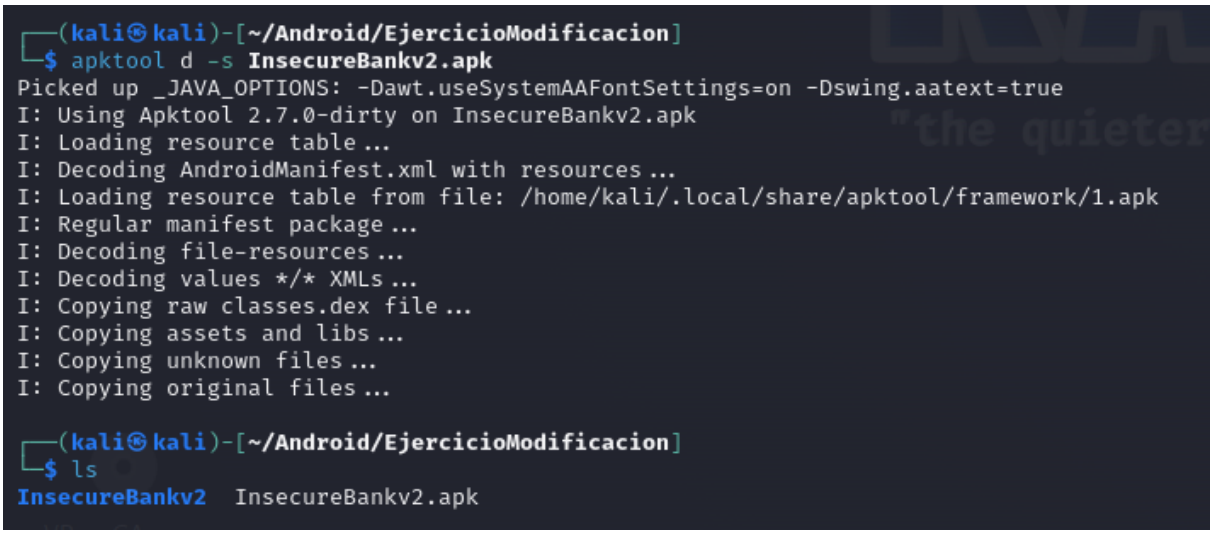
Ejercicio modificación de código

Primero veo el contenido de la apk con apktool

```
sudo apktool d -s InsekureBank
```



dentro del directorio InsecureBank nos ha generado un fichero classes.dex que contiene el codigo de la apk, debemos pasarlo a .jar para poder ver su contenido con el siguiente comando:

```
sudo enjarify classes.dex -o classes.jar
```

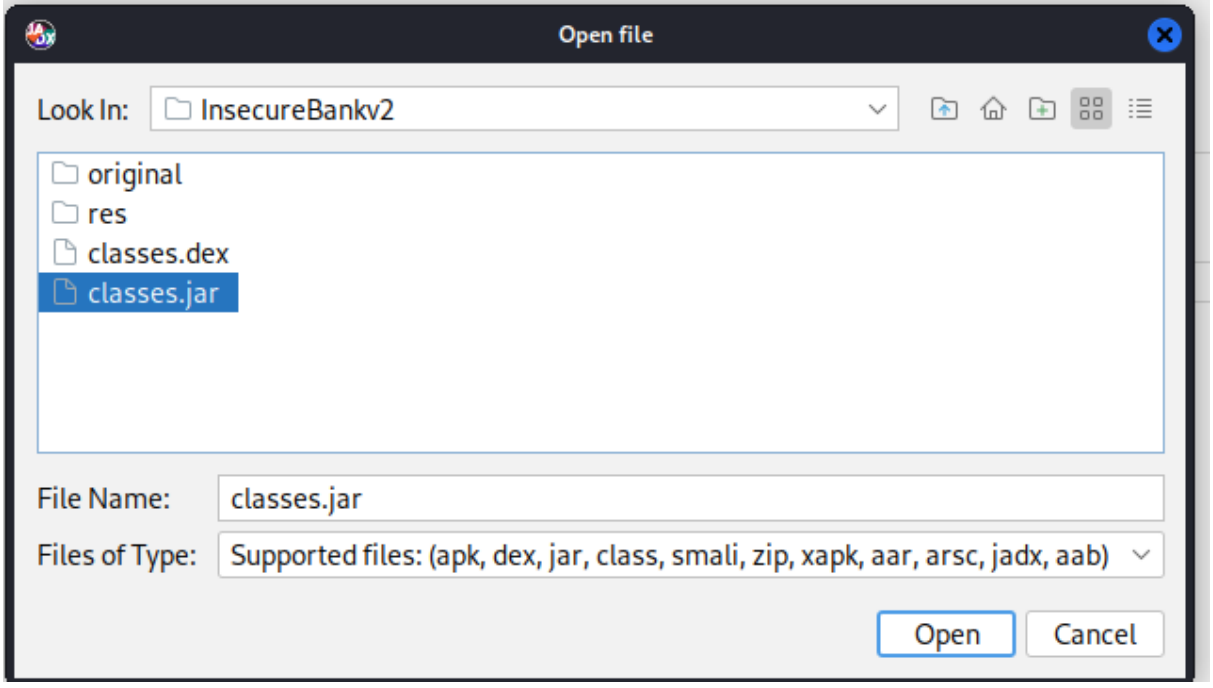
```
┌──(kali㉿kali)-[~/Android/EjercicioModificacion/InsecureBankv2]
└─$ sudo enjarify classes.dex -o classes.jar
[sudo] password for kali:
Using python3 as Python interpreter
1000 classes processed
2000 classes processed
3000 classes processed
4000 classes processed
5000 classes processed
6000 classes processed
Output written to classes.jar
6529 classes translated successfully, 0 classes had errors

┌──(kali㉿kali)-[~/Android/EjercicioModificacion/InsecureBankv2]
└─$ ls
AndroidManifest.xml  apktool.yml  classes.dex  classes.jar  original  res
```

