

EJERCICIOS MODIFICACION DE APLICACIÓN

PREREQUISITOS

- ANDROID
- KALI LINUX

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

- Realizar un análisis estático sobre la aplicación InsecureBankv2.apk y modificarla para poder crear usuarios y passwords en la aplicación

Android conectado

```
(root@kali)-[~]  
# adb connect 10.0.2.16:5555  
connected to 10.0.2.16:5555  
  
(root@kali)-[~]  
# adb shell  
x86_64:/ $
```

Bajamos la aplicación de insecurebank.apk e inspeccionamos que hay dentro de cada carpeta.

```

(root@kali)-[/home/veronica/Descargas]
# ls
cacert.der
de.zertapps.dvhma.openui5_1.0.0_6.3.0_debug.apk
dvhma
dvhma.apk
InsecureBankv2.apk
'Laptop scan_lzv3r3.pdf'
Metasploitable2_black_7ojrms.pdf
Metasploitable2_black_uznify.pdf

(root@kali)-[/home/veronica/Descargas]
# apktool d -s InsecureBankv2.apk
I: Using Apktool 2.6.1-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 ...

(root@kali)-[/home/veronica/Descargas]
#

```

```

(root@kali)-[/home/veronica/Descargas]
# ls
cacert.der
de.zertapps.dvhma.openui5_1.0.0_6.3.0_debug.apk
dvhma
dvhma.apk
InsecureBankv2.apk
InsecureBankv2
InsecureBankv2.apk

(root@kali)-[/home/veronica/Descargas]
# cd InsecureBankv2

(root@kali)-[/home/veronica/Descargas/InsecureBankv2]
# ls
AndroidManifest.xml  apktool.yml  assets  classes.dex  original  res

(root@kali)-[/home/veronica/Descargas/InsecureBankv2]
#

```

Inspeccionamos el contenido e ingresamos a la carpeta assets y vemos un archivo dns que contiene un script que sirve para la manipulación de contenido validación de forms y cambios dinámicos de contenido.

```
(root@kali)-[/home/veronica/Descargas/InsecureBankv2]
# ls
AndroidManifest.xml  apktool.yml  assets  classes.dex  original  res

(root@kali)-[/home/veronica/Descargas/InsecureBankv2]
# cd assets

(root@kali)-[/home/veronica/Descargas/InsecureBankv2/assets]
# ls
dns.html
```

```
(root@kali)-[/home/veronica/Descargas/InsecureBankv2/assets]
# cat dns.html
abc
<script>alert(1)</script>
```

En la carpeta original hay dos files una manifestación de contenido pero al leer se encuentra encriptada y una carpeta META que contiene distintas certificaciones como Contiene un conjunto de datos que pueden llegar a ser muy útiles cuando intentamos seguir los pasos de un único desarrollador de malware en el marco de una campaña de códigos maliciosos. Para leer la información en él almacenada podemos utilizar la herramienta keytool de JRE con la siguiente línea de comando, otra CERT.SF que es el file de firma y el manifest es un archivo específico contenido en un archivo Jar. Se usa para definir datos relativos a la extensión y al paquete

```
(root@kali)-[/home/veronica/Descargas/InsecureBankv2/original]
# ls
AndroidManifest.xml  META-INF

(root@kali)-[/home/veronica/Descargas/InsecureBankv2/original]
# nano AndroidManifest.xml

(root@kali)-[/home/veronica/Descargas/InsecureBankv2/original]
# cd META-INF

(root@kali)-[/home/veronica/Descargas/InsecureBankv2/original/META-INF]
# ls
CERT.RSA  CERT.SF  MANIFEST.MF

(root@kali)-[/home/veronica/Descargas/InsecureBankv2/original/META-INF]
#
```

