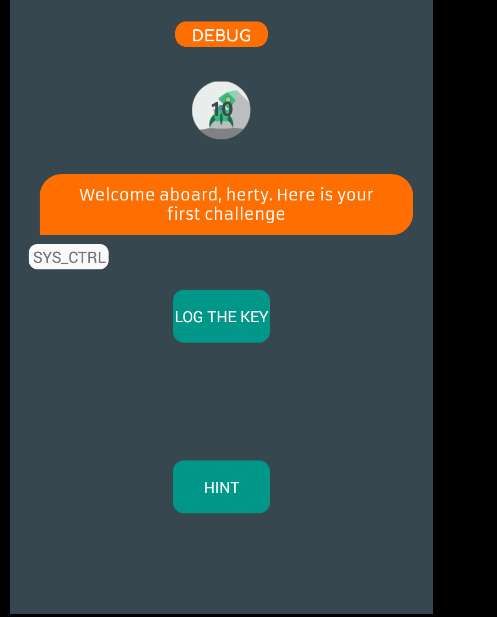
Extreme vulnerable Android Labs(EVABS) writeup

Debug

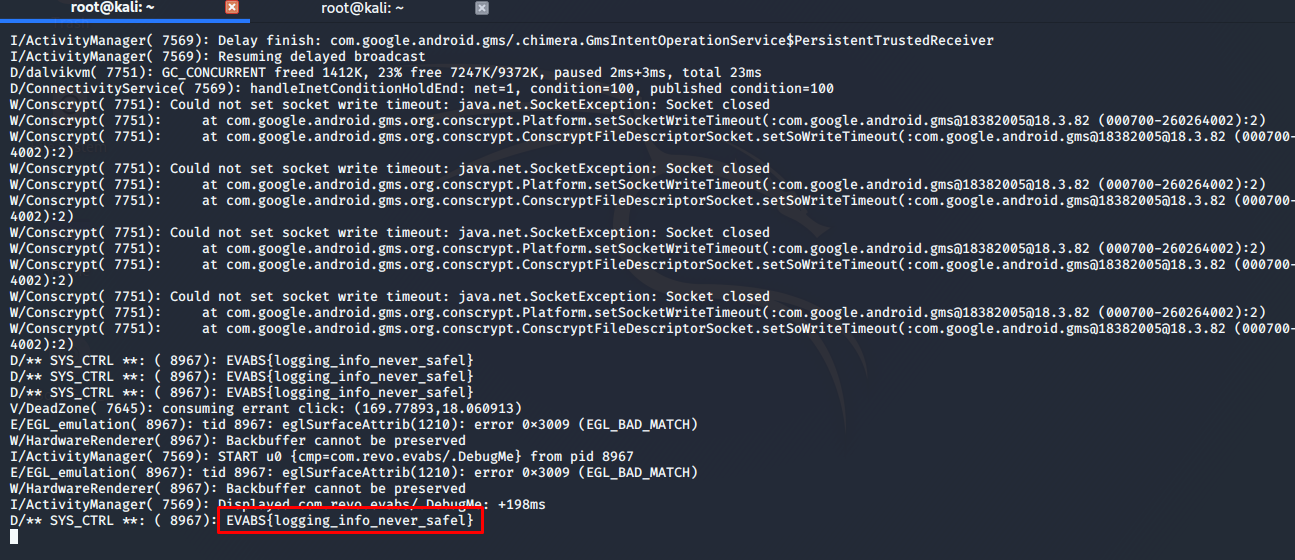
1. Connect to the emulator using the ADB and then in the terminal type

