

使用 pyinstxtractor.py 将exe反编译

使用winhex修补文件头

使用uncompyle6将pyc文件反编译为py文件

```
ts2.txt ts1.txt ts3.txt new 1 emmmn.py
1 # uncompyle6 version 3.7.2
2 # Python bytecode 3.8 (3413)
3 # Decompiled from: Python 3.7.7 (tags/v3.7.7:d7c567b08f, Mar 10 2020, 10:41:24) [MSC v.1900 64 bit (AMD64)]
4 # Embedded file name: emmmn.py
5 # Compiled at: 1995-09-28 00:18:56
6 # Size of source mod 2**32: 272 bytes
7 import time
8 flag = 'bwl][lhE[-o3]pNh-Ac#aUIy'
9
10 def change_a(fstr):
11     temp = ''
12     for i in fstr:
13         temp += chr(ord(i) - 4)
14
15     return temp
16
17
18 def change_b(origin):
19     temp = ''
20     Num = 4
21     num = len(origin) // Num
22     for i in range(Num):
23         for j in range(num):
24             temp += origin[(j * Num + i)]
25
26     return temp
27
28
29 if __name__ == '__main__':
30     user_input = input('Please enter the flag: ')
31     print('emmmn, Let me check', end='', flush=True)
32     for i in range(3):
33         print('.', end='', flush=True)
34         time.sleep(1)
35
36     print('.', end='', flush=True)
37     user_input = change_a(user_input)
38     time.sleep(1)
39     print('.', end='', flush=True)
40     user_input = change_b(user_input)
41     time.sleep(1)
42     print('.', flush=True)
43     fflag = 1
44     for i in range(0, len(user_input)):
45         if ord(user_input[i]) != ord(flag[i]):
46             print("No, it's wrong.")
47             fflag = 0
```

解题脚本

```
1
2 def de1(flag):
3     temp = ""
4     n = 0
5     Num = 4
6     num = len(flag)//Num
7     while n < num:
```

```
8         for i in range(0,len(flag),num):
9             if (n+i) < len(flag):
10                 temp += flag[n+i]
11             n = n + 1
12         return temp
13
14
15 def de2(flag):
16     temp = ""
17     for i in flag:
18         temp += chr(ord(i)+4)
19     return temp
20
21
22 flag = "bw1][lhE[-o3]pNh-Ac#aUIy"
23 flag = de2(flag)
24 flag = de1(flag)
25 print(flag)
26
27 # flag{It'5_Rea1lY_s1Mp7E}
```