BÁO CÁO THỰC HÀNH

**Bài thực hành số 04: Android Pentesting**

**Môn học:** Bảo mật Web và Ứng dụng

**Lớp:** NT213.P12.ANTT.1

**THÀNH VIÊN THỰC HIỆN (Nhóm xx):**

|  |  |  |
| --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** |
| 1 | Phan Nguyễn Nhật Trâm | 22521501 |

|  |
| --- |
| **Điểm tự đánh giá** |
| **10** |

**ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| Tổng thời gian thực hiện | 5 ngày |
| Phân chia công việc |  |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị |  |

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

MỤC LỤC

[**A.** BÁO CÁO CHI TIẾT 2](#_Toc181743192)

[1. Phân tích tĩnh (Static Analysis) 2](#_Toc181743193)

[a. Phân tích thủ công 2](#_Toc181743194)

[2. Dịch ngược (Reverse Engineering) 5](#_Toc181743195)

[3. Phân tích động 8](#_Toc181743196)

[4. Hooking với Frida 9](#_Toc181743197)

[a. Cài đặt 9](#_Toc181743198)

[b. Thực hành 9](#_Toc181743199)

# BÁO CÁO CHI TIẾT

## Phân tích tĩnh (Static Analysis)

### Phân tích thủ công

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

A screenshot of a computer code

Description automatically generated

1. Code bất thường cần phân tích

* Thông tin password không được mã hoá có thể dẫn đến lỗ hổng Identification and Authentication Failures

var4.add(new BasicNameValuePair("username", this.this$0.username));

var4.add(new BasicNameValuePair("password", this.this$0.password));

* Khi tài khoản là devadmin thì request đến endpoint đặc biệt có thể quan sát trên URL. Điều này có thể gây ra lỗ hổng Broken Access Control

HttpPost var5 = new HttpPost(this.this$0.protocol + this.this$0.serverip + ":" + this.this$0.serverport + "/devlogin");

* Ghi log về thông tin đăng nhập, thông tin có thể bị khai thác thông qua lỗ hổng Security Logging and Monitoring Failures

Log.d("Successful Login:", ", account=" + this.this$0.username + ":" + this.this$0.password);

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

* Dữ liệu lưu trữ không an toàn vì không được mã hoá

A computer screen with white text

Description automatically generated

1. Dữ liệu người dùng trong cơ sở dữ liệu là plaintext

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

* Thông tin không lưu lại

A screen shot of a computer screen

Description automatically generated

1. Kiểm tra thông tin bằng từ khoá

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

A computer code on a black background

Description automatically generated

1. Thông tin mã hoá trong thư mục sao lưu

* Có 2 thông tin cần mã hoá an toàn
  + Mật khẩu
  + Tên người dùng: dự đoán hiện đang được mã hoá bằng base64