En res se puede ver el contenido de la app en su totalidad, como esta contruida y estructurada la aplicación, todos los detalles como login, etc.

```
(root@kali)-[/home/veronica/Descargas/InsecureBankv2/res]
# ls
anim drawable-xxhdpi-v4 values-af values-da values-es-rUS values-hi values-iw values-large-v14 values-ms-rMY values-ro values-sw values-v11 values-w600dp-v13 values-z
color drawable-xxhdpi-v4 values-am values-de values-et-rEE values-hr values-ja values-large-v4 values-nb values-ru values-sw600dp-v13 values-v14 values-w720dp-v13 values-z
drawable drawable-xxhdpi-v4 values-ar values-el values-fa values-hu values-ka-rGE values-lo-rLA values-nl values-sk values-th values-vi values-w820dp-v13 values-z
drawable-hdpi-v4 layout-v11 values-bg values-en-rGB values-fi values-hy-rAM values-km-rKH values-lt values-pl values-sl values-tl values-w360dp-v13 values-xlarge-v4
drawable-mdpi-v4 menu values-ca values-en-rIN values-fr values-in values-ko values-lv values-pt values-sr values-tr values-w480dp-v13 values-zh-rCN
drawable-xhdpi-v4 values values-cs values-es values-fr-rCA values-it values-land values-mn-rMN values-pt-rPT values-sv values-uk values-w500dp-v13 values-zh-rHK

(root@kali)-[/home/veronica/Descargas/InsecureBankv2/res]
# cd manu
cd: no existe el fichero o el directorio: manu

(root@kali)-[/home/veronica/Descargas/InsecureBankv2/res]
# cd menu
# ls
do_login.xml file_pref.xml main.xml

(root@kali)-[/home/veronica/Descargas/InsecureBankv2/res/menu]
# cd color
cd: no existe el fichero o el directorio: color

(root@kali)-[/home/veronica/Descargas/InsecureBankv2/res/menu]
# cd ..

(root@kali)-[/home/veronica/Descargas/InsecureBankv2/res]
# cd color
# ls
abc_search_url_text_holo.xml
```

Procedemos a pasar la aplicación a lenguaje java,

```
(root@kali)-[/home/veronica/Descargas/InsecureBankv2]
# enjarify classes.dex -o classes.jar
Using python3 as Python interpreter
Output written to classes.jar
768 classes translated successfully, 0 classes had errors

(root@kali)-[/home/veronica/Descargas/InsecureBankv2]
# ls
AndroidManifest.xml apktool.yml assets classes.dex classes-enjarify.jar classes.jar original res
```

Abrimos la aplicación luyten para la lectura de classes.jar y abrimos el archivo classes.jar

Podemos ver que debug esta en true por lo que podemos realizar modificaciones a la aplicación.

```
AccessibilityServiceInfoCompatIcs.class x TransportMediatorJ
1 package com.android.insecurebankv2;
2
3 public final class BuildConfig
4 {
5     public static final boolean DEBUG = true;
6 }
7
```

Vemos el password pattern

```
import androidx.appcompat.app.AppCompatActivity;
import android.os.Bundle;
import android.view.View;
import android.widget.Button;
import android.widget.EditText;
import android.widget.Toast;

public class ChangePassword extends AppCompatActivity {

    private static final String PASSWORD_PATTERN = "((?=.*\\d)(?=.*[a-z])(?=.*[A-Z])(?=.*[@#$%]).{6,20})";
    Button changePassword_button;
    EditText changePassword_text;
    private Matcher matcher;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_change_password);
        changePassword_button = findViewById(R.id.change_password_button);
        changePassword_text = findViewById(R.id.change_password_text);
        matcher = Pattern.compile(PASSWORD_PATTERN);
    }

    public void changePassword(View view) {
        String password = changePassword_text.getText().toString();
        if (matcher.matches(password)) {
            Toast.makeText(this, "Password is valid", Toast.LENGTH_SHORT).show();
        } else {
            Toast.makeText(this, "Password is not valid", Toast.LENGTH_SHORT).show();
        }
    }
}
```

Informacion sobre el encriptado.

```
public class CryptoClass
{
    String base64Text;
    byte[] cipherData;
    String cipherText;
    byte[] ivBytes;
    String key;
    String plainText;

    public CryptoClass() {
        this.key = "This is the super secret key 123";
        this.ivBytes = new byte[16];
    }
}
```

Y muchas otras informaciones que pueden ser relevantes.

- Utilizar la herramienta jadx-gui para realizar un análisis estático de la aplicación InsecureBankv2.apk y Analizar la clase LoginActivity, en el método onCreate. ¿Ves alguna comprobación que se haga respecto a la creación de usuarios?

Esta herramienta se parece mucho a luyten pero se ve mejor la clasificación de clases y tiene un resumen de la aplicación. Muestra el numero de classes, métodos, instrucciones, campos y los problemas que presenta.

