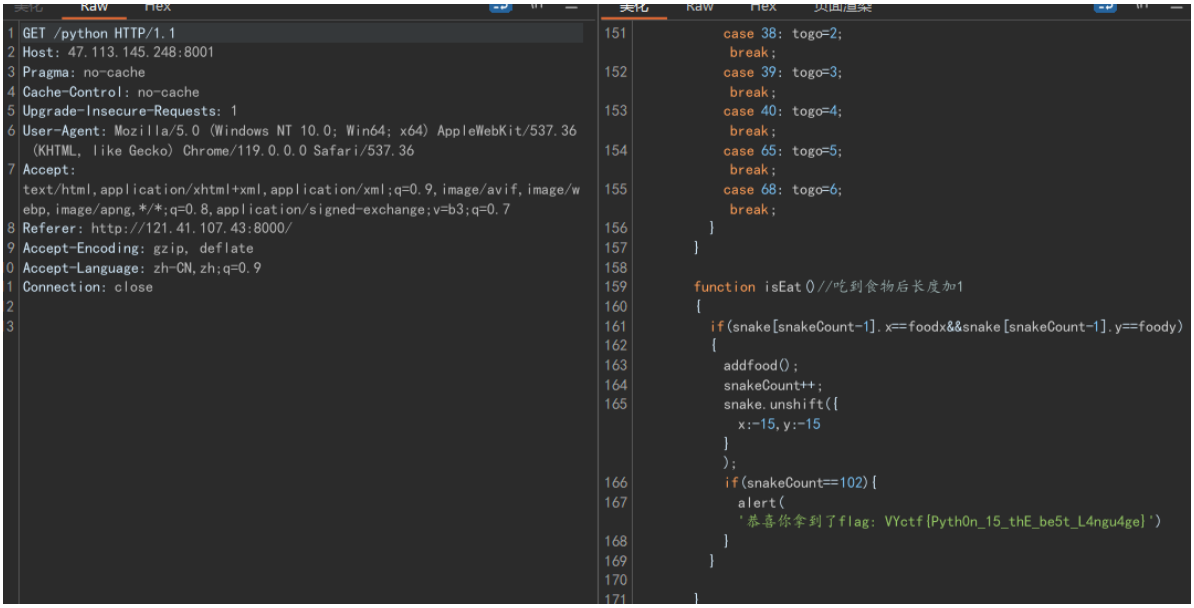
VYctf2023 wp by Y7syeu

WEB

玩蛇(签到)

抓包即可

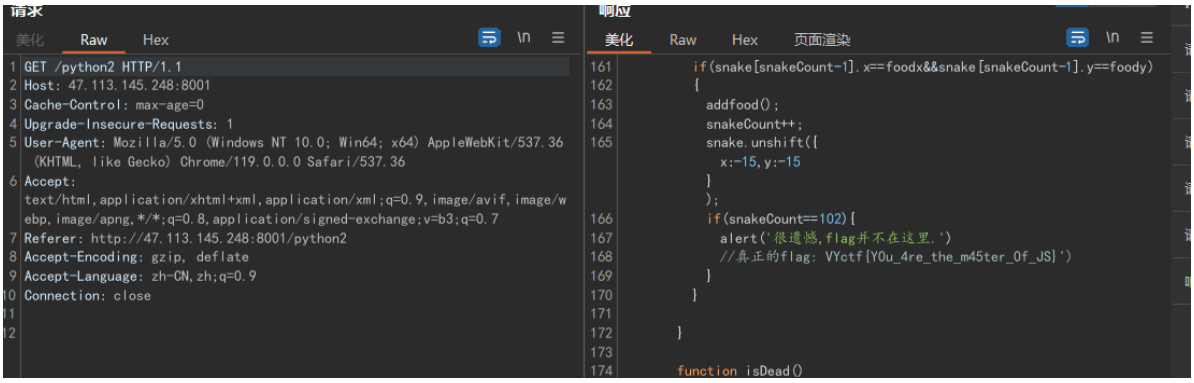


```
GET /python HTTP/1.1
Host: 47.113.145.248:8001
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://121.41.107.43:8000/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
            case 38: togo=2;
             break;
            case 39: togo=3;
             break;
            case 40: togo=4;
             break;
            case 65: togo=5;
             break;
            case 68: togo=6;
             break;
          }
        }

        function isEat()//吃到食物后长度加1
        {
          if(snake[snakeCount-1].x==foodx&&snake[snakeCount-1].y==foody)
          {
            addfood();
            snakeCount++;
            snake.unshift({
              x:-15,y:-15
            }
            );
            if(snakeCount==102){
              alert(
              '恭喜你拿到了flag: VYctf{PythOn_15_thE_be5t_L4ngu4ge}')
            }
          }

        }
```

