签退问卷

填写问卷拿分

玩蛇2.0

死亡后F12查看源码
搜索flag

```
t-1].y==foody) { addfood(); snakeCount++; snake.unshift(
.') //真正的flag: VYctf{Y0u_4re_the_m45ter_0f_JS}') } } }
y>585||snake[snakeCount-1].x<0||snake[snakeCount-1].y<0)
```

玩蛇(签到)

死亡后F12查看源码
搜索flag

```
alert('恭喜你拿到了flag: VYctf{Pyth0n_15_thE_be5t_L4ngu4ge}') } } }
Count-1].y>585||snake[snakeCount-1].x<0||snake[snakeCount-1].y<0)
```

小恐龙

F12查看源码
一眼顶针

```
▼<div class="flag"> flex
  ▶<li style="color: #89504e">···</li>
  ▶<li style="color: #470d0a">···</li>
  ▶<li style="color: #1a0a00">···</li>
  ▶<li style="color: #00000d">···</li>
  ▶<li style="color: #494844">···</li>
  ▶<li style="color: #520000">···</li>
  ▶<li style="color: #001d00">···</li>
```
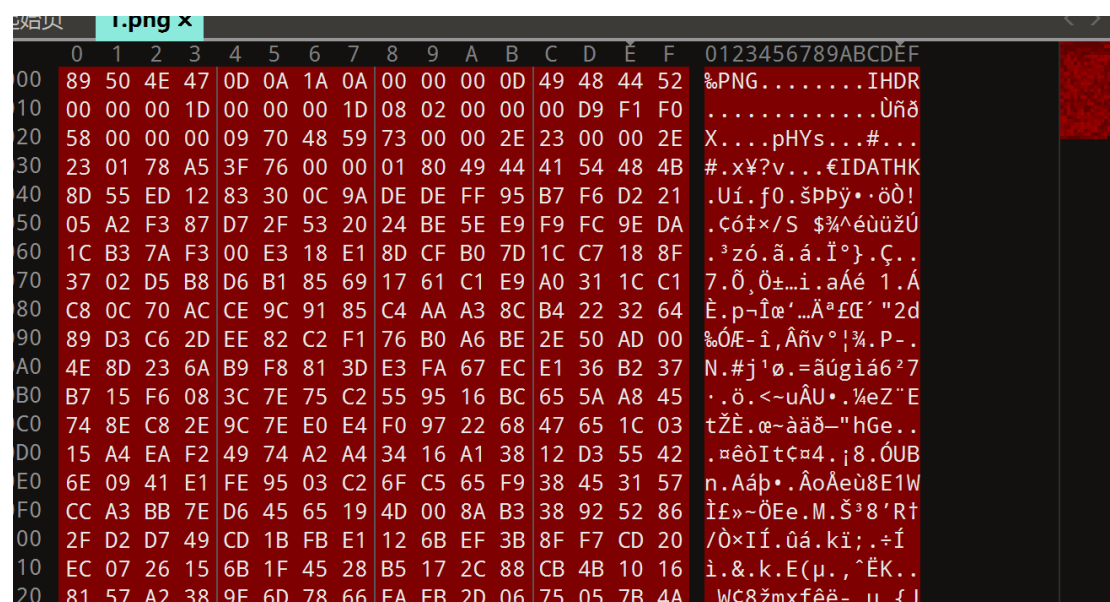
89504e47 PNG图片格式开头
提取出来

89504e470d0a1a0a0000000d494844520000001d0000001d0802000000d9f1f058000000097048
597300002e2300002e230178a53f760000018049444154484b8d55ed1283300c9adedeff95b7f6d
22105a2f387d72f532024be5ee9f9fc9eda1cb37af300e318e18dcfb07d1cc7188f3702d5b8d6b185
691761c1e9a0311cc1c80c70acce9c9185c4aaa38cb422326489d3c62dee82c2f176b0a6be2e50ad
004e8d236ab9f8813de3fa67ece136b237b715f6083c7e75c2559516bc655aa845748ec82e9c7ee0
e4f097226847651c0315a4eaf24974a2a43416a13812d355426e0941e1fe9503c26fc565f9384531
57cca3bb7ed64565194d008ab3389252862fd2d749cd1bfbe1126bef3b8ff7cd20ec0726156b1f45
28b5172c88cb4b10168157a2389e6d7866eaeb2d0675057b4a0988eb016863890e104fb39a6c61
3fbcc117e24e0daee20614cb8165bcba09227a13f09a86dffd82e548a1c3de82b5a5f0e10a2677d39
2aebb99917489ce36b2defe8f852017b717ba94dc9ab2149c1cb7737474cce1fabff9859dee2c0b57
5dad6f2adfe095fbd8cbd8f2121d5beb3fcf86e7ec0bead81585c1ea8b5172d4b1ef82a9df814e3bb
efa0201257ae732ac524a0000000049454e44ae426082