**Cmd**: adb logcat

1. Now navigate to the challenge page and click on Log the key

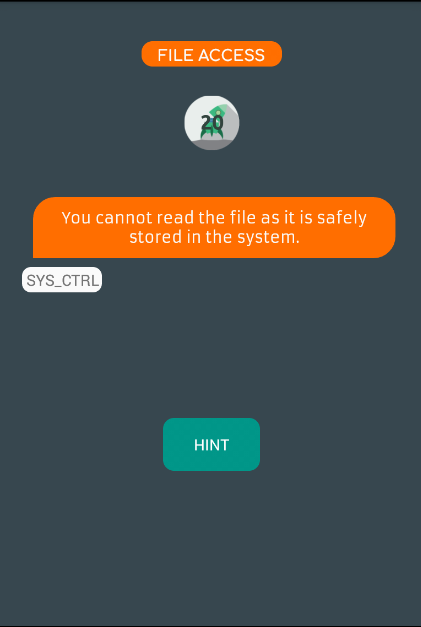


1. It can be observed in the logs that the flag has been present.



Challenge2:File Access

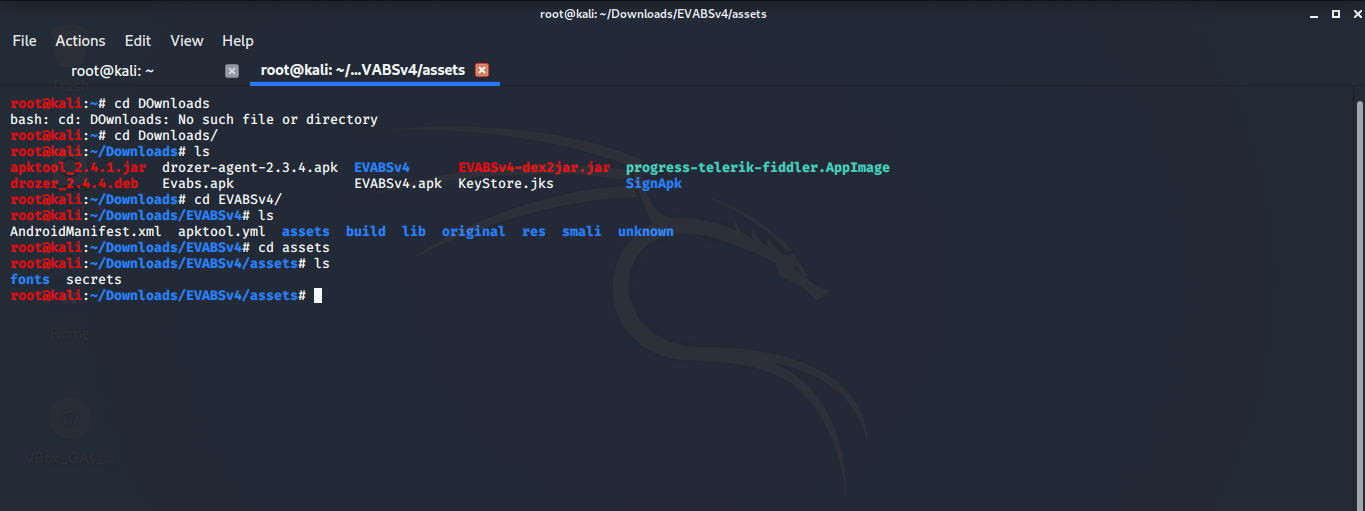
1. Navigate to the challenge



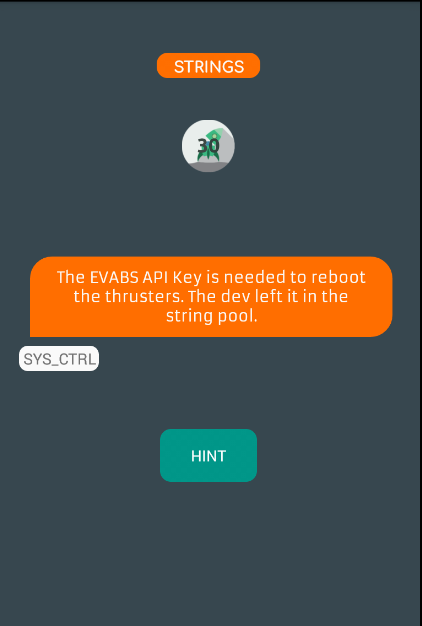
1. Now decompile the application using apktool by using command

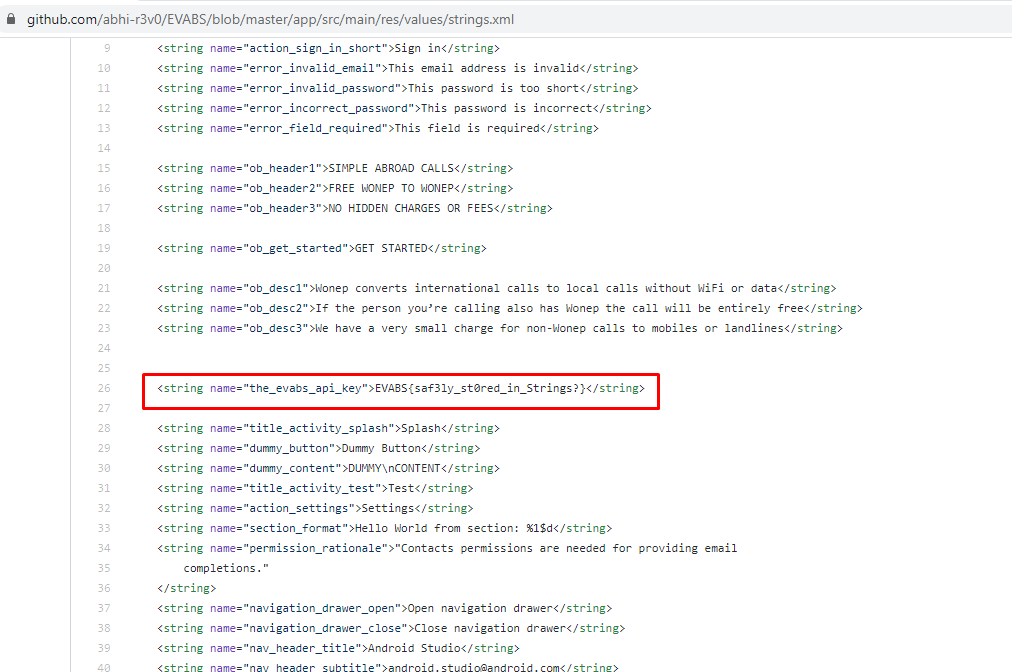
**Cmd:**apktool d EVABSV4.apk

1. Now Navigate to the assets folder in the application there we can find a file named secrets which has the flag to this challenge