玩蛇2.0

抓包即可



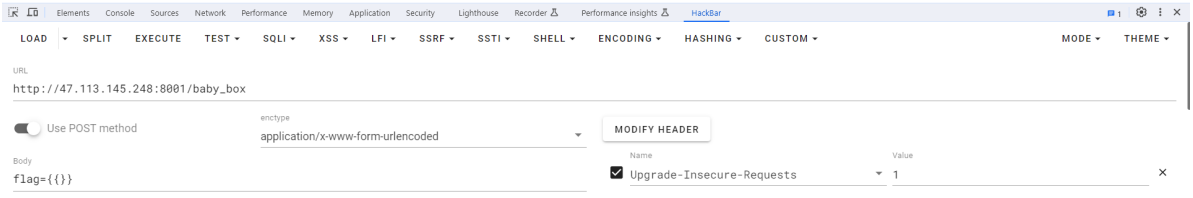
```
GET /python2 HTTP/1.1
Host: 47.113.145.248:8001
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://47.113.145.248:8001/python2
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
        if(snake[snakeCount-1].x==foodx&&snake[snakeCount-1].y==foody)
        {
          addfood();
          snakeCount++;
          snake.unshift({
            x:-15,y:-15
          }
          );
          if(snakeCount==102){
            alert('很遗憾,flag并不在这里.')
            //真正的flag: VYctf{YOu_4re_the_m45ter_Of_JS}')
          }
        }

      }

      function isDead()
```

玩具沙盒

post传参

干得漂亮! flag是vyctf{th1s_is_c0de9ate_baby_b0x}




```
  if request.method == "POST":
•     payload = request.form['flag']
•     result = sandbox(payload)
```

```
 if len(payload) > 0x8:
•     return '这可太长了!'


  try:
•     to_feed = base64.b64decode(payload)
  except:
•     return '这可不是base64!'
```

从源码可以得到post传参flag 然后经典{{}}

小恐龙

hint:多余的颜色是不是在暗示什么?

源码有如下 再通过hint尝试把color提取出来 头部一眼十六进制png

```
89504e470d0a1a0a0000000d494844520000001d0000001d0802000000d9f1f05800000009704859
7300002e2300002e230178a53f760000018049444154484b8d55ed1283300c9adedeff95b7f6d221
05a2f387d72f532024be5ee9f9fc9eda1cb37af300e318e18dcfb07d1cc7188f3702d5b8d6b18569
1761c1e9a0311cc1c80c70acce9c9185c4aaa38cb422326489d3c62dee82c2f176b0a6be2e50ad00
4e8d236ab9f8813de3fa67ece136b237b715f6083c7e75c2559516bc655aa845748ec82e9c7ee0e4
f097226847651c0315a4eaf24974a2a43416a13812d355426e0941e1fe9503c26fc565f938453157
cca3bb7ed64565194d008ab3389252862fd2d749cd1bfbe1126bef3b8ff7cd20ec0726156b1f4528
b5172c88cb4b10168157a2389e6d7866eaeb2d0675057b4a0988eb016863890e104fb39a6c613fbc
c117e24e0daee20614cb8165bcba09227a13f09a86dffd82e548a1c3de82b5a5f0e10a2677d392ae
bb99917489ce36b2defe8f852017b717ba94dc9ab2149c1cb7737474cce1fabff9859dee2c0b575d
ad6f2adfe095fbd8cbd8f2121d5beb3fcf86e7ec0bead81585c1ea8b5172d4b1ef82a9df814e3bbe
fa0201257ae732ac524a0000000049454e44ae426082
```