导入010

查看为二维码扫码可有

已解码数据 1:

位置:(2.1,6.1)-(45.7,6.2)-(2.2,49.7)-(45.7,49.7)
颜色正常,正像
版本:3
纠错等级:M,掩码:0
内容:
VYctf{fxxk_met4redctf_2023}
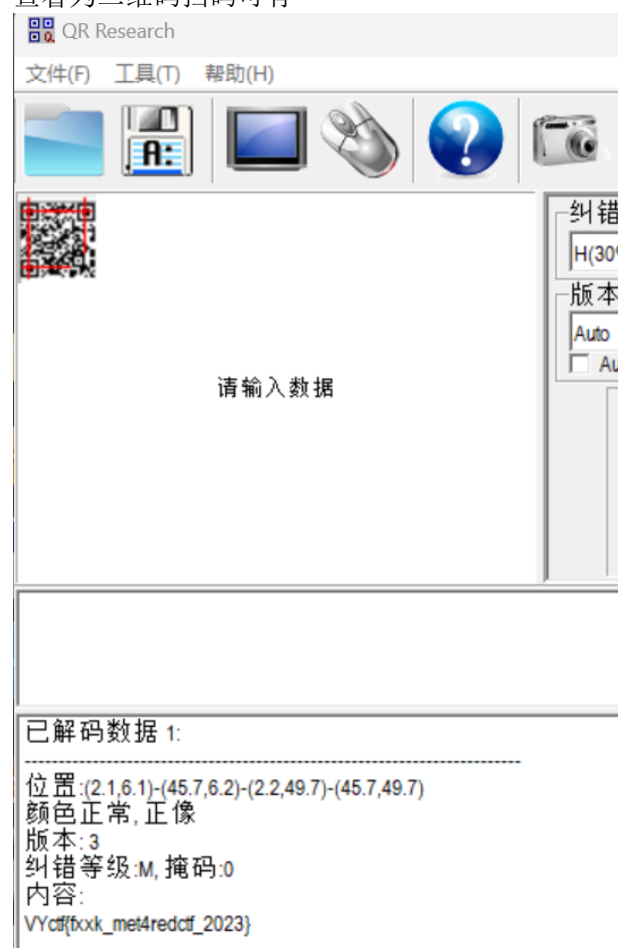
拿到flag