Con la herramienta jadx-gui podemos ver el codigo del fichero classes.jar.

```
sudo jadx-gui
```

selecciono el fichero .jar



Al analizar la clase LoginActivity, en el método onCreate me fijo en la condicion del if el cual si el string que recoge es “no” no muestra un boton llamado createUser, lo que nos hace pensar que si pones el string “yes” puede hacer que sea visible.

```
@Override // android.app.Activity
protected void onCreate(Bundle bundle) {
    super.onCreate(bundle);
    setContentView(R.layout.activity_log_main);
    if (getResources().getString(R.string.is_admin).equals("no")) {
        findViewById(R.id.button_CreateUser).setVisibility(8);
    }
```

Para modificar esta cadena abro el fichero strings.xml situado en el siguiente directorio

```
/InsecureBankv2/res/values
```

cambio el valor del string is_admin de “no” a “yes”

```
<string name="is_admin">yes</string>
<string name="loginscreen_password">Pas
```

Empaqueto la apk modificada, pero primero hago una copia

```
┌──(kali㉿kali)-[~/Android/EjercicioModificacion]
└─$ cp -r InsecureBankv2 InsecureBankv2_mod
```

```
┌──(kali㉿kali)-[~/Android/EjercicioModificacion]
└─$ apktool b InsecureBankv2_mod
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty
I: Copying InsecureBankv2_mod classes.dex file ...
I: Checking whether resources has changed ...
I: Building resources ...
W: aapt: brut.common.BrutException: brut.common.BrutException: Could not extract resource: /prebuilt/linux/aapt_64 (defaulting to $PATH binary)
I: Building apk file ...
I: Copying unknown files/dir ...
I: Built apk into: InsecureBankv2_mod/dist/InsecureBankv2.apk
```

firmo la apk modificada con:

sudo java -jar /home/kali/Android/Software/AplicacionesMóviles/Uber-APK-Signer/uber-apk-signer-1.1.0.jar -a dist -out InsecureBankv2Modified.apk

```
┌──(kali㉿kali)-[~/Android/EjercicioModificacion/InsecureBankv2_mod]
└─$ sudo java -jar /home/kali/Android/Software/AplicacionesMóviles/Uber-APK-Signer/uber-apk-signer-1.1.0.jar -a dist -out InsecureBankv2Modified.apk
source:
        /home/kali/Android/EjercicioModificacion/InsecureBankv2_mod/dist
zipalign location: BUILT_IN
        /tmp/uapksigner-461063923272277058/linux-zipalign-29_0_2157043647867065399 81.tmp
keystore:
        [0] 161a0018 /tmp/temp_2342290406153983836_debug.keystore (DEBUG_EMBEDDED)

01. InsecureBankv2.apk

        SIGN
        file: /home/kali/Android/EjercicioModificacion/InsecureBankv2_mod/dist/InsecureBankv2.apk (3.28 MiB)
        checksum: fb68260bf91e0311cdcb54c42ad9723bca64bf2c791488908492f0b8591bc6c3 (sha256)
        - zipalign success
        - sign success

        VERIFY
        file: /home/kali/Android/EjercicioModificacion/InsecureBankv2_mod/InsecureBankv2Modified.apk/InsecureBankv2-aligned-debugSigned.apk (3.32 MiB)
        checksum: 7d39b70d0183825ccc4ce534f32ae300b759f5f885cc7ba0d9d99d48d86495c6 (sha256)
        - zipalign verified
        - signature verified [v1, v2, v3]
                Subject: CN=Android Debug, OU=Android, O=US, L=US, ST=US, C=US
                SHA256: 1e08a903aef9c3a721510b64ec764d01d3d094eb954161b62544ea8f187b5953 / SHA256withRSA
                Expires: Thu Mar 10 15:10:05 EST 2044

[Mon Jan 15 09:00:26 EST 2024][v1.1.0]
Successfully processed 1 APKs and 0 errors in 0.98 seconds.
```

instalo en el dispositivo y veo que aparece el boton