Yêu cầu 5 Viết chương trình giải mã đoạn dữ liệu mã hoá



1. Hàm mã hoá và giải mã mật khẩu của ứng dụng

A screenshot of a computer

Description automatically generated

1. Kết quả giải mã AES-CBC

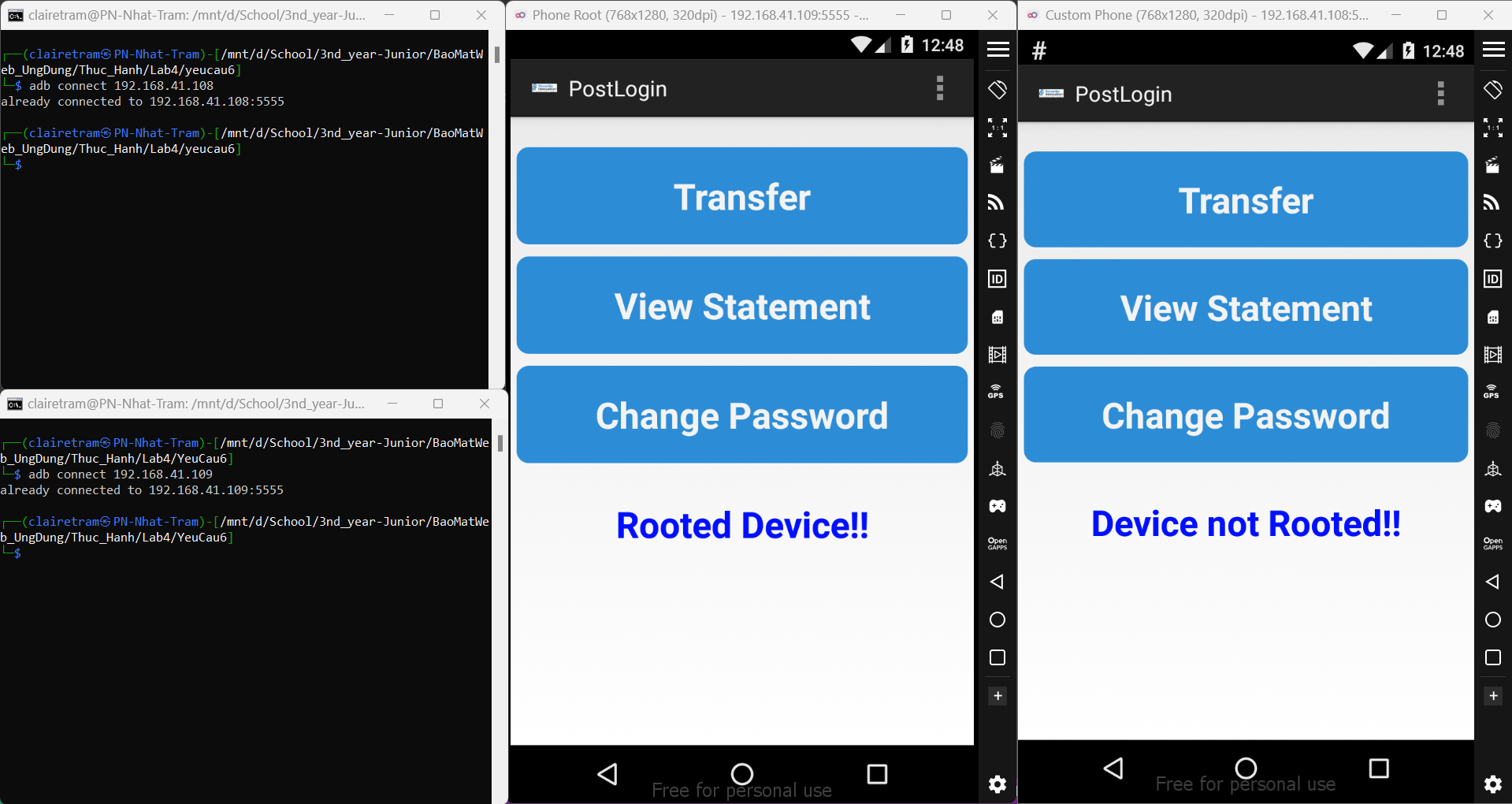
## Dịch ngược (Reverse Engineering)

A screenshot of a login screen

Description automatically generated

1. Install thành công (xuất hiện Create User)

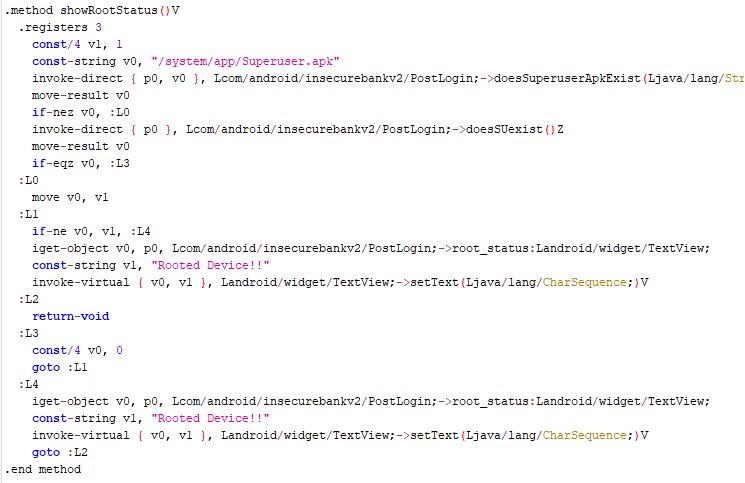
Yêu cầu 6: Sinh viên điều chỉnh mã nguồn ứng dụng sao cho luôn hiển thị trạng thái “Rooted Device!!” với bất kỳ trạng thái nào của thiết bị.



