MIS 4203 - Independent Studies

Network Traffic Analysis

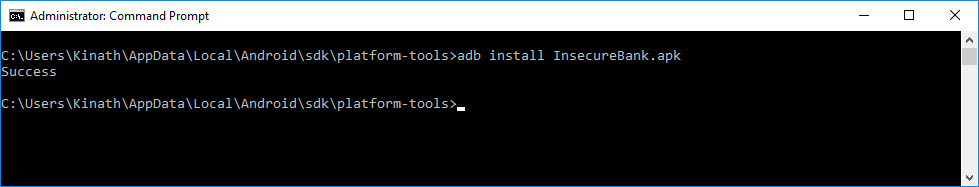
R.A.D.K.Rupasinghe

2016MIS022

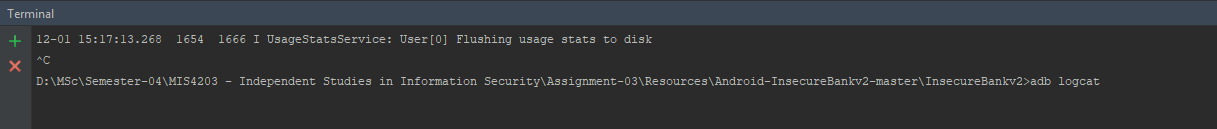
2018

**Insecure Logging**

Install the application.



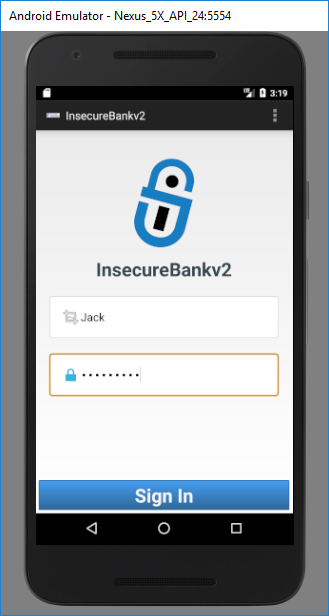
Monitor the application log with logcat.



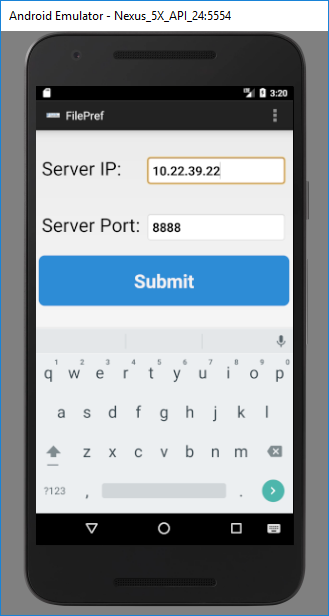
Run the application



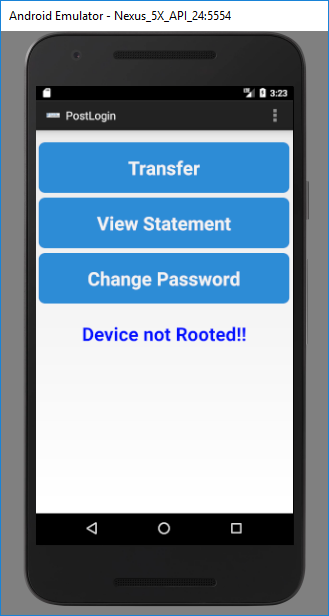
Enter the user credentials and log in to the application.



