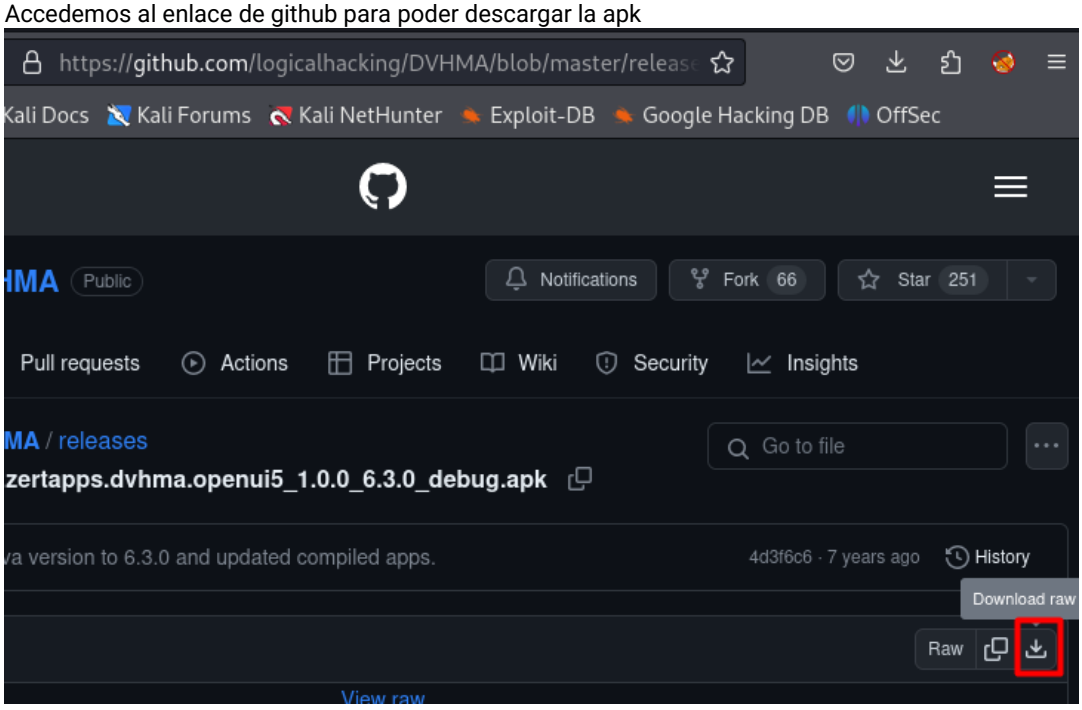
EJERCICIOS MODIFICACIÓN DE CÓDIGO EN APLICACIÓN Prerrequisitos

Android
Kali Linux

Ejercicio - Apktool, Enjarify, Luyten, Jadx-gui, Uber-apk-signer, Adb y Android

- Realizar ingeniería inversa sobre la aplicación InsecureBankv2.apk y modificar el código para poder crear usuarios y passwords en la aplicación. Para ello:
- Utilizar la herramienta jadx-gui para realizar un análisis del código de la aplicación InsecureBankv2.apk
- Analizar la clase LoginActivity, en el método onCreate. ¿Ves alguna comprobación que se haga respecto a la creación de usuarios?
- Cambiar el valor de la clave en el fichero strings.xml de los recursos de la aplicación a "yes".
- Empaquetar y firmar la aplicación.
- Instalar el nuevo .apk en Android y comprobar si está habilitada la opción de crear usuarios.

