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

目录

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^

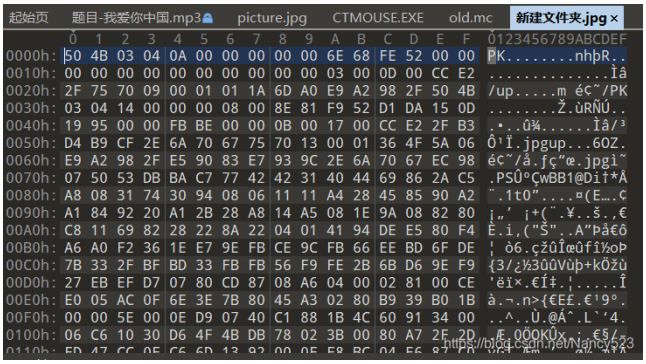
打了小几十把 脸黑没办法 期间遇到过环境卡死 3段flag闪退 环境罢工（

八神说 是python的错跟套神没关系呜呜呜

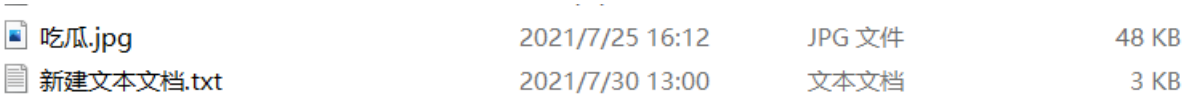
```
ctfshow{White_give_game_only_waste_your_timehahaha}
```

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



修改后缀为.zip后解压打开 得到



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

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

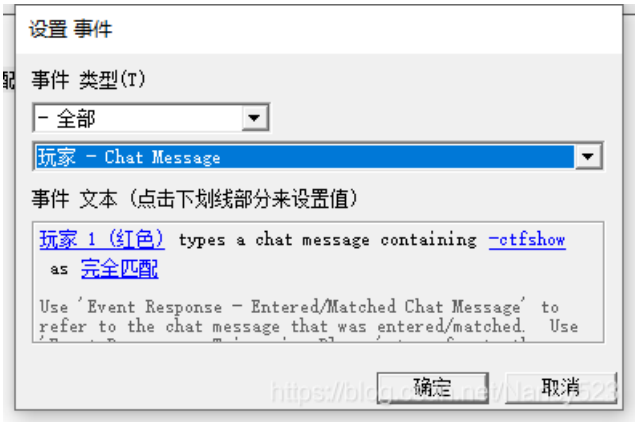
> ctfshow{yOu_w1N_tHE_BING0_G4me!}

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.

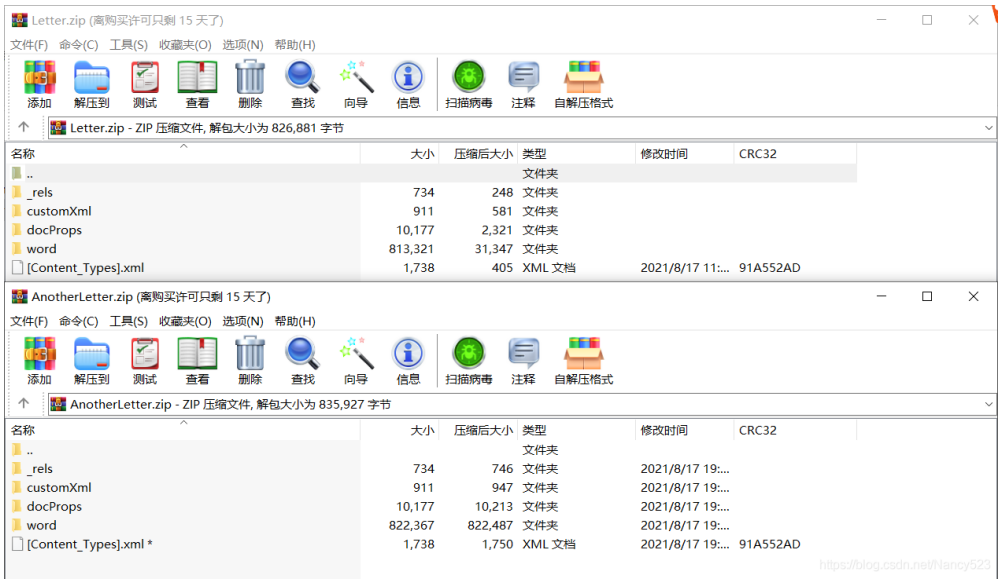
Maybe it's just useless, just like my old phone number 15746525561, and something other ... or is it?.

