

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



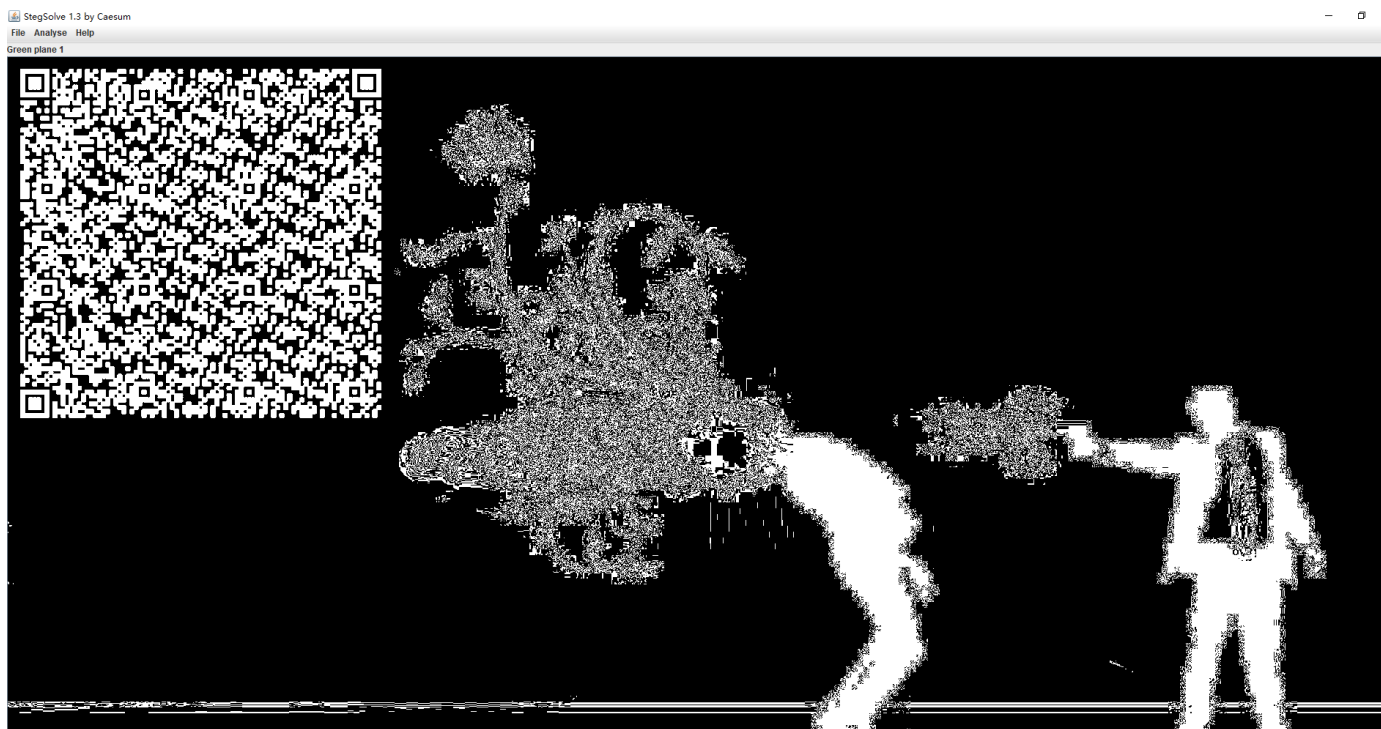
[CTF 专栏收录该内容](#)

31 篇文章 0 订阅

订阅专栏

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

```
03F3D0AB6266A57630000000000000000010000040000000730D0000006400008400005A0000640100532802000000630000000
0030000000800000043000000734E0000006401006402006403006404006405006406006407006708007D00006408007D010
0781E007C0000445D16007D02007C01007400007C0200830100377D0100712B00577C010047486400005328090000004E6941000
000696C000000697000000069680000006961000000694C00000069620000007400000000280100000074030000006368722803000
00074030000007374727404000000666C6167740100000069280000000028000000007307000000746573742E7079520300000010
0000730A0000000011E0106010D0114014E2801000005203000000280000000028000000002800000007307000000746573742
E707974080000003C6D6F64756C653E0100000730000000
```

- 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

16进制到文本字符串

加密或解密字符串长度不可以超过10M 当前长度: 682

```

1  03F30D0AB6266A5763000000000000000100000040000000730D0000006400008400005A00006401005328020000006300000000030000000800000043000000734E
0000006401006402006403006404006405006406006407006408007D00006408007D0100781E007C0000445D16007D02007C01007400007C0200830100377D0
100712B00577C010047486400005328090000004E6941000000696C000000697000000069680000006961000000694C000000696200000074000000002801000000740
3000000636872280300000074030000007374727404000000666C616774010000006928000000028000000007307000000746573742E7079520300000001000000730
A00000000011E0106010D0114014E280100000052030000002800000002800000002800000007307000000746573742E707974080000003C6D6F64756C653E01000
0007300000000
  
```

16进制转字符 字符转16进制 测试用例 清空结果 复制结果

```

1  暱&jWc.....@...s
2  ...d...d...S(...c.....C...sN...d...d...d...d...d...d...g...d...d...x...|...D...)|...t...|...q...+...W|...GHd...S(
...NiA...|...j...p...ih...ia...iL...ib...t...t...chr(...t...t...str...flag...t...|(...s...test.pyR...s
3  .....
4  ...N(...R...(...s...test.py...<module>...s...
  
```

- 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 uncomyle6 反编译

```

C:\Windows\system32\cmd.exe

C:\Users\... \Desktop>uncomyle6 -o 123.py 123.pyc
123.pyc --
# Successfully decompiled file
  
```

- 反编译成功，打开py文件

```

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

- 调用flag函数得到flag