- Accedemos al enlace de github para poder descargar la apk



- Instalamos apktool

- Convertimos la apk en un fichero que pueda ser modificable

```
┌──(root㉿kali)-[/home/kali/Descargas]
└─# apktool d -s InsecureBankv2.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=tr
ue
I: Using Apktool 2.7.0-dirty on InsecureBankv2.apk
I: Loading resource table ...
I: Decoding AndroidManifest.xml with resources ...
I: Loading resource table from file: /root/.local/share/apktool/framework/1
.apk
I: Regular manifest package ...
I: Decoding file-resources ...
I: Decoding values */* XMLs ...
I: Copying raw classes.dex file ...
I: Copying assets and libs ...
I: Copying unknown files ...
I: Copying original files ...
```

- Accedemos al fichero obtenido

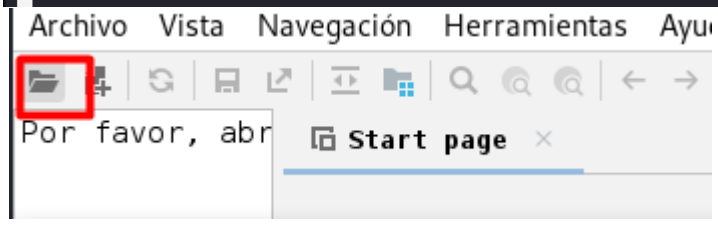
```
┌──(root㉿kali)-[/home/kali/Descargas/InsecureBankv2]
└─# ls
AndroidManifest.xml  apktool.yml  classes.dex  original  res
```

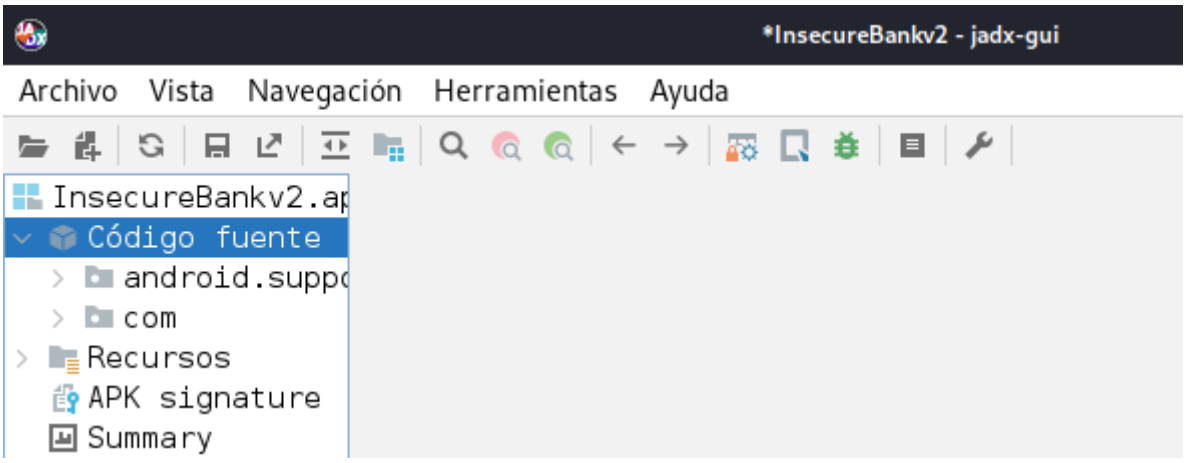
- Convertimos el archivo .dex a JAVA

```
┌──(root㉿kali)-[/home/kali/Descargas/InsecureBankv2]
└─# enjarify classes.dex -o classes.jar
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
```

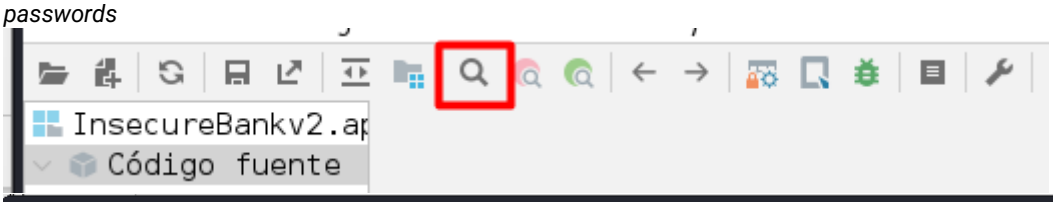
- Abrimos jadx-gui y buscamos la ruta en la que se encuentra InsecureBank

