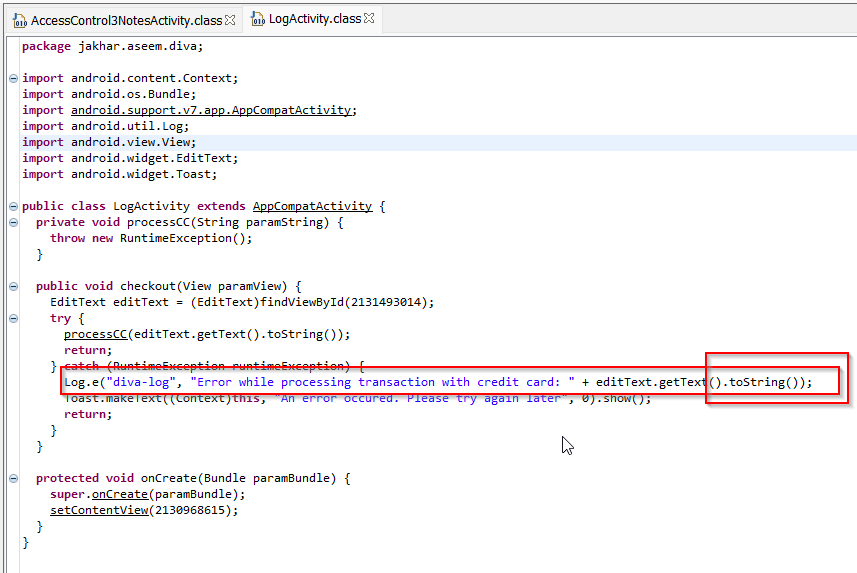
**Application Name: Diva.apk**

**1.INSECURE LOGGING**

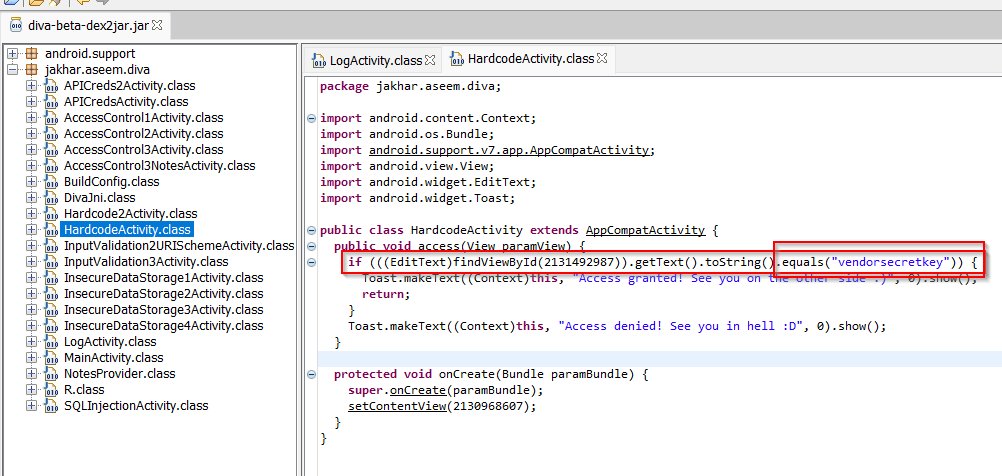
Log.e is used with string datatype. All data can be visible in logcat in plain text, data is not encrypted and anyone can see credential in logcat



**HARDCODING ISSURES PART-1**

HardcodeActivity.class

To access user, have to enter vendor key. This key hardcoded in class anyone can use this key to access application



**INSECURE DATA STORAGE PART-1**

InsecureDataStorage1Activity.class

User have to save their username and password in application. As application is using Sharedpreferences in string data type. the user will not have to fill in details again and again. as data is stored in plan text anyone can view it



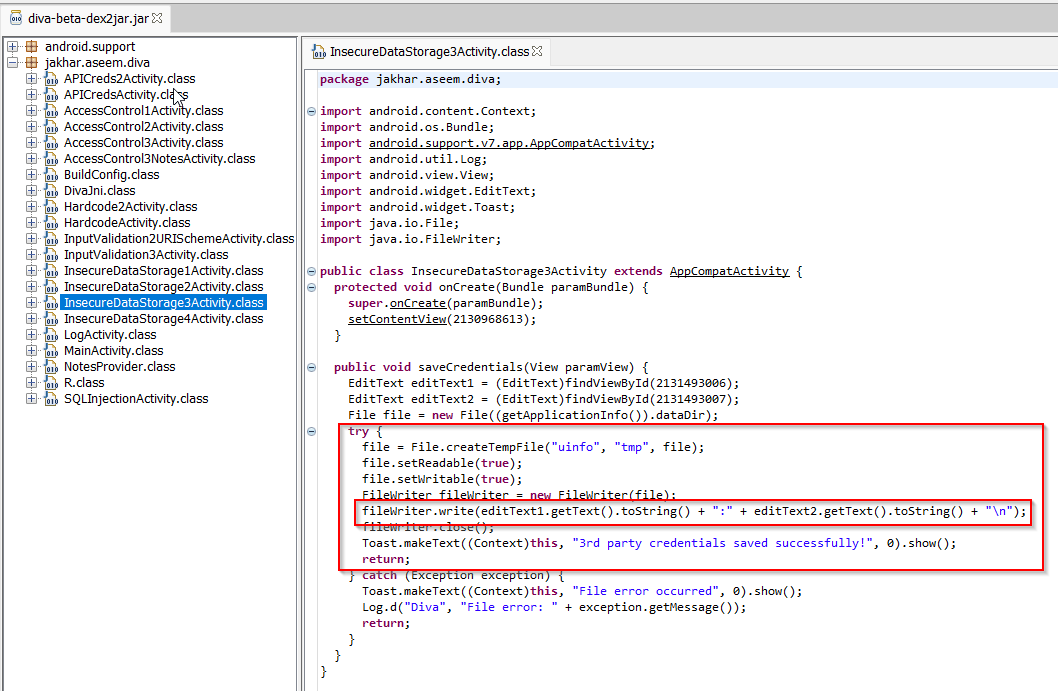
**INSECURE DATA STORAGE PART-2**

User have to save their username and password in application. As application is using Sharedpreferences in string data type. As codes Username and Passwords are stored in database “ids2”. anyone can access database