192.168.41.108

192.168.41.109

1. Thiết bị trước khi điều chỉnh mã nguồn



1. Code smali đã sửa

A screenshot of a computer code

Description automatically generated

1. Code Java tương ứng

* Quá trình:
  + Xem code tập tin apk bằng bằng chương trình Bytecode-Viewer-2.9.22.jar
  + Giải nén và dịch ngược file APK

apktool d InsecureBankv2.apk

* + Chỉnh sửa file PostLogin.smali
  + Recomplie lại tập tin apk

apktool b InsecureBankv2 -o InsecureBankv3.apk

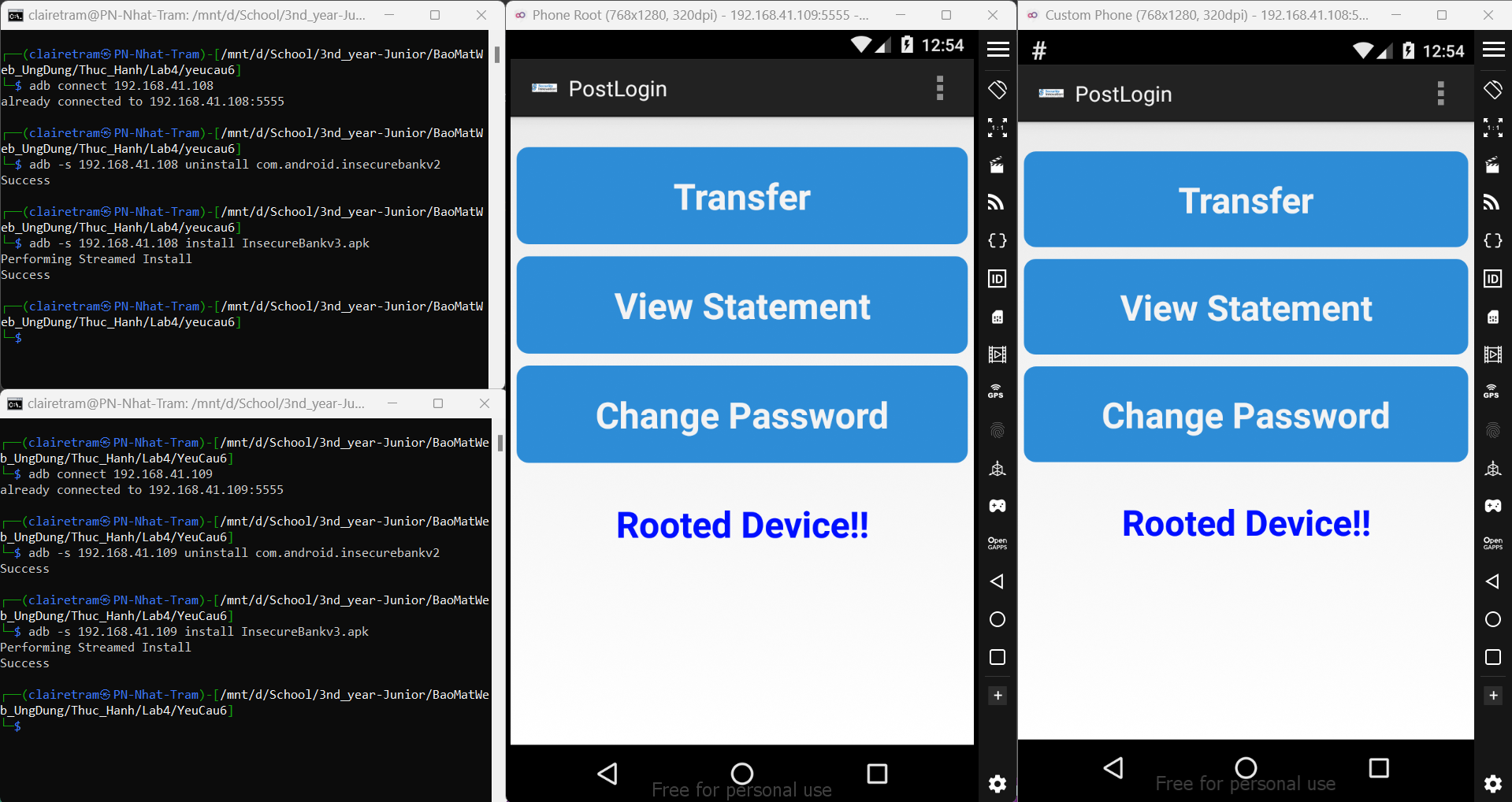
* + Tạo Keystore

keytool -genkey -v -keystore InsecureBankv3.keystore -alias InsecureBankv3 -keyalg RSA - keysize2048 -validity 10000

