Lab 6: Local Data Extraction

Overview

Android applications can store the data locally, in the Shared preferences or in SQLite Database so let's solve the second CTF challenge by extracting the data from the local storage to obtain the password

Steps

1. In the terminal navigate to labs > local_data_extraction 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 local_data_extraction branch
      `git checkout local_data_extraction`
      and build a new debug app

2. Install the new version of the hack app
    - `adb install hack.apk`

3. Open Device File Explorer
    - run the hack app, when the app starts it will insert the data into the local storage, disconnect your Android device from the USB cable so the Device File Explorer can refresh its content to view the inserted data
    - open Device File Explorer from the right bottom of Android Studio or go to the View > Tool Windows > and click Device File Explorer to open it
    - in the File Explorer you will see the structure of Android System files, open data > data folder, you will find a list of the installed applications so open our app which is com.afif.hack
    - in our app storage you will find the Shared Preferences and the Database so install the SQLite plugin in Android Studio to view the contacts table
    - in the HackSharedPref.xml you will find the flag

4. View the local storage from the terminal
    - go to the shell using this command
      `adb shell`
    - execute run-as and pass the package name to enter the app storage
      `run-as com.afif.hack`
    - enter the Shared Preferences
      `cd shared_prefs`

- print the HackSharedPref.xml file content using cat utility
  `cat HackSharedPref.xml`
  the flag will be printed to the console, the same result in Android Studio

5. Enter the flag

   - use this flag to access the Info Activity, now we have solved the CTF challenge level 2