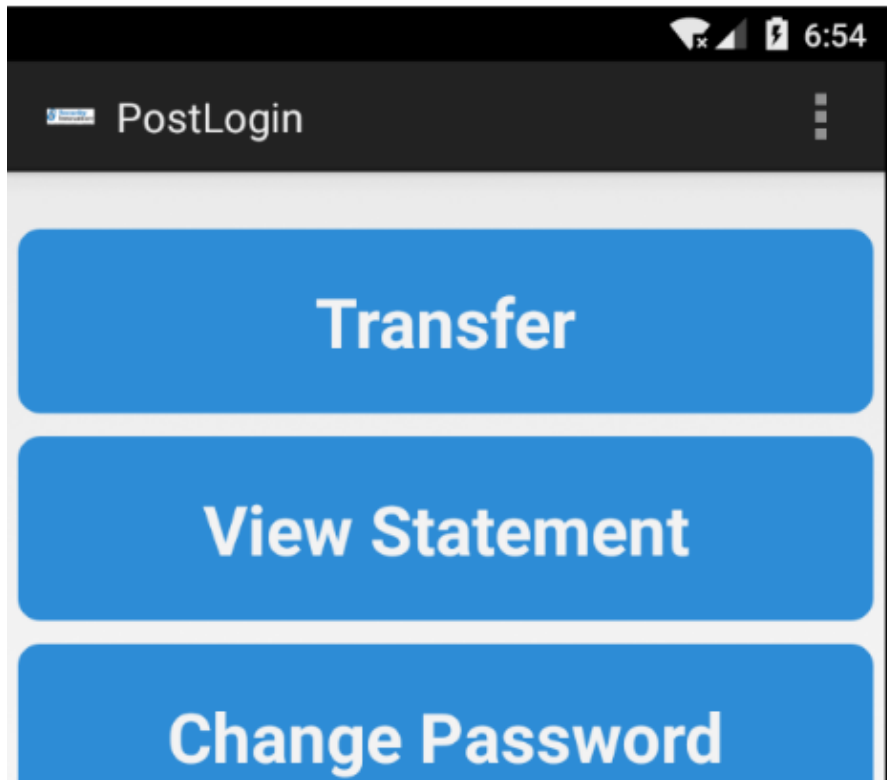
Ta thấy được thông tin bị mã hoá là mật khẩu của tài khoản Dinesh.