用010导入

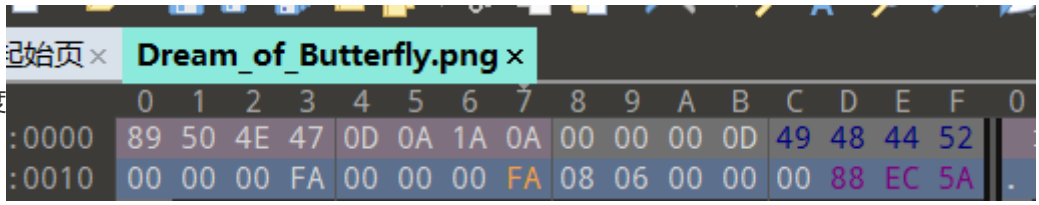
得到一个二维码扫码出flag

（misc无处不在

MISC

缺少的专辑(签到)

简单改高度

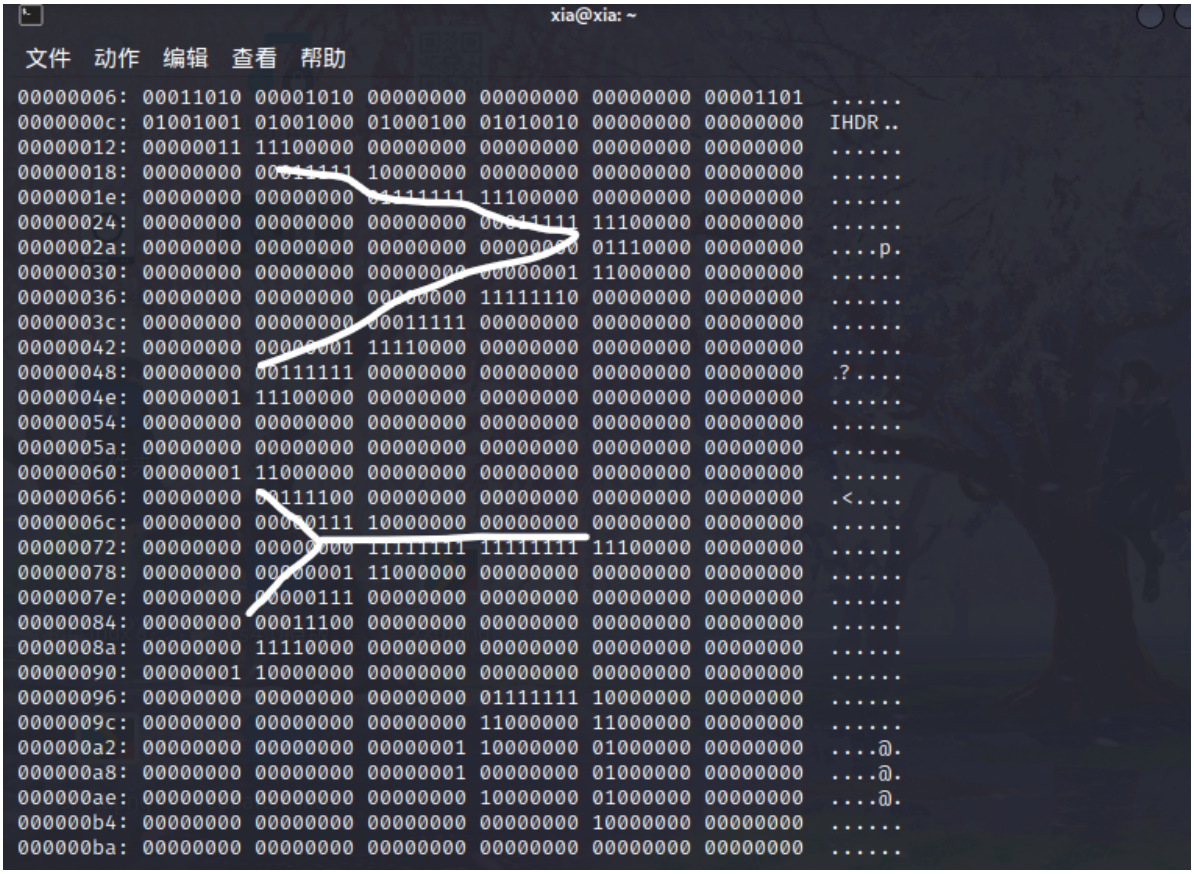


这亦是一种图片（足够抽象

hint：如果看不见图片, 不要心急, 也许图片正以另一种形式存在着, 观察它的名字.

