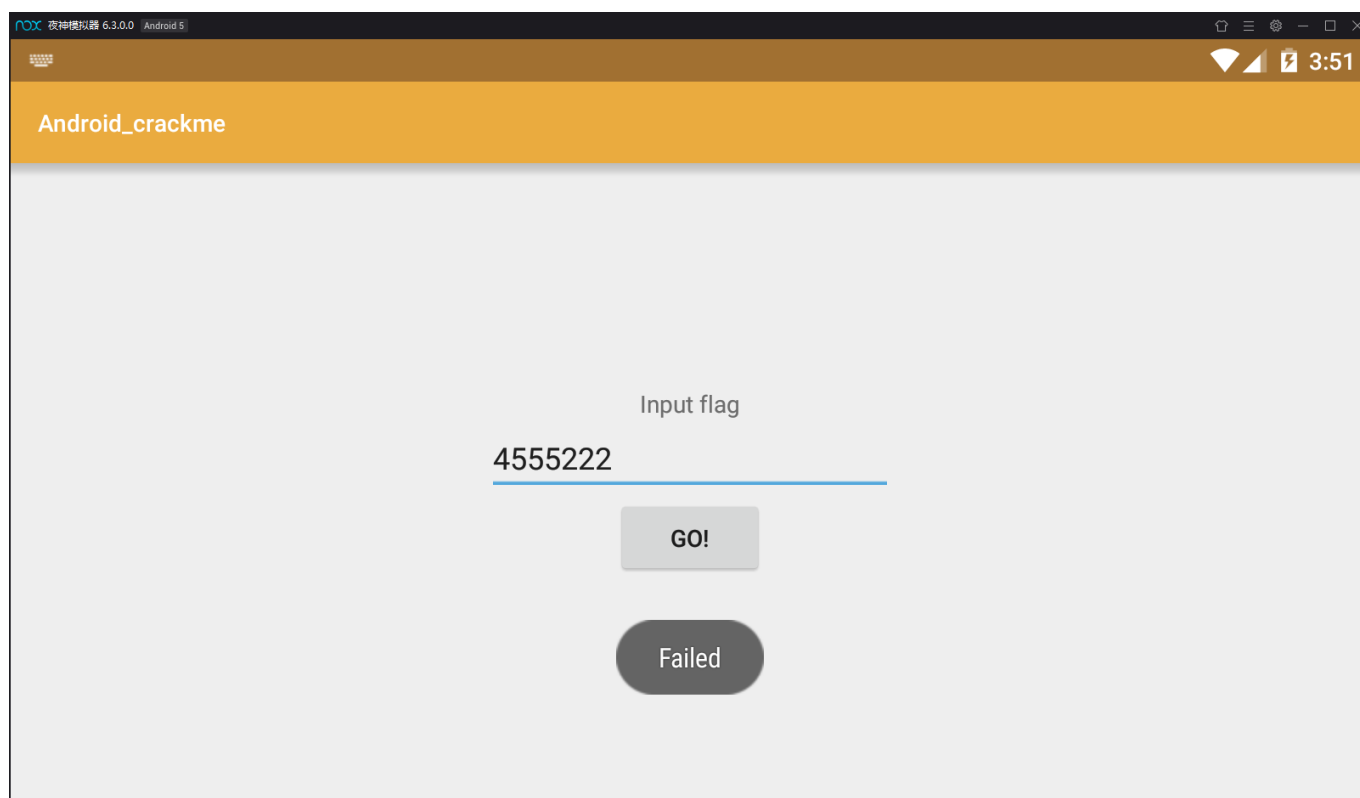
