## 说明

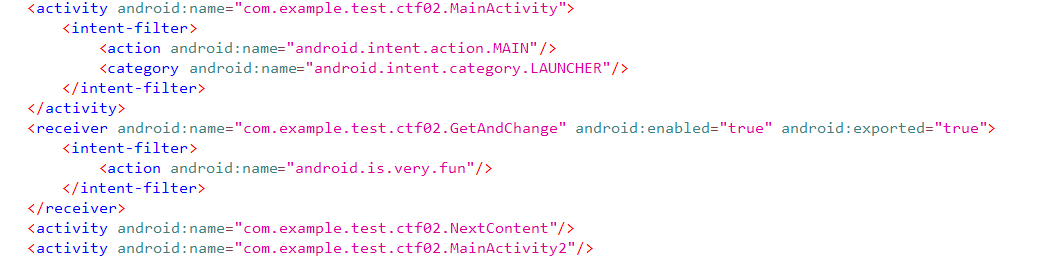
非常简单的审计进入后可以获取第一个密码，进入之后还需要输入第二个密码，这个时候可以apktool反编译找到图片，也可以在AndroidManifest.xml中找到广播中找到密码。

## 解题

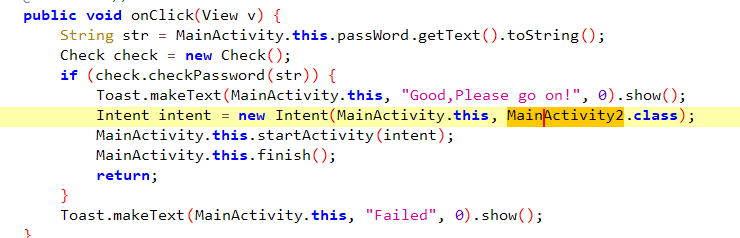
可以看到活跃目录是：com.example.test.ctf02.MainActivity

广播的名字是：com.example.test.ctf02.GetAndChange

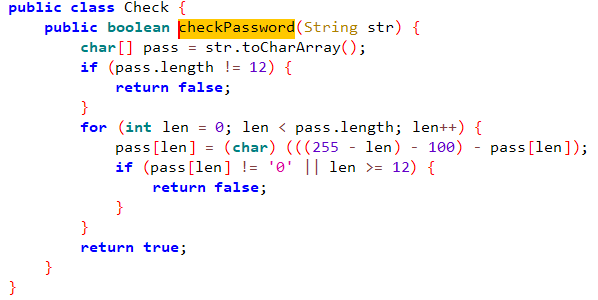
当我们输入android.is.very.fun时就会执行GetAndChange