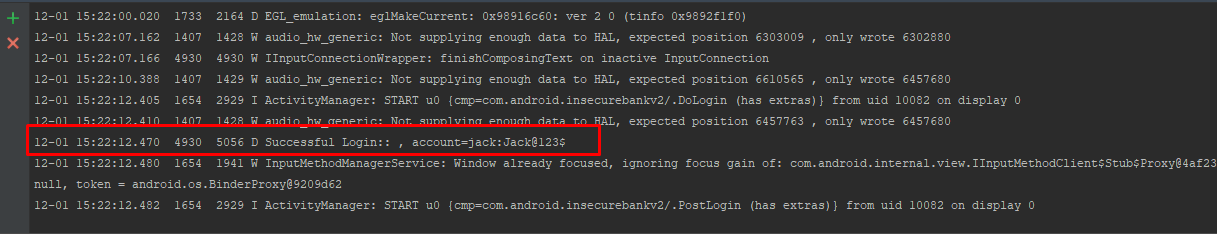
Enter the server the information.



Sign in to the application



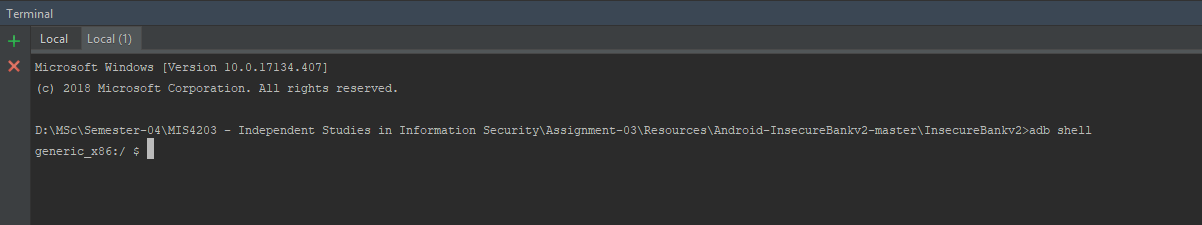
Analyzing the log will show that the user credentials are in plain text in the application log.



Therefore application logging is not secure.