这亦是一种图片

```
┌──(root💀LAPTOP-J00D0L02)-[/mnt/c/Users/ASUA/Desktop]
└─# xxd -b xxd.png
00000000: 10001001 01010000 01001110 01000111 00001101 00001010  .PNG..
00000006: 00011010 00001010 00000000 00000000 00000000 00001101  ......
0000000c: 01001001 01001000 01000100 01010010 00000000 00000000  IHDR..
00000012: 00000011 11100000 00000000 00000000 00000000 00000000  ......
00000018: 00000000 00011111 10000000 00000000 00000000 00000000  ......
0000001e: 00000000 00000000 01111111 11100000 00000000 00000000  ......
00000024: 00000000 00000000 00000000 00011111 11100000 00000000  ......
0000002a: 00000000 00000000 00000000 00000000 01110000 00000000  ....p.
00000030: 00000000 00000000 00000000 00000001 11000000 00000000  ......
00000036: 00000000 00000000 00000000 11111110 00000000 00000000  ......
0000003c: 00000000 00000000 00011111 00000000 00000000 00000000  ......
00000042: 00000000 00000001 11110000 00000000 00000000 00000000  ......
00000048: 00000000 00111111 00000000 00000000 00000000 00000000  .?....
0000004e: 00000001 11100000 00000000 00000000 00000000 00000000  ......
00000054: 00000000 00000000 00000000 00000000 00000000 00000000  ......
0000005a: 00000000 00000000 00000000 00000000 00000000 00000000  ......
00000060: 00000001 11000000 00000000 00000000 00000000 00000000  ......
00000066: 00000000 00111100 00000000 00000000 00000000 00000000  .<....
0000006c: 00000000 00000111 10000000 00000000 00000000 00000000  ......
00000072: 00000000 00000000 11111111 11111111 11100000 00000000  ......
```
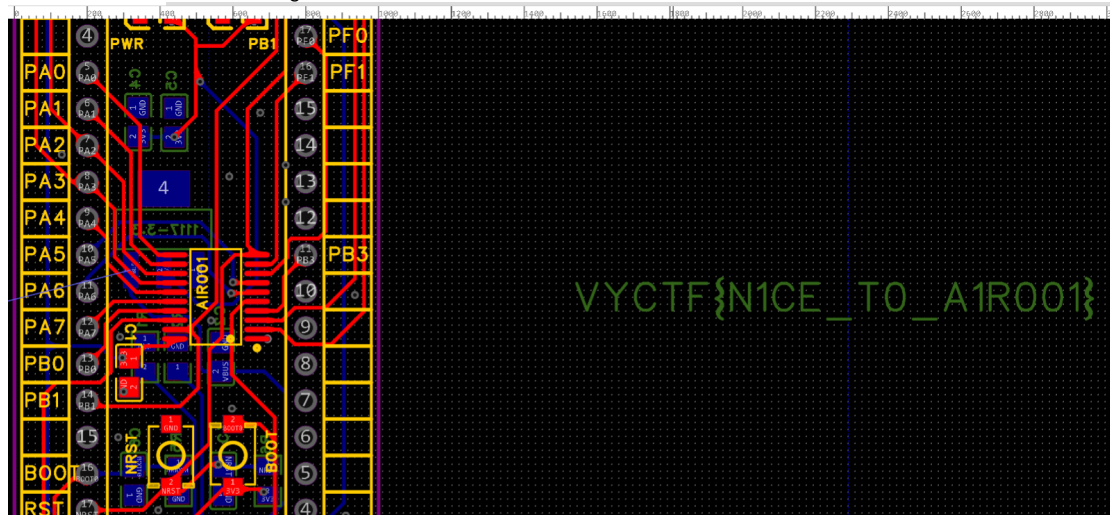
该说不说，确实有点费眼睛。

缺少的专辑(签到)

Png图片还原宽高即可
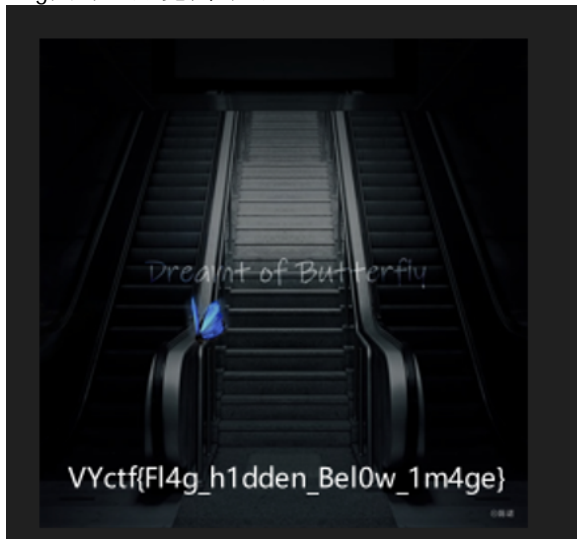
雪(snow)

一步搞定

Air001

嘉立创打开即可得到flag

简单ino(签到)

打开看到flag数组，此时考虑数字转ASCII码

```
int flag[20] = {118, 121, 995, 116, 102, 123, 104, 101, 492, 108, 482, 95,
  65, 114, 100, 117, 493, 110, 482, 125};
```

118-v 121-y 以此类推 995取前两位99-c即可得到flag

大家一起和平地玩耍吧(签到)

签到没写出来，靠玩过关的，有点丢人了

毁灭与重生 (DEBUG)