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

Date with your fucking flag and be alone forever.

Bye.

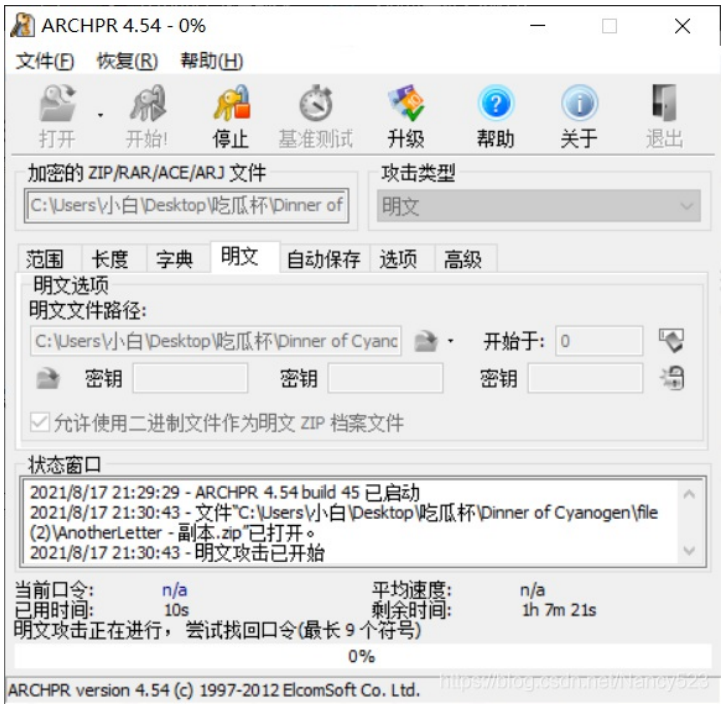
another打开报错 两者010editor打开 发现均可为压缩包（第一次发现这种神奇的文件 ）修改后缀为zip 发现another为加密压缩包 密码未知



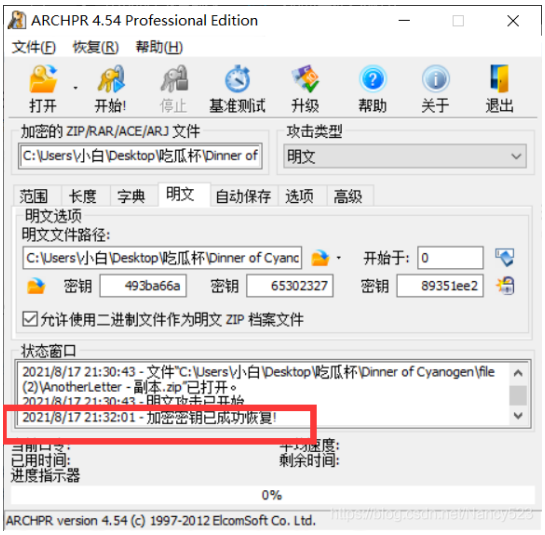
观察最后一个文件 联想到之前做的一个题目 最后一个文件的大小跟crc32码完全一致 故为明文破解