Input

Files

- /home/veronica/Descargas/InsecureBankv2/classes.jar

Code sources

- Count: 768

Counts

- Classes: 768
- Methods: 6350
- Fields: 3532
- Instructions: 254118 (units)

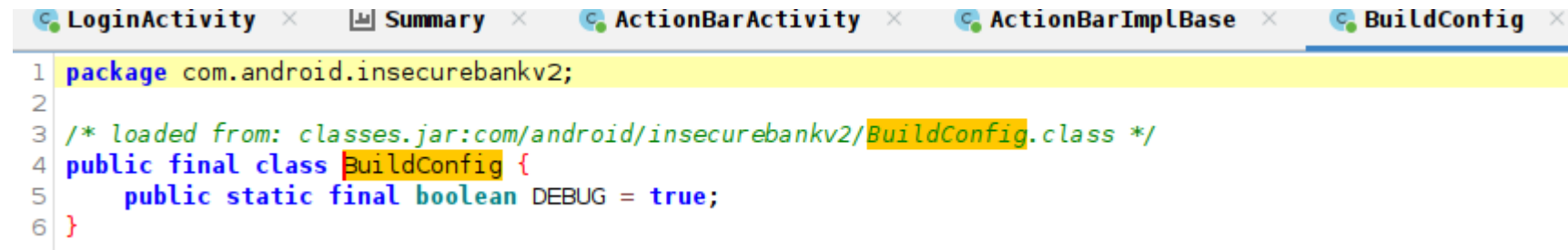
Decompilation

- Top level classes: 268
- Not loaded: 266 (99,25%)
- Loaded: 0 (0,00%)
- Processed: 1 (0,37%)
- Code generated: 1 (0,37%)

Issues


- Errors: 0
- Warnings: 0
- Nodes with errors: 0
- Nodes with warnings: 0
- Total nodes with issues: 0
- Methods with issues: 0
- Methods success rate: 100,00%

Tambien podemos visualizar el debug true.



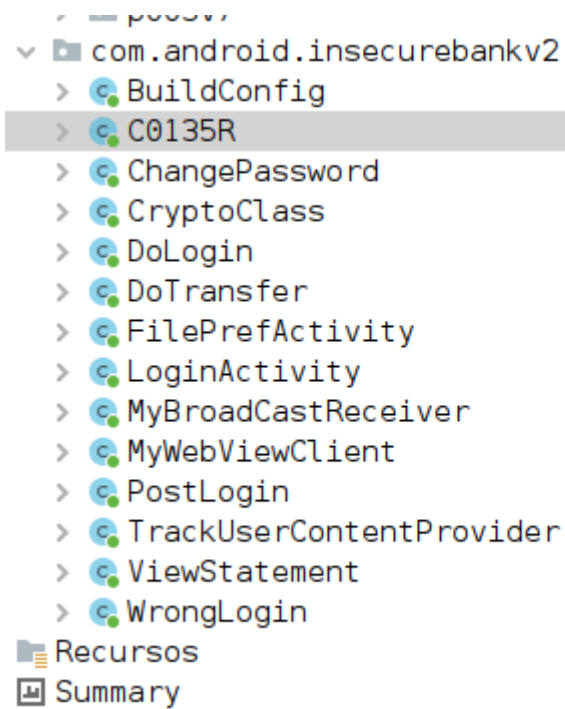
```
1 package com.android.insecurebankv2;
2
3 /* loaded from: classes.jar:com/android/insecurebankv2/BuildConfig.class */
4 public final class BuildConfig {
5     public static final boolean DEBUG = true;
6 }
```

Podemos ver mejor los recursos que utiliza la app



- ✓ Recursos
 - android
 - support
 - v4
 - accessibilityservice
 - app
 - content
 - database
 - graphics
 - hardware
 - internal
 - media
 - net
 - os
 - print
 - text
 - util
 - view
 - widget
 - v7
 - app
 - appcompat
 - internal
 - view
 - widget
 - com
 - android
 - insecurebankv2
 - Summary

Todas las secciones que posee la app como por y las actividades como login activity, fileprefactivity, el tipo de encriptamiento que mencionamos es base64. Reconocemos que se trata de una aplicacon hibrida, ya que vemos la classe mywebviewclient, la verficacion de estados, y si de pronto el cliente olvida sus credenciales que procede a realizarse.



Si vamos a la sección de login activity vemos.