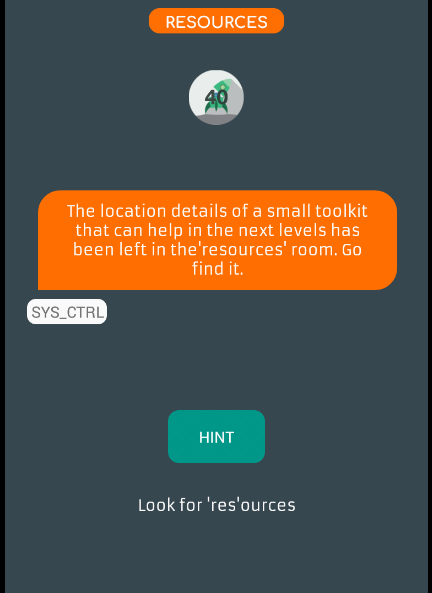
Challenge3:Strings

1. Navigate to the challenge page ow 
2. Now Navigate to the path shown in the image it can be observed that the api key has been disclosed

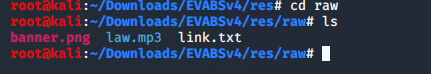


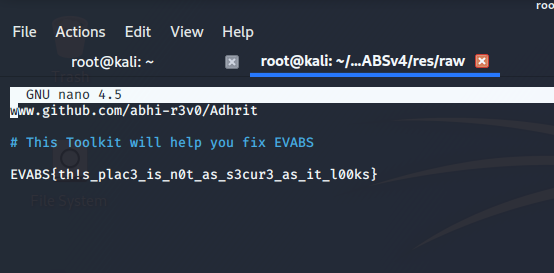
Challenge4: resources

1. Navigate to the challenge



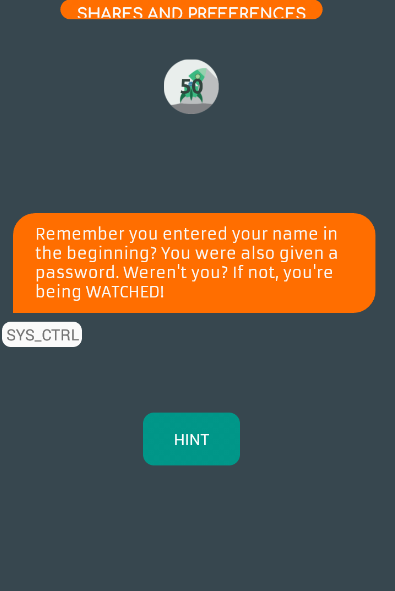
1. Now decompile the application using the apktool and the navigate to the raw folder in the res folder where we can find link.txt file
2. Open it we can observe that out flag is present over there



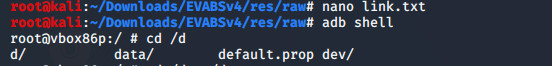


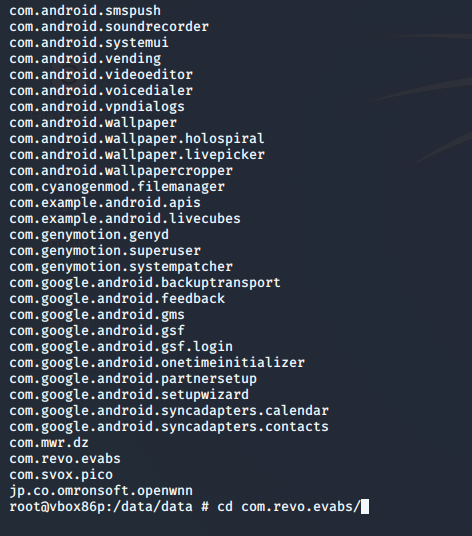
Challenge 5:

