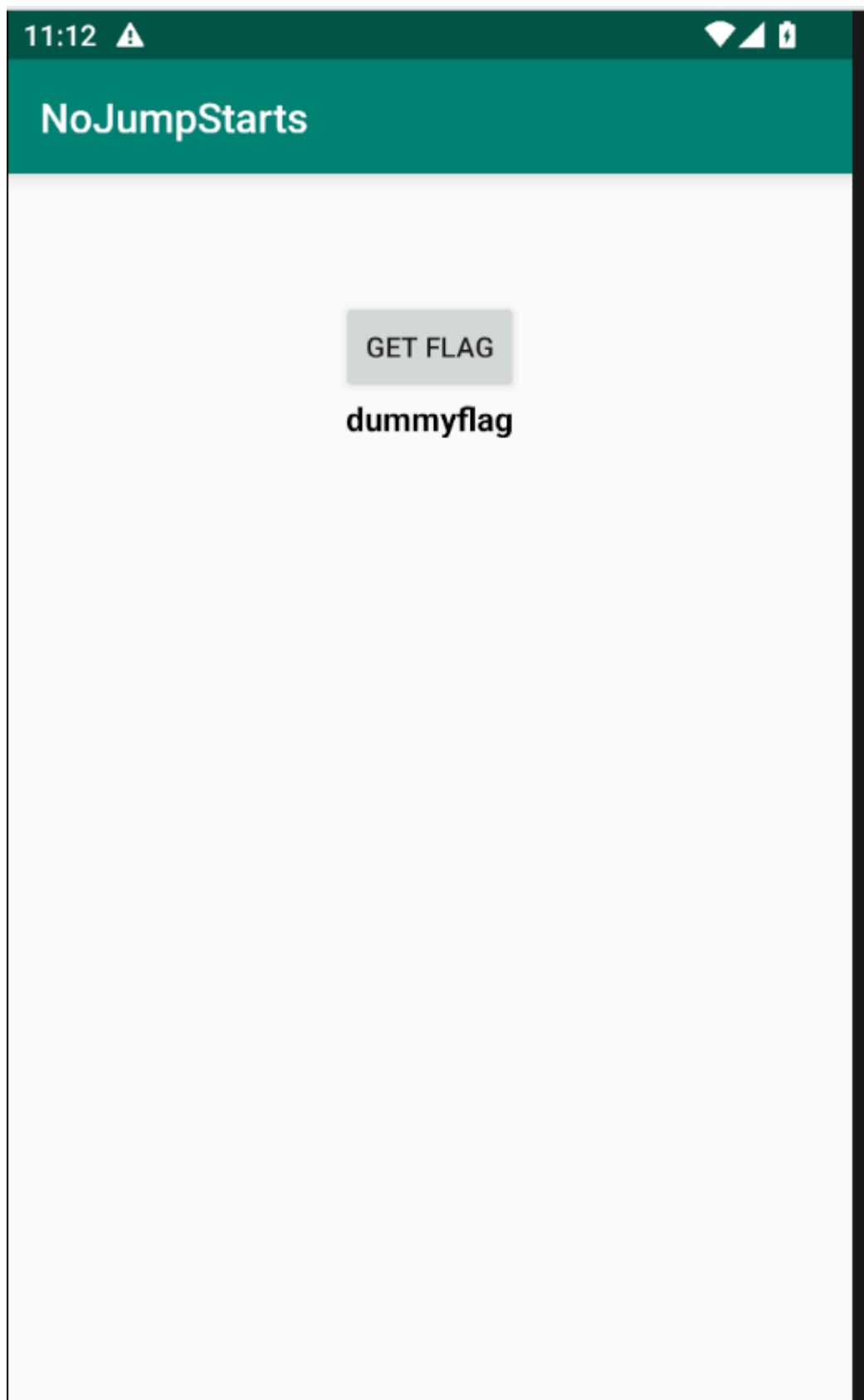


2-nojumpstarts- exploiting

ده ثاني challenge معانا من تحديات exploiting في ال challenge ده هو فيه اكثر من activity كل activity معتمد علي الثاني الفكرة فيه ان لازم نبدا من عند activity معين علشان نجيب flag ومن اسمه برده no jump start خرينا بقي نشرحه

