CTF 内涵的软件 stage1

原创

艺博东 于 2020-10-06 18:00:14 发布 10113 收藏 5
分类专栏： 网络攻防 文章标签： CTF

本文链接：https://blog.csdn.net/HYD696/article/details/108906098

文章目录

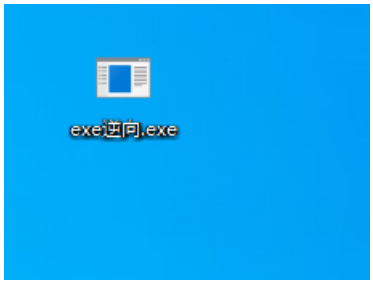
一、内涵的软件

题目描述： 图片有内涵，exe也可以有内涵，也许你等不到答案，赶快行动起来吧！！！(答案为flag{}形式，提交{}内内容即可)
题目附件： 附件1

1、附件1

链接：https://pan.baidu.com/s/1BzQc84cvoE0rA7pddlQrDw
提取码：pxxw

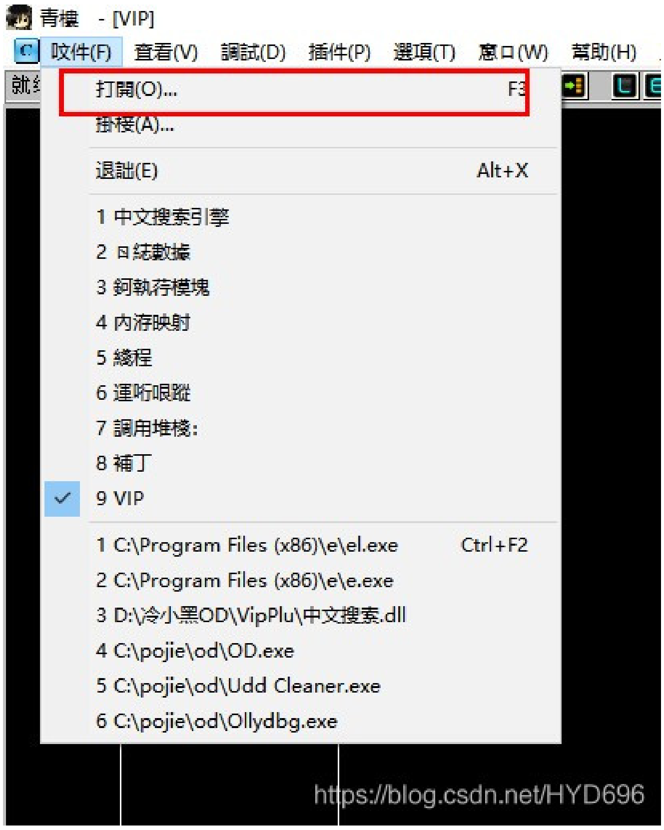
2、文件



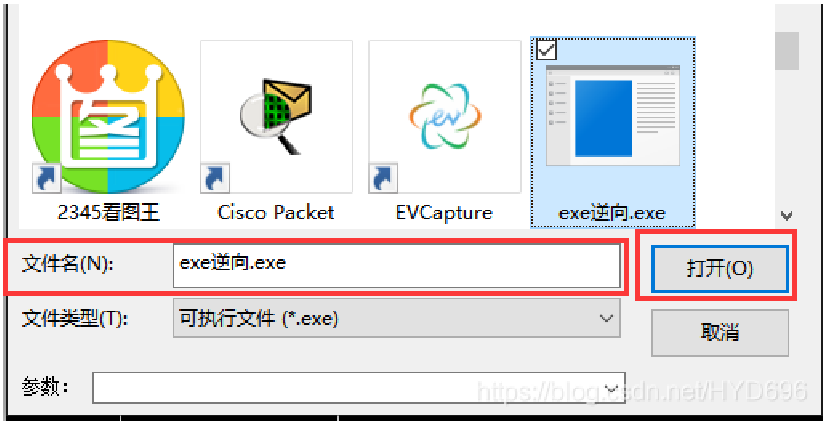
3、用逆向工具包打开程序查看源代码—>ollydbg


QQ交流群：985055356
ollydbg
C32Asm
exeinfope
PEID 9.5
提取文件
PUSH
FFI
Everything
替换图标
E-DEBUG
LordPE
ImportREC
版权修改器
窗口侦探
灰色按钮
录屏工具
软件手术刀
CE6.8
XH补丁
x64_dbg
进程信息
填写进程：
例如:QQ
获取的PID：
获取的句柄：
获取的地址：
获取信息
超级进程
获取句柄
注册机制作
抓包
软件逆向 软件加密防破解 Q929929496