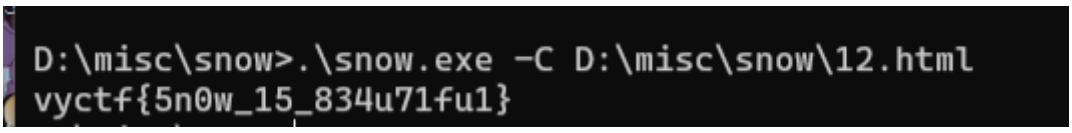
hint：世界上也许不只有十进制和十六进制

那只有xxd二进制



就这样慢慢认

雪(snow)



crypto

古老的语言(签到)

转换为python直接跑

```
import os
import sys



def interpret_brainfuck(input_file):
    try:
        with open(input_file, 'r', encoding='utf-8') as file:
            program = file.read()
    except FileNotFoundError:
        print('\033[31m[false] \033[0m找不到文件')
        return

•    output_file = input_file[:-3] + '.txt' if input_file.endswith('.bf') else
'default.txt'

•    with open(output_file, 'w', encoding='utf-8') as new_file:
•        memory = [0] * 256
•        address = 0
•        stack = []
•        program_counter = 0

•        while program_counter < len(program):
•            instruction = program[program_counter]

•            if instruction == 'o':
•                address += 1
•            elif instruction == 'w':
•                address -= 1
•            elif instruction == '*':
•                memory[address] += 1
•            elif instruction == '@':
•                memory[address] -= 1
•            elif instruction == '.':
•                data = chr(memory[address])
•                new_file.write(data)
•                print(data, end='')
•            elif instruction == ',':
•                input_data = input('')
•                memory[address] = ord(input_data[0])
•            elif instruction == 'v':
•                stack.append(program_counter)
•            elif instruction == '~':
•                if memory[address] != 0:
•                    program_counter = stack[-1]
•                else:
•                    stack.pop()
•            else:
•                pass

•            program_counter += 1
```

```
        print("")


if __name__ == "__main__":
    if len(sys.argv) < 2:
        print('\033[31m[false] \033[0m请至少添加一个文件!')
        sys.exit(1)

    input_file = sys.argv[1]
    interpret_brainfuck(input_file)
```

```
VYctf{welcOme_tO_cryptO}
```

素数分解

```
# 简单的rsa加密技术

E = 7

N = P * Q

\# N = 2771

phin = (P-1) * (Q-1)

D = pow(E, -1, phin)

\# print(D)

\# D = 1111

PT = open("./flag.ct","w")

with open("./flag.pt","r") as file:

  for f in file.read():

    PT.write(chr((ord(f) ** E) % N))

PT.close()
```

题给了加密 由题素数分解可以直接求出PQ

```
# 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)
```

```
vyctf{R5a_1s_MOdern_pA55wOrd}
```

小小的也很可爱哦

```
P = 487

\# D = ?

E1 = 31

\# E2 = pow(E1, D, P)

E2 = 168

R = 11



def enc(PT, E1, E2, R, P):

  C1 = pow(E1, R, P)

  C2 = ""

  for i in PT:

•     data = (i * pow(E2, R)) % P
```

```
    C2 += chr(data)

  return C1,C2



with open("./flag.pt","rb") as PT:

  C1,C2 = enc(PT.read(), E1, E2, R, P)



with open("./flag.ct","w") as CT:

  CT.write("C1 is:"+str(C1)+"\nC2 is:"+C2)



print("C1 is:"+str(C1)+"\nC2 is:"+C2)
```

在附件flag.ct中告诉了C1的值 直接通过源代码求私钥

```
P = 487
E1 = 31
C1 = 162
R = 11



def find_all_possible_d_values(P, E1, R, C1):
    possible_d_values = []
    for D in range(P):
        \# 尝试解密
        decrypted_C1 = pow(E1, R * D, P)
        if decrypted_C1 == C1:
            possible_d_values.append(D)
    return possible_d_values

all_possible_D_values = find_all_possible_d_values(P, E1, R, C1)


if all_possible_D_values:
    for D in all_possible_D_values:

        E2 = pow(E1, D, P)

        print(f"Found D: {D}")
        print(f"Calculated E2: {E2}")
        print(f"Decrypted C1: {pow(E1, R * D, P)} (should match C1: {C1})")
        print("-" * 20)
else:
    print("No valid D found.")
```