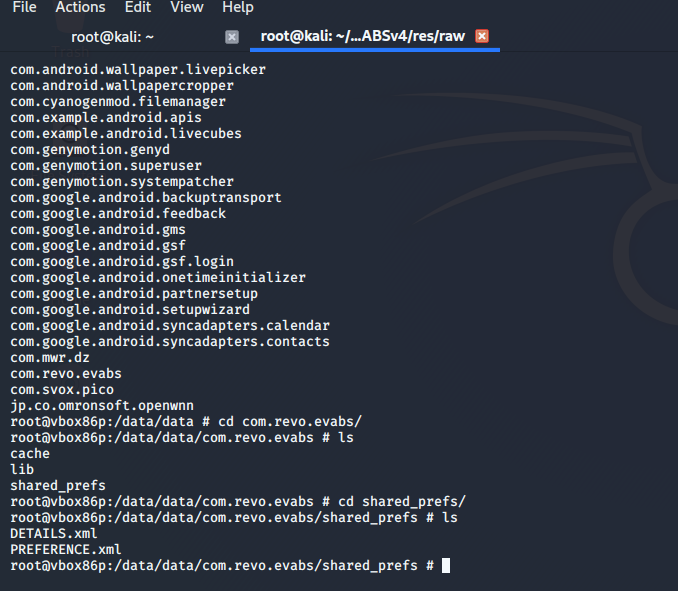
1. Navigate to the challenge



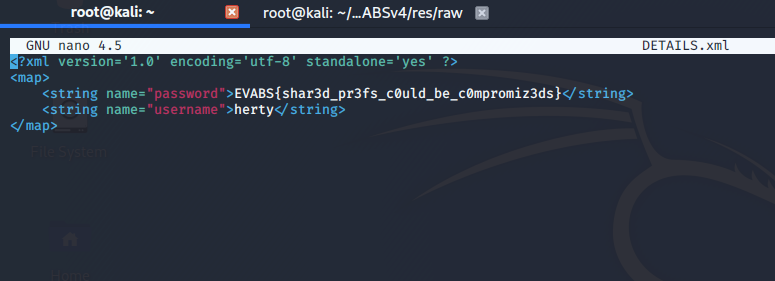
1. Now connect to the emulator using adb and then navigate to the shared prefs In the local storage





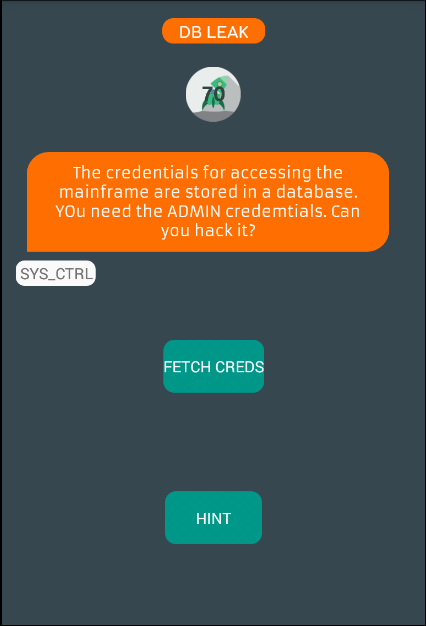


1. Now exit out of adb shell and pull the details folder using adb pull command and open that file it can be observed that the flag is present over there

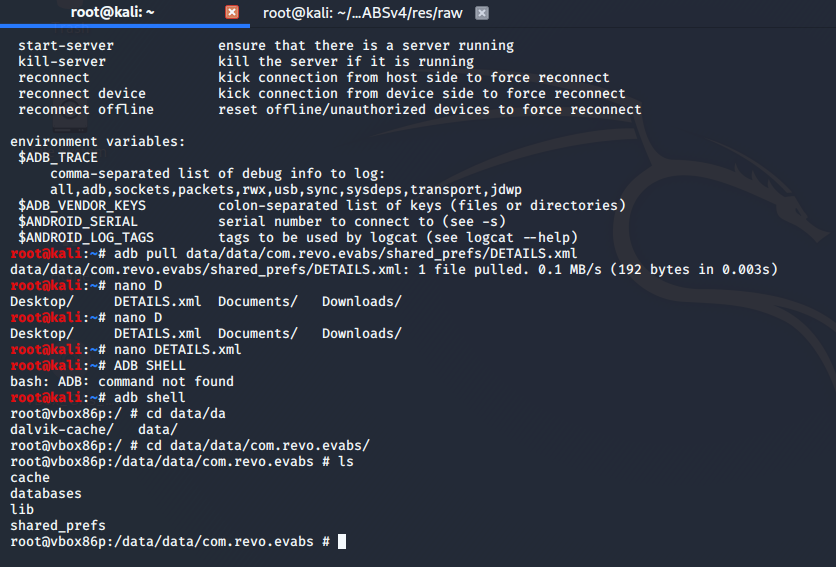


Challenge6:

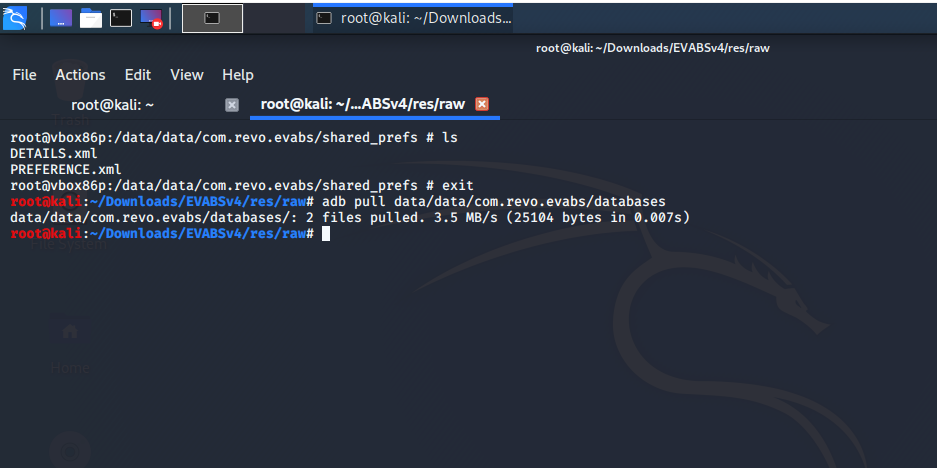
1. Navigate to the challenge



1. Now navigate to the databases folder using adb

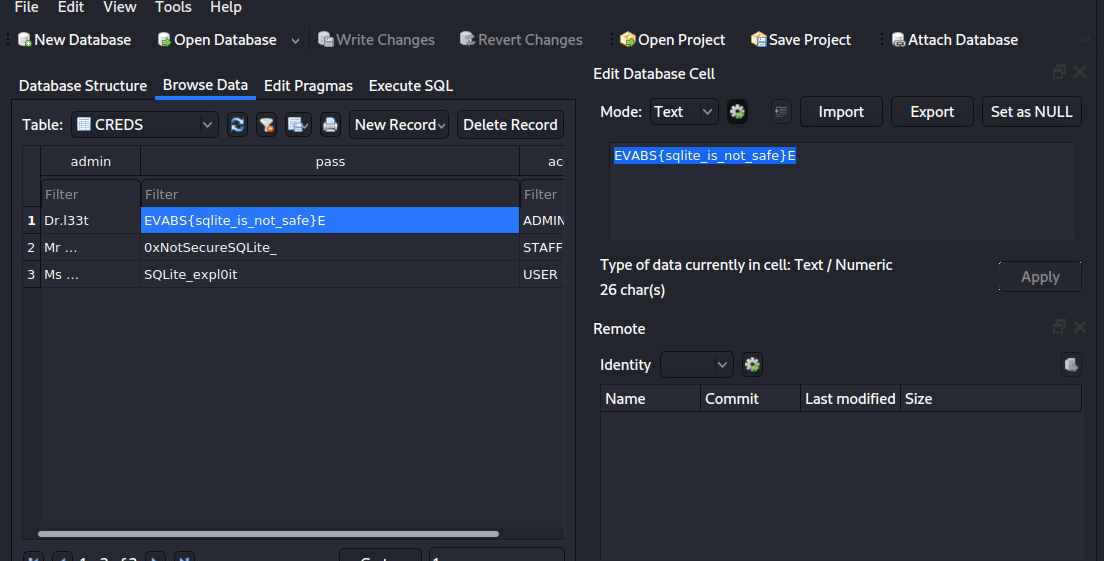


1. Now pull that db using adb pull command



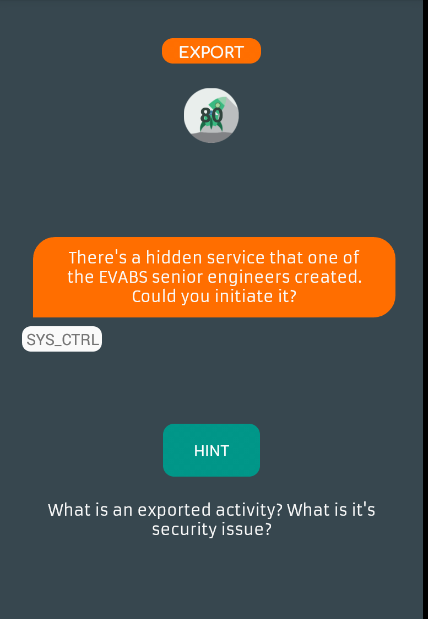
1. Now using the DB browser command open that file we can observe that our flag is present over there

Cmd:sqlitebrowser MAINFRAME\_ACCESS



Challenge 7:

1. Navigate to the challenge page



1. Install drozer apk in mobile and drozer in attacking system now connect to the drozer using the following commands

**Cmd:**adb forward tcp:31415 tcp:31415

Drozer console connect

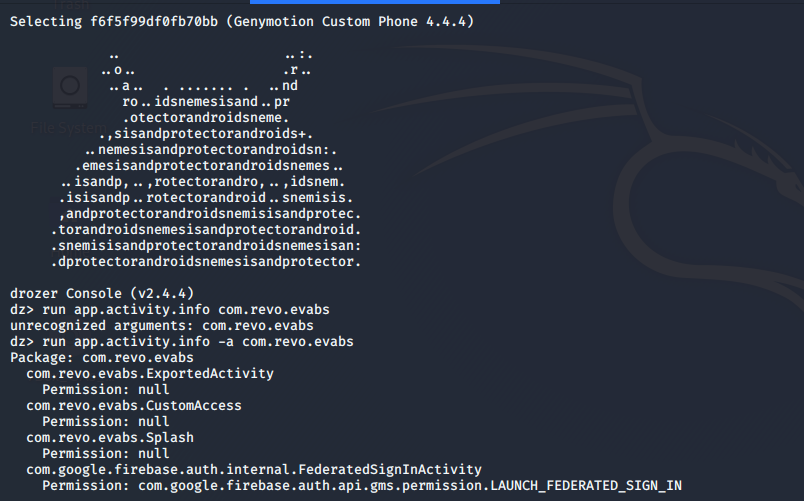
1. Now execute the following commands to get the flag