هنا اه اول با بندوس علي Get Flag بيحصلنا كلمة وطبعاً مش ده flag



اول اجة لازم analyze AndroidMeniFast.xml

1- analyzing AndroidMeniFast.xml file








هنا اهو هو في 4 activities هما **MainActivity, A, B,C** وخلي بالك هنا **C** بيحتوي علي **intent** يحتوي علي **action =getflag**

```

android:appcomponentfactory= android.support.v4.app.CoreComponentFactory >
<activity android:name="com.mobisec.nojumpstarts.MainActivity">
    <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
</activity>
<activity android:name="com.mobisec.nojumpstarts.A"/>
<activity android:name="com.mobisec.nojumpstarts.B"/>
<activity android:name="com.mobisec.nojumpstarts.C">
    <intent-filter>
        <action android:name="mobisec.intent.getflag"/>
        <category android:name="android.intent.category.DEFAULT"/>
    </intent-filter>
</activity>
</application>
</manifest>

```

نا برده دي بقي الملفات اللي موجودة فيه

- >  A
- >  B
- >  BuildConfig
- >  C
- >  Main
- >  MainActivity
- >  R

2- analyzing MainActivity

```

public class MainActivity extends AppCompatActivity {
    public static String flag = "dummyflag";

    void setFlag(Intent intent) {
        String flag2;
        if (intent != null && (flag2 = intent.getStringExtra("flag")) != null) {
            flag = flag2;
            Log.e("MOBISec", "flag set correctly");
        }
    }

    public void getFlag() throws Exception {
        Intent i = Main.buildIntent("Main", "A", null);
        startActivityForResult(i, 400);
    }

    @Override // android.support.v7.app.AppCompatActivity, android.support.v4.app.FragmentActivity, android.
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        setFlag(getIntent());
        Button getFlagButton = (Button) findViewById(R.id.getflag);
        final TextView flagWidget = (TextView) findViewById(R.id.flag);
        getFlagButton.setOnClickListener(new View.OnClickListener() { // from class: com.mobisec.nojumpstart
            @Override // android.view.View.OnClickListener
            public void onClick(View v) {
                flagWidget.setText("Getting flag...");
                flagWidget.setTextColor(ViewCompat.MEASURED_STATE_MASK);
                try {
                    MainActivity.this.getFlag();
                } catch (Exception e) {
                    Log.e("MOBISec", "Exception while getting the flag:" + Log.getStackTraceString(e));
                    flagWidget.setText("An error occurred when getting flag");
                }
            }
        });
    }

    @Override // android.support.v4.app.FragmentActivity, android.app.Activity
    public void onActivityResult(int requestCode, int resultCode, Intent data) {
        super.onActivityResult(requestCode, resultCode, data);
        TextView flagWidget = (TextView) findViewById(R.id.flag);
        if (requestCode == 400) {
            String flag2 = data.getStringExtra("flag");
            if (flag2 != null) {
                flagWidget.setText(flag2);
            } else {
                flagWidget.setText("flag was null");
            }
        }
    }
}

```

هنا **setFlag** function يتاخذ **Intent** ويتشوف ان هو بيحتوي **flag** ولا لا ولو فيه بتطبع في **log** الرسالة

```

void setFlag(Intent intent){
    String flag2;
    if(intent!=null&&(flag2=intent.getStringExtra("flag"))!=null){
        flag=flag2;
        log.e("MOBISec","flag set corrcorrectly")
    }
}

```

هنا **getFlag** function بتتبع ل **Main.buildIntent ("Main","A",null)** اللي هنشوف دي بتعمل ايه وتعمل **startActivityForResult(intent,400)**

```

public void getFlag() throws Exception {
    Intent i = Main.buildIntent("Main", "A", null);
    startActivityForResult(i, 400);
}