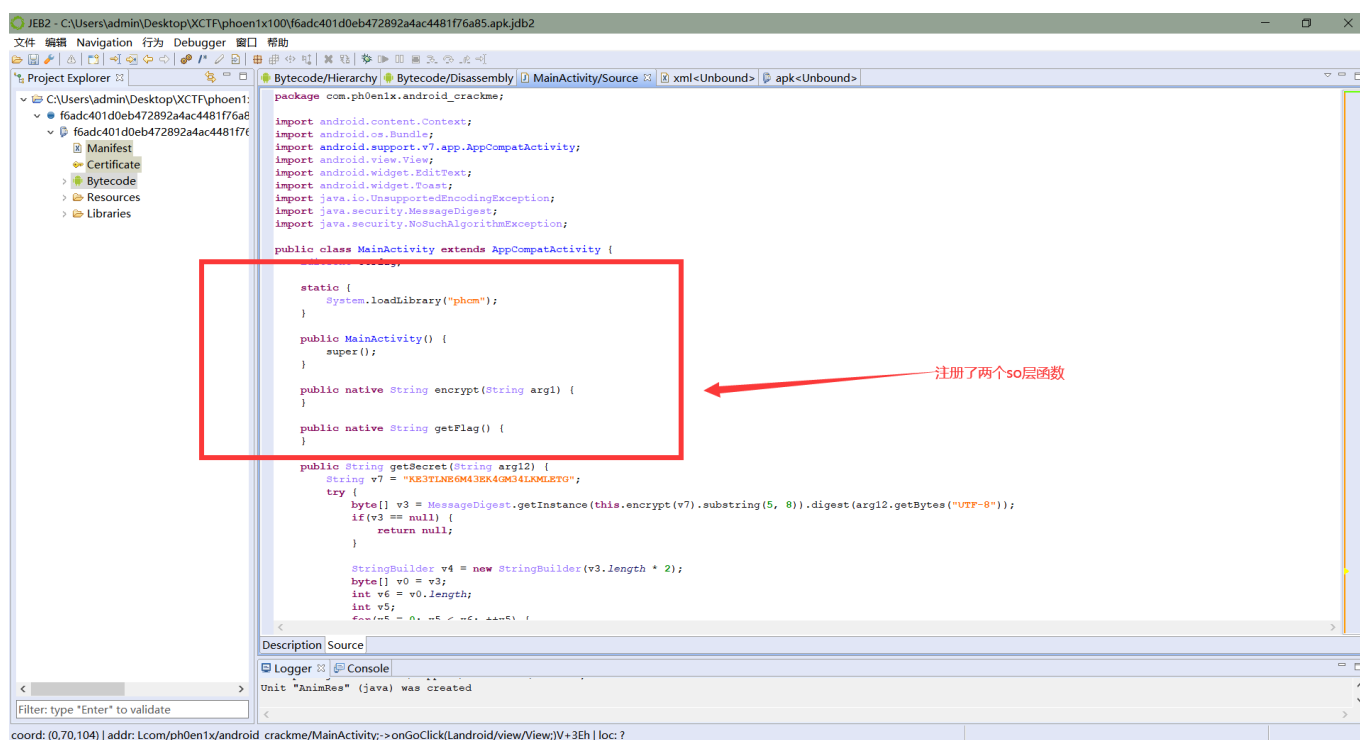