**Cmd:**run app.package.list

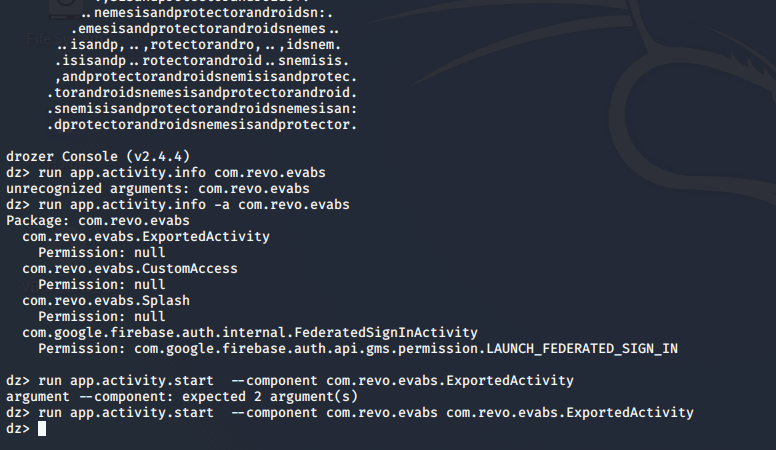
run app.package.info com.revo.evabs

run app.package.attacksurface com.revo.evabs

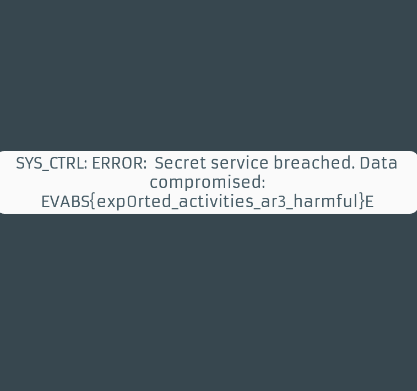
run app.activity.info -a com.revo.evabs



run app.activity.start –component com.revo.evabs com.revo.evabs.ExportedActivity

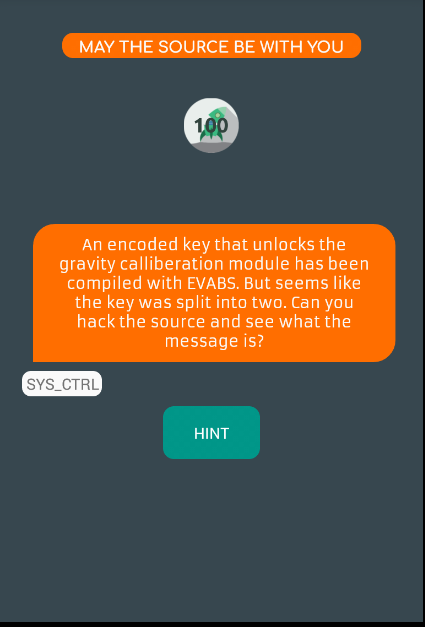


1. It can be observed that the flag is shown



Challenge 8:

1. Navigate to the challenge

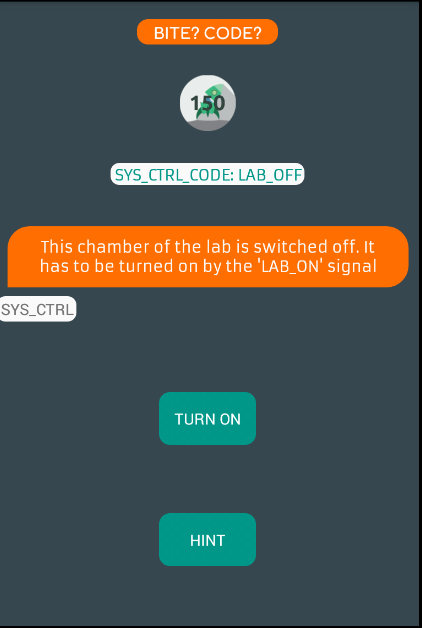


1. Now create a jar file from apk using dex2jar tool and open it using the jd-gui application
2. It can be observed that the code in the base 64 format is the flag so decode it and we can get the flag as

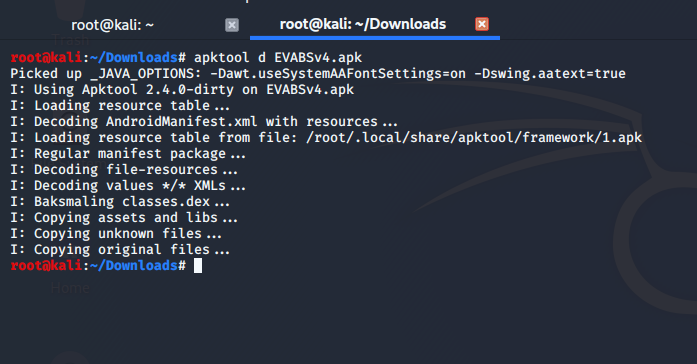
EVABS{nev3r\_st0re-s3ns!tiv3\_data\_1n\_7h3\_s0urcec0de}

Challenge 9:

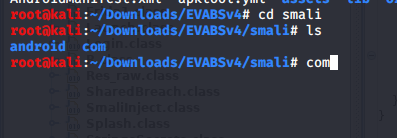
1. Navigate to the Challenge



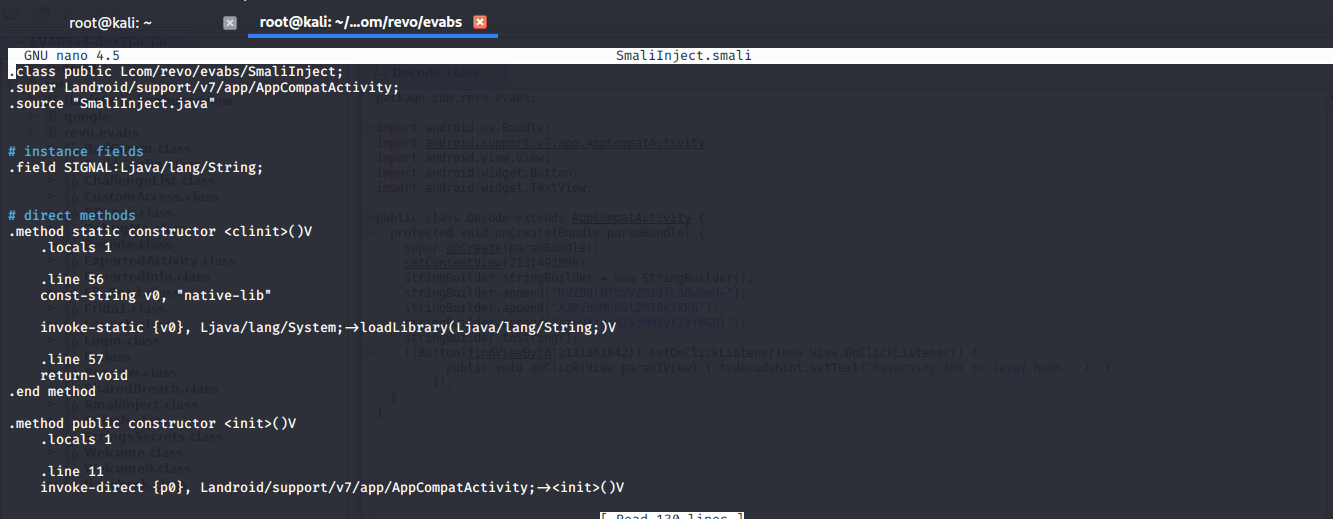
1. Now decompile the application using apktool



1. Navigate to smali folder in t6he decompiled app folder



1. Navigate to evabs folder present in smali and open smaliInject.smali

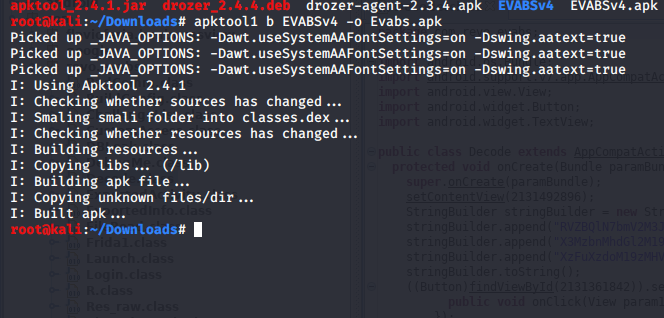


1. In the following line change LAB to ON

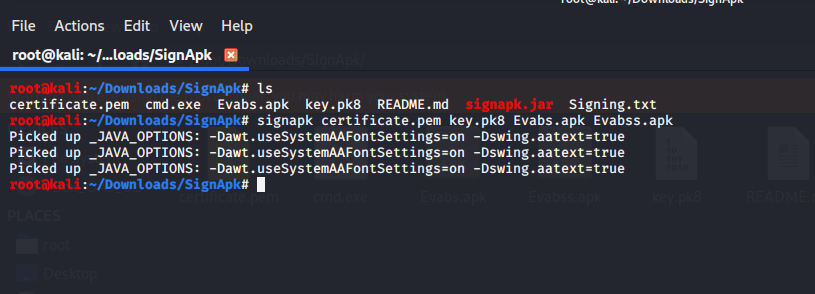


1. Now save the application and recompile it using the same apktool using following command

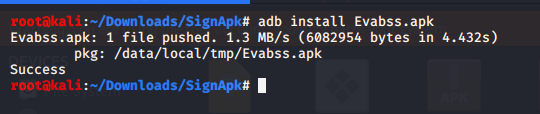
**Cmd:apktool b EVABSV4 -o Evabs.apk**



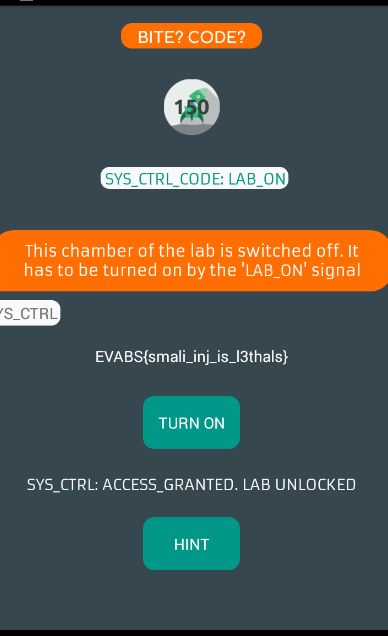
1. Now sign it with apksign tool using the following command



