

ABU DHABI POLYTECHNIC

# INFORMATION SECURITY ENGINEERING TECHNOLOGY

OCT- Secure Mobile.App Dev

# DIVA Android App

Prepared By:

Dua’a Abuhamdi

# ACCESS CONTROL ISSUES - Part 1:

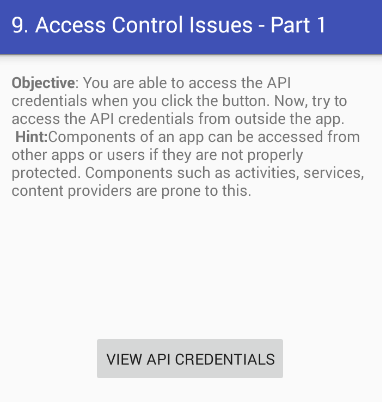


Figure 1.34

Accessing credentials from “View API Credentials” Button is completely legal. There is no issue in it. We need to check that can we directly access credentials without going through this activity or this checkpoint. In order to do that first we have to get the name of activity which will appear after it, for that we take the help of logcat which is discussed earlier.

Run logcat command from android shell then click on “View API Credentials” Button a log will generated related to this which gives us name of next activity as shown in figure 1.35 below:

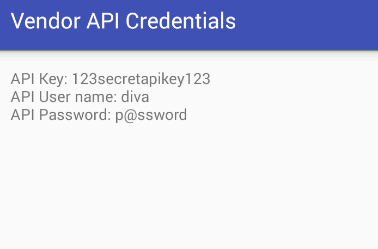


Figure 1.35

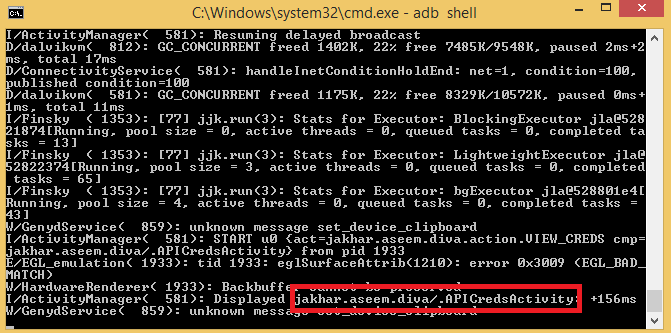


Figure 1.36

As we got the activity name. Now let’s try to access it from adb activity manager directly.

**adb shell am start -n jakhar.aseem.diva/.APICredsActivity**

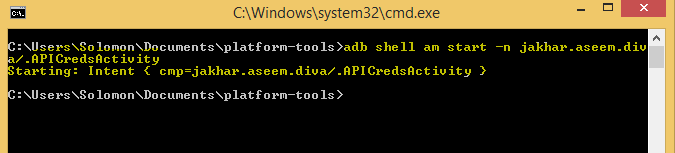


Figure 1.37

As you can see we got access of API Credentials without any restriction or authentication. This also means that other apps can also access these credentials.

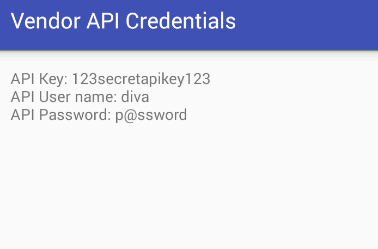


Figure 1.38

Here Access Control Issues - Part 1 challenge is completed.

# ACCESS CONTROL ISSUES - PART 2:

Let’s try to access the credentials with these details we have found and disabling check pin.

**adb shell am start -n jakhar.aseem.diva/.APICreds2Activity -a jakhar.aseem.diva.action.View\_CREDS2 --ez check\_pin false**

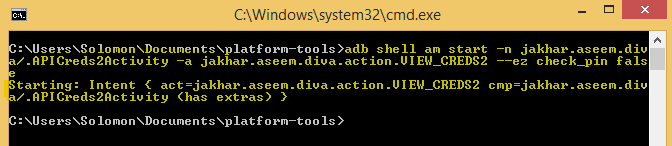


Figure 1.44

Now you will see in your VM Credentials appeared.

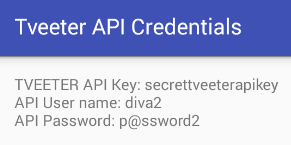


Figure 1.45

Here Access Control Issues - Part 2 challenge is completed.

# ACCESS CONTROL ISSUES - PART 3:

Apparently we cannot access notes without pin. Let’s try to access activity using content provider.

adb shell content query --uri content://jakhar.aseem.diva.provider.notesprovider/notes/

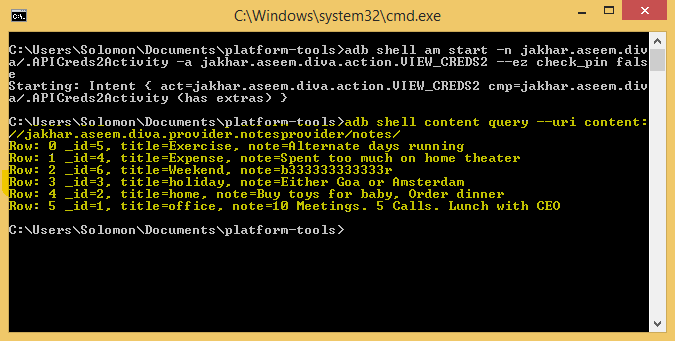


Figure 1.46

Here Access Control Issues - Part 3 challenge is completed.