

ctfshow 吃瓜杯八月赛 Misc WriteUp

原创

[FW_Suica](#) 于 2021-08-18 15:22:00 发布 401 收藏 1

分类专栏: [ctf](#) 文章标签: [安全](#) [经验分享](#)

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/Nancy523/article/details/119753020>

版权



[ctf](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

目录

- 1、Misc游戏签到
- 2、吃瓜
- 3、EZbingo
- 4、魔王
- 5、Dinner of Cyanogen
- 6、Music Game
- 7、一群强盗

1、Misc游戏签到



别问 问就是玩游戏 套神说的) : 多选杀戮 没有杀戮就选背刺 少选能量瓶子 吓死就对了^q^

打了小几十把 脸黑没办法 期间遇到过环境卡死 3段flag闪退 环境罢工 (

八神说 是python的错跟套神没关系呜呜呜

```
ctfshow{White_give_game_only_waste_your_timehahaha}
```

2、吃瓜

下载附件得到新建文件夹.jpg 010editor打开发现pk头 说明为zip压缩包

```
起始页 题目-我爱你中国.mp3 picture.jpg CTMOUSE.EXE old.mc 新建文件夹.jpg x
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 50 4B 03 04 0A 00 00 00 00 00 6E 68 FE 52 00 00 PK.....nhpR..
0010h: 00 00 00 00 00 00 00 00 00 00 03 00 0D 00 CC E2 .....Ia
0020h: 2F 75 70 09 00 01 01 1A 6D A0 E9 A2 98 2F 50 4B /up.....m ec"/PK
0030h: 03 04 14 00 00 00 08 00 8E 81 F9 52 D1 DA 15 0D .....Z.URNU..
0040h: 19 95 00 00 FB BE 00 00 0B 00 17 00 CC E2 2F B3 ..0%.....Ia/3
0050h: D4 B9 CF 2E 6A 70 67 75 70 13 00 01 36 4F 5A 06 0'i.jpgup...6OZ.
0060h: E9 A2 98 2F E5 90 83 E7 93 9C 2E 6A 70 67 EC 98 ec"/a.fc"e.jpgi~
0070h: 07 50 53 DB BA C7 77 42 42 31 40 44 69 86 2A C5 .PSU°cWBB1@Dit*A
0080h: A8 08 31 74 30 94 08 06 11 11 A4 28 45 85 90 A2 ".1t0"....r(E....C
0090h: A1 84 92 20 A1 2B 28 A8 14 A5 08 1E 9A 08 82 80 j' i+(.Y.S.€
00A0h: C8 11 69 82 28 22 8A 22 04 01 41 94 DE E5 80 F4 E.i("S".A"pà€δ
00B0h: A6 A0 F2 36 1E E7 9E FB CE 9C FB 66 EE BD 6F DE |δ6.çz0ieof1%oP
00C0h: 7B 33 2F BF BD 33 FB FB 56 F9 FE 2B 68 D6 9E F9 {3/2%300V0p+k0ZU
00D0h: 27 EB EF D7 07 80 CD 87 08 A6 04 00 02 81 00 CE 'ei×.€I#.}.....I
00E0h: E0 05 AC 0F 6E 3E 7B 80 45 A3 02 80 B9 39 B0 1B à.-n>{€€€.€19°.
00F0h: 00 00 5E 00 0E D9 07 40 C1 88 1B 4C 60 91 34 00 ..^..U.@^".L'4.
0100h: 06 C6 10 30 D6 4F 4B DB 78 02 3B 00 80 A7 2E 2D E.000kux...€5/
0110h: FD 47 CF 0E C6 6D 13 82 00 0E F8 BC 04 E6 qmpR//0103sun.jeuNan043
```