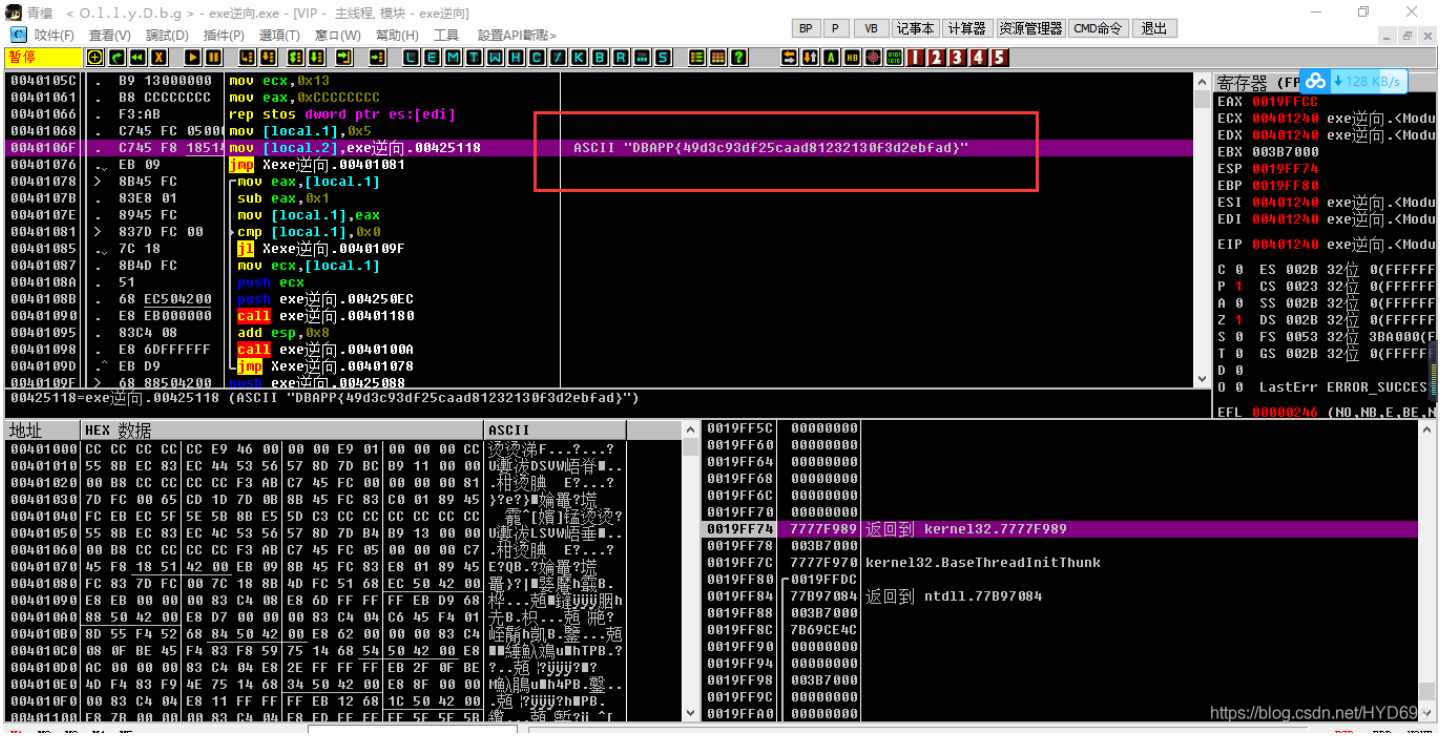
4、打开


青樓 - [VIP]
吹件(F)
查看(V)
調試(D)
插件(P)
選項(T)
窗口(W)
幫助(H)
打開(O)... F3
退出(E) Alt+X
1 中文搜索引擎
5 綫程
7 調用堆棧:
8 補丁
9 VIP
1 C:\Program Files (x86)\e\el.exe Ctrl+F2
2 C:\Program Files (x86)\e\e.exe
4 C:\pojie\od\OD.exe
5 C:\pojie\od\Udd Cleaner.exe
6 C:\pojie\od\Ollydbg.exe
https://blog.csdn.net/HYD696

5、文件名—>打开


2345看图王
Cisco Packet
EVCapture
exe逆向.exe
文件名(N):
exe逆向.exe
打开(O)
文件类型(T):
可执行文件 (*.exe)
取消
参数:
https://blog.csdn.net/HYD696