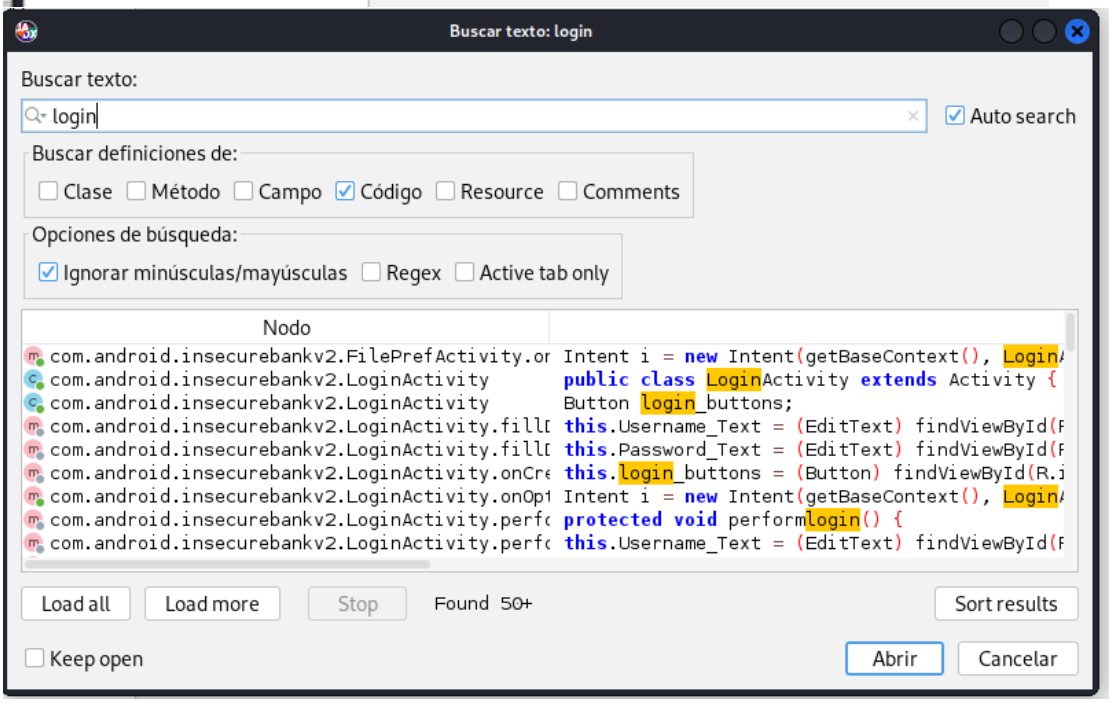
```
┌──(root㉿kali)-[/home/kali/Descargas/InsecureBankv2]
└─# jadx-gui
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=tr
ue
```





- Una vez dentro buscaremos con una palabra clave (*login*) para poder encontrar información de usuarios y *passwords*

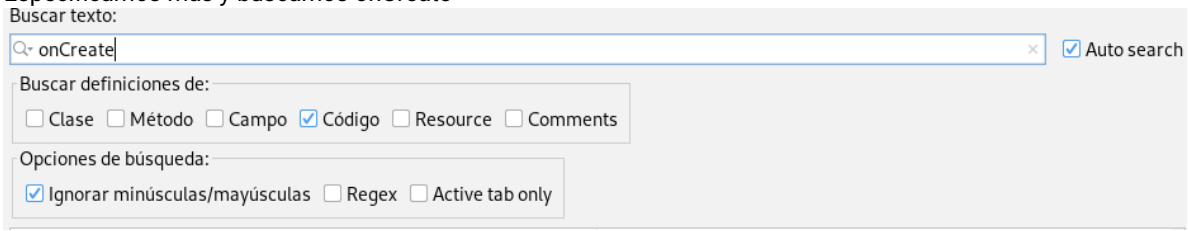




Buscando admin he encontrado lo siguiente; lo que quiere decir esto es que si no eres admin no te deja entrar