No veo ningún tipo de comprobación de usuario en login activity específicamente en el método onCreate de hecho el create user esta deshabilitado si lo cambiamos a si puede aparecer el botón.


```

@Override // android.app.Activity
protected void onCreate(Bundle bundle) {
    super.onCreate(bundle);
    setContentView(C0135R.layout.activity_log_main);
    if (getResources().getString(C0135R.string.is_admin).equals("no")) {
        findViewById(C0135R.C0137id.button_CreateUser).setVisibility(8);
    }
    this.login_buttons = (Button) findViewById(C0135R.C0137id.login_button);
    this.login_buttons.setOnClickListener(new View.OnClickListener() { // from class: com.android.insecurebankv2.LoginActivity.1
        @Override // android.view.View.OnClickListener
        public void onClick(View view) {
            LoginActivity.this.performlogin();
        }
    });
    this.fillData_button = (Button) findViewById(C0135R.C0137id.fill_data);
    this.fillData_button.setOnClickListener(new View.OnClickListener() { // from class: com.android.insecurebankv2.LoginActivity.2
        @Override // android.view.View.OnClickListener
        public void onClick(View view) {
            try {
                LoginActivity.this.fillData();
            } catch (UnsupportedEncodingException | InvalidAlgorithmParameterException | InvalidKeyException | NoSuchAlgorithmException |
                e.printStackTrace();
            }
        }
    });
}

@Override // android.app.Activity
public boolean onCreateOptionsMenu(Menu menu) {
    getMenuInflater().inflate(C0135R.C0138menu.main, menu);
    return true;
}

```

- Cambiar el valor de la clave en el fichero strings.xml de los recursos de la aplicación a "yes".

```
GNU nano 7.1
<?xml version="1.0" encoding="utf-8"?>
<resources>
  <string name="abc_action_mode_done">Done</string>
  <string name="abc_action_bar_home_description">Navigate home</string>
  <string name="abc_action_bar_up_description">Navigate up</string>
  <string name="abc_action_menu_overflow_description">More options</string>
  <string name="abc_searchview_description_search">Search</string>
  <string name="abc_searchview_description_query">Search query</string>
  <string name="abc_searchview_description_clear">Clear query</string>
  <string name="abc_searchview_description_submit">Submit query</string>
  <string name="abc_searchview_description_voice">Voice search</string>
  <string name="abc_activitychooserview_choose_application">Choose an app</string>
  <string name="abc_activity_chooser_view_see_all">See all</string>
  <string name="abc_shareactionprovider_share_with_application">Share with %s</string>
  <string name="abc_shareactionprovider_share_with">Share with</string>
  <string name="app_name">InsecureBankv2</string>
  <string name="hello_world">Hello world!</string>
  <string name="loginscreen_username">Username:</string>
  <string name="action_settings">Preferences</string>
  <string name="action_exit">Restart</string>
  <string name="loginscreen_password">Password:</string>
  <string name="title_activity_file_pref">FilePref</string>
  <string name="server_ip">Server IP:</string>
  <string name="server_port">Server Port:</string>
  <string name="pref_submit">Submit:</string>
  <string name="title_activity_setting_preferences">SettingPreferences</string>
  <string name="title_activity_login">LoginActivity</string>
  <string name="title_activity_log_main">LogMainActivity</string>
  <string name="title_activity_do_login">DoLogin</string>
  <string name="title_activity_login_action">LoginAction</string>
  <string name="title_activity_post_login">PostLogin</string>
  <string name="title_activity_wrong_login">WrongLogin</string>
  <string name="title_activity_do_transfer">DoTransfer</string>
  <string name="title_activity_view_statement">ViewStatement</string>
  <string name="is_admin">yes</string>
  <string name="title_activity_change_password">ChangePassword</string>
  <string name="title_activity_exit">ExitActivity</string>
</resources>
```