6、慢慢找



7、OK

DBAPP{49d3c93df25caad81232130f3d2ebfad}

49d3c93df25caad81232130f3d2ebfad

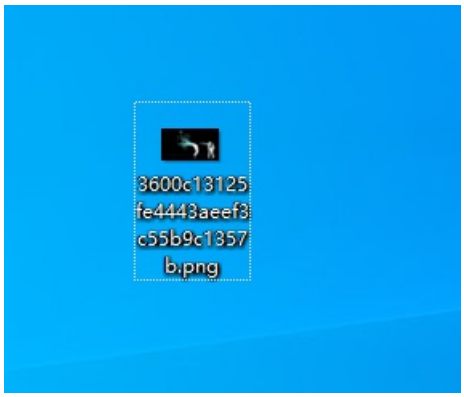
二、stage1

难度系数： ★★
题目来源： XCTF 3rd-GCTF-2017
题目附件： 附件1

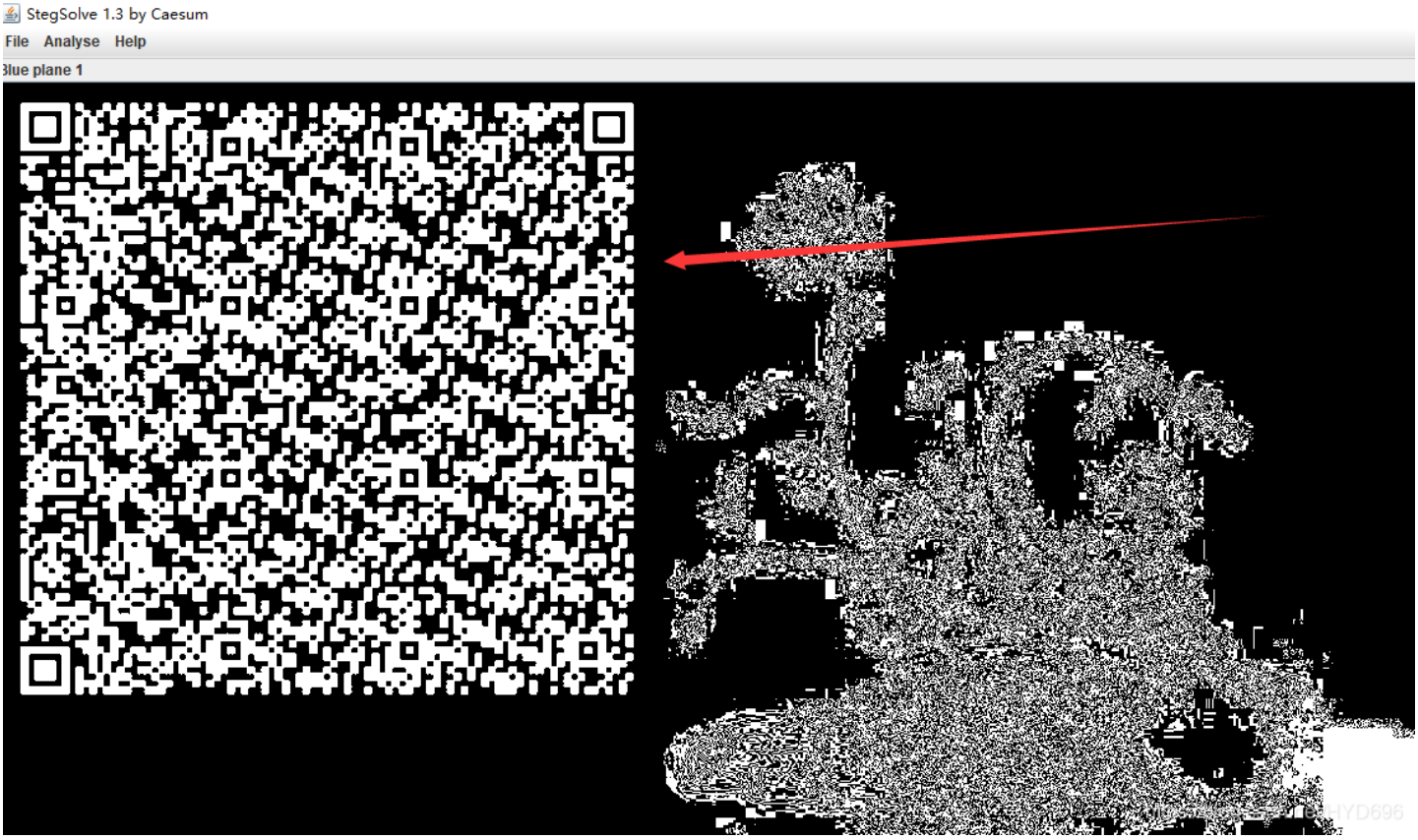
1、附件1

链接：https://pan.baidu.com/s/1FoDs-U4c-Ac5mjTpXmn_Mw
提取码：thyl

2、文件



3、用进 Stegsolve打开



然后出现了二维码

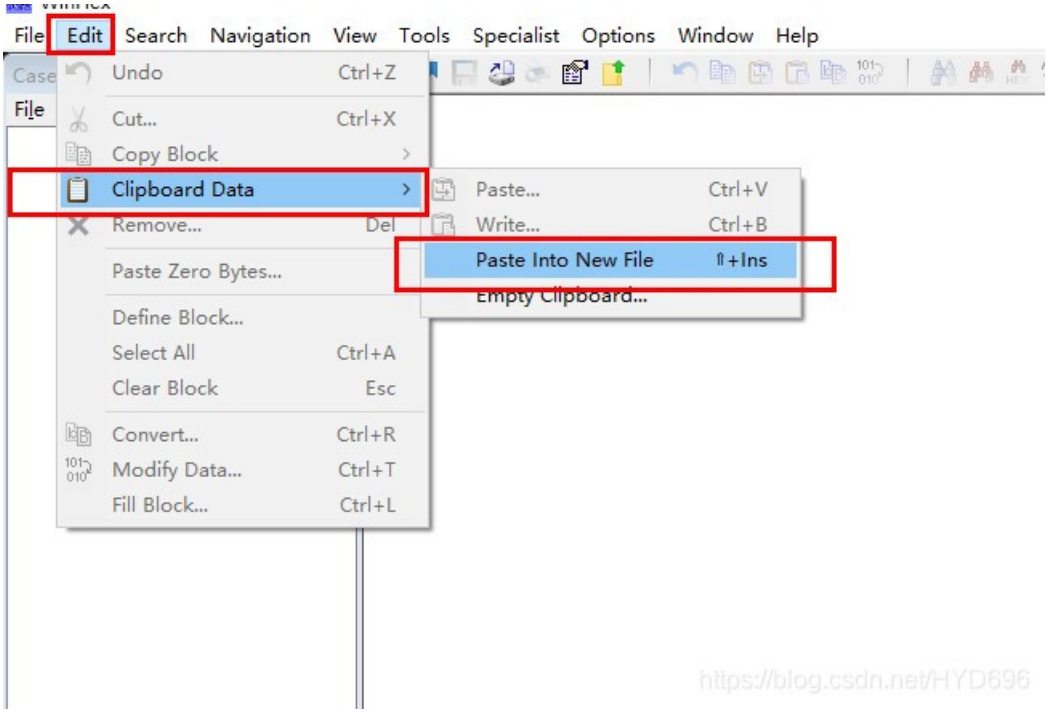
4、微信扫一扫

03F30D0AB6266A5763000000000000000001000

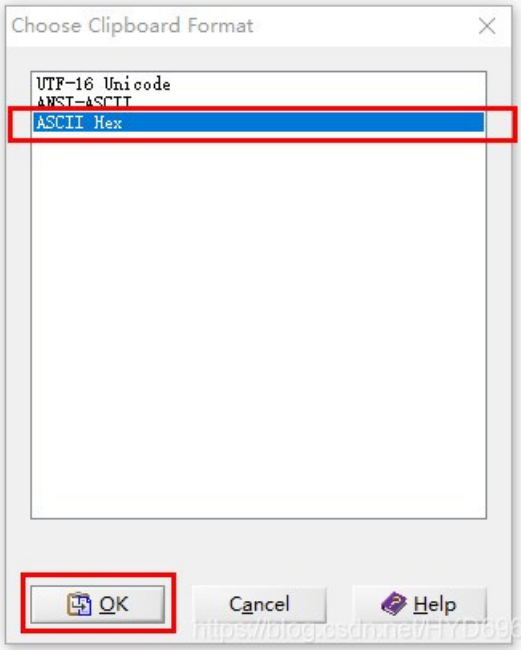
03F30D0AB6266A576300000000000000000010000004000000073 0D0000006400008400005A0000640100532802000000630000000030000000800000043000000734E0000006401006402006403006404006405006406006405006407006708007D00006408007D0100781E007C0000445D16007D02007C01007400007C0200830100377D0100712B00577C010047486400005328090000004E6941000000696C0000006970000000696800000069610000006 94C0000006962000000740000000028010000007403000000636872280300000074030000007374727404000000666C6167740100000069280000000028000000007307000000746573742E707952030000000100000073 0A00000000011E0106010D0114014E2801000000520300000028000000002800000000280000000073070000007465737 42E707974080000003C6D6F64756C653E010000007300000000