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

- Especificamos más y buscamos onCreate



```
com.android.insecurebankv2.LoginActivity.onCreate(Bundle
com.android.insecurebankv2.LoginActivity.onCreate(Bundle
com.android.insecurebankv2.LoginActivity.onCreateOptions
```

```
protected void onCreate(Bundle savedInstanceState) {
super.onCreate(savedInstanceState);
public boolean onCreateOptionsMenu(Menu menu) {
```

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

```
@Override // android.app.Activity
public boolean onCreateOptionsMenu(Menu menu) {
    getMenuInflater().inflate(R.menu.main, menu);
    return true;
}
```

- Para cambiar el archivo strings.xml accedemos al directorio res y con el comando nano cambiamos “no” por “yes”

```
┌──(root㉿kali)-[/home/…/Descargas/InsecureBankv2/res/values]
└─# ls
attrs.xml  colors.xml  drawables.xml  integers.xml  strings.xml
bools.xml  dimens.xml  ids.xml        public.xml    styles.xml
```

- Con ctrl+w buscamos admin y cambiamos el parametro

```
<string name="decline">Decline</string>
<string name="hello_world">Hello world!</string>
<string name="is_admin">yes</string>
```

- Guardamos y estaría perfecto
- Para poder empaquetar y firmar volvemos a aplicar el comando *apktool* pero con el parámetro b para poder crear el directorio dist

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

- Accedemos al directorio creado para poder comprobar que tenemos el directorio dist

```
┌──(root㉿kali)-[/home/kali/Descargas/InsecureBankv2]
└─# ls
AndroidManifest.xml  build       classes.jar  original
apktool.yml          classes.dex  dist         res
```

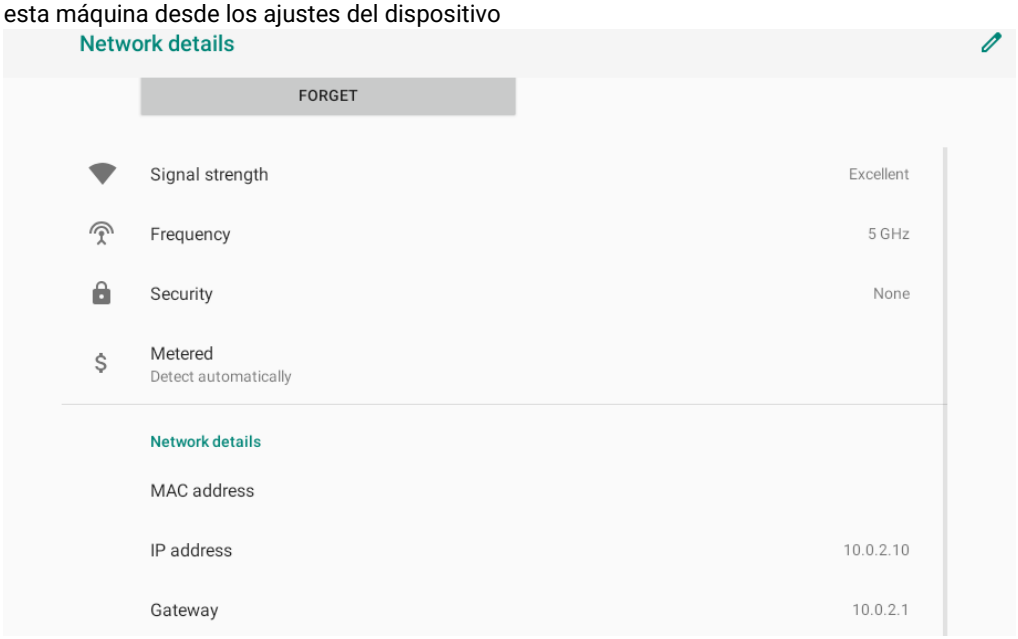
- Una vez confirmado utilizaremos el comando java -jar con una ruta de salida .apk

```
┌──(root㉿kali)-[/home/kali/Descargas/InsecureBankv2]
└─# java -jar ~/Software/AplicacionesMóviles/Uber-APK-Signer/uber-apk-signe
r-1.1.0.jar -a dist --out InsecureBankv2.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=tr
ue
source:
        /home/kali/Descargas/InsecureBankv2/dist
zipalign location: BUILT_IN
        /tmp/uapksigner-16565117338213573023/linux-zipalign-29_0_2146561582
51010309386.tmp
keystore:
        [0] 161a0018 /tmp/temp_11558727856607546087_debug.keystore (DEBUG_E
MBEDDED)

01. InsecureBankv2.apk

        SIGN
        file: /home/kali/Descargas/InsecureBankv2/dist/InsecureBankv2.apk (
3.28 MiB)
        checksum: 6e858f5848f13ffa2db95a9c60488a0c9653dd13a140b747b07488791
be6b999 (sha256)
        - zipalign success
        - sign success

        VERIFY
        file: /home/kali/Descargas/InsecureBankv2/InsecureBankv2.apk/Insecu
reBankv2-aligned-debugSigned.apk (3.32 MiB)
```