```

هنا هو بقي في **Main.buildIntent** بتحول اللي بييجيلها مثلا **Main-to-A** وبتعمل **sign** باستخدام **private key** باستخدام **RSA encryption** للرسالة دي وبتنشئ **new Component** اللي هو **A** وبتبعثه الرسالة و **signature** وهو بيتأكد فعلا من خلال فانكشن عنده

```
public static Intent buildIntent(String src, String dst, String chain) {
    String msg;
    try {
        if (chain == null) {
            msg = src + "-to-" + dst;
        } else {
            msg = chain + "/" + src + "-to-" + dst;
        }
        byte[] sign = sign(msg);
        Intent i = new Intent();
        ComponentName cn = new ComponentName(BuildConfig.APPLICATION_ID, "com.mobisec.nojumpstarts." + dst);
        i.setComponent(cn);
        i.putExtra("authmsg", msg);
        i.putExtra("authsign", sign);
        return i;
    } catch (Exception e) {
        return null;
    }
}
```

هنا دي الفانكشن اللي بتعمل **encryption** باستخدام **RSA private key**

```
public static byte[] sign(String msg) throws Exception {
    byte[] msgbytes = msg.getBytes();
    PrivateKey privKey = getPrivateKey();
    Signature s = Signature.getInstance("SHA256withRSA");
    s.initSign(privKey);
    s.update(msgbytes);
    byte[] signature = s.sign();
    return signature;
}
```

ودي الفانكشن اللي تعمل **verify** بتأكد فعلا هل الرسالة معمول ليها **sign** ولا لا

```
public static boolean verify(String msg, byte[] signature) {
    try {
        byte[] msgbytes = msg.getBytes();
        PublicKey pubKey = getPublicKey();
        Signature s = Signature.getInstance("SHA256withRSA");
        s.initVerify(pubKey);
        s.update(msgbytes);
        boolean res = s.verify(signature);
        return res;
    } catch (Exception e) {
        Log.e("MOBISec", "exception when verifying: " + Log.getStackTraceString(e));
        return false;
    }
}
```

Activity A

```
AndroidManifest.xml x MainActivity x Main x A x
package com.mobisec.nojumpstarts;

import android.content.Intent;
import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;

/* loaded from: classes2.dex */
13 public class A extends AppCompatActivity {
    private static String expectedMsg = "Main-to-A";

14     private void reply(String flag) {
15         Intent resIntent = new Intent();
16         resIntent.putExtra("flag", flag);
17         setResult(-1, resIntent);
18         finish();
    }

    @Override // android.support.v7.app.AppCompatActivity, android.support.v4.app.FragmentActivity, a
22     protected void onCreate(Bundle savedInstanceState) {
23         super.onCreate(savedInstanceState);
24         setContentView(R.layout.activity_a);
26         Intent data = getIntent();
27         String msg = data.getStringExtra("authmsg");
28         byte[] sign = data.getByteArrayExtra("authsign");
32         if (msg != null && sign != null && msg.equals(expectedMsg) && Main.verify(msg, sign)) {
34             Intent intent = Main.buildIntent("A", "B", msg);
35             startActivityForResult(intent, 401);
        } else {
38             reply("A: broken auth");
        }
    }

    @Override // android.support.v4.app.FragmentActivity, android.app.Activity
43     public void onActivityResult(int requestCode, int resultCode, Intent data) {
44         super.onActivityResult(requestCode, resultCode, data);
47         if (requestCode == 401) {
49             String flag = data.getStringExtra("flag");
50             reply(flag);
        }
    }
}
```

Activity B

```

AndroidManifest.xml x MainActivity x Main x A x B x
package com.mobisec.nojumpstarts;

import android.content.Intent;
import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;

/* loaded from: classes2.dex */
12 public class B extends AppCompatActivity {
    private static String expectedMsg = "Main-to-A/A-to-B";

13     private void reply(String flag) {
14         Intent resIntent = new Intent();
15         resIntent.putExtra("flag", flag);
16         setResult(-1, resIntent);
17         finish();
    }

    @Override // android.support.v7.app.AppCompatActivity, android.support.v4.app.FragmentActivity
21     protected void onCreate(Bundle savedInstanceState) {
22         super.onCreate(savedInstanceState);
23         setContentView(R.layout.activity_b);
24         Intent data = getIntent();
25         String msg = data.getStringExtra("authmsg");
26         byte[] sign = data.getByteArrayExtra("authsign");
27         if (msg != null && sign != null && msg.equals(expectedMsg) && Main.verify(msg, sign)) {
31             Intent intent = Main.buildIntent("B", "C", msg);
33             startActivityForResult(intent, 402);
34         } else {
37             reply("B: broken auth");
        }
    }

    @Override // android.support.v4.app.FragmentActivity, android.app.Activity
42     public void onActivityResult(int requestCode, int resultCode, Intent data) {
43         super.onActivityResult(requestCode, resultCode, data);
44         if (requestCode == 402) {
46             String flag = data.getStringExtra("flag");
48             reply(flag);
49         }
    }
}