6. Yêu cầu 6

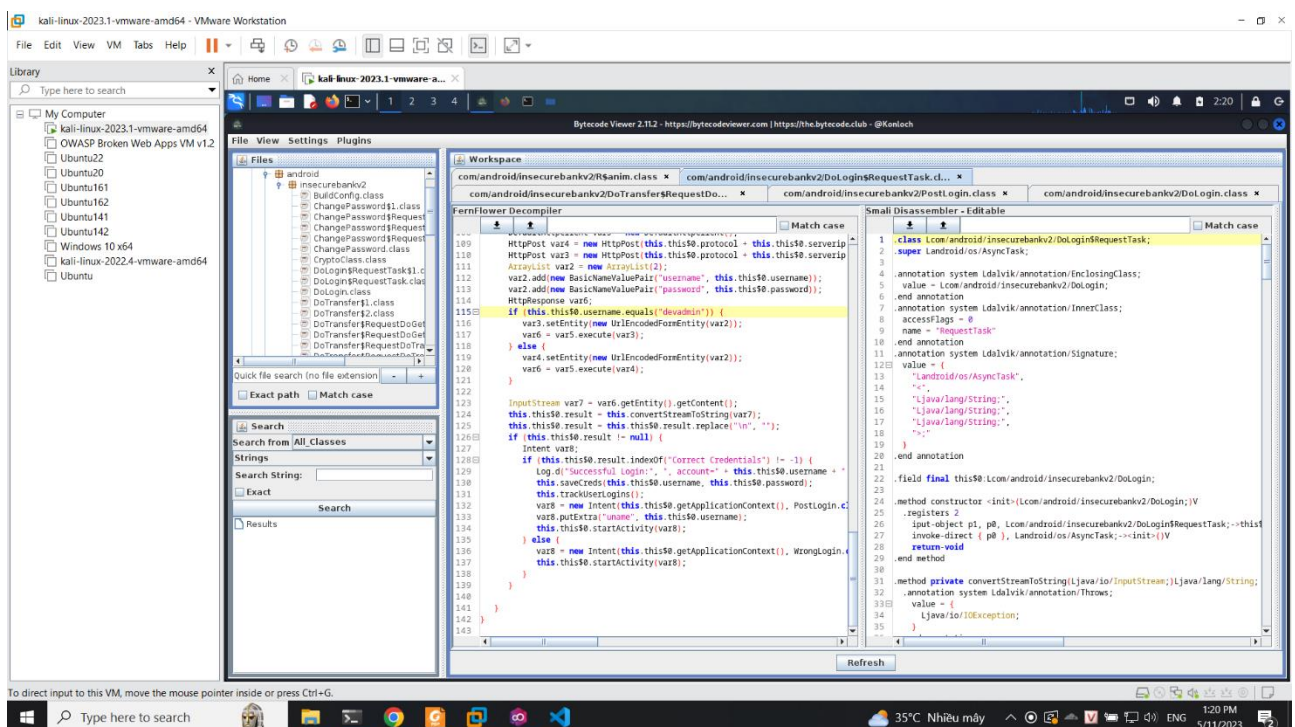
Thực hiện login không cần account



Thực hiện kiểm tra thì thấy đã login



Thực hiện đọc và phân tích code



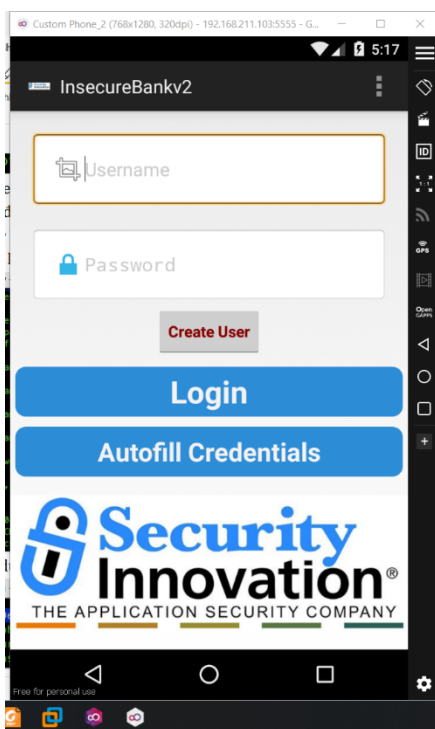
Tiếp tục thực hiện việc giải nén apk, decompile và thực hiện chỉnh sửa
Ở đây ta chỉnh leo quyền admin như hình


```
PowerShell
PS D:\platform-tools> ./adb devices
List of devices attached
192.168.211.102:5555    device

PS D:\platform-tools> ./adb install InsecureBankv3.apk
Performing Streamed Install
adb: failed to install InsecureBankv3.apk: Failure [INSTALL_FAILED_UPDATE_INCOMPATIBLE: Package com.android.insecurebankv2 signatures do not match previousl
y installed version; ignoring!]
PS D:\platform-tools> ./adb devices
List of devices attached
192.168.211.103:5555    device

PS D:\platform-tools> ./adb install InsecureBankv3.apk
Performing Streamed Install
Success
PS D:\platform-tools>
```

Ở đây ta thấy chương trình đã được leo quyền admin



Tiếp tục thực hiện chỉnh sửa code để cài đặt root device

Cách 1 chỉnh code trên java là if(true) thì kết quả sẽ luôn trả về root

```

44  });
45  this.changepasswd_button = (Button) findViewById(R.id.button_ChangePasswd);
46  this.changepasswd_button.setOnClickListener(new View.OnClickListener() { // from class: com.a
47      @Override // android.view.View.OnClickListener
48      public void onClick(View v) {
49          PostLogin.this.changePasswd();
50      }
51  });
52  }
53
54  void showRootStatus() {
55      boolean isrooted = doesSuperuserApkExist(s:"/system/app/Superuser.apk") || doesSUexist();
56      if (true) {
57          this.root_status.setText("Rooted Device!!");
58      } else {
59          this.root_status.setText("Device not Rooted!!");
60      }
61  }
62
63  private boolean doesSUexist() {
64      Process process = null;
65      try {
66          process = Runtime.getRuntime().exec(new String[]{"system/xbin/which", "su"});
67          BufferedReader in = new BufferedReader(new InputStreamReader(process.getInputStream()));