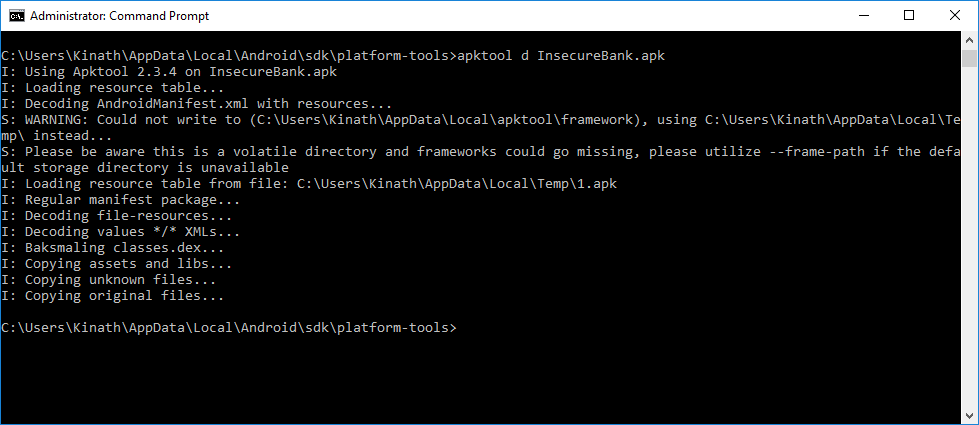
**Weak Encryption Used**

Open the ADB shell

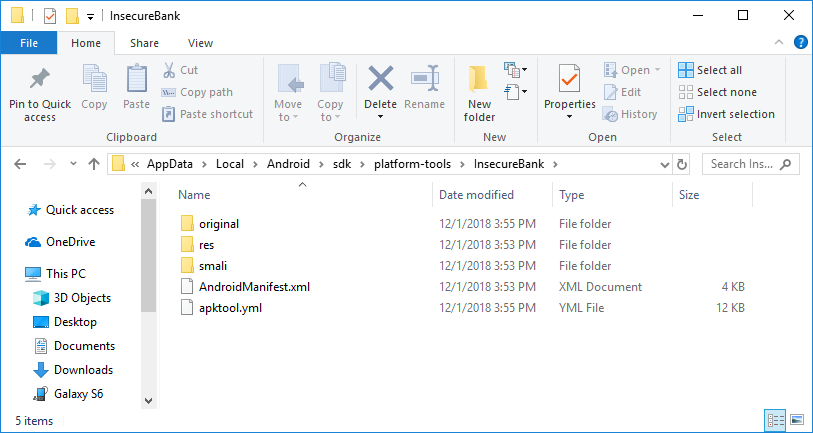


**Exploit Broadcast Receivers/Weak change password implementation**

Decompile the APK with apktool.



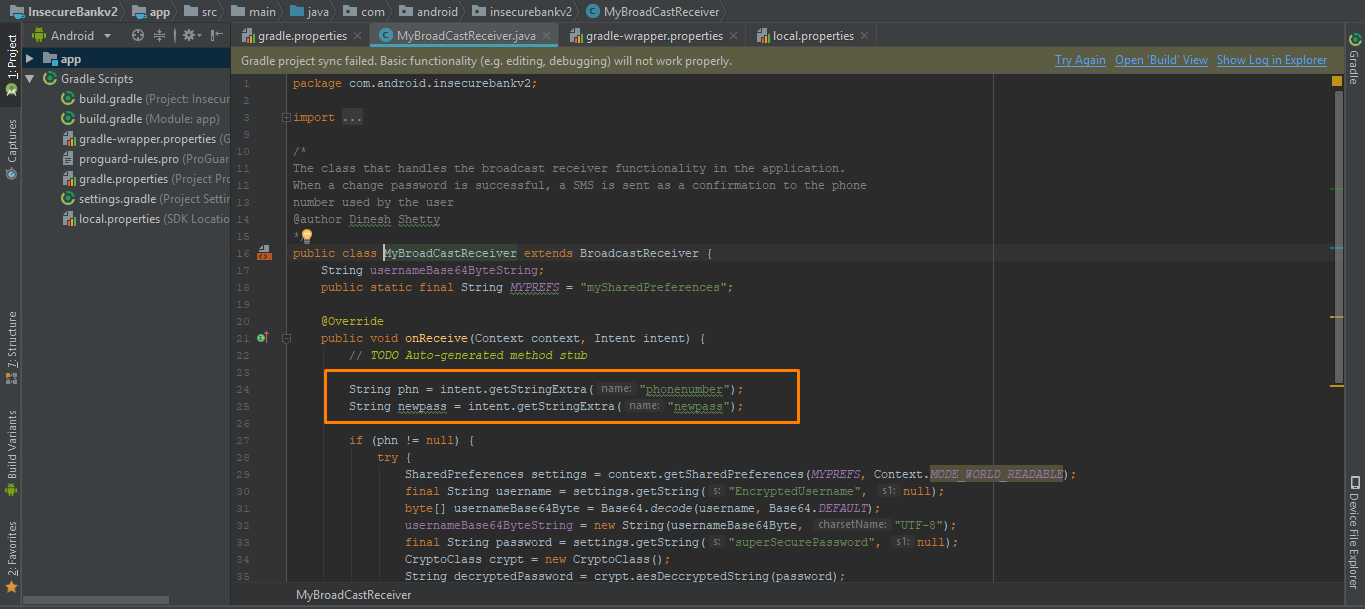
Locate the decompiled application.