修改后缀为.zip后解压打开 得到

 吃瓜.jpg	2021/7/25 16:12	JPG 文件	48 KB
 新建文本文档.txt	2021/7/30 13:00	文本文档	3 KB

文本文档里面的内容复制到浏览器打开 为一个二维码hhhh

扫描得到一串字符 一眼看出是打乱的flag

复制 cfhwc19abika_ets0{h_u_e_ui1}



吃瓜图片中 属性发现花朵加密 密码为sunny



然后 然后 我死在这个两个西瓜了，，，疯狂的想 两个西瓜是不是两个图片 跟吃瓜本身图片去进行一系列操作，， 那天晚上思路被固定死了（Tao: 你想多了 而且是想太多了）

做梦梦到做出来了 早晨爬起来突然想起栅栏密码，，好嘛 两个西瓜就是栅栏2 将打乱的flag栅栏2解密 得到flag:

```
ctfshow{ch1_9ua_bei_kuai_1e}
```

3、EZbingo

手撸的 不懂原理 玩 就硬玩

```
ctfshow{yOu_w1N_tHE_BING0_G4me!}
```

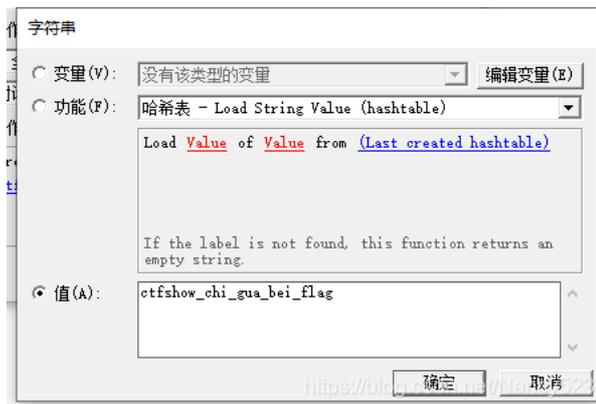
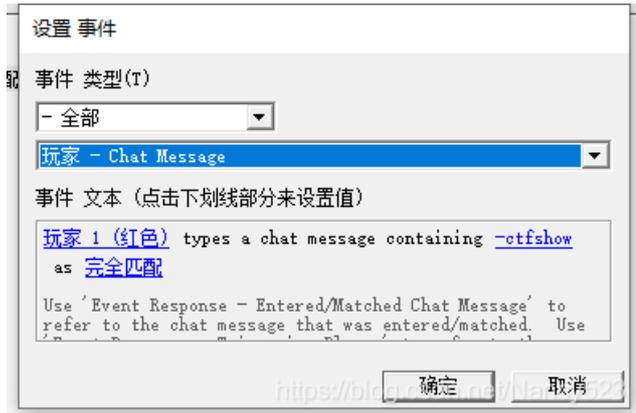
4、魔王

后面群主加的签到题 下载得到w3x后缀文件 百度为魔兽争霸3的地图

打开 提示为打败大魔王得到flag em真给他打死了给了个假的flag（优美中国话



联想到一题 超级玛丽 于是用地图编辑器打开 寻找触发事件编辑器



预期解：在游戏中按下回车 输入-ctfshow（其实相当于自定义了一个金手指作弊码



```
ctfshow{ctfshow_chi_gua_bei_flag}
```

5、Dinner of Cyanogen

动态附件 下载解压得到两个doc文件 letter打开：得到第一段flag

Shalisha:↓

Hey there.↓

I'm writing to return the flag to you, because we broke up last week.↓

So here is the first part: ctfshow{f.↓

I don't know what it means, or why you are interested in it.↓

Maybe it's just useless, just like my old phone number 15746525561, and something other ... or is it?.↓

