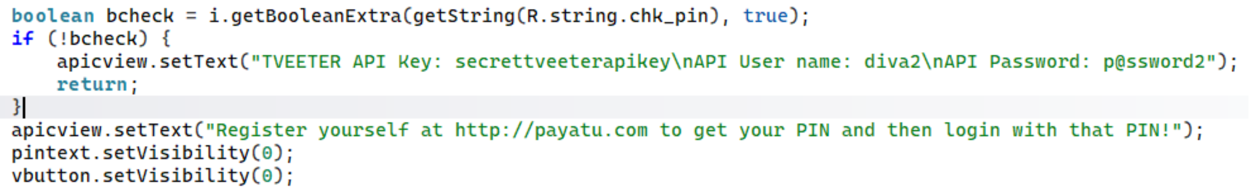
Access Control Issues – Part 2

1. The objective of this lab is to try to access the API credentials from outside the app without knowing the PIN.

2. I get the activity name via this command “**dumpsys window | grep mCurrentFocus**”. Its name is “**AccessControl2Activity**”. In this activity, he targets an action and checks if there any activity can handle this action. If activity exists, he will start the intent, and if not, he will make toast message with the error.

3. From manifest file, I found an activity named “**APICreds2Activity**”. Now, we have two choices. The first one, we can implement an android application with explicit intent directly to the known activity. The second one is to run a command to start this activity via **adb** in cmd and pass the extra boolean data. I will solve it by the second option.

4. This is the vulnerable code. He takes the value that passed from the “**APICreds2Activity**” and check if it is false, he will display the API credentials. If it is true, he will not display it.



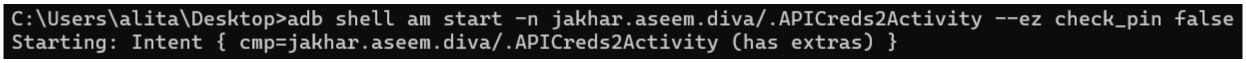
```
boolean bcheck = i.getBooleanExtra(getString(R.string.chk_pin), true);
if (!bcheck) {
    apicview.setText("TVEETER API Key: secrettveeterapikey\nAPI User name: diva2\nAPI Password: p@ssword2");
    return;
}
apicview.setText("Register yourself at http://payatu.com to get your PIN and then login with that PIN!");
pintext.setVisibility(0);
vbutton.setVisibility(0);
```

5. I went back to the terminal and wrote this command to start the activity that contains the API credentials from outside the application. I tried this command, but it didn’t work: **adb shell am start jakhar.aseem.diva/.APICreds2Activity --ez chk_pin false**. The issue was that the **chk_pin** variable is alias for **check_pin**. I know this from **strings.xml**.

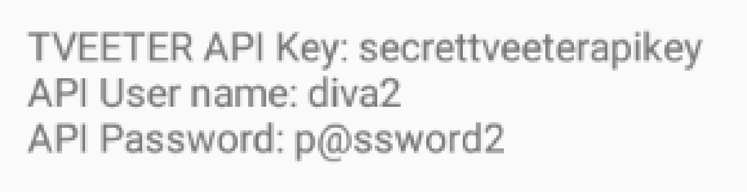
6. I modified the command and sent it again. **adb shell am start jakhar.aseem.diva/.APICreds2Activity --ez check_pin false**

this command starts the **APICreds2Activity** and passes extra boolean variable with name = “**check_pin**” and value = **false.**

7. Finally, I get the API credentials without needing the PIN.



```
C:\Users\alita\Desktop>adb shell am start -n jakhar.aseem.diva/.APICreds2Activity --ez check_pin false
Starting: Intent { cmp=jakhar.aseem.diva/.APICreds2Activity (has extras) }
```



TVEETER API Key: secrettveeterapikey
API User name: diva2
API Password: p@ssword2