```

Activity C

```

package com.mobisec.nojumpstarts;

import android.content.Intent;
import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;

/* loaded from: classes2.dex */
12 public class MainActivity extends AppCompatActivity {
    private static String expectedMsg = "Main-to-A/A-to-B/B-to-C";

    13 private void reply(String flag) {
    14     Intent resIntent = new Intent();
    15     resIntent.putExtra("flag", flag);
    16     setResult(-1, resIntent);
    17     finish();
    }

    21 @Override // android.support.v7.app.AppCompatActivity, android.support.v4.app.FragmentActivity, android.
    22 protected void onCreate(Bundle savedInstanceState) {
    23     super.onCreate(savedInstanceState);
    24     setContentView(R.layout.activity_c);
    25     Intent data = getIntent();
    26     String msg = data.getStringExtra("authmsg");
    27     byte[] sign = data.getByteArrayExtra("authsign");
    31     if (msg != null && sign != null && msg.equals(expectedMsg) && Main.verify(msg, sign)) {
    33         reply(MainActivity.flag);
    } else {
    36         reply("broken auth");
    }
    }
}

```

الخلاصة بقي هنا ايه اللي بيحصل او ايه ملخص اصلا Challenge ده

اول حاجة في four activity (MainActivity, A, B, C) بيبيع للتاني message ,signature وان الرسالة دي متشفرة باستخدام RSA private key هو مدهولنا كده تمام

كل activity بيناكد فعلا هل الرسالة اللي جياهه من activity اللي قبله فعلا هي ولا لا كده تمام ودلوقتي هنشوف ازاي هما بيعتوا ل بعض

1- Main activity send for A activity ---> ("Main-to-A" , signature("Main-to-A"))

2- A activity send for B activity ---> (("Main-to-A/A-to-B"), signature("Main-to-A/A-to-B")))

3- B activity send for C activity ---> (("Main-to-A/A-to-B/B-to-C"), signature("Main-to-A/A-to-B/B-to-C")))

كده فهمنا ازاي كل واحد بيعت للتاني نيجي بقي اول ما C بيجيوله اخر رسالة ويبينناكد فعلا ان هي تمام يقوم هو بقي باعت Flag ل B وبعد كده B بيعته ل A وبعد كده A بيعته ل MainActivity

الحل هنا بقي هو ان احنا ننشئ signature باستخدام private key لل "Main-to-A/A-to-B/B-to-C" message . بعد كده نبعته ل C باستخدام action getflag

Code for Generate Signature

```

from cryptography.hazmat.primitives import serialization, hashes
from cryptography.hazmat.primitives.asymmetric import padding
import base64