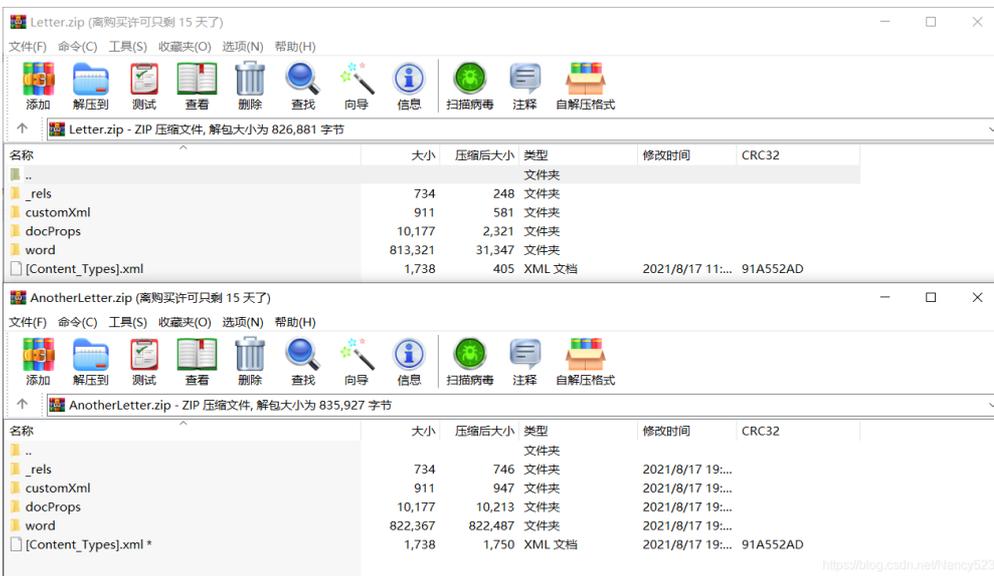
Whatever, I've change the number, never call me again.↓

Date with your fucking flag and be alone forever.↓

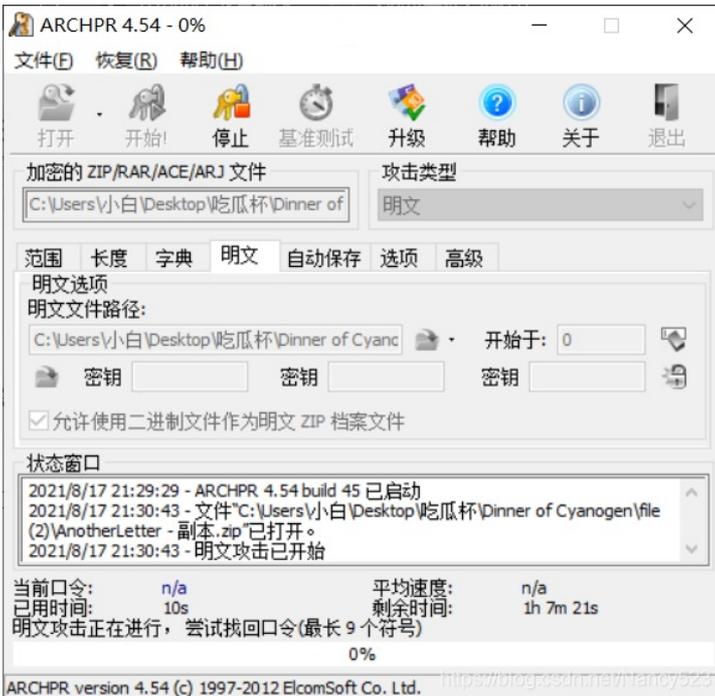
Bye.↓

<https://blog.csdn.net/Nancy523>

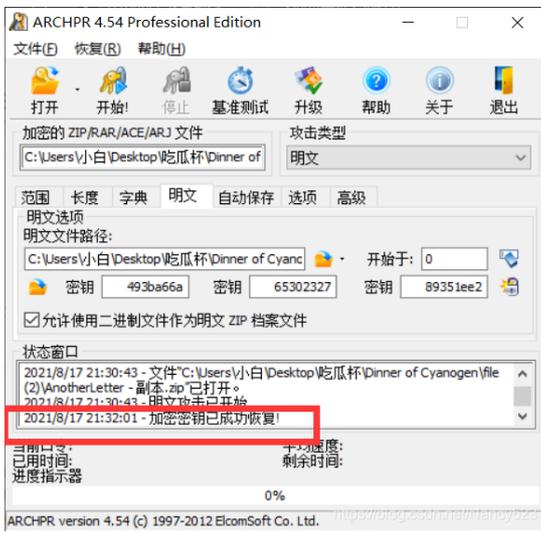
another打开报错 两者010editor打开 发现均可为压缩包（第一次发现这种神奇的文件）修改后缀为zip 发现another为加密压缩包 密码未知