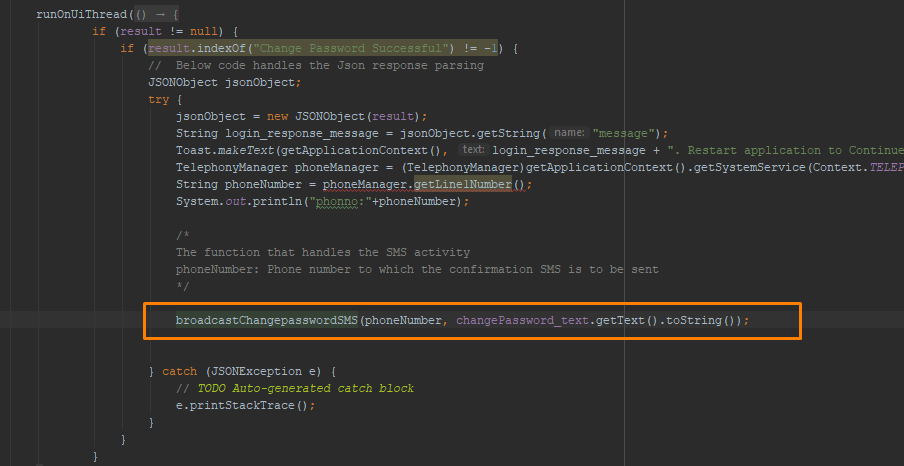
Then we can analyze the AndroidManifest.xml here. Highlighted area shows the Broadcast Receiver.



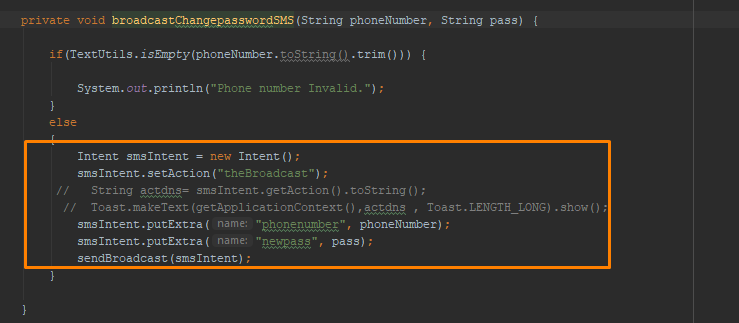
As we have the source code we can identify the class and it’s description.



Analyzing the code shows that the broadcast message is received on changing the password. When the user has forgotten the password it sends the username with the change password as a text.

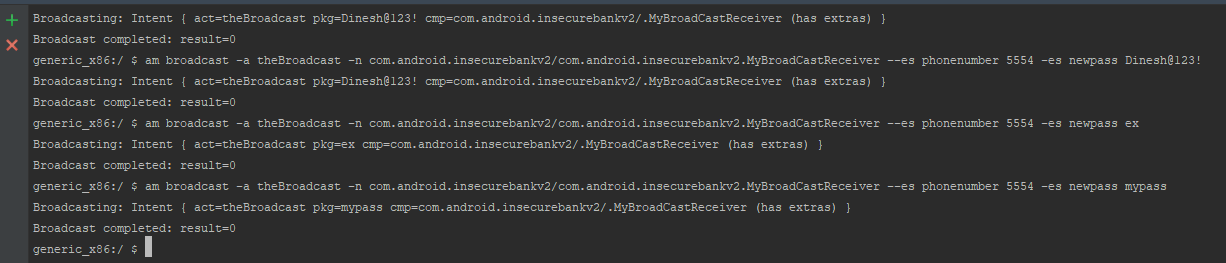


It does not encrypt it.



Reference: <https://stackoverflow.com/questions/22634446/sending-intent-to-broadcastreceiver-from-adb>

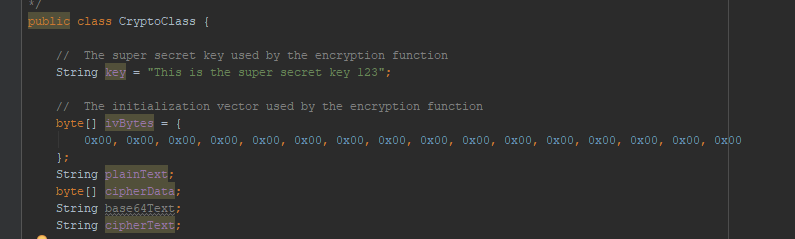
Let’s try to send a message to broadcast receiver.