* + Sử dụng công cụ apksigner ký chữ ký số

apksigner sign --ks InsecureBankv3.keystore InsecureBankv3.apk

* + Tiến hành cài lại và mở ứng dụng

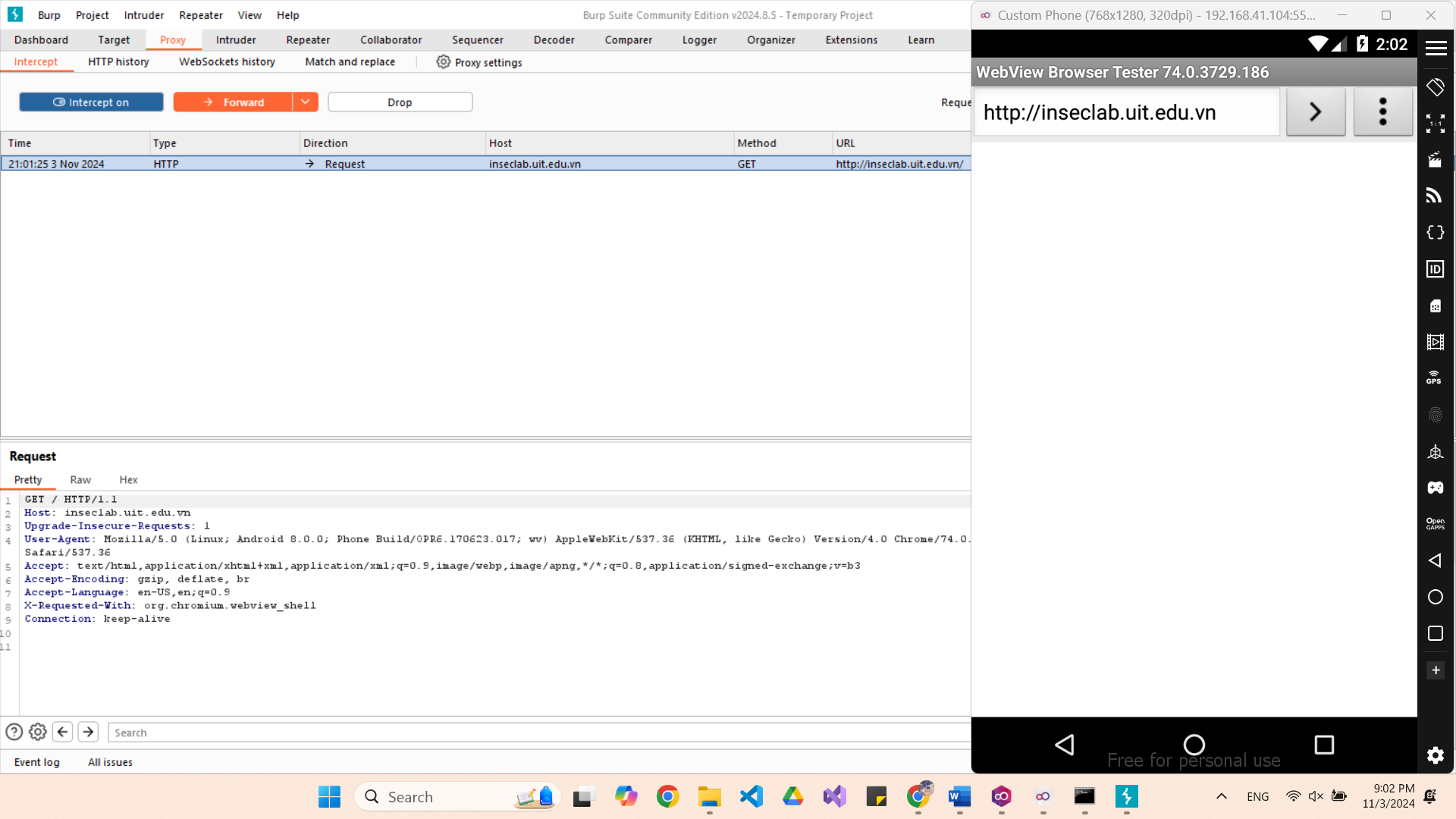


192.168.41.108