观察最后一个文件 联想到之前做的一个题目 最后一个文件的大小跟crc32码完全一致 故为明文破解
 将未加密的压缩包中的最后一个文件解压出来 用7zip压缩 压缩等级仅存储 加密算法ZipCrypto
 arch打开:



跑个2分钟左右手动停止



原因：



(又学到了新知识

将解密完的压缩包打开 在..\word\flag.xml中发现第二段 flag

51,800 条结果 时间不限

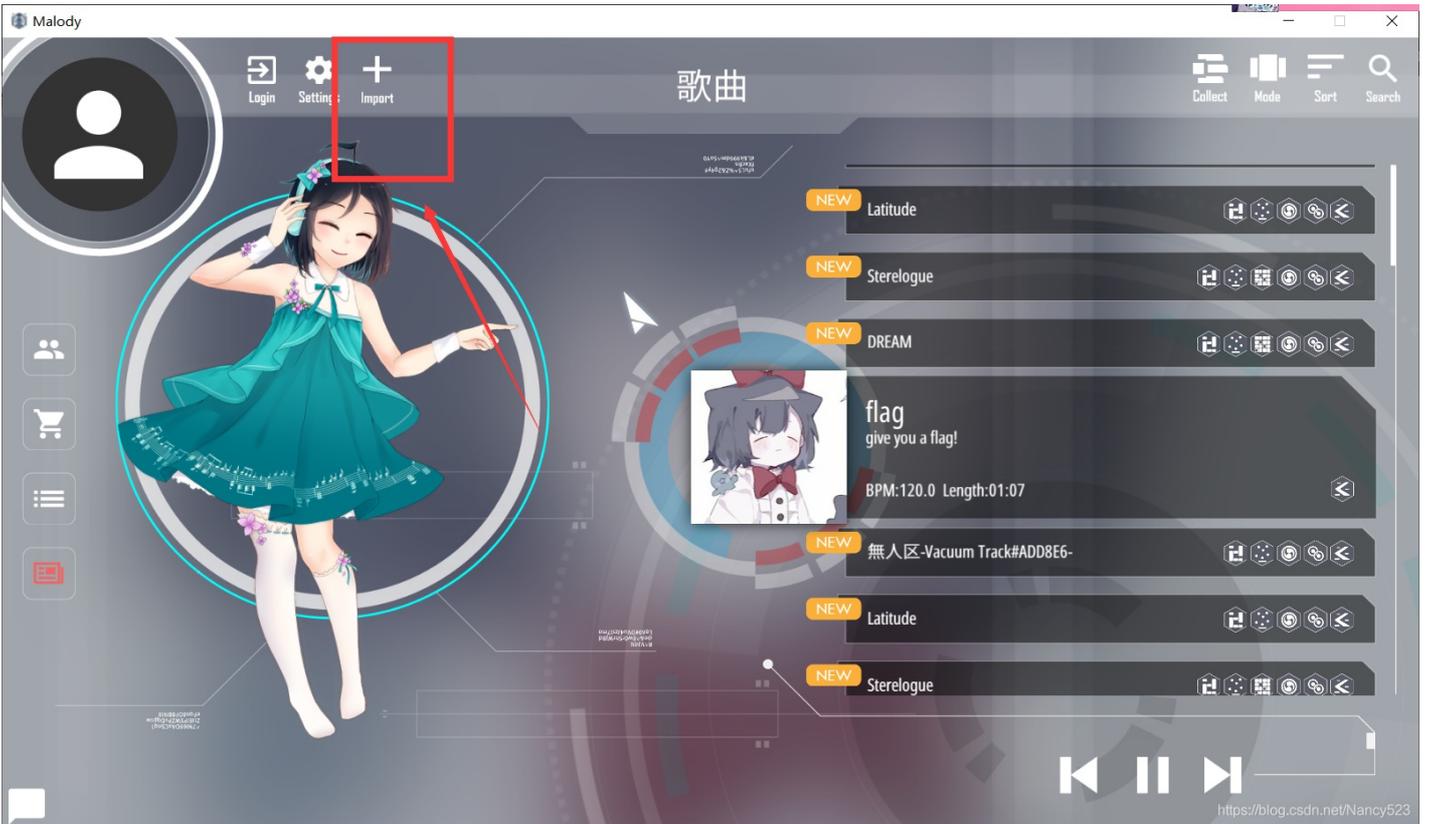
哔哩哔哩专栏 - Bilibili

https://www.bilibili.com/read/cv4366143

2020-1-15 · [工具/原料]一个完整的Malody Package文件,一份 rmstZ_20190726.ht
mcz文件为例:Malody Package文件,后缀为.mcz[流程]:1.将.mcz文件的后缀改为.zip, \$
缀2.打开这个文件,在一个完整的Malody Package文件中

发现为malody的自制谱文件