According to the code, user should receive a message with the new password.

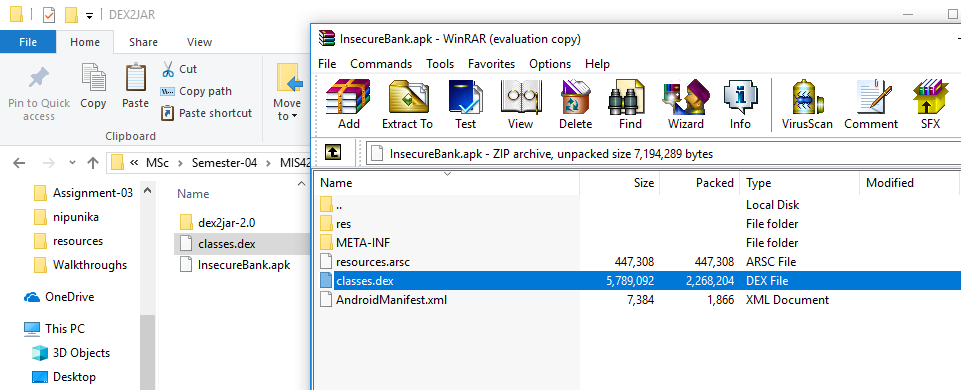
**Weak Cryptography Implementation/** **Hardcoded secrets**

Through the code it can be seen that there is class named CryptoClass which contains the key as a hardcoded one.

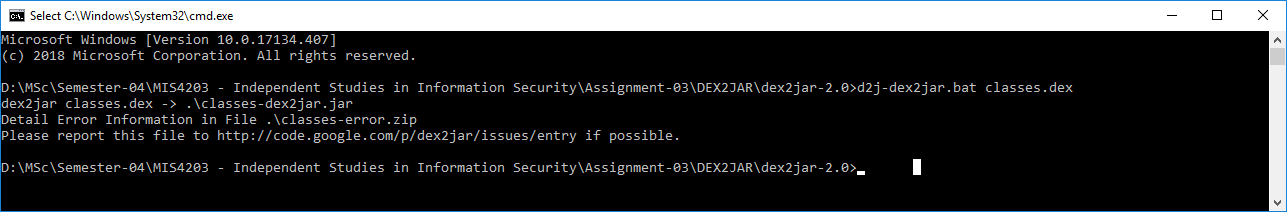


We might see this in the decompiled application too.

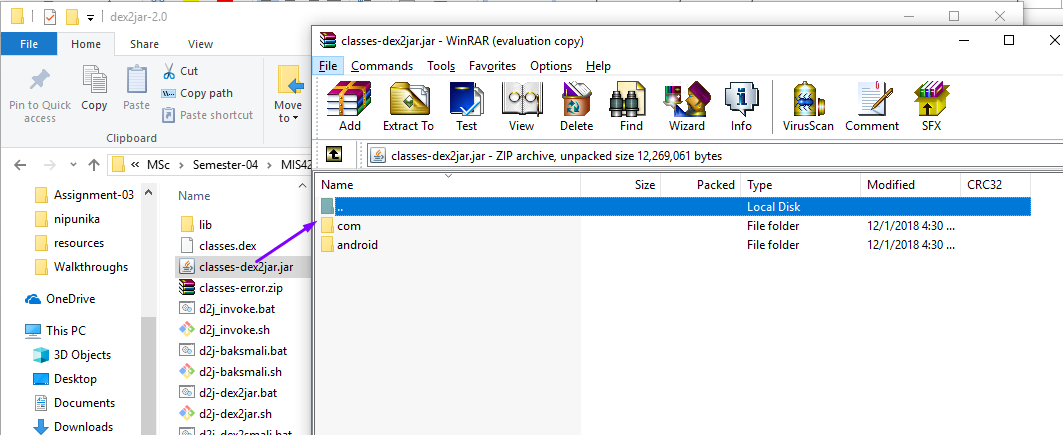
Let’s unzip the APK file and get the dex files.