恭喜通关demo，前面的剧情开发组

少女折寿中ing

按下'回到菜单'可回到主界面重新

VYctf{We1c0me_t0_VycTf}

别管，出flag了就行

base64逆向



```
.rdata:00403106                 db    0
.rdata:00403107                 db    0
.rdata:00403108 ; const struct _EXCEPTION_POINTERS ExceptionInfo
.rdata:00403108 ExceptionInfo   _EXCEPTION_POINTERS <offset dword_404018, offset dword_404068>
.rdata:00403108                                      ; DATA XREF: sub_4012E9+EE↑o
.rdata:00403108                                      ; sub_4013EF+C3↑o
.rdata:00403110 aDnljdgz7vzmxyz db 'dnljdGZ7VzMxYzBtM183MF92eWM3Zn0=',0
.rdata:00403110                                      ; DATA XREF: _main+94↑o
.rdata:00403131                 align 4
.rdata:00403134 ; const char Format[]
.rdata:00403134 Format          db 'please input flag:',0
.rdata:00403134                                      ; DATA XREF: _main+13↑o
.rdata:00403147                 align 4
.rdata:00403148 ; const char Control[]
.rdata:00403148 Control         db 0Ah,0              ; DATA XREF: _main+3E↑o
.rdata:0040314A                 align 4
.rdata:0040314C ; const char aSuccess[]
.rdata:0040314C aSuccess        db 'success',0Ah,0    ; DATA XREF: _main+C7↑o
.rdata:00403155                 align 4
.rdata:00403158 aError          db 'error',0Ah,0      ; DATA XREF: _main+CC↑o
.rdata:0040315F                 align 10h
.rdata:00403160 byte_403160     db 41h                ; DATA XREF: sub_401040+7D↑r
.rdata:00403160                                      ; sub_401040+89↑r ...
.rdata:00403161 aBcdefghijklmno db 'BCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/',0
```

根据题目有一眼等号base64
解码有

dnljdGZ7VzMxYzBtM183MF92eWM3Zn0=

二进制
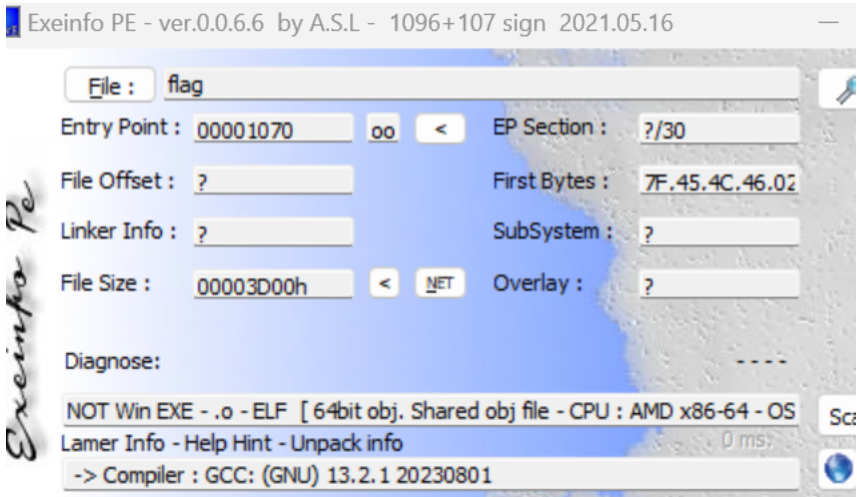
IDA64打开

```
1 __int64 __fastcall shl_flag(int a1)
2 {
3   return (unsigned int)(a1 >> 1);
4 }
```

右移1位，即除2即可
```
v8 = __readfsqword(0x28u);
v6[0] = 236;
v6[1] = 242;
v6[2] = 198;
v6[3] = 232;
v6[4] = 204;
v6[5] = 246;
v6[6] = 166;
v6[7] = 208;
v6[8] = 216;
v6[9] = 190;
v6[10] = 98;
v6[11] = 230;
v6[12] = 190;
v6[13] = 154;
v6[14] = 96;
v6[15] = 236;
v6[16] = 202;
v6[17] = 190;
v6[18] = 232;
v6[19] = 208;
v6[20] = 202;
v6[21] = 190;
v6[22] = 196;
v6[23] = 98;
v6[24] = 220;
v6[25] = 104;
v6[26] = 228;
v6[27] = 242;
v6[28] = 190;
v6[29] = 232;
v6[30] = 96;
v6[31] = 190;
v6[32] = 232;
v6[33] = 208;
v6[34] = 202;
v6[35] = 190;
v6[36] = 216;
v6[37] = 202;
```
除2以后转ASCII码即为flag
懒得写脚本，直接换了