- Reempaquetar y firmar la aplicación

```
(root@kali)-[/home/veronica/Descargas]
# apktool b InsecureBankv2_mod
I: Using Apktool 2.6.1-dirty
Exception in thread "main" java.lang.NoClassDefFoundError: org/apache/commons/text/StringEscapeUtils
    at brut.androlib.meta.YamlStringEscapeUtils.unescapeString(YamlStringEscapeUtils.java:141)
    at brut.androlib.meta.ClassSafeConstructor$ConstructStringEx.construct(ClassSafeConstructor.java:58)
    at org.yaml.snakeyaml.constructor.Constructor$ConstructScalar.constructStandardJavaInstance(Constructor.java:452)
    at org.yaml.snakeyaml.constructor.Constructor$ConstructScalar.construct(Constructor.java:403)
    at org.yaml.snakeyaml.constructor.BaseConstructor.constructObjectNoCheck(BaseConstructor.java:270)
    at org.yaml.snakeyaml.constructor.BaseConstructor.constructObject(BaseConstructor.java:253)
    at org.yaml.snakeyaml.constructor.SafeConstructor.processDuplicateKeys(SafeConstructor.java:108)
    at org.yaml.snakeyaml.constructor.SafeConstructor.flattenMapping(SafeConstructor.java:81)
    at org.yaml.snakeyaml.constructor.Constructor$ConstructMapping.constructJavaBean2ndStep(Constructor.java:252)
    at org.yaml.snakeyaml.constructor.Constructor$ConstructMapping.construct(Constructor.java:207)
    at org.yaml.snakeyaml.constructor.Constructor$ConstructYamlObject.construct(Constructor.java:358)
    at org.yaml.snakeyaml.constructor.BaseConstructor.constructObjectNoCheck(BaseConstructor.java:270)
    at org.yaml.snakeyaml.constructor.BaseConstructor.constructObject(BaseConstructor.java:253)
    at org.yaml.snakeyaml.constructor.BaseConstructor.constructDocument(BaseConstructor.java:207)
    at org.yaml.snakeyaml.constructor.BaseConstructor.getSingleData(BaseConstructor.java:191)
    at org.yaml.snakeyaml.Yaml.loadFromReader(Yaml.java:477)
    at org.yaml.snakeyaml.Yaml.loadAs(Yaml.java:470)
    at brut.androlib.meta.MetaInfo.load(MetaInfo.java:70)
    at brut.androlib.Androlib.readMetaFile(Androlib.java:273)
    at brut.androlib.Androlib.build(Androlib.java:287)
    at brut.androlib.Androlib.build(Androlib.java:280)
    at brut.apktool.Main.cmdBuild(Main.java:255)
    at brut.apktool.Main.main(Main.java:82)
Caused by: java.lang.ClassNotFoundException: org.apache.commons.text.StringEscapeUtils
    at java.base/jdk.internal.loader.BuiltinClassLoader.loadClass(BuiltinClassLoader.java:641)
    at java.base/jdk.internal.loader.ClassLoaders$AppClassLoader.loadClass(ClassLoaders.java:188)
    at java.base/java.lang.ClassLoader.loadClass(ClassLoader.java:520)
    ... 23 more
```

Luego de empaquetar no pude firmar por lo que aplique lo mencionado por Manuel.

The screenshot shows the Android Studio interface. On the left, the 'EXPLORER' pane shows the project structure for 'INSECUREBANKV2', including folders like 'assets', 'build', 'dist', 'java_src', 'original', 'res', 'smali', and files like '.gitignore', 'AndroidManifest.xml', and 'apktool.yml'. The 'strings.xml' file is open in the main editor, showing XML content for strings. The 'OUTPUT' tab is active, displaying the following build logs:

```
res > values > strings.xml
1  <?xml version="1.0" encoding="utf-8"?>
2  <resources>
3      <string name="abc_action_mode_done">Done</string>
4      <string name="abc_action_bar_home_description">Navigate home</string>
5      <string name="abc_action_bar_up_description">Navigate up</string>

I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: /home/veronica/Descargas/InsecureBankv2/dist/InsecureBankv2.apk
Rebuilding process was successful
-----
Signing InsecureBankv2/dist/InsecureBankv2.apk
-----
java -jar /home/veronica/.apklab/uber-apk-signer-1.2.1.jar -a /home/veronica/Descargas/InsecureBankv2/dist/InsecureBankv2.apk --allowResign --overwrite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
source:
/home/veronica/Descargas/InsecureBankv2/dist
zipalign location: BUILT_IN
/tmp/uapksigner-10381170210728904663/linux-zipalign-29_0_27081071408203895960.tmp
keystore:
[0] 161a0018 /tmp/temp_1947911086620047296_debug.keystore (DEBUG_EMBEDDED)
01. InsecureBankv2.apk
SIGN
file: /home/veronica/Descargas/InsecureBankv2/dist/InsecureBankv2.apk (0.89 MiB)
checksum: 28421acfbcf8053d4f52f3a61612e9e54aa22dac6bde89d0c3530bf7347b85ee (sha256)
- zipalign success
- sign success
VERIFY
file: /home/veronica/Descargas/InsecureBankv2/dist/InsecureBankv2.apk (0.91 MiB)
checksum: 73d2d087ef25c0c3c3cac35062824f5cd3cb2cb3b5b47d9b3898da07575c9f35 (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 21:10:05 CET 2044
[Thu Jan 12 02:13:40 CET 2023][v1.2.1]
Successfully processed 1 APKs and 0 errors in 0.40 seconds.
Signing process was successful
```

No puede testear con la aplicación virtual porque no supe como meterla dentro de la aplicación. Vere la corrección.

De igual manera encontré la forma de testearla.