1. Now uninstall the previously installed apk and install Evabss.apk using adb

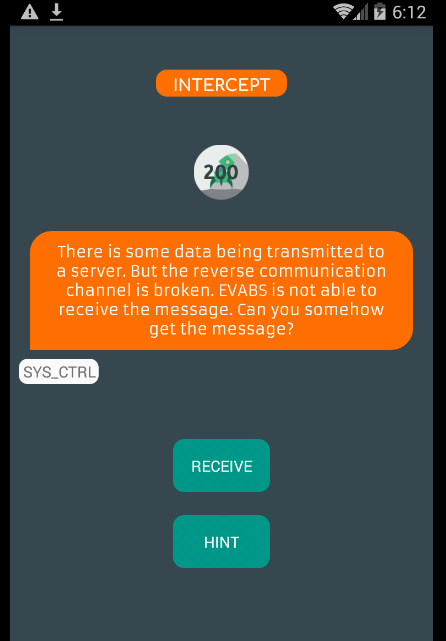


1. Now navigate to the challenge and click on TURN On it can be observed that challenge had been solved

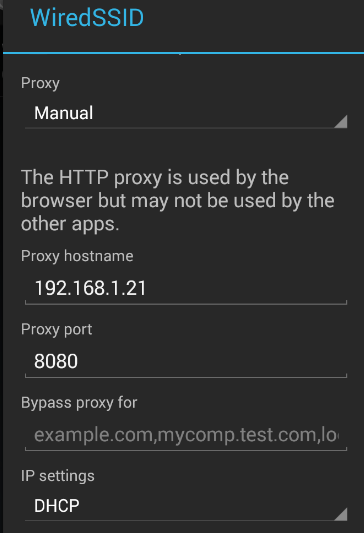


**Challenge 10:**

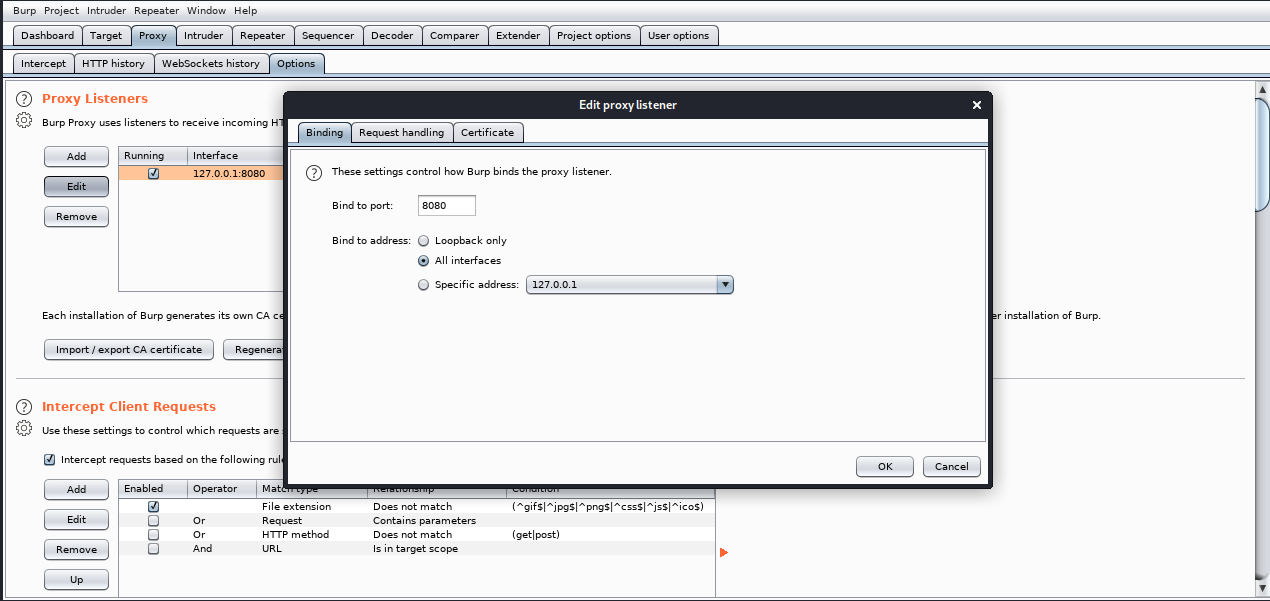
1. Navigate to the challenge



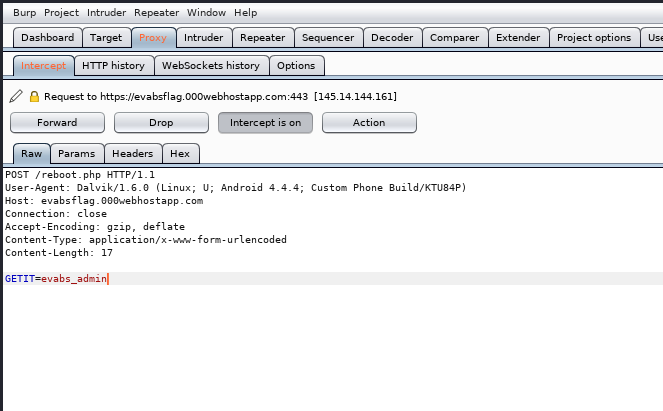
1. Make proxy changes so in the wifi settings so that all the traffic is gone through the burp suite



1. Now open burpsuite and set proxy options to any in the burpsuite



1. Now in the android emulator click on receive and makesure to turn on the intercept in the burpsuite



1. Now click on actions and send it to repeater there click on go It can be observed that the f;lag is in response