求出D=244然后直接做

```
# 定义解密函数
def decrypt(D, C2, E2, R, P):
    decrypted_data = ""
    for char in C2:
        decrypted_char = (ord(char) * pow(pow(E2, R, P), -D, P)) % P
        decrypted_data += chr(decrypted_char)
    return decrypted_data


\# 已知的参数
P = 487
E1 = 31
E2 = 168
R = 11
D = 244  # 你已知的 D 的值

\# 以二进制模式读取文件内容
file_path = "D:/chrome/elgamal/flag.ct"
with open(file_path, "rb") as file:
    content = file.read()

\# 获取 C2 密文部分
c2_index = content.find(b"C2 is:")  # 查找 C2 的位置
if c2_index != -1:
    C2 = content[c2_index + len(b"C2 is:"):].decode().strip()
    \# 解密数据
    decrypted_data = decrypt(D, C2, E2, R, P)
    \# 输出解密结果
    print("Decrypted Data:", decrypted_data)
else:
    print("Error: C2 not found in file.")

\# 打印文件内容的十六进制表示
hex_content = " ".join(format(byte, '02x') for byte in content)
print("File Content (Hex):", hex_content)
```

```
VYctf{ElG4m4l_15_4n_45ymmetr1c_encrypt1On_4lgOr1thm}
```

iot

简单ino(签到)

hint：什么, 这不只是一个单纯的程序, 也许能从元件上得到灵感

hint：显示屏大小为16x2

```
// lcd1602:SCL is uno:A5, lcd1602:SDA is uno:A4, lcd1602:VCC is num:V5,
lcd1602:GND is uno:GND.

#include <LiquidCrystal_I2C.h>

LiquidCrystal_I2C lcd(0x27, 20, 4);
```

```
int flag[20] = {118, 121, 995, 116, 102, 123, 104, 101, 492, 108, 482, 95, 65,
114, 100, 117, 493, 110, 482, 125};
int line[20] = {10, 3, 14, 4, 0, 13, 10, 3, 14, 0, 14, 0, 0, 7, 13, 5, 14, 0,
14, 7};
int i = 0;

void setup() {
  lcd.init();
  lcd.backlight();
  lcd.setCursor(0, 0);
  lcd.print("Hello vYctf!");
}

void loop() {
  delay(1000);
  lcd.clear();
  lcd.print("flag is:");
  lcd.setCursor(line[i], 1);
  lcd.print(flag[i]);
  i++;
}
```

读代码的flag入手 118由ascii对照为v 尝试拿去转ASCII（剔除大于126的）

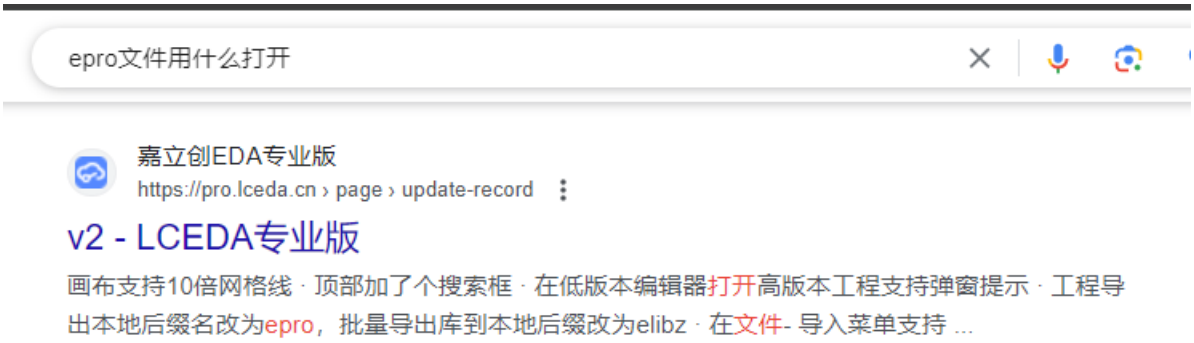
```
118, 121, 99, 116, 102, 123, 104, 101, 49, 108, 48, 95, 65, 114, 100, 117, 49, 110, 48, 125
```

