# XCTF MISC 高手区 stage1

原创

T0m0rrow 于 2021-01-07 16:41:45 发布 98 收藏

分类专栏： CTF



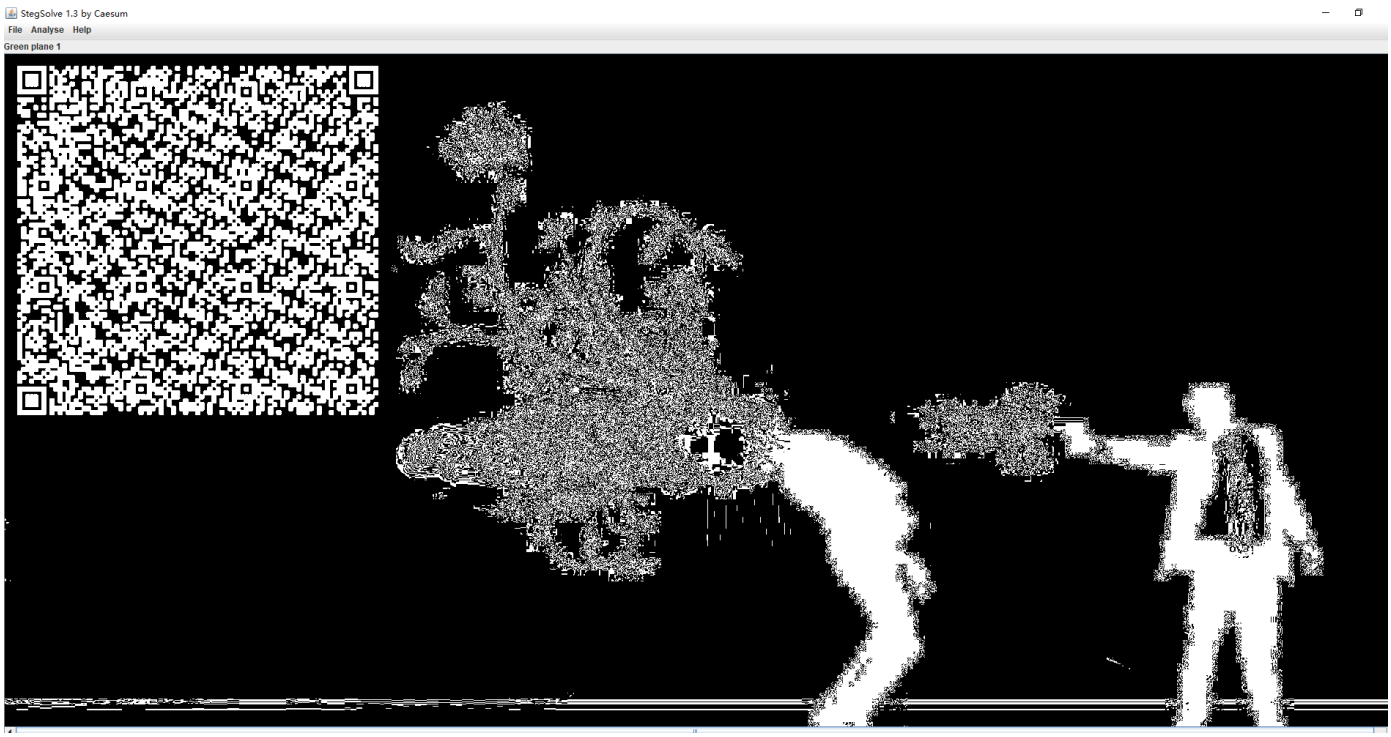
本文链接：https://blog.csdn.net/duwanglai/article/details/112318786