- Verificamos que se ha hecho correcto y por tanto entramos en el repositorio para ver el archivo creado

```
┌──(root㉿kali)-[/home/kali/Descargas/InsecureBankv2]
└─# cd InsecureBankv2.apk

┌──(root㉿kali)-[/home/kali/Descargas/InsecureBankv2/InsecureBankv2.apk]
└─# ls
InsecureBankv2-aligned-debugSigned.apk
```

- Para instalar el nuevo paquete accedemos a la ova de Android y en esta misma buscamos cual es la IP de esta máquina desde los ajustes del dispositivo



- Una vez conocemos la IP nos conectamos desde la Kali

```
┌──(root㉿kali)-[/home/kali/Descargas/InsecureBankv2/InsecureBankv2.apk]
└─# adb connect 10.0.2.10:5555
connected to 10.0.2.10:5555
```

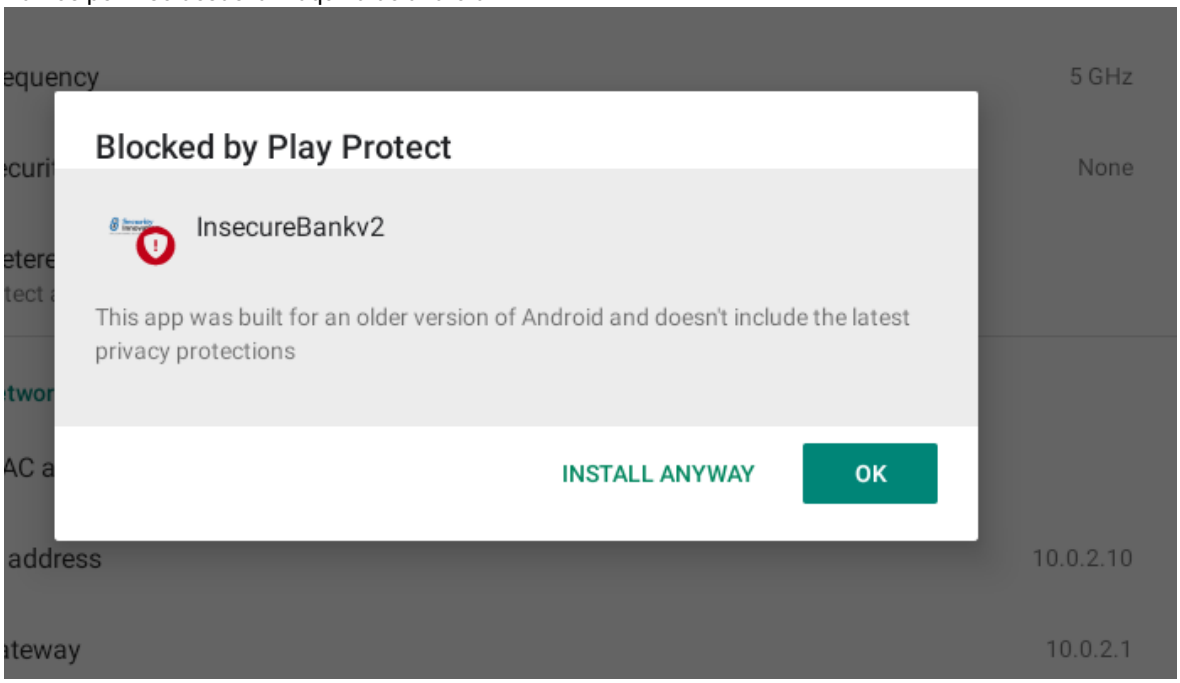
- Para confirmar que estamos conectados ponemos en marcha el siguiente comando

```
┌──(root㉿kali)-[/home/kali/Descargas/InsecureBankv2/InsecureBankv2.apk]
└─# adb shell
x86_64:/ $
```

