

## Identity Crisis

A .apk file with just a login screen and when a password is tried it says access denied so we try to decompile the apk file

```
(docx@kali) - [~/Identity_Crisis]
$ jadx-gui $(pwd)/identity_crisis.apk
INFO - Checking for updates ...
INFO - Update channel: STABLE, current version: 1.5.3
INFO - output directory: identity_crisis
INFO - loading ...
INFO - No updates found
WARN - Found duplicated class: kotlin.coroutines.jvm.internal.DebugProbesKt, count: 2. Only one will be loaded!
      classes.dex
      identity_crisis.apk:DebugProbesKt.bin
INFO - Loaded classes: 7101, methods: 55858, instructions: 1538016
INFO - Resetting disk code cache, base dir: /home/docx/.cache/jadx/projects/identity_crisis-e058268448d41894aea5fa32c7ae0b4b/code
New Volume
```

since developers often leave secrets in Resources -> resources.arsc -> res -> values -> strings.xml we search there and find this

```
49 | <string name="debug_key">SGCTF{NOt_Th3_Fl4g_K33p_L00king}</string>
```

which is a fake flag

the description said “Stop looking at what the app does, and look at what the app is.”

so we look inside Resources -> AndroidManifest.xml and we find this

```
25 | <meta-data
    |     android:name="com.ctf.secret.API_KEY"
    |     android:value="SGCTF{M4nif3st_D3st1ny_Unl0cked}"/>
```

which the real flag

SGCTF{M4nif3st\_D3st1ny\_Unl0cked}