```



```
PRIVKEY = ""-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA0vKu6oHF6wkA+gDdqhcsreLz1Y9KLdNQBSSrlvWcZxmMglQU
4oL017CvuTAqSWJmPls00c0fNy6yE+iOA2SrhTM0RJ229fl6VDcFyHnG4grmcfs1
j2J3lCAssdON5tgrbRvt/FRrkF06x7rLCWiQbcWZgt/Yj+ONbPHeHIImSzUkNkJC
MmlwIv/l/Oz1gN6Pn6KZQxiASSqR5uS7v92vYXGpusLjvfLpFzCEBYbBEpguxmQF
pfvyKZQHiimiEgqvWvOaNv8FKNi2/eELD3jre6U0ng/eSlhP9FKrt109xdgw96ff
VYK0o9o9IjM44RZFyvtJLIBGYI7uwaAgJK+rFQIDAQABAOIBACD/rbUpj9hw1CKH
uCU/ctHQyuH+hFAe2kmzrtPyoADQ0lYg6RN2AO8syJBjpHnOVsgyXmMb2Kwf2z1
2CFXwi0YEXkaYuCfoi9CXDk8M4xwwBPcgceoU6RsVBGNUolmD4UF9XifjCQNMDF
C7XxEYbafmUmtY3rHtiIDYLQKUViRe/gisYtWC1OdAZ0s/Q/rdpf9EVCcmKD1Dxc
8zoRA8gmF4EwJrVwpqvdSqmwtQPGjrkFfv0fxJk5iYiId+FONKtcXFvmZ7i0o9bB
BeJdmJySlOr/9oCs29R/ZUkW13H9zGftKX0pp64qgxy/yGoe/lQunzYete5l5X1t
e/wnORECgYEA9ktAziObm/7uDHL3hpi6rj7SKE7EvxB2mvfLGfXNUM3t4c1K8Sdp
61H7rufuv+Ebz4PpS7pm2sctUmXvlp0Z+HxOsqDEKU/0FByN2O8Qnc5H8yFfTVLR
MYws4EqvDcsG9J7YywlRlQ+z1Fy18VEgGcgWWoiKNAPrKcTMMo07/dsCgYEA20LX
PIxtS6J0s1Xk16kF9oCIKOiSsJ3vbRjSU2ffewOJYhCizMrjyDhfUcuED3mDGg0i
7ctAWPuRfQ4z13ku5GCQ711mh5F3wA+mLr7vRVUwEk2F4PUL81LkwblJl4mEb3Gj
/pCiEeYy9mrr8N3JAXK0f4hYdITlmFtXvQtyZc8CgYEAjOnRUh+dUESy94AnmqKX
bEoVA2rNtmM8+Lz9PwUbSzgG+kHytrbOKwzk6tVYDABHYRsfX2wGnPWIQLSbt7J6
wWidviWtFdXg2ADeRlFAMglrsPdPB3Zyqd5yjlEshr+6YwrfDotuWdJ6GO5SSpcX
vqhz4ahtKgVz7pniGqS0UjECgYAMyymj7s2xzBjjHe/sZYBjkbxgJrHofE6sHvam
xzjTBLHPdwkiYg3gcOme7DEYdg6gRoPzPBjVGFi0409DE18ZFElgriJ9Zo+GNWOM
9rcfZIkZiEx3g9TerceLRjRlEyKbfhYDlIzgXn46wqJhu48vDrhZeKswoVCEQ1Ar
R6+1lIQKBgF78mW4Si37+WtTdsPE6tA8wzqXJJE7+6geD4tkVKovU25yGsyinihXV
T3mhPCK7rJ5EoksAdrGKEmX50lJqF0vwjUYNxtTLvpIraYKQsXlIaT3m4sI3Blco
rfqFhHLw9qfYnmQQXhaXGBhZLQFYMKaYURg5/Z55Xmpmr//mK58m
-----END RSA PRIVATE KEY-----""
```

```
message = "Main-to-A/A-to-B/B-to-C".encode()
```

```
private_key = serialization.load_pem_private_key(
    PRIVKEY.encode(),
    password=None,
)
```

```
signature = private_key.sign(
    message,
    padding.PKCS1v15(),
    hashes.SHA256()
)
```

```
b64_signature = base64.b64encode(signature).decode()
```

```
print(f"Message: {message.decode()}")
print(f"Base64 Signature: {b64_signature}")
```

نستخدم بقي start-activity for intent

```
adb shell am start -n com.mobisec.nojumpstarts/.C -a mobisec.intent.getflag
--es authmsg "Main-to-A/A-to-B/B-to-C" --es authsign
"YRLhLEnrmbZScKLpYYQNuDpkWSSfBRLMb5rrX3mTmUVZpipT4dVtwvXxP0WsF97quFZfubH32hs
7okrKo9O4YRlaYE+AkNlc3fUZMC3L1CD8++PKYDuVT1X8v3wGzWhBpAjWZxUYiJP6wOdpLzoByQc
mPf9IBam0L74KkcNRS8zGvB8MeXdZ7WX9ITRo2gvQRIwvnVhEiwPHKRixH26UKL4HeHNWJkAbuQT
6uHXx1iiu47kwCJgJdqT9HOI3t4bvyPRRHQAwtgaZlpbLu48spq8RKoYqRTJOBtp1lcG343GHey
34is6gmeJhPbFBSxSdwIostH7atb+dAfJeQZV4A=="
```

كده بقي اول ما نعمل start-activity هنجيب flag