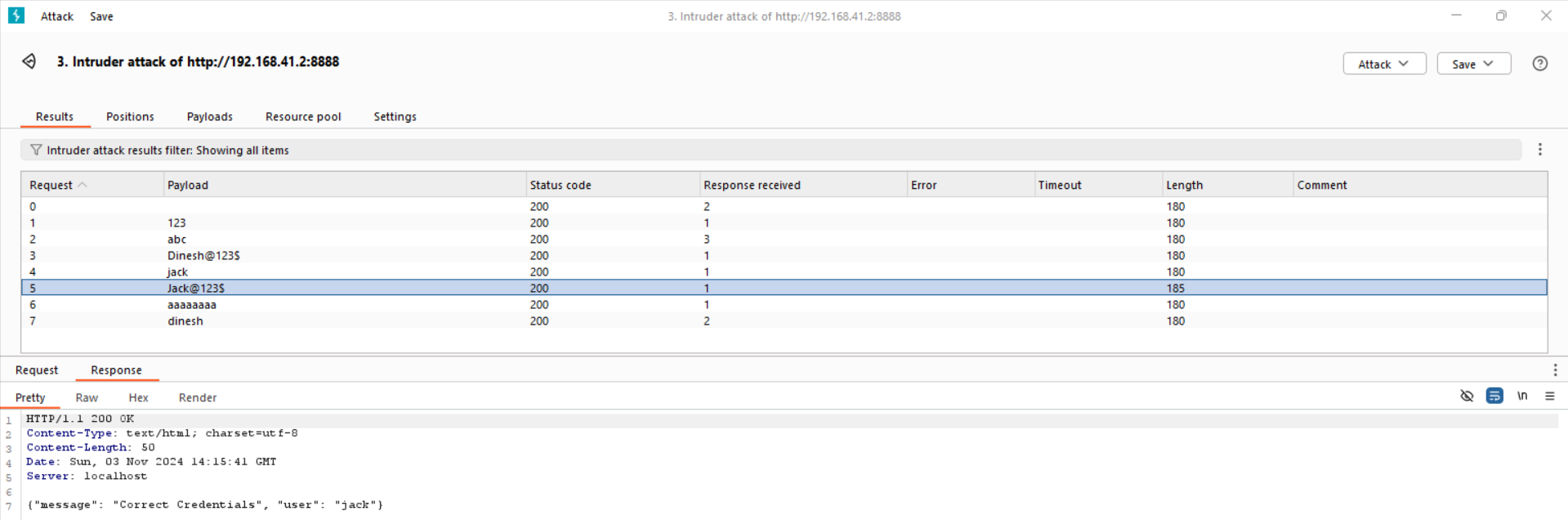
192.168.41.109

1. Kết quả đăng nhập

## Phân tích động



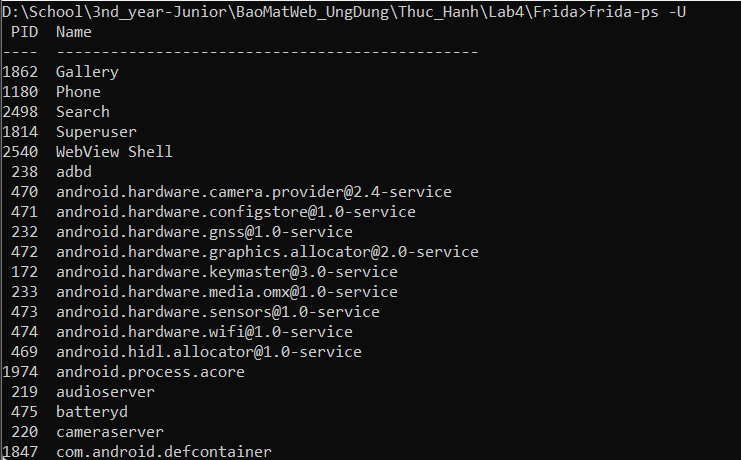
1. Cấu hình điện thoại ảo ‘proxy’ thông qua Burp Suite