5、放入 WinHext 中，发现如下信息，将文件保存为.pyc 格式

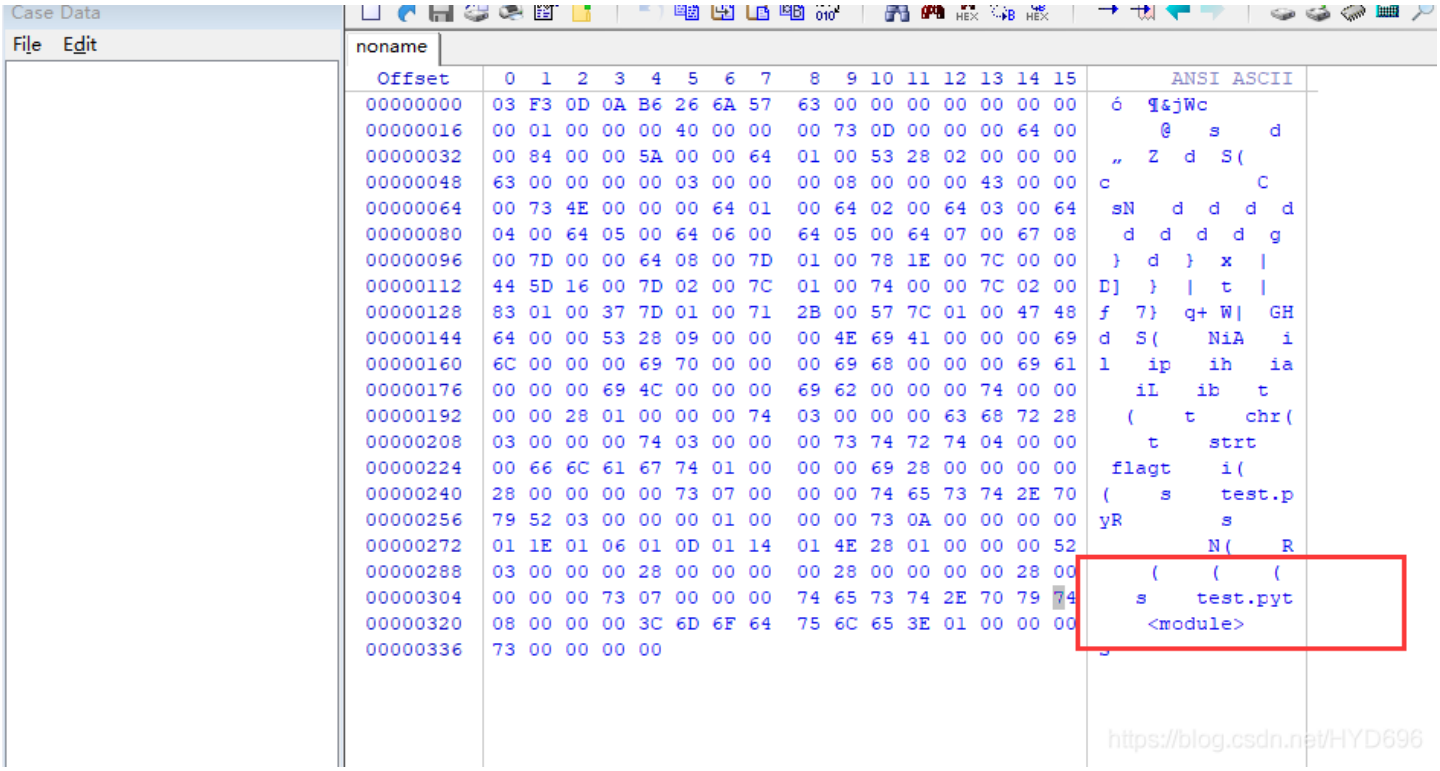
5.1 Edit—>Clipboard Data—>Paste Into New File