vyctf{he1l0_Ardu1n0}

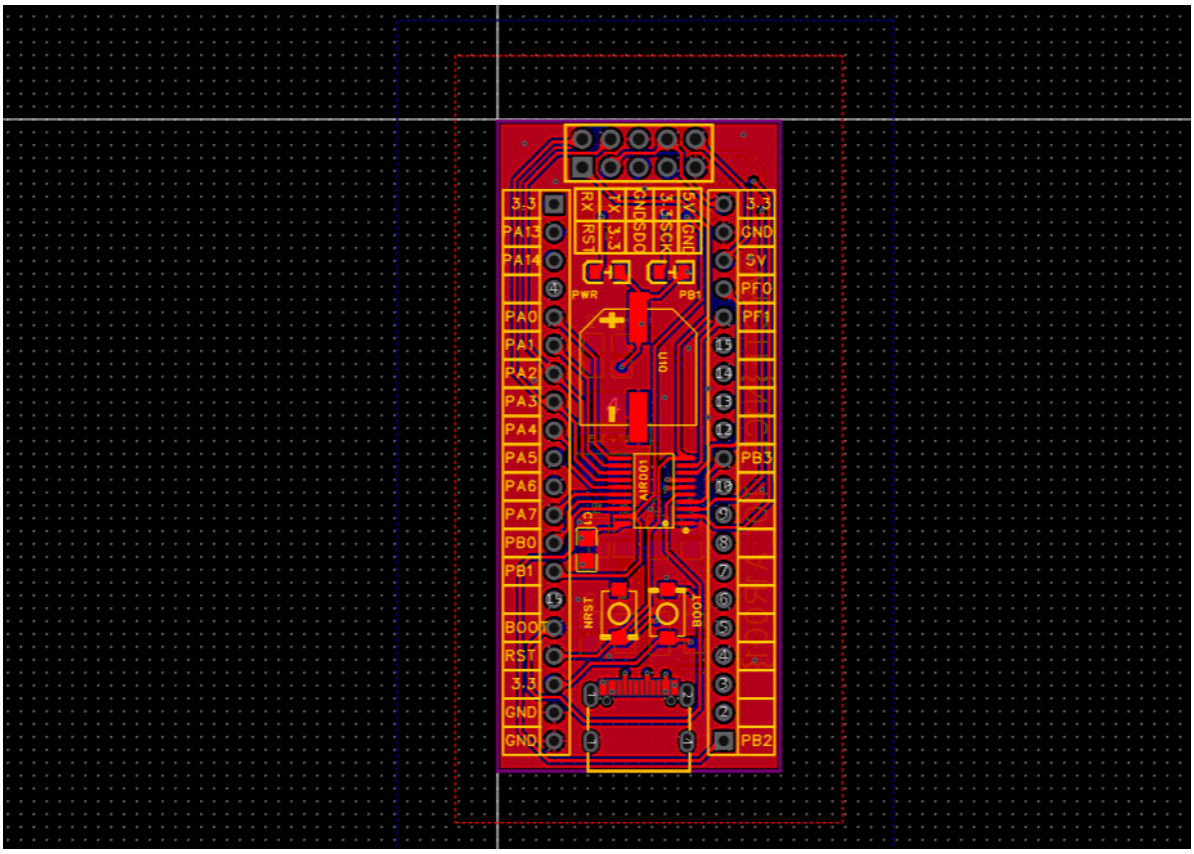
不太懂iot 唉

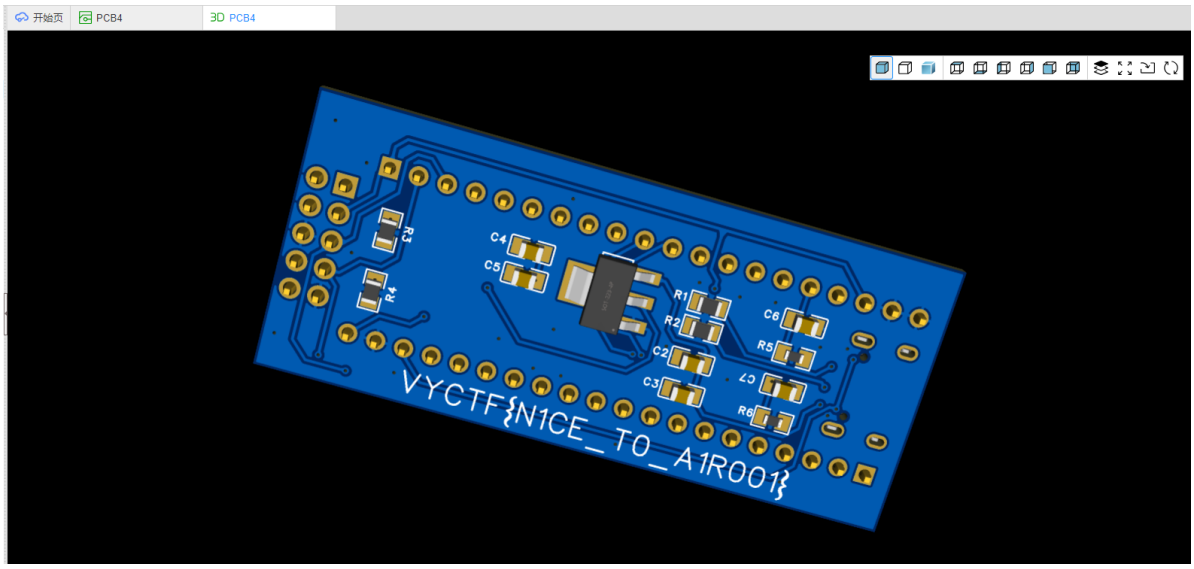
Air001

epro文件（（（直接网上搜发现是



就尝试瞎整 正常导入后是个二维的





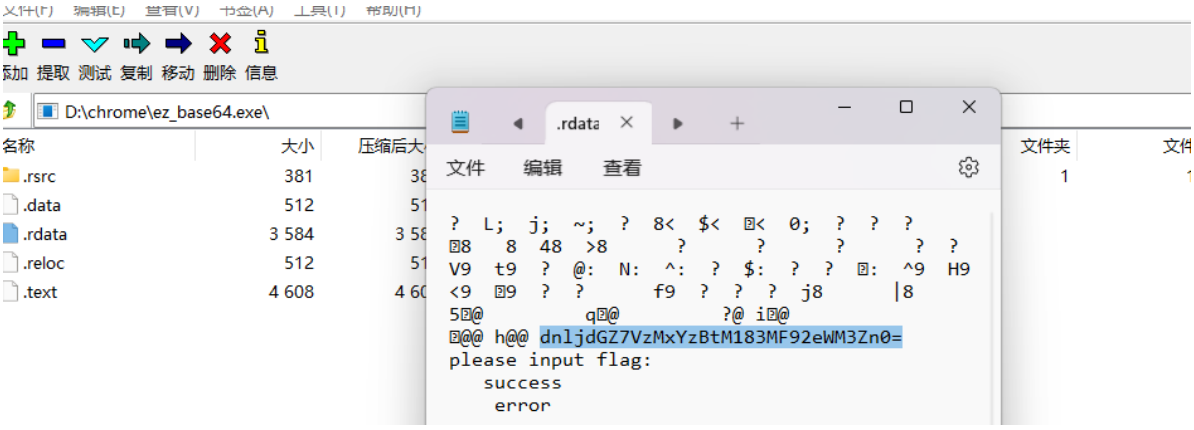
瞎捣鼓后换成3D展示 得到flag

reverse

大家一起和平地玩耍吧(签到)

base64逆向

打开文件随便看



疑似base64

不太懂re

二进制

hint：注意main函数附近

ida打开f5查看

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

```
unsigned __int64 v8; // [rsp+F8h] [rbp-18h]

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;
```

直接遍历数组，除以二，转换为ASCII并打印

```
v6 = [236, 242, 198, 232, 204, 246, 166, 208, 216, 190, 98, 230, 190, 154, 96,
236, 202, 190, 232, 208, 202, 190, 196, 98, 220, 104, 228, 242, 190, 232, 96,
190, 232, 208, 202, 190, 216, 202, 204, 232, 250]

for num in v6:
    num //= 2
    ascii_char = chr(num)
    print(ascii_char, end='')

print()
```

```
vyctf{Shl_1s_MOve_the_b1n4ry_tO_the_left}
```

virus

kawaii病毒

hint：这么kawaii的病毒, 如果依它所想做点什么, 它会不会告诉你flag呢?

hint:

```
int filenum()
{
```

```
    WIN32_FIND_DATA findFileData;
    HANDLE hFind = FindFirstFile("*", &findFileData);
    if (hFind == INVALID_HANDLE_VALUE)
    {
        printf("Can't find file");
        return 1;
    }
    int fileCount = 0;
    do {
        if (findFileData.dwFileAttributes & FILE_ATTRIBUTE_DIRECTORY) {
            continue;
        }
        fileCount++;
    }
    while (FindNextFile(hFind, &findFileData) != 0);
    FindClose(hFind);
    return fileCount;
}
```

跟着说的来就行 随便搞个目录建个文件再删掉