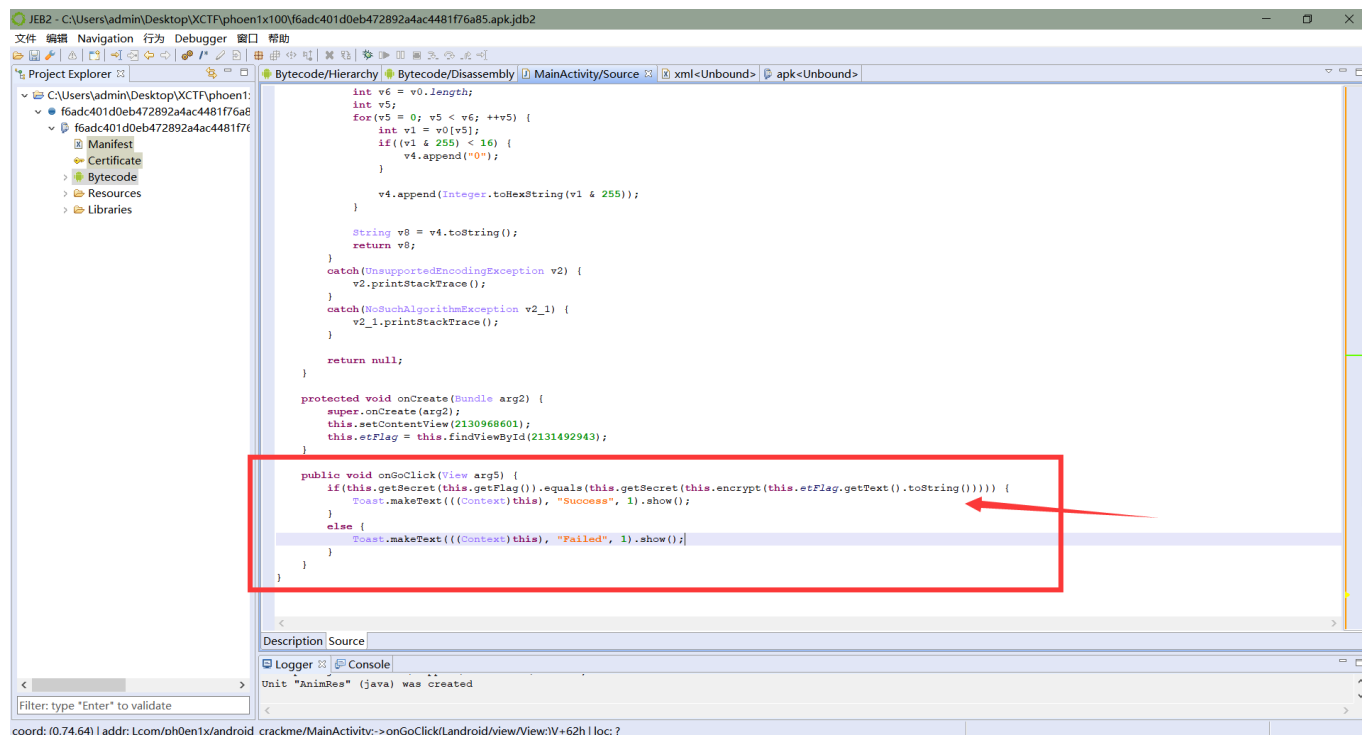