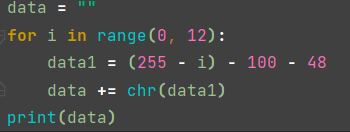
第一段：



使用checkPassword对输入的字符串进行检查：

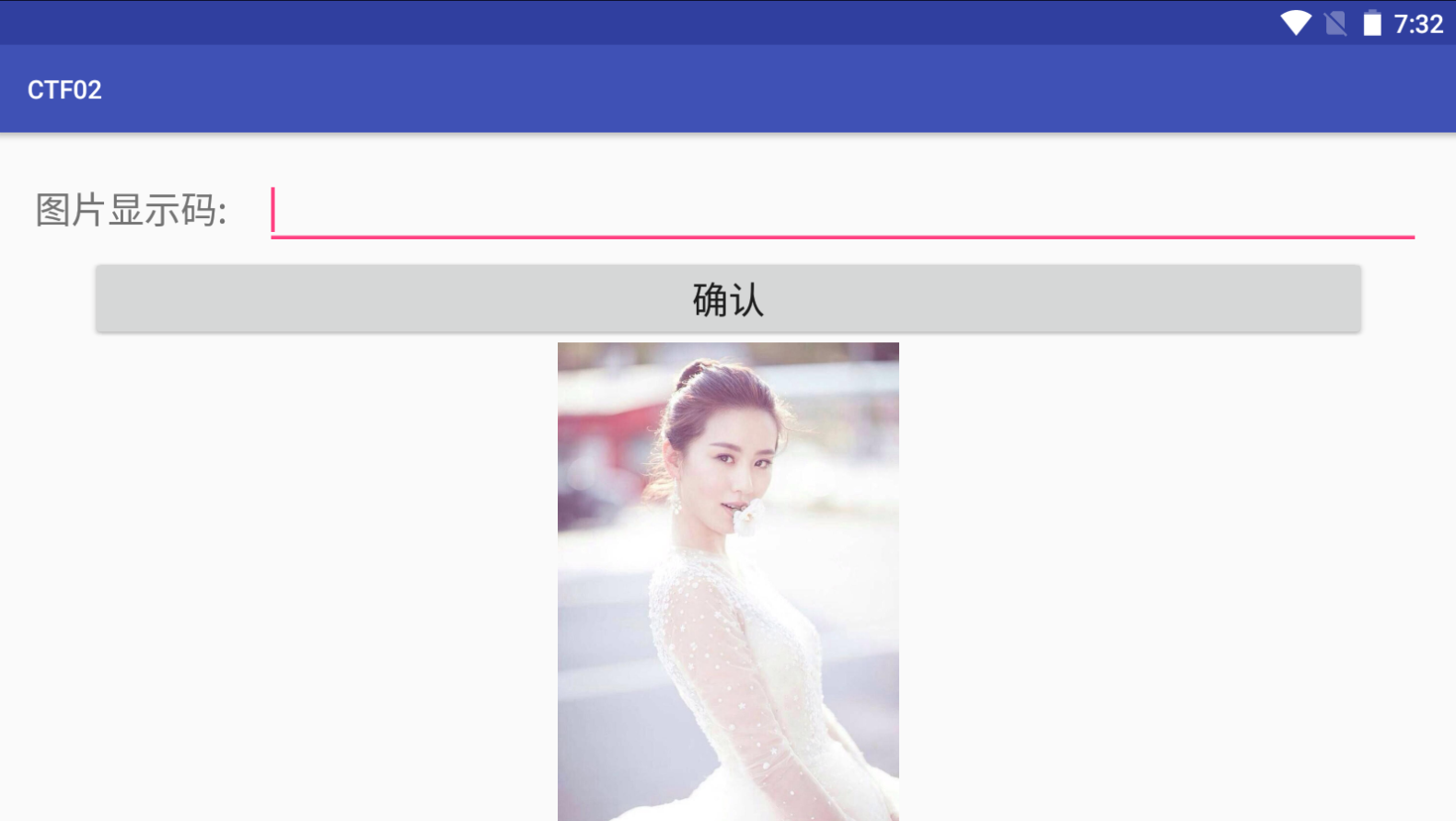


255减去该字符的下标再减去100再减去该字符然后转为ASCII后必须是字符0，因此：

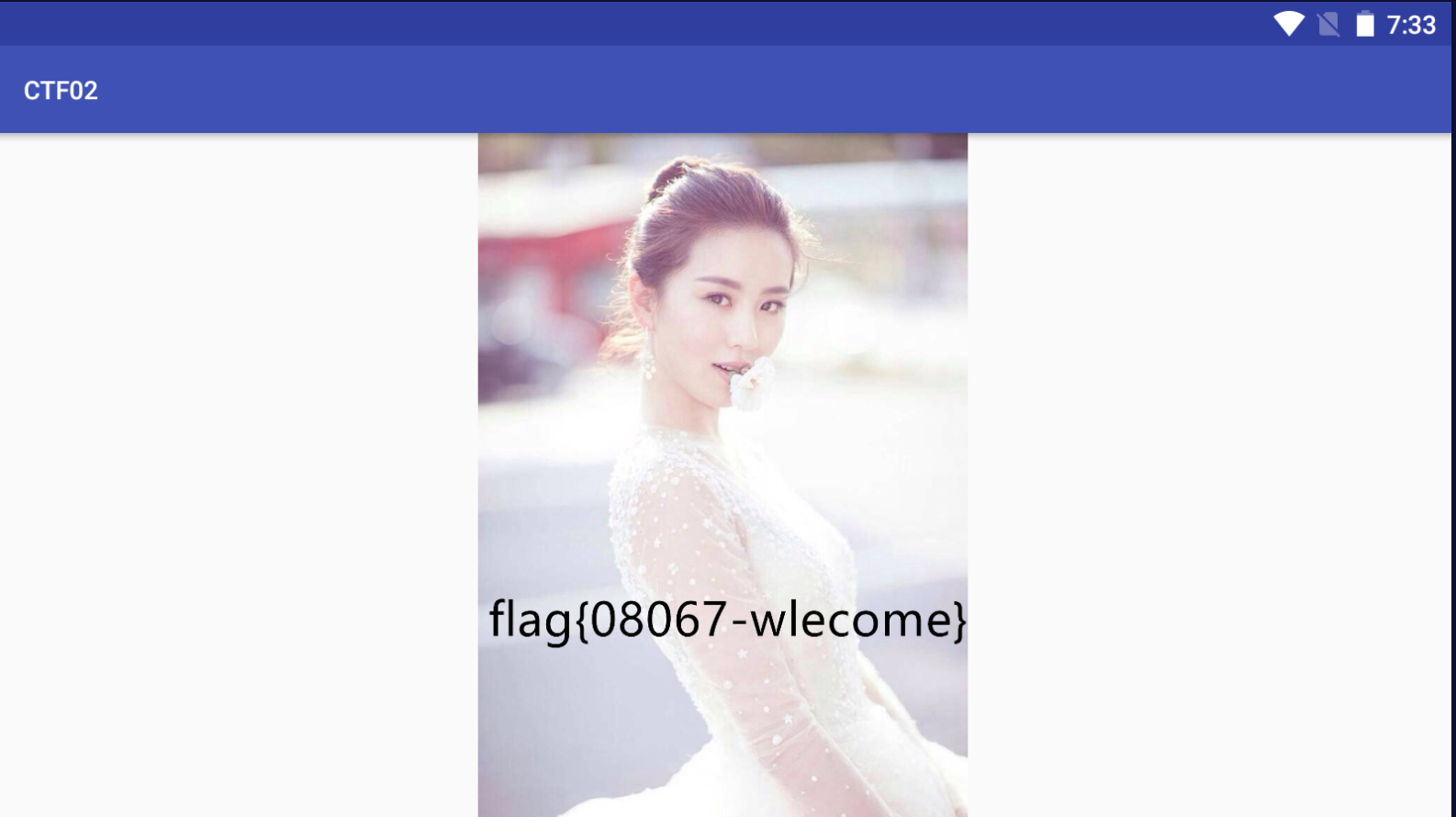


得到password：kjihgfedcba`

输入后：



此时可以选择输入刚才注册的广播中action的Android:name的值输入进去得到flag：



也可以直接用apktool反编译apk：



这是一个图片，把扩展名改为jpg就可以查看了：

