

# VYctf2023 WriteUp

## Kada\_Duck

## 排名

第9名

## 解题思路

## WEB

### 3 题

#### 1. 签到问卷

填写就行

#### 2. 玩蛇2.0

发现F12和检查都触发不了，用view-source:url来查看源代码

```
view-source:47.113.145.248:8001/python2

129         case 6: snake.push({x:snake[snakeCount-1].x+15,y:snake[snakeCount-1].y+15}); break;
130         default: snake.push({x:snake[snakeCount-1].x+15,y:snake[snakeCount-1].y});
131     }
132     snake.shift();//删除数组第一个元素
133     ctx.clearRect(0,0,900,600);//清除画布重新绘制
134     isEat();
135     isDead();
136     drawtable();
137 }
138
139 function keydown(e)
140 {
141     switch(e.keyCode)
142     {
143         case 37: togo=1; break;
144         case 38: togo=2; break;
145         case 39: togo=3; break;
146         case 40: togo=4; break;
147         case 65: togo=5; break;
148         case 68: togo=6; break;
149     }
150 }
151
152 function isEat()//吃到食物后长度加1
153 {
154     if(snake[snakeCount-1].x==foodx&&snake[snakeCount-1].y==foody)
155     {
156         addfood();
157         snakeCount++;
158         snake.unshift({x:-15,y:-15});
159         if(snakeCount==102){
160             alert('很遗憾,flag并不在这里.')
161             //真正的flag: VYctf{Y0u_4re_the_m45ter_of_JS}')
162         }
163     }
164 }
165
166 }
```

#### 3. 玩蛇(签到)

和第二题一样，view-source:就行了

```
view-source:47.113.145.248:
不安全 | view-source:47.113.145.248:8001/python
百度 百度翻译-200种语... 下载图片 高等数学上册 第七... U校园 阿里云盘资源 党二十大广告模板
129         case 0: snake.push({x:snake[snakeCount-1].x+15, y:snake[snakeCount-1].y+15}); break,
130         default: snake.push({x:snake[snakeCount-1].x+15, y:snake[snakeCount-1].y});
131     }
132     snake.shift();//删除数组第一个元素
133     ctx.clearRect(0, 0, 900, 600);//清除画布重新绘制
134     isEat();
135     isDead();
136     drawtable();
137 }
138
139 function keydown(e)
140 {
141     switch(e.keyCode)
142     {
143         case 37: togo=1; break;
144         case 38: togo=2; break;
145         case 39: togo=3; break;
146         case 40: togo=4; break;
147         case 65: togo=5; break;
148         case 68: togo=6; break;
149     }
150 }
151
152 function isEat()//吃到食物后长度加1
153 {
154     if(snake[snakeCount-1].x==foodx&&snake[snakeCount-1].y==foody)
155     {
156         addfood();
157         snakeCount++;
158         snake.unshift({x:-15, y:-15});
159         if(snakeCount==102){
160             alert('恭喜你拿到了flag: VYctf{Pyth0n_15_thE_be5t_L4ngu4ge}');
161         }
162     }
163 }
164 }
```

## REVERSE

### 2 题

#### 1.base64逆向

目的是v8与字符串相同，那么如何相同呢，看一下v8的生成，发现sub\_401040是base64解码，所以用cyberchef就解出来了。

Version 9.32.3

Last build: 2 years ago

设置 关于 / 支持

请选择需要的操作 (Operations)

Search...

Favourites (常用)

To Base64 (转换为Base64)

From Base64 (Base64转换)

To Hex (转换为16进制)

From Hex (16进制转换)

To Hexdump (16进制转存)

From Hexdump (来自16进制转存)

URL Decode

Regular expression

Entropy

Fork

Magic

Data format (数据转换)

Encryption / Encoding (加密/编码)

方法 (Recipe)

Magic

Depth 3

Intensive mode

Extensive language support

Crib (known plaintext string or regex)

STEP 

BAKE!

 自动

输入 (Input)

dn1jdGZ7VzNxYzBtM183MF92eW43Zn0=

start: 32 end: 32 length: 32 lines: 1

输出 (Output)

Recipe (click to load)	Result snippet	Properties
From_Base64 (Base64转换) ('A-Za-z0-9+/', true)	vyctf{W31c0m3_70_vyc7f}	Valid UTF8 Entropy: 3.71
From_Base64 (Base64转换) ('A-Za-z0-9+\\/= ', true)	vyctf{W31c0m3_70_vyc7f}	Valid UTF8 Entropy: 3.71
	dn1jdGZ7VzNxYzBtM183MF92eW43Zn0=	Matching ops: Decode NetBIO5 Name, From Base64 (Base64转换) Valid UTF8 Entropy: 4.44

#### 2.二进制

要求输出的字符串为v6字符串每个ascii码除2对应的字符串

写一个cpp，输出一下就行了。

```
vyctf{Shl_1s_M0ve_the_b1n4ry_t0_the_left}
```

```
-----  
Process exited after 0.05214 seconds with return value 0  
请按任意键继续. . .
```

exp 请粘贴代码，不允许截图。

## iot

---

### 1题

1.Air001

发现后缀名不认识，.epro文件，搜索后发现可能是嘉立创的项目，结合hint，用专业版打开，反转一下板子，就能看见Flag了。

## crypto

---

### 1题

1.素数分解

已经给出密文，由于编码问题不太会从.ct文件中读取，所以只能做预处理，正向对每个ascii码值加密，然后做映射得到明文。

```
enc = 'hQm0kK88eKf8wHjEKडस0'  
mp = {}  
for i in range(1000):  
    mp[pow(i,E,N)] = i  
    # print(i,pow(i,D,N))  
  
for f in enc:  
    print(chr(mp[ord(f)]),end='')
```

## virus

---

# 1题

## 1.kawaii病毒

通过提示的源码，发现要删掉一个文件，他就会给flag，所以建个文件夹，把他放进去，里面创个空文件，然后运行病毒，把他删掉即可。