# Lab 5: Equality Check

## Overview

In this lab, we will start to apply the patching there is a password to prevent unauthorized access to Info Activity and we don't know this password so we need to bypass the password check to access the Info Activity

## Steps

1. In the terminal navigate to labs > equality_check folder
    - you will find APk File which is hack.apk you can use it for this lab or open the Hack project in Android Studio and switch to the bypass_equality_check branch
      `git checkout bypass_equality_check`
      and build a new release app

2. Decompile the APK using apktool
    - execute this command
      `apktool d hack.apk`
    - a new folder will be generated using apktool called hack, this folder contains the app decompiled code

3. Patch the MainActivity$1.smali
    - from the path hack > smali_classes3 > com > afif > hack, open the MainActivity$1.smali file in the editor that you prefer, you will find a call to isCorrectPassword method like this

      ```
      invoke-virtual {v0, v1}, Lcom/afif/hack/MainActivity;->isCorrectPassword(Ljava/lang/String;)Z

      move-result v0

      if-eqz v0, :cond_0
      ```

    - as you see the call result moved to the v0 register then there is an if condition to check if the v0 register is equal to zero, which means if the isCorrectPassword returned true
    - just change the condition from equal zero into not equal zero like this
      `if-nez v0, :cond_0`
    - now if the isCorrectPassword method returned false then the condition will be true

4. Build the app using apktool
    - `apktool b hack`
    - a new APK file will be generated in the hack > dist folder

5. Align the APK to 4-byte memory boundary

- **for Windows**
  - `zipalign -p -f -v 4 hack\dist\hack.apk hack_aligned.apk`
- **for Linux**
  - `zipalign -p -f -v 4 hack/dist/hack.apk hack_aligned.apk`
- the result is a new APK called hack_aligned.apk in the equality_check folder

6. Sign the new aligned APK

- **for Windows**
  - `apksigner sign --v2-signing-enabled --ks ..\sign\certificate.jks --ks-key-alias hack --ks-pass pass:Test1234 --key-pass pass:Test1234 hack_aligned.apk`
- **for Linux**
  - `apksigner sign --v2-signing-enabled --ks ../sign/certificate.jks --ks-key-alias hack --ks-pass pass:Test1234 --key-pass pass:Test1234 hack_aligned.apk`

7. Install the APK

- delete the previous version of the hack app and install this version
- `adb install hack_aligned.apk`
- now we can bypass the check, run the app and when you enter any wrong password the condition will be true and the Info Activity will be shown