素数分解

```
# 已知的值
P = 17
Q = 163
D = 1111
N = P * Q

\# 解密函数
def rsa_decrypt(ciphertext, D, N):
    plaintext = ""
    for char in ciphertext:
        num = ord(char)
        m = pow(num, D, N)
        plaintext += chr(m)
```

return plaintext

\# 读取密文
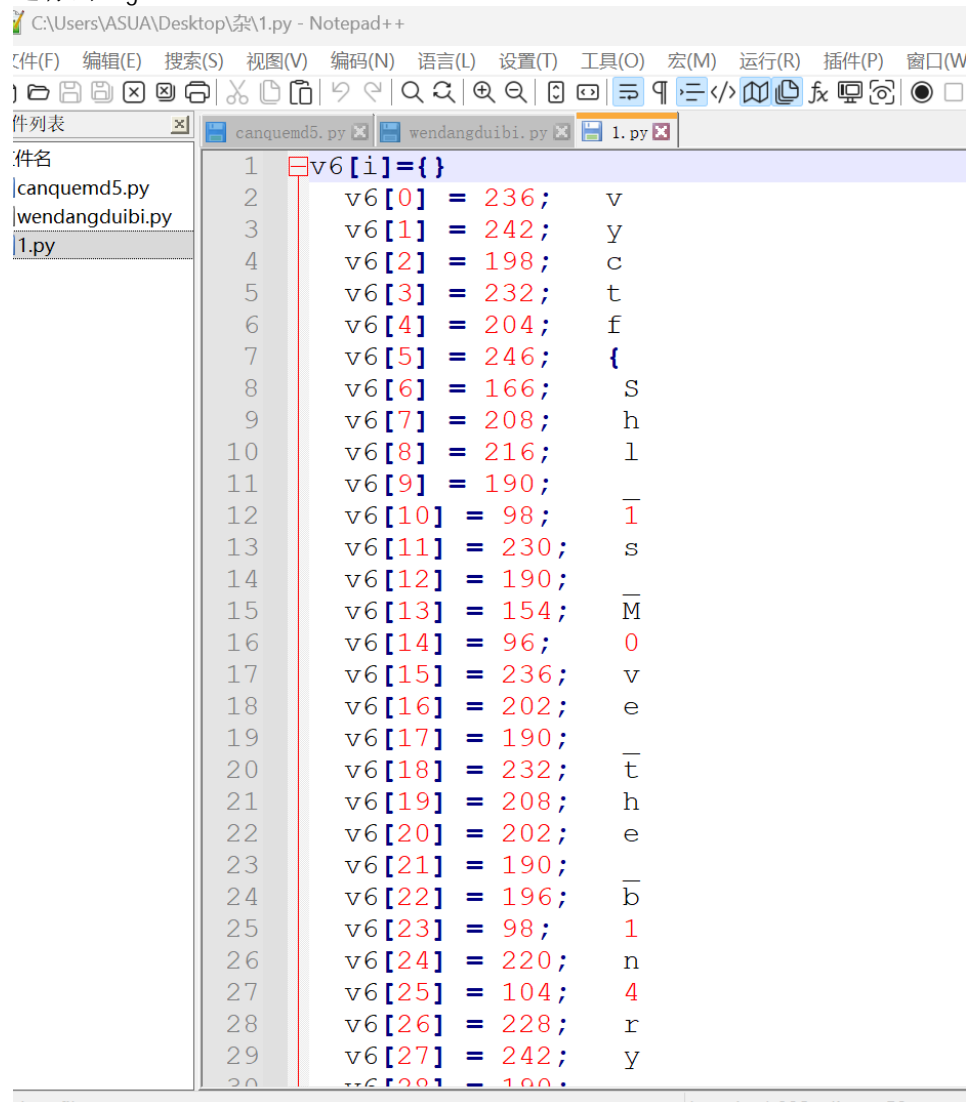with open("./flag.ct", "r", encoding="utf-8") as file:
    ciphertext = file.read()

\# 解密
plaintext = rsa_decrypt(ciphertext, D, N)

\# 将解密后的明文写入文件
with open("./decrypted_message.txt", "w", encoding="utf-8", errors="ignore") as output_file:
    output_file.write(plaintext)

print("Decrypted message:", plaintext)

运行出flag

```
v6[i]={}
v6[0] = 236;        v
v6[1] = 242;        y
v6[2] = 198;        c
v6[3] = 232;        t
v6[4] = 204;        f
v6[5] = 246;        {
v6[6] = 166;         S
v6[7] = 208;         h
v6[8] = 216;         l
v6[9] = 190;        _
v6[10] = 98;         1
v6[11] = 230;        s
v6[12] = 190;       _
v6[13] = 154;        M
v6[14] = 96;         0
v6[15] = 236;        v
v6[16] = 202;        e
v6[17] = 190;       _
v6[18] = 232;        t
v6[19] = 208;        h
v6[20] = 202;        e
v6[21] = 190;       _
v6[22] = 196;        b
v6[23] = 98;         1
v6[24] = 220;        n
v6[25] = 104;        4
v6[26] = 228;        r
v6[27] = 242;        y
```

拿到flag就行