下载一个win版本的malody V 导入谱子 编辑铺面

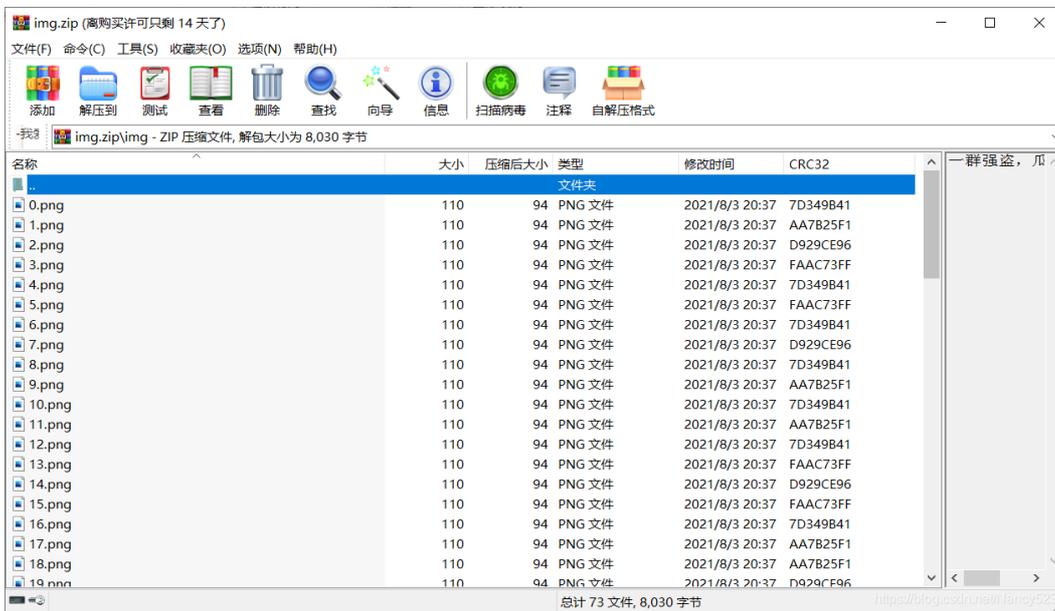


手撿flag: (你ctf届全是二刺猿)

```
ctfshow{bgm_is_nice}
```

7、一群强盗

下载得到附件 是一堆灰色的图片 比赛时候联想到图片可能是异或操作或者进制转换, 然后就没有然后了
复现:



观察发现CRC32只有4种 联想到比赛时候想到的进制转换 可能是四进制

因为flag格式开头为ctfshow 所以尝试将“c”转换为四进制 刚好得到“1203” 猜想成立

嗯 我只会手撸 脚本不会写 (插个套神的脚本吧

```
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)
```

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。

记得最后将结果的空格字符串转换为下划线

```
ctfshow{56_robber}
```