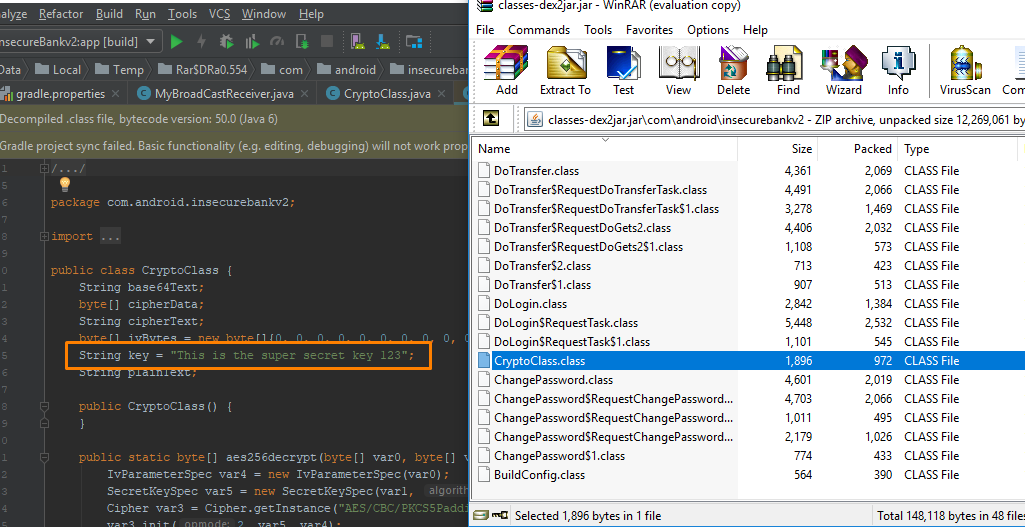
Convert the dex file into a jar file.



Now it’s possible to open the jar file with WinRar and analyze the classes through IntelliJ De-compiler.



What we have identified through the code can now be seen from the decompiled class itself.



Therefore this is a weak cryptography implementaion scenario.

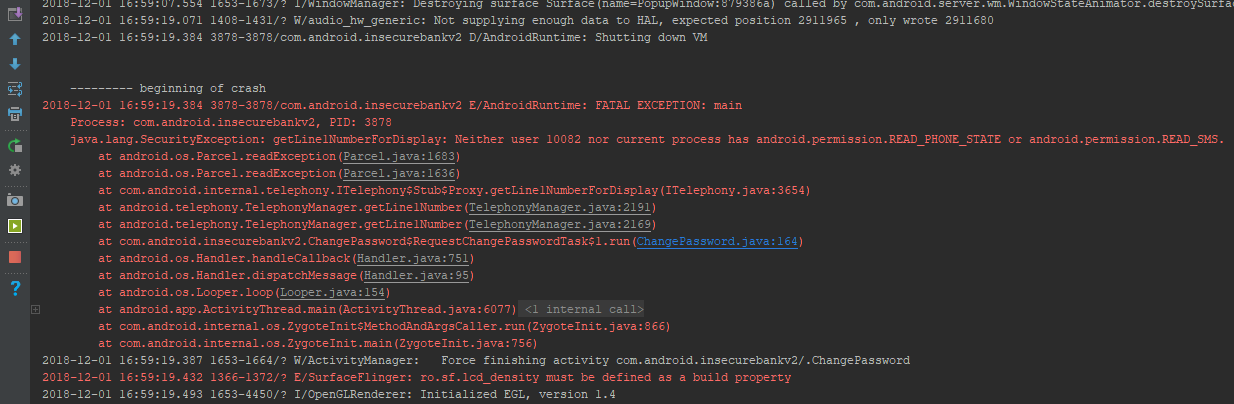
generic\_x86:/ $ am broadcast -a theBroadcast -n com.android.insecurebankv2/com.android.insecurebankv2.MyBroadCastReceiver --es phonenumber 5554 -es newpass mypass