1、拖进夜神中安装运行，主界面只有一个输入框和一个按钮，随便输入信息，点击按钮后，弹出信息**Failed!**，如下图所示：

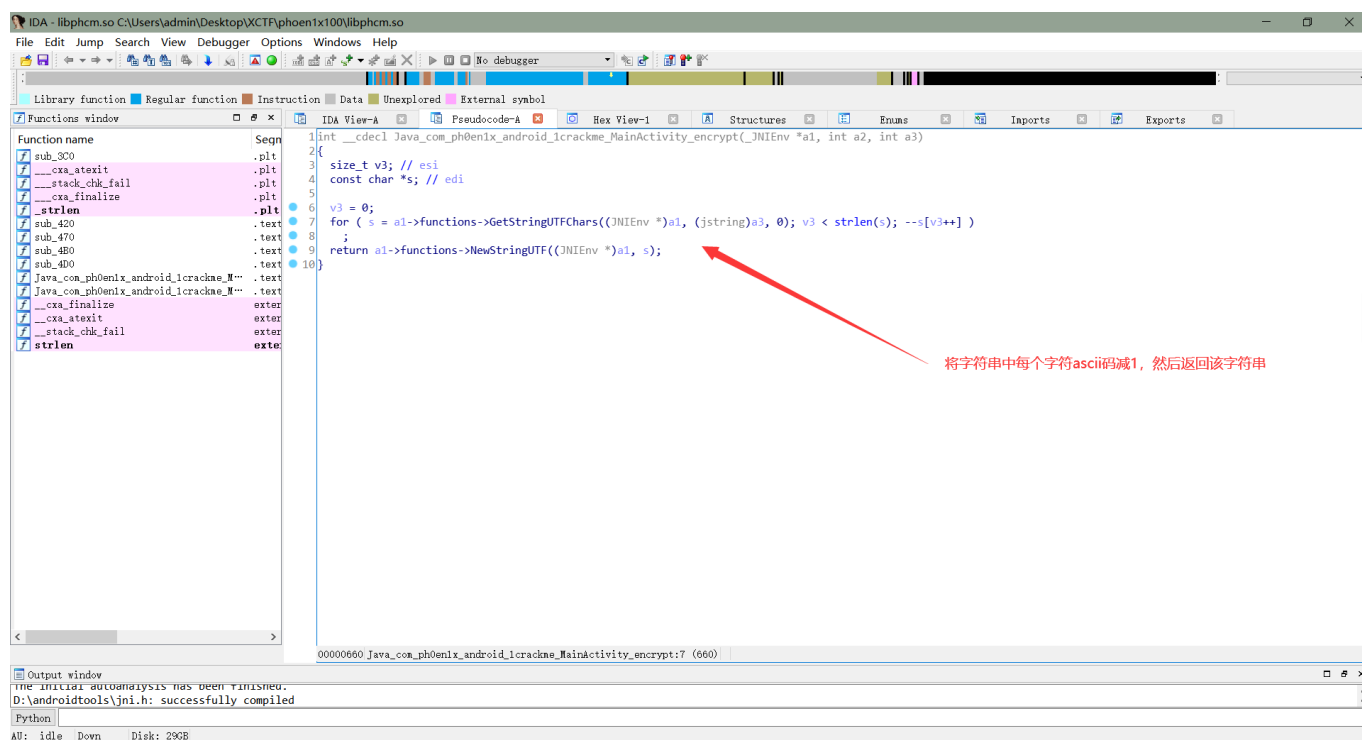


2、查壳后无壳直接使用JEB反编译，查看MainActivity.java文件，发现要弹出信息**Success**逻辑如下：首先在so层注册了两个静态函数--**encrypt(String)**、**getFlag()**函数，然后在java层有个函数**getSecret(String)**，将so层函数**getFlag**返回值经过**getSecret**函数加密后与我们在输入框中输入的字符串经过**encrypt**函数后在经过**getSecret**函数加密比较，如果一致，则返回**Success**，由于比较的两个字符串最外层都经过**getSecret**函数加密，所有我们不需要在管**getSecret**函数，直接让内部两个字符串一直一致即可得到**flag!!!**





3、使用IDA打开so文件，静态分析一下encrypt函数，发现逻辑很简单，就是将传进来的字符串的每个字符的ASCII码减一；对于getFlag函数，由于该函数没有输入只有输出，直接用frida Hook该函数得到返回值即可，如下图所示：



```

E: > py > frida > phcm.py > ...
1 import frida
2 import sys
3
4 jscode = """
5 Java.perform(function(){
6     Interceptor.attach(Module.findExportByName("libphcm.so", "Java_com_ph0enix_android_1crackme_MainActivity_getFlag"), {
7         onEnter: function(args) {
8         },
9         onLeave: function(retval){
10             var String_java = Java.use('java.lang.String');
11             var args_4 = Java.cast(retval, String_java);
12             send("getFlag()==>"+args_4);
13         }
14     });
15 });
16 """
17 def printMessage(message, data):
18     if message['type'] == 'send':
19         print('[*] {0}'.format(message['payload']))
20     else:
21         print(message)
22
23 process = frida.get_remote_device().attach('com.ph0enix.android_crackme')
24 script = process.create_script(jscode)

