# xctf攻防世界 MISC高手进阶区 适合作为桌面、stage1

原创

l8947943 于 2022-01-14 21:15:21 发布 5639 收藏

分类专栏： 攻防世界misc之路 文章标签： misc



本文链接：https://blog.csdn.net/l8947943/article/details/122502057





## 1. 进入环境，下载附件

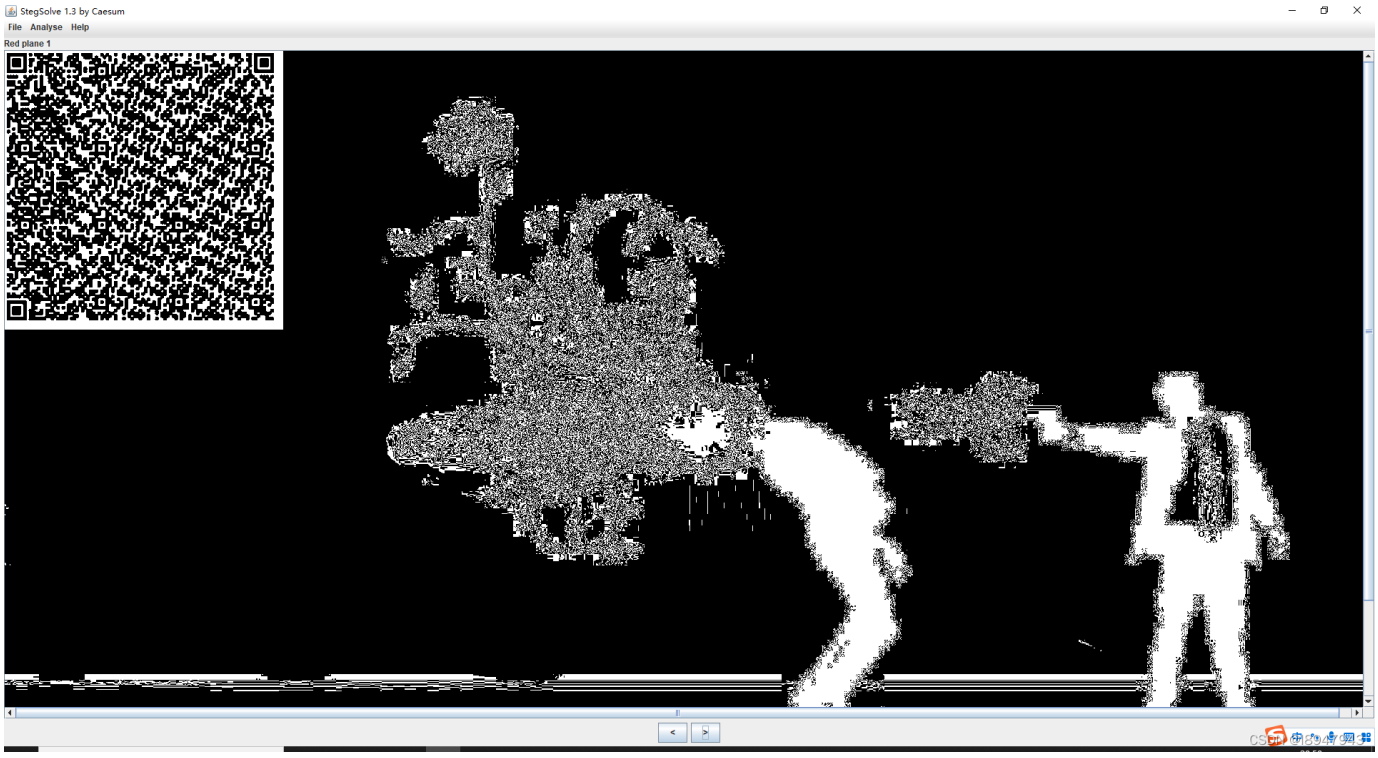
发现是一张png图片，如图：


妈的，有点酷，就是看不出信息

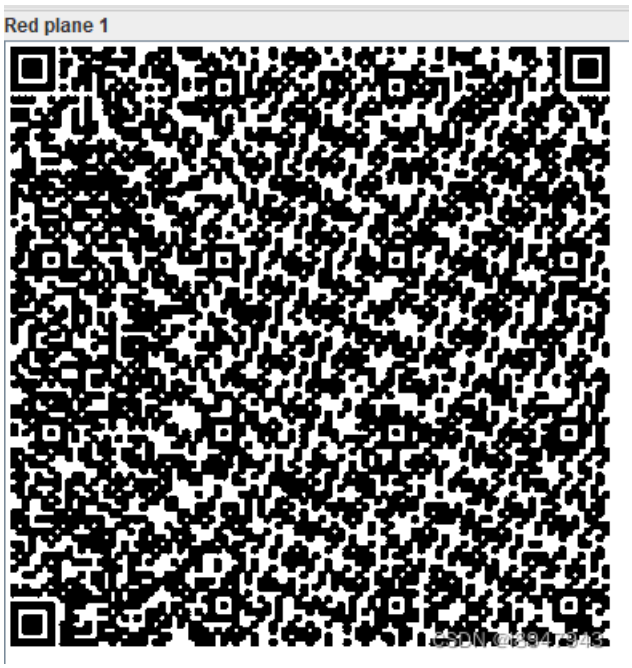
## 2.问题分析

### 尝试StegSolve

打开图片后一通乱翻，发现了一张二维码，如图：




放大：

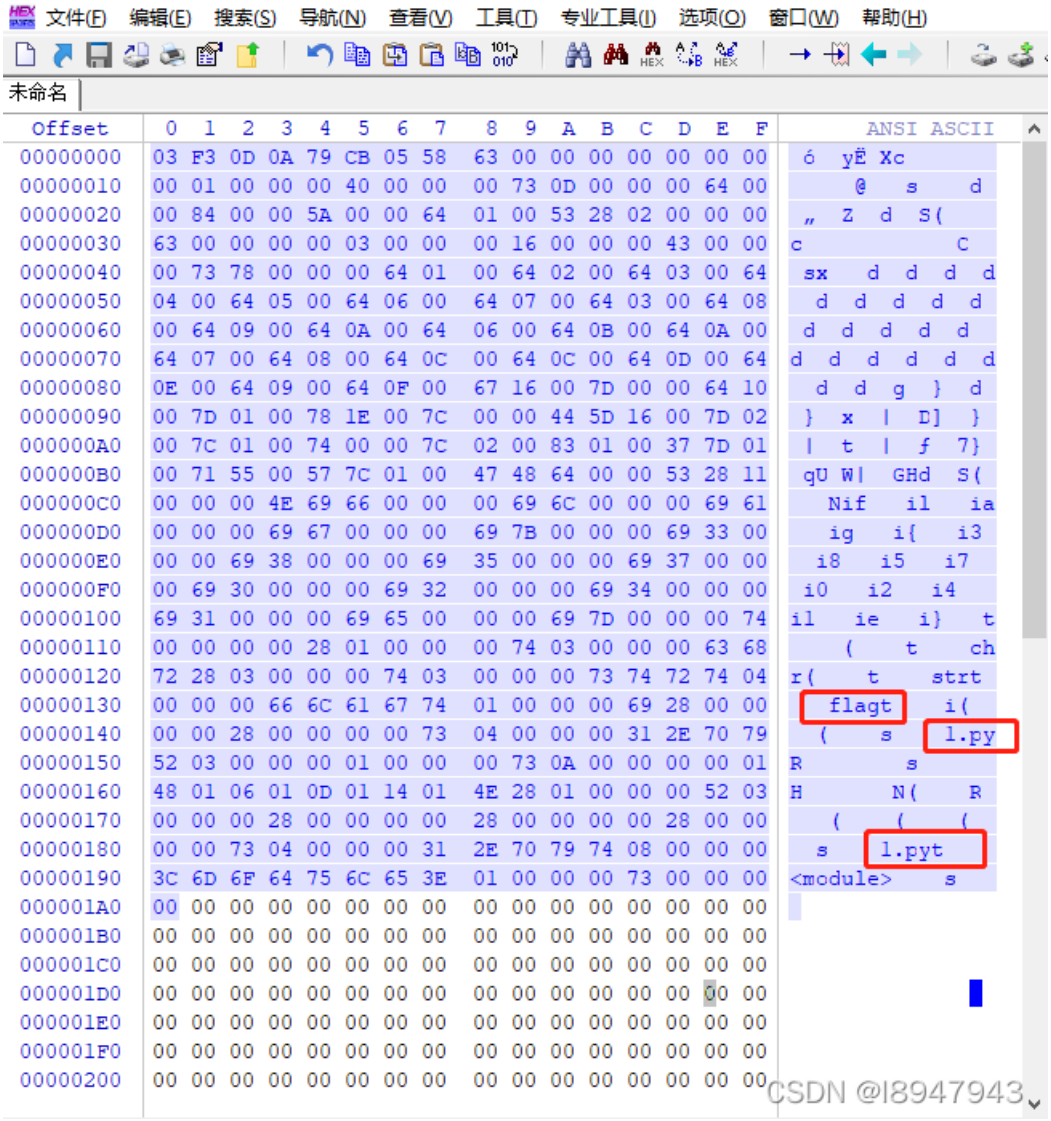



### 尝试转码

扫出来是一堆字符：

```
03F30D0A79CB055863000000000000000001000000400000007 30D0000006400008400005A0000640100532802000000630000000
0030000001600000043000000737800000064010064020064030064040064050064060064070064030064080064090064 0A0064060
0640B00640A00640700640800640C00640C00640D00640E00640900640F006716007D00006410007D0100781E007C0000445D160
07D02007C01007400007C0200830100377D0100715500577C0100474864000053281100000 04E6966000000696C00000069610000
006967000000697B0000006933000000693800000069350000006937000000693000000069320000006934000000693100000069 65
000000697D0000007400000000280100000074030000006368722803000000740300000073747274040000000666C61677401000000
692800000000280000000073040000003 12E70795203000000010000007 30A0000000001480106010D0114014E2801000000520300
0000280000000028000000002800000000730400000031 2E707974080000003C6D6F64756C653E010000007300000000
```

特征是从0-F，感觉是16进制文件，我们尝试扔到winhex中，看看这些是什么意思，如图：




可以看到有py和pyt文件，判断可能可以进行pyc反编译。**什么是pyc？传送门：https://www.yuanrenxue.com/tricks/what-is-pyc-file.html**

### 3. 反编译

打开conda环境，依次输入：

```
# 安装uncompyle包
pip install uncompyle
# 将res.pyc反编译成result.py
uncompyle6 res.pyc > result.py
```

反编译后的代码如下：

```
def flag():
    str = [
     102, 108, 97, 103, 123, 51, 56, 97, 53, 55, 48, 51, 50, 48, 56, 53, 52, 52, 49, 101, 55, 125]
    flag = ''
    for i in str:
        flag += chr(i)

    print flag
# okay decompiling res.pyc
```

运行一下呗：结果如图：


最终答案为：`flag{38a57032085441e7}`

stage1的最终答案为：`AlphaLab`