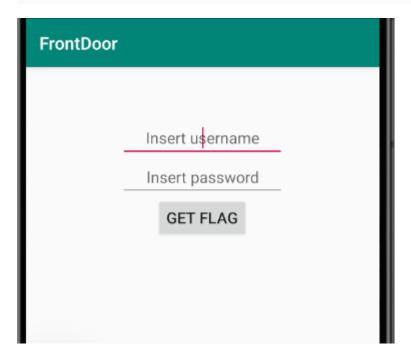
1-frontdoor- exploiting

هبدأ بقي في CTF علشان نعمل exploit للتطبيق وده اول CTF معانا هو

1-install app on emulator

adb install frontdoor.apk



هنا هو بيطلب username and password بس احنا منعرفش ايه هما username , password هنا هو بيطلب عشان كده لازم نروح نحلل التطبيق

2- analyze app with jadx-gui

jadx-gui frontdoor.apk

هنشوف اول حاجة ملف MeniFast.xml

3-Check AndroidMeniFast.xml file

مفهوش غير activity واحد اللي هو MainActivity ومش هعرف نستفاد منه بأي معلومات

```
🟭 AndroidManifest.xml × 🏿 © Flag × 🗬 MainActivity × 🗬 R × 🗬 BuildConfig ×
    <?xml version="1.0" encoding="utf-8"?>
    <manifest xmlns:android="http://schemas.android.com/apk/res/android"</pre>
        android:versionCode="1
        android:versionName="1.0"
        android:compileSdkVersion="28"
        android:compileSdkVersionCodename="9"
        package="com.mobisec.frontdoor
        platformBuildVersionCode="28"
        platformBuildVersionName="9">
        <uses-sdk
            android:minSdkVersion="22"
            android:targetSdkVersion="28"/>
3
        <uses-permission android:name="android.permission.INTERNET"/>
4
        <application
            android: theme="@style/AppTheme"
            android:label="@string/app_name"
            android:icon="@mipmap/ic_launcher"
android:debuggable="true"
            android:allowBackup="true"
            android:supportsRtl="true"
            android:usesCleartextTraffic="true"
            android:roundIcon="@mipmap/ic_launcher_round"
            android:appComponentFactory="android.support.v4.app.CoreComponentFactory">
            <activity android:name="com.mobisec.frontdoor.MainActivity">
                <intent-filter>
6
7
                    <action android:name="android.intent.action.MAIN"/>
8
                    <category android:name="android.intent.category.LAUNCHER"/>
6
                </intent-filter>
5
            </activity>
4
        </application>
2
    </manifest>
```

هرموح بقي نشوف ملف اللي هو بيعمل Check Flag

4- analyze flag file

```
Flag
     package com.mobisec.frontdoor;
     import java.io.BufferedReader;
     import java.io.InputStreamReader;
     import java.net.HttpURLConnection;
import java.net.URL;
     import java.nio.charset.StandardCharsets;
     /* loaded from: classes2.dex */
10
     class Flag {
         private static String sUrl = "http://10.0.2.2:31337/getflag";
         private static boolean debug = false;
11
19
         public static String getFlag(String username, String password) throws Exception {
              String urlParameters;
              if (debug) {
21
                  urlParameters = "username=testuser&password=passtestuser123";
              } else
                  urlParameters = "username=" + username + "&password=" + password;
              byte[] postData = urlParameters.getBytes(StandardCharsets.UTF_8);
25
26
              int postDataLength = postData.length;
              String request = sUrl + "?" + urlParameters;
28
              URL url = new URL(request);
29
              HttpURLConnection conn = (HttpURLConnection) url.openConnection();
              conn.setRequestMethod("GET");
30
              conn.setRequestProperty("Content-Type", "application/x-www-form-urlencoded");
conn.setRequestProperty("charset", "utf-8");
conn.setRequestProperty("Content-Length", Integer.toString(postDataLength));
31
32
33
34
              conn.setUseCaches(false);
36
              BufferedReader rd = new BufferedReader(new InputStreamReader(conn.getInputStream()));
37
              String content = BuildConfig.FLAVOR;
              while (true) {
39
                   String line = rd.readLine();
                   if (line != null) {
                       content = content + line + "\n";
                   } else {
43
                       return content;
             }
         }
```

هنا اه هو بيبعت request لل server اللي هو 10.0.2.2:31337 وبيجيب flag وفيه قيمة اللي هي debug =false ودي بيشوف لو هو debug بيبعت في url parameters ان username username ودي بيشوف لو هو testuser and password =passtestuser123 وبكده احنا عرفنا ايه هو username وبكده احنا عرفنا ايه هو username وبكده احنا عرفنا ايه هو username وبكده احنا عرفنا ايه هو

```
class Flag {
    private static String sUrl = "http://10.0.2.2:31337/getflag";
    private static boolean debug = false;

Flag() {
    }

    public static String getFlag(String username, String password) throws Exception {
        String urlParameters;
        if (debug) {
                  urlParameters = "username=testuser&password=passtestuser123";
        } else {
                 urlParameters = "username=" + username + "&password=" + password;
        }
}
```