```

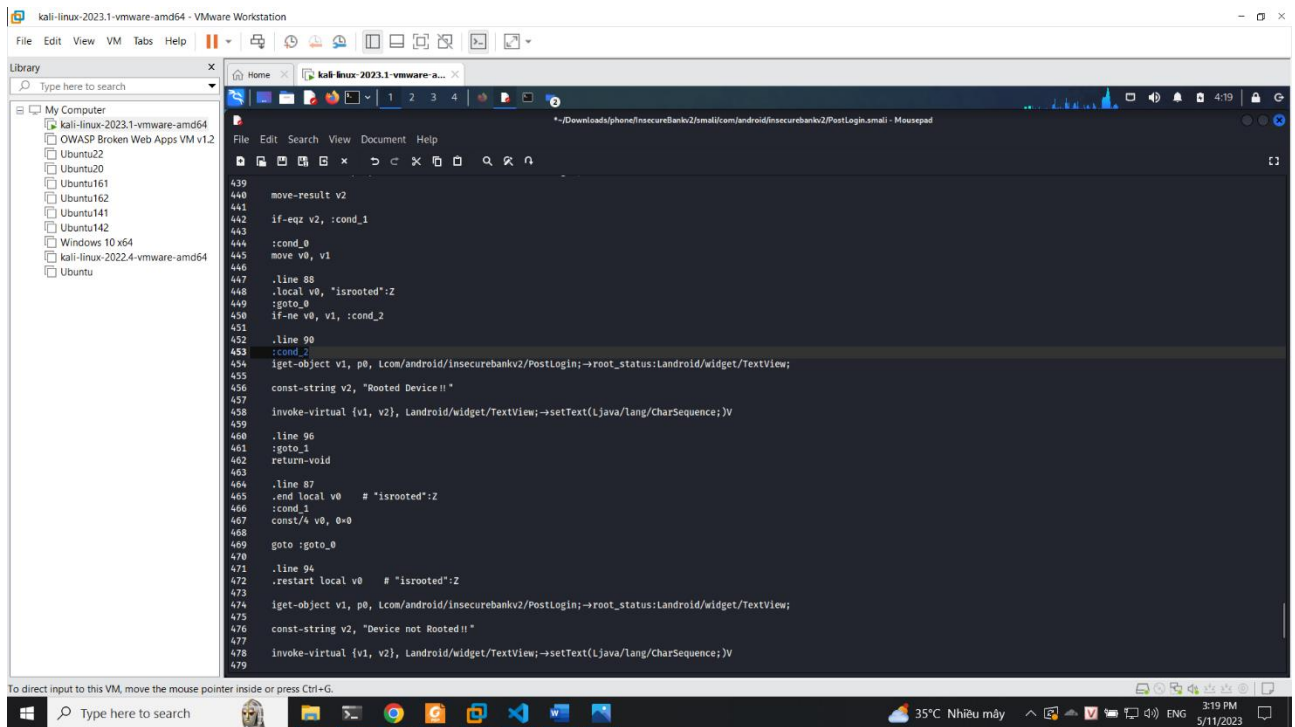
Cách 2: Chỉnh code trả về luôn là root device trên mọi trường hợp của code assembly

```

439  move-result v2
440
441  if-eqz v2, :cond_1
442
443  :cond_0
444  move v0, v1
445
446  .line 88
447  .local v0, "isrooted":Z
448  goto_0
449  if-ne v0, v1, :cond_2
450
451  .line 90
452  iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;→root_status:Landroid/widget/TextView;
453
454  const-string v2, "Rooted Device!!"
455
456  invoke-virtual {v1, v2}, Landroid/widget/TextView;→setText(Ljava/lang/CharSequence;)V
457
458  .line 96
459  goto_1
460  return-void
461
462  .line 87
463  .end local v0 # "isrooted":Z
464  :cond_1
465  const/4 v0, 0x0
466
467  goto :goto_0
468
469  .line 94
470  .restart local v0 # "isrooted":Z
471  :cond_2
472  iget-object v1, p0, Lcom/android/insecurebankv2/PostLogin;→root_status:Landroid/widget/TextView;
473
474  const-string v2, "Rooted Device!!"
475
476  invoke-virtual {v1, v2}, Landroid/widget/TextView;→setText(Ljava/lang/CharSequence;)V
477
478  goto :goto_1
479

```

Cách 3 chỉnh func cond_2 về nơi root device để kết quả luôn trả về ở root device



7. Yêu cầu 7

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 **.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/Tên Cá nhân đã đăng ký với GV).
Ví dụ: [NT101.K11.ANTT]-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.**
- 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. Khuyến khích:

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

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

HẾT