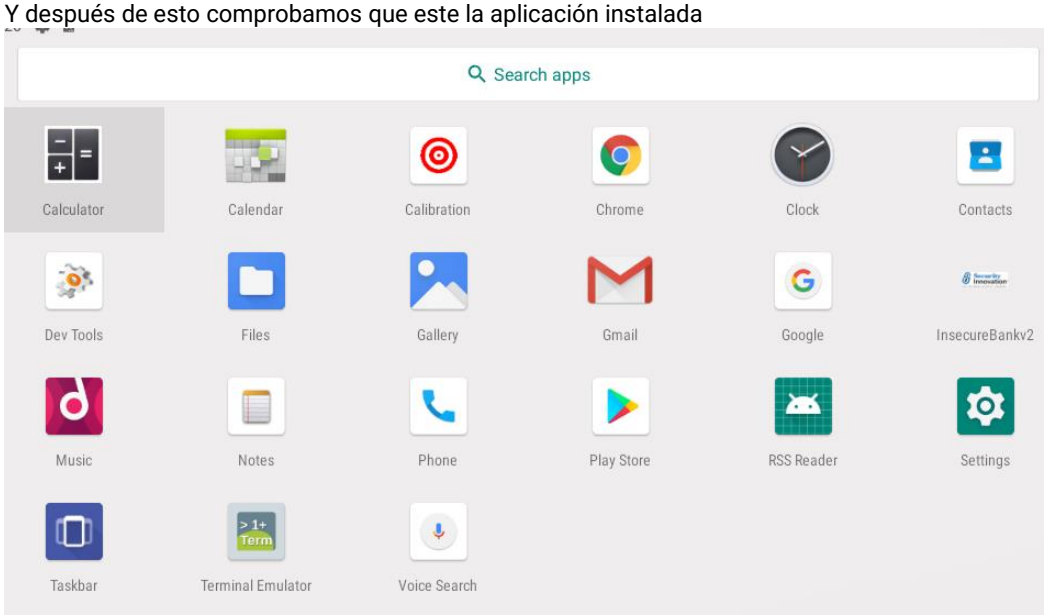
- Una vez comprobado que estamos conectado aplicamos el siguiente comando, donde especificamos la ruta del anterior repositorio creado

```
┌──(root㉿kali)-[/home/kali/Descargas/InsecureBankv2/InsecureBankv2.apk]
└─# adb install /home/kali/Descargas/InsecureBankv2/InsecureBankv2.apk/Inse
cureBankv2-aligned-debugSigned.apk
Performing Streamed Install
```

- Damos permiso desde la máquina de android



- Y después de esto comprobamos que este la aplicación instalada



- Comprobamos que hayamos hecho el ejercicio e ingresamos en la app