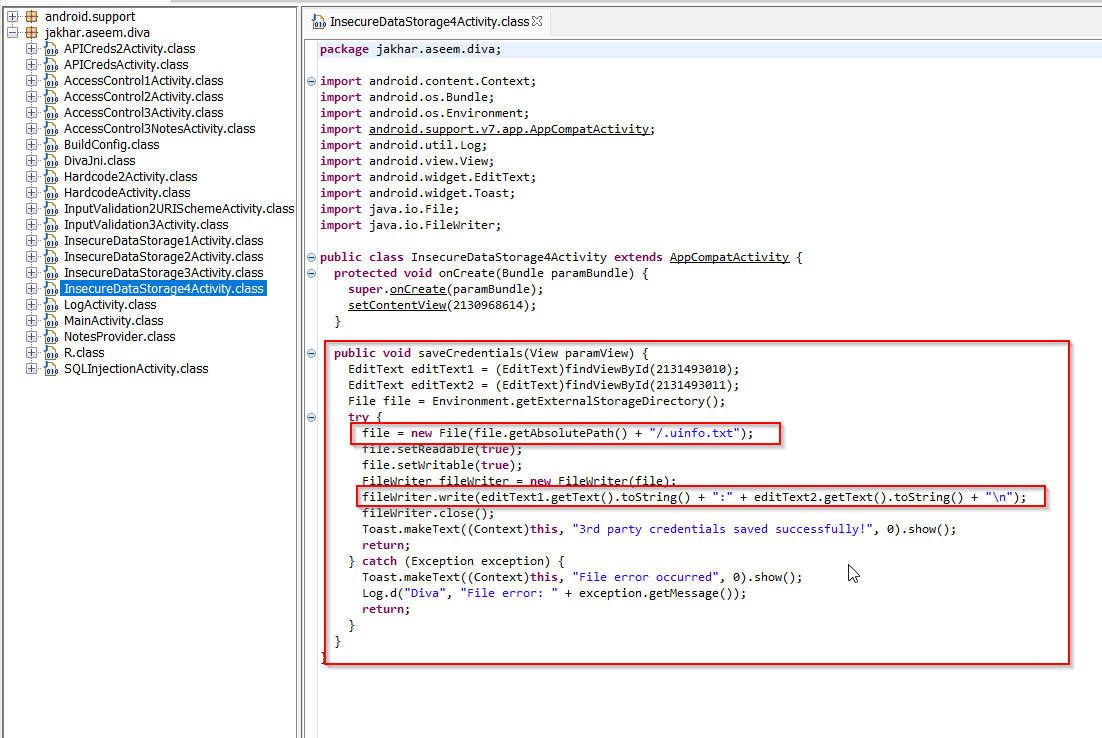
INSECURE DATA STORAGE PART-3

User have to save their username and password in application. As application is using Sharedpreferences in string data type. As codes Username and Passwords are stored in **tmp** file named as **uinfo**.

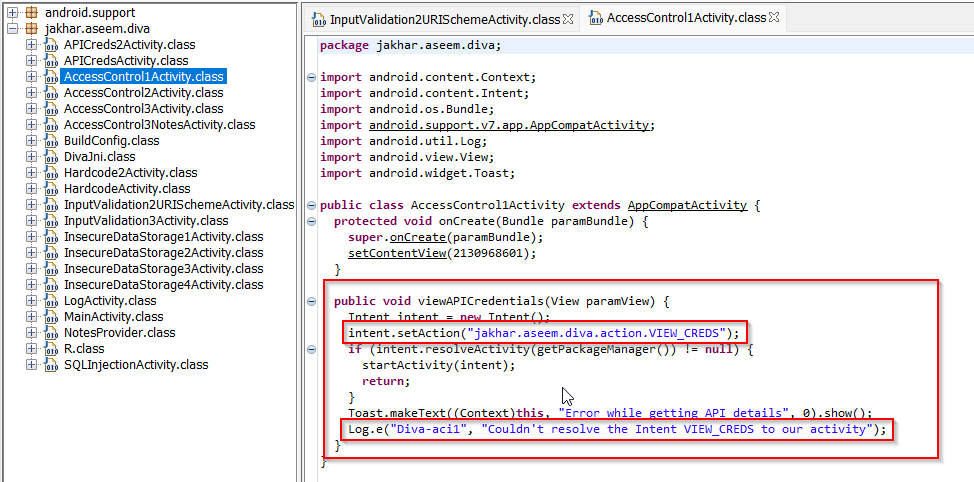


**INSECURE DATA STORAGE PART-4**

User have to save their username and password in application. As application is using Sharedpreferences in string data type. As codes Username and Passwords are stored in **/.uinfo.txt** directory its under root directory . All the credential are stored in plaintext.



**ACCESS CONTROL ISSUES PART-1**



**ACCESS CONTROL ISSUES PART-2**