1. Bruteforce mật khẩu đăng nhập

## Hooking với Frida

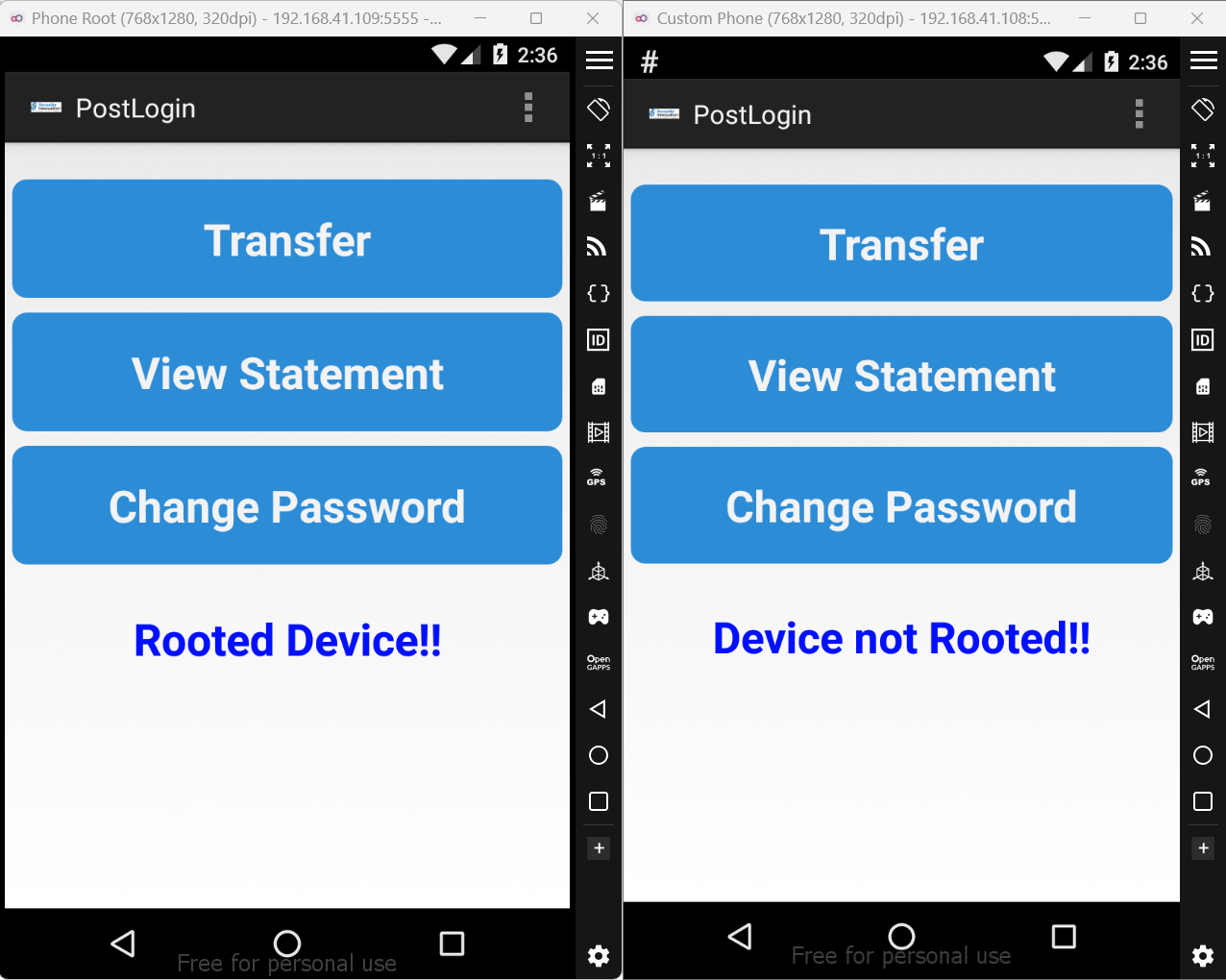
### Cài đặt



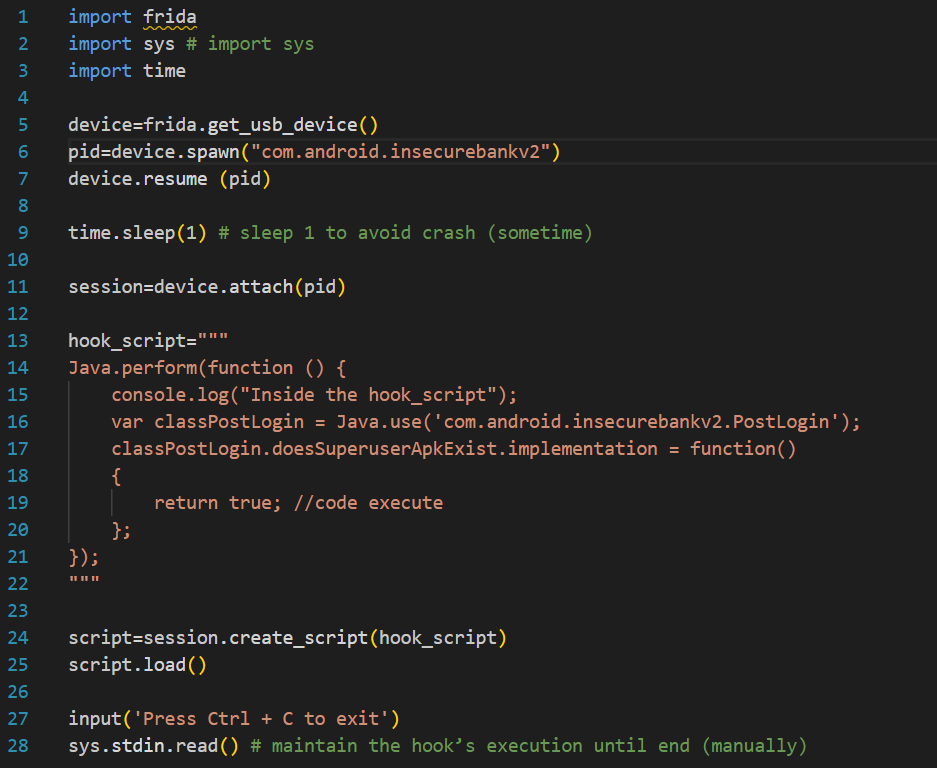
1. Cài đặt Frida thành công

### Thực hành

Yêu cầu 7: Hoàn thiện đoạn code và demo



1. Thiết bị khi chưa hook



1. Hoàn thiện đoạn code

A screenshot of a computer

Description automatically generated

1. Kết quả ghi đè