## stage1

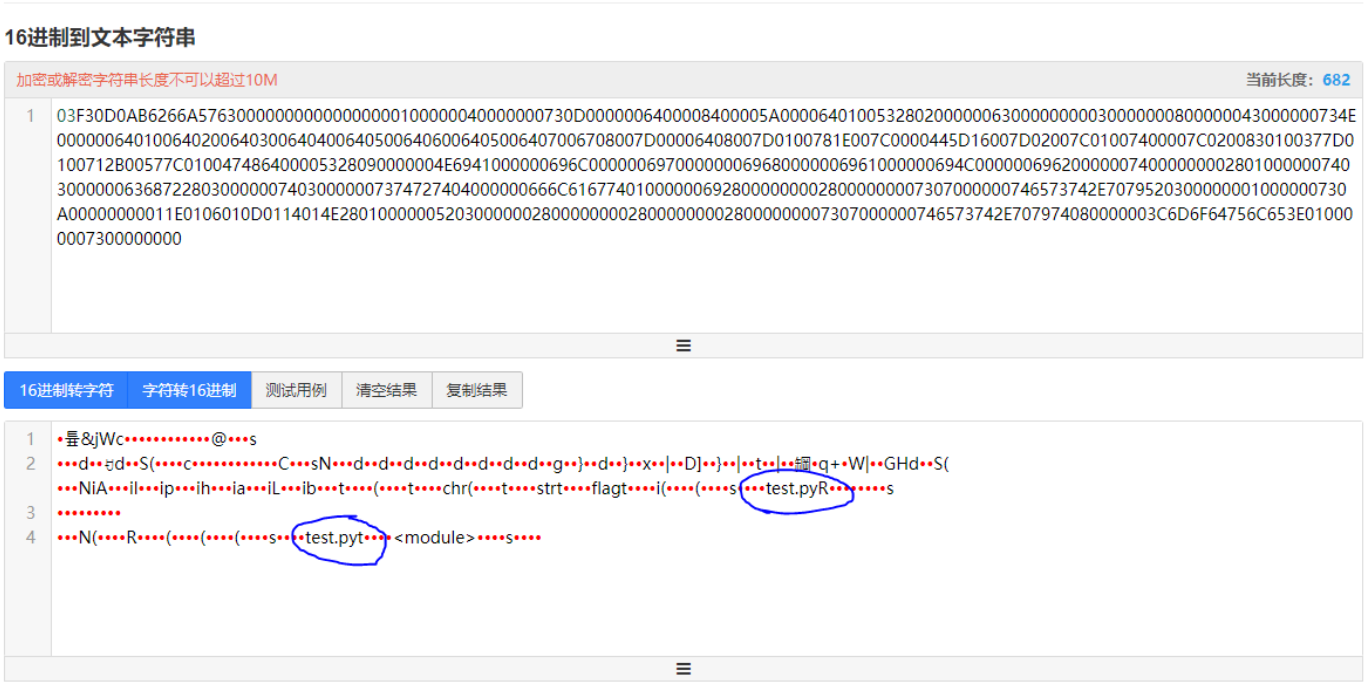
- 用 `stegsolve` 打开图片，左右切换，发现二维码



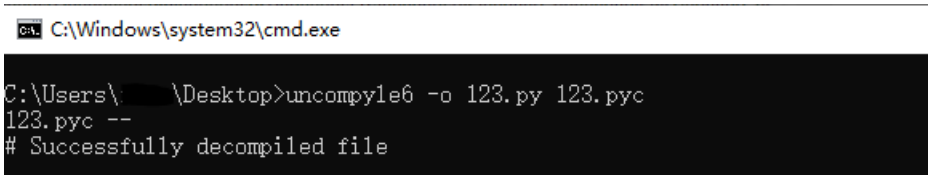

- 扫描得到一串十六进制编码

```
03F30D0AB6266A576300000000000000000100000040000000730D0000006400008400005A0000640100532802000000630000000
0030000000800000043000000734E0000006401006402006403006404006405006406006405006407006708007D00006408007D010
0781E007C0000445D16007D02007C01007400007C0200830100377D0100712B00577C0100474864000053280900000004E6941000
000696C0000006970000000696800000069610000006 94C0000006962000000740000000028010000007403000000636872280300
0007403000000737472740400000066 6C6167740100000069280000000028000000007307000000746573742E70795203000000010
00000730A00000000011E0106010D0114014E2801000000520300000028000000002800000000280000000073070000007465737 42
E707974080000003C6D6F64756C653E010000007300000000
```

- 尝试转换成字符串，显示乱码，但是其中包含test.py这几个字符




- 根据经验我们推断这可能是pyc文件。将这串编码用010editor保存为pyc文件，然后用`uncompyle6`反编译




- 反编译成功，打开py文件

```
6
7
8   def flag():
9       str = [
10          65, 108, 112, 104, 97, 76, 97, 98]
11      flag = ''
12      for i in str:
13          flag += chr(i)
14
15      print flag
```

- 调用flag函数得到flag

AlphaLab