Broadcasting: Intent { act=theBroadcast pkg=mypass cmp=com.android.insecurebankv2/.MyBroadCastReceiver (has extras) }

Broadcast completed: result=0

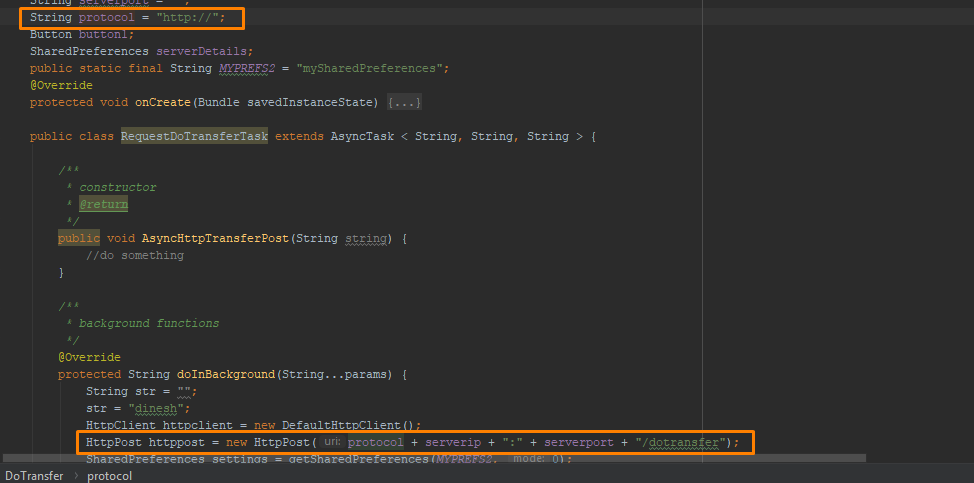
**Observed an Application Crash**

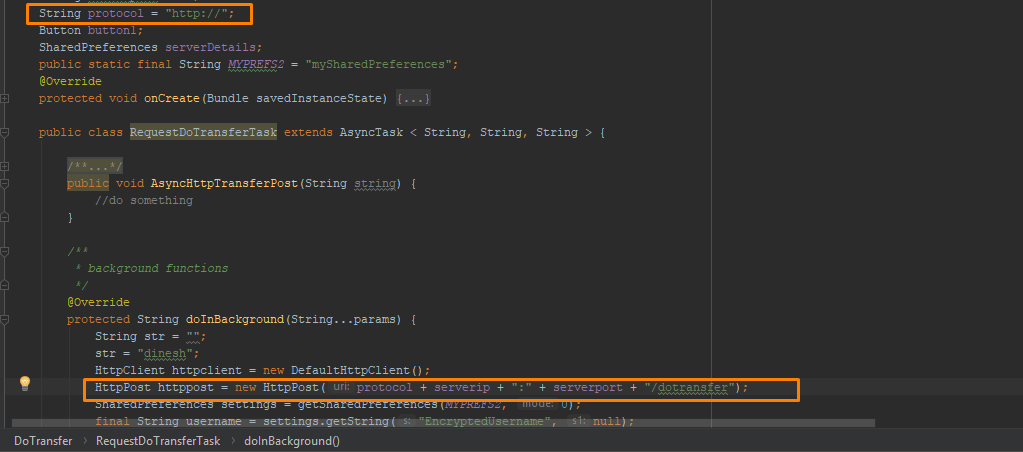
When trying to use the forgotten password functionality it threw an exception.



**Insecure HTTP Connections**

When analyzing the code, it can be seen that all the HTTP requests seen the code are just HTTP requests. Not HTTP requests.





**Login with Hardcoded Passwords**