```

输出 终端 调试控制台 问题

PS C:\Users\admin> & D:/python3.7/python3.7.exe e:/py/frida/phcm.py  
[\*] getFlag()==>ek'fz@q2~x/c~fndmr~6/~rb qanqntfg~E hq]

getFlag函数的返回值

## Frida代码:

```

import frida
import sys

jscode = """
Java.perform(function(){

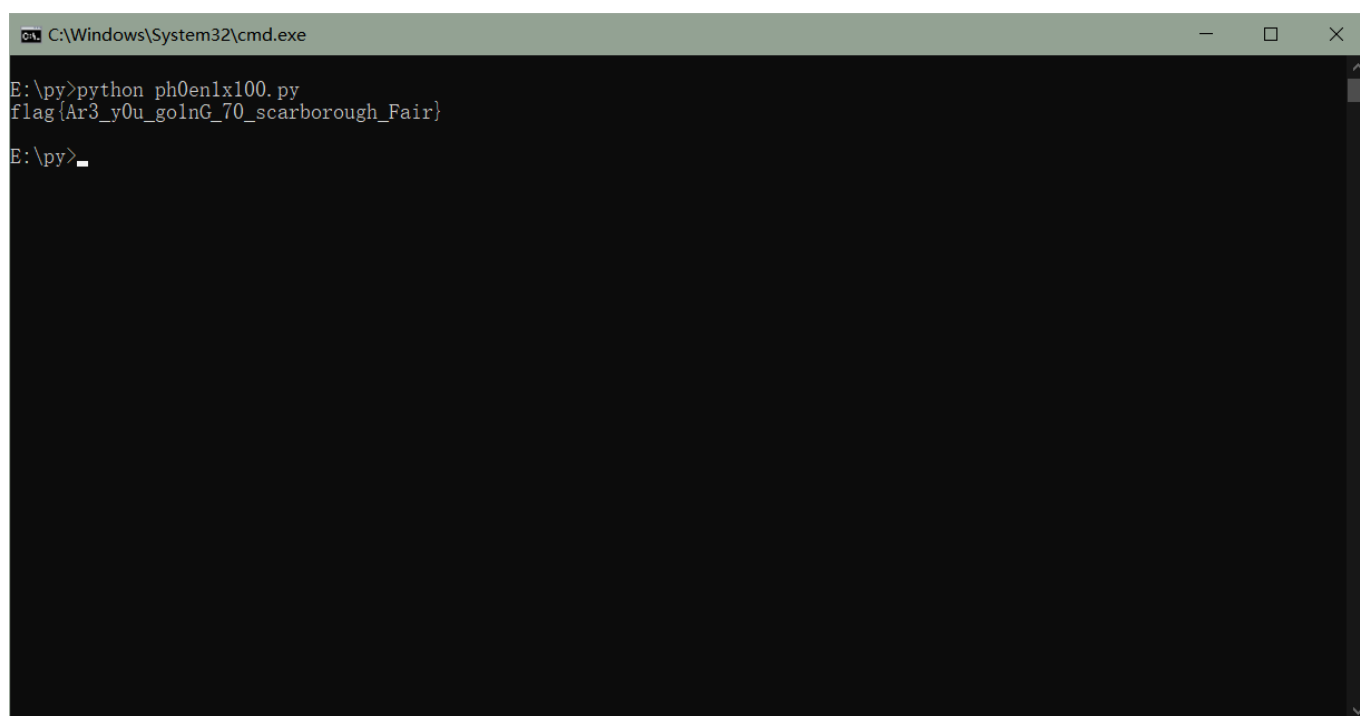
Interceptor.attach(Module.findExportByName("libphcm.so", "Java_com_ph0enix_android_1crackme_MainActivity_getFlag"), {
    onEnter: function(args) {
    },
    onLeave: function(retval){
        var String_java = Java.use('java.lang.String');
        var args_4 = Java.cast(retval, String_java);
        send("getFlag()==>"+args_4);
    }
});
});
"""

def printMessage(message, data):
    if message['type'] == 'send':
