# Practice Case

**Haku Bank**

**Haku Bank** is a new private company that focuses on manage customers’ financial, newly built in 2023. When customers need to engage services provided by Haku Bank, they can go to the bank located in Jakarta. But lately, customers complained about the complicated procedures they need to proceed, also taking too much time to engage services in Haku Bank. In order of the problem response regarding this matter, Haku Bank developed an application to simplify the process of engaging bank’s services.

The application has been developed in form of **mobile application**. The feature that has been developed in the mobile application are **checking account balance** and **transfer fund to another account**. In process of mobile application development, they are obediently followed the process of Software Development Life Cycle (SDLC). But because of this matter, they have a problem in Testing phase from SDLC, which needs security testing.

One day, representative of Haku Bank engaged your service to do security testing in the Haku Bank mobile application. Long story short, they asked you to analyze the Haku Bank mobile application. To test the security of mobile application, test can be conducted in 2 types of analysis, which is static analysis and dynamic analysis. Your colleague will handle the dynamic analysis, meanwhile your job is to do **static analysis**.

Not to forget, you are still new in mobile application penetration testing. Responded to that matter, here are the questions that you need to answer:

## General Questions

1. Is the application secure enough? Or there are any concerns related to security issue in the mobile application?
2. If there are still some security issues reside in the application, tell readers precisely and concisely the security issues or vulnerabilities that you have found when testing the app!

## Technical Questions

### Information Gathering and Application Feature(s) Mapping Questions

1. Is there any root device checking written in mobile application source code? Pinpoint and screenshot the source code related to root device checking!
2. How the authentication conducted in the mobile application? How to make yourself authenticated? Tell the readers step by step, followed by screenshots to support each of your statement(s) (**Do not alter the source code yet, this phase requires you to do information gathering first**).
3. How many accounts that have been pre-registered when you executed the application? List all the accounts that have been pre-registered!
4. Are there any other special check(s) conducted in the mobile application (other than root device checking)? If there are, where are those special check(s) conducted? What procedures that each special check(s) do? Support your claim and statements with screenshots.

### Advanced Information Gathering Questions

1. Are there any activities in the mobile application that you can instantiate (start) without interactively execute the application from Android phone? If there are, which activities and how can it happen?
2. Could you access the mobile application data from *adb shell*? If can, how to access the mobile application data from *adb shell*? How come yourself can access the mobile application data (pinpoint which problematic configuration caused this problem)? Support your explanations with data that you have extracted, also screenshots.

### Reverse Engineering and Tampering Application Questions

1. How to bypass root device checking? Support your explanation with screenshots and procedures, also results of tampered APK installed in Android phone.
2. Related to [Information Gathering and Application Feature(s) Mapping Questions](#_Information_Gathering_and), question 4, how to enable yourself to have the feature that protected by those special check(s)? Support your explanation with screenshots and procedures, also results of tampered APK installed in Android phone.

### Special Questions

1. There is a credential that you can use to transfer unlimited money to another account. How to find the specified credential? Also, tell the readers the account number, card number, and passcode of specified credential.