5.2 ASCII Hex—>OK

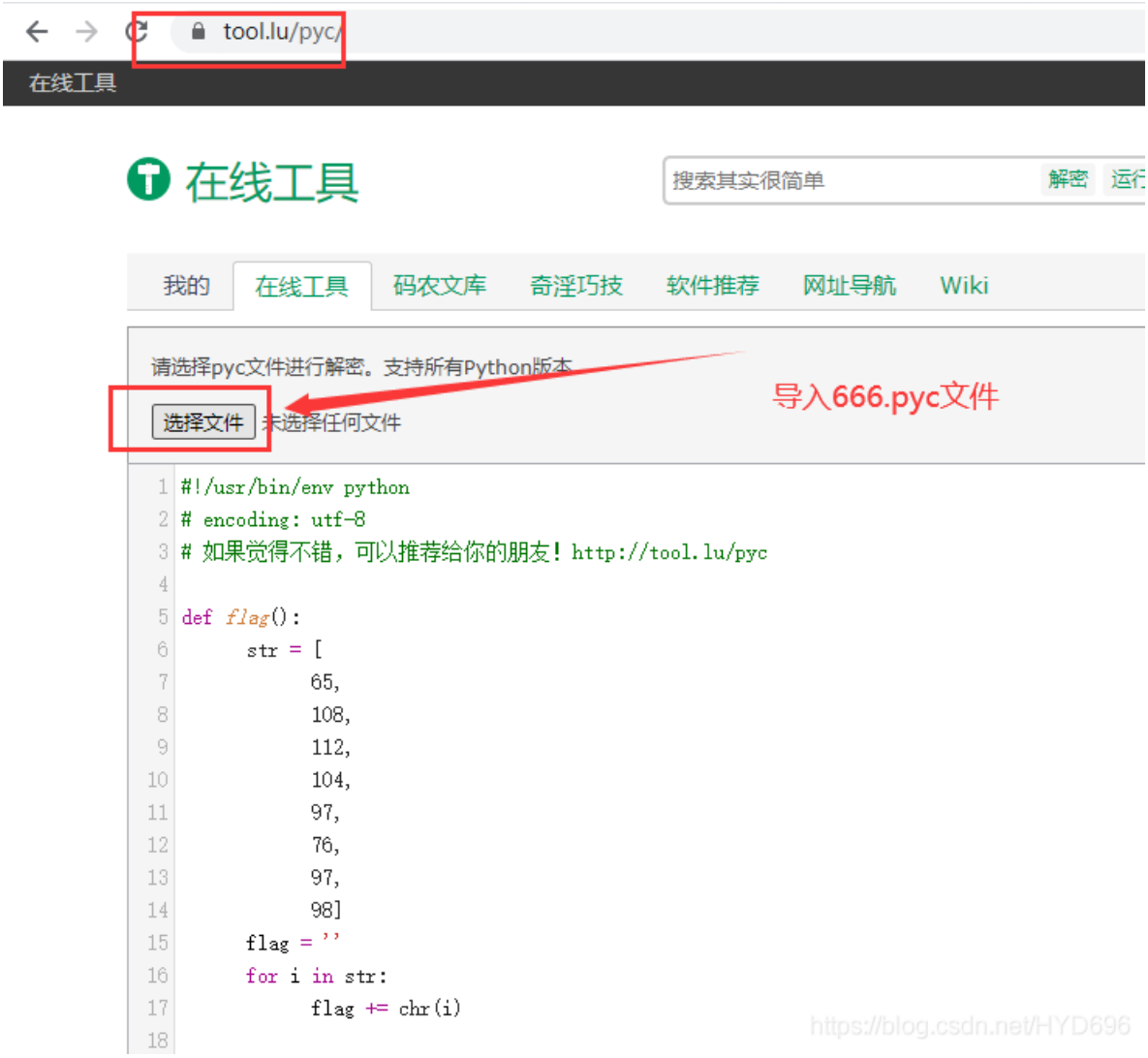


5.3 之后，提示是.pyt 文件—>是 python文件的编译文件，保存为 666.pyc 文件



6、反编译

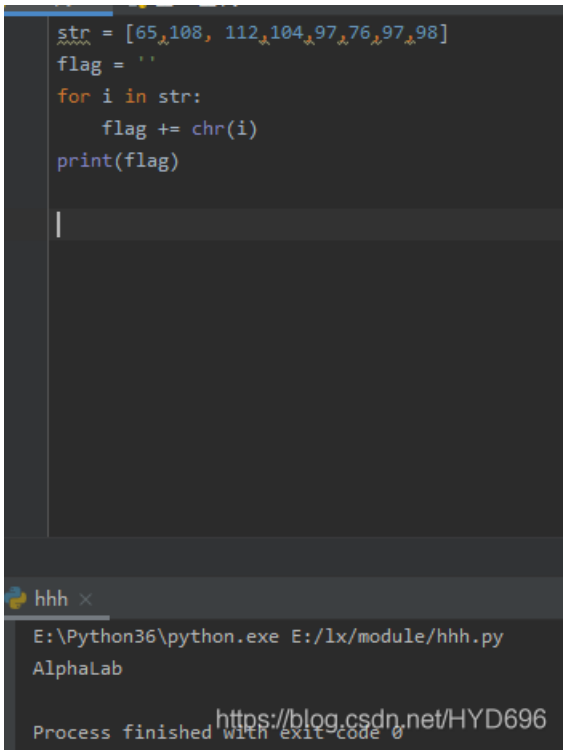
在线工具：https://tool.lu/pyc/



7、获得python脚本代码

```
str = [65,108, 112,104,97,76,97,98]
flag = ''
for i in str:
    flag += chr(i)
print(flag)
```

8、 python 环境运行得到flag



9、OK

AlphaLab