        print('[*] {0}'.format(message['payload']))
    else:
        print(message)

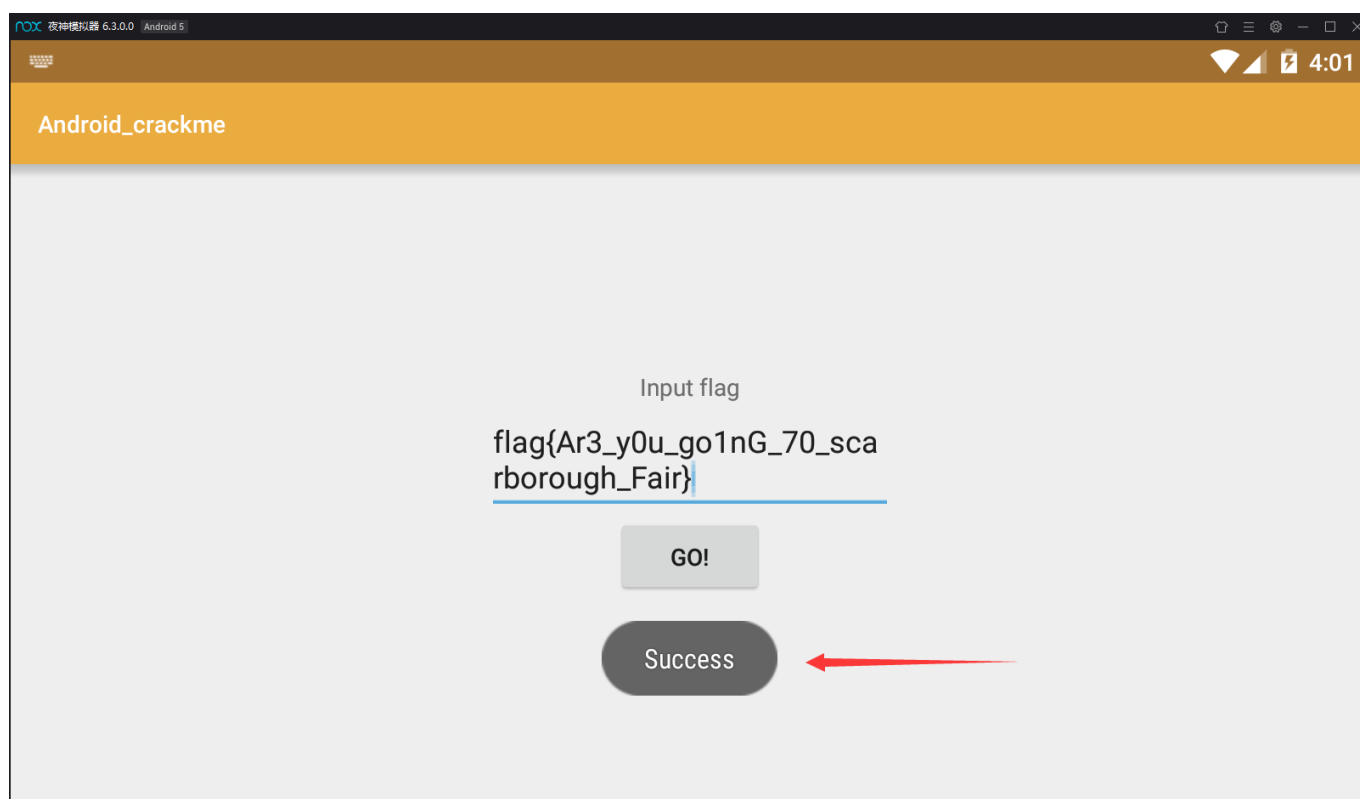
process = frida.get_remote_device().attach('com.ph0enix.android_crackme')
script = process.create_script(jscode)
script.on('message', printMessage)
script.load()
sys.stdin.read()

```

4、得到以上信息后，使用**python**脚本跑出**flag**即可，如下所示：



```
C:\Windows\System32\cmd.exe
E:\py>python ph0en1x100.py
flag{Ar3_y0u_g01nG_70_scarborough_Fair}
E:\py>
```



**python**脚本：

```
Flag = 'ek`fz@q2^x/t^fn0mF^6/^rb`qanqntfg^E`hq|'

flaglist = list(Flag)

stringlist = []
```

```
for ch in flaglist:
    stringlist.append(chr(ord(ch) + 1))

print(''.join(stringlist))
```