بس عاوين نغير قيمة debug ل true يبقي paramters هما username ,password فلازم نروح نفك التطبيق ونغير القيمة بتاعت debug ل true

6- open flag.smali file and chagne the value of debug

before change the value

```
1 .line 15
2  const/4 v0, 0x
3
4  sput-boolean v0, Lcom/mobisec/frontdoor/Flag;->debug:Z
5
6  return-void
7 .end method
```

after change value

```
.line 15
const/4 v0, 0x1
sput-boolean v0, Lcom/mobisec/frontdoor/Flag;->debug:Z
return-void
.end method
```

6-build the app with apktool

```
apktool b frondoor
```

7- signing the new apk & use zipalign to config lines

```
zipalign -v 4 frontdoor/dist/frondoor.apk out.apk
```

8- sign key

```
apksigner sign --ks-key-alias hextree -ks ~/android-app-hack.keystore out.apk
```

9-the value is changed on the new app

```
ns Help
# AndroidManifest.xml × © Flag
                                                          package com.mobisec.frontdoor;
         import iava.io.BufferedReader:
         import java.io.InputStreamRea
         import java.net.HttpURLConnection;
import java.net.URL;
         import java.nio.charset.StandardCharsets;
            * loaded from: classes2.dex */
         class Flag {
    private static String sUrl = "http://10.0.2.2:31337/getflag";
    release debug = true;
   10
   11
   19
               public static String getFlag(String username, String password) throws Exception {
                      tring urlParameters;
                    if (debug) {
                         urlParameters = "username=testuser&password=passtestuser123";
                         urlParameters = "username=" + username + "&password=" + password;
                    byte[] postData = urlParameters.getBytes(StandardCharsets.UTF_8);
                    int postDataLength = postData.length;
String request = SUrl + "?" + urlParameters;
URL url = new URL(request);
   26
   28
                    URL urt = new URL(request);

HttpURLConnection conn = (HttpURLConnection) url.openConnection();

conn.setRequestMethod("GET");

conn.setRequestProperty("Content-Type", "application/x-www-form-urlencoded");

conn.setRequestProperty("Charset", "utf-8");

conn.setRequestProperty("Content-Length", Integer.toString(postDataLength));
   30
                    conn.setUseCaches(false);
                    BufferedReader (d = new BufferedReader(new InputStreamReader(conn.getInputStream()));
String content = BuildConfig.FLAVOR;
   36
                    while (true) {
   String line = rd.readLine();
   39
                         if (line != null)
                              content = content + line + "\n";
   43
                               return content;
```

کدہ بقی ہو ہیحط default ان url parameters is عدہ بقی ہو ہیحط username=testuser&password=passtestuser123

هنا اه بقي اللي اللي هيحصل هو هنا اول ما اعمل click on button هياخد username ,password اللي هدخلهم وبيوعتهم لل function اللي هي getflag

```
@Override // android.view.View.OnClickListener
public void onClick(View v) {
    String username = usernameWidget.getText().toString();
    String password = passwordWidget.getText().toString();
    flagWidget.setText("Getting flag...");
    flagWidget.setTextColor(ViewCompat.MEASURED_STATE_MASK);
    try {
        String result = Flag.getFlag(username, password());
        flagWidget.setText(result);
    } catch (Exception e) {
        Log.e("MOBISEC", "Exception while getting the flag:" + Log.getStackTraceString(e));
        flagWidget.setText("An error occurred");
    }
});
}
});
}
```

هنا بقي get flag ا function اللي بتشوف فيمة debug فهي هتبقي true علشان احنا غيرناها فبيعت بقي get flag اللي هو محددهم ويكمل request عادي

```
package com.mobisec.frontdoor;
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.HttpURLConnection;
import java.net.URL;
import java.nio.charset.StandardCharsets;
/* loaded from: classes2.dex */
class Flag {
    private static String sUrl = "http://10.0.2.2:31337/getflag";
    private static boolean debug = true;
    Flag() {
    public static String betFlag(String username, String password) throws Exception {
        String urlParameters;
       if (debug) {
           urlParameters = "username=testuser&password=passtestuser123";
        } else {
            urlParameters = "username=" + username + "&password=" + password;
        byte[] postData = urlParameters.getBytes(StandardCharsets.UTF_8);
        int postDataLength = postData.length;
        String request = sUrl + "?" + urlParameters;
        URL url = new URL(request);
        HttpURLConnection conn = (HttpURLConnection) url.openConnection();
        conn.setRequestMethod("GET");
        conn.setRequestProperty("Content-Type", "application/x-www-form-urlencoded");
conn.setRequestProperty("charset", "utf-8");
        conn.setRequestProperty("Content-Length", Integer.toString(postDataLength));
        conn.setUseCaches(false);
        BufferedReader rd = new BufferedReader(new InputStreamReader(conn.getInputStream()));
        String content = BuildConfig.FLAVOR;
        while (true) {
            String line = rd.readLine();
            if (line != null) {
                content = content + line + "\n";
            } else {
                return content;
       }
   }
}
```

برده كان في حل تاني بدل ما اغير كل ده هو اخد username ,passwrod وادخلهم انا وخلاص

the flag is MOBISEC{noob_hackers_only_check_for_backdoors}