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：



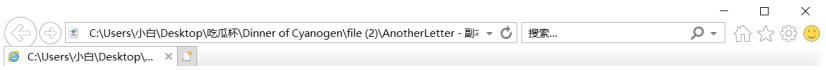
跑个2分钟左右手动停止

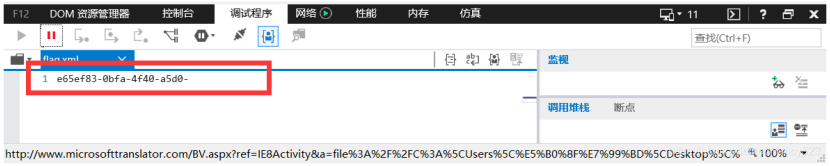


原因：

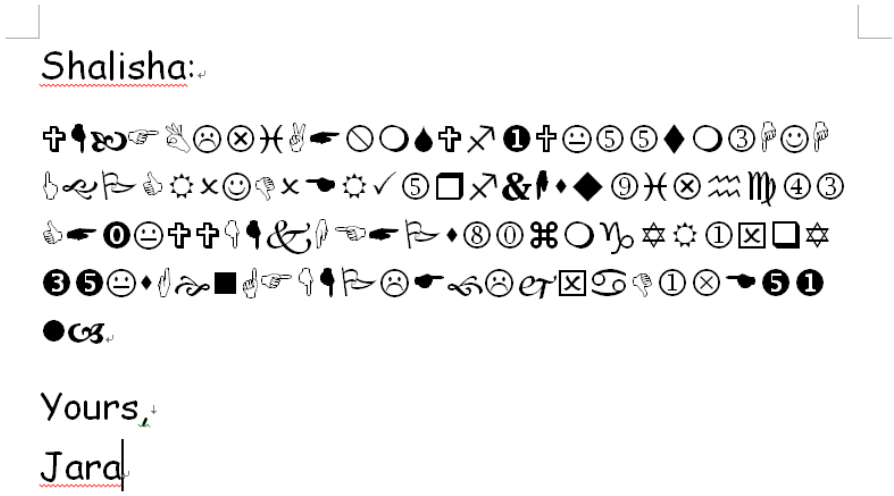
（又学到了新知识

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



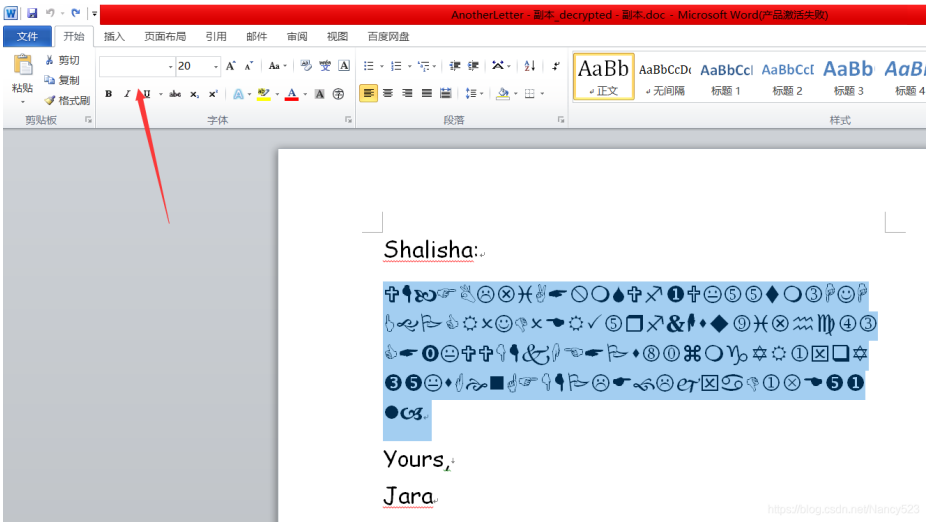


将破解完的压缩包 后缀改为doc 打开得到:



发现信件内容刚好104个字符 13位

全选发现没有显示字体格式

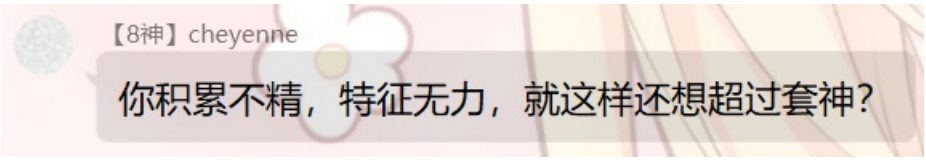


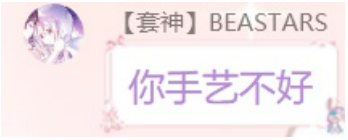
说明字符经过处理 挨个看发现两种格式 wingdings跟wingdings2 wingdings转化为0 wd2转换为1 再经过二进制转ascii

得到flag:

> ctfshow{fe65ef83-0bfa-4f40-a5d0-ba216e650fc2}

（复盘过程中手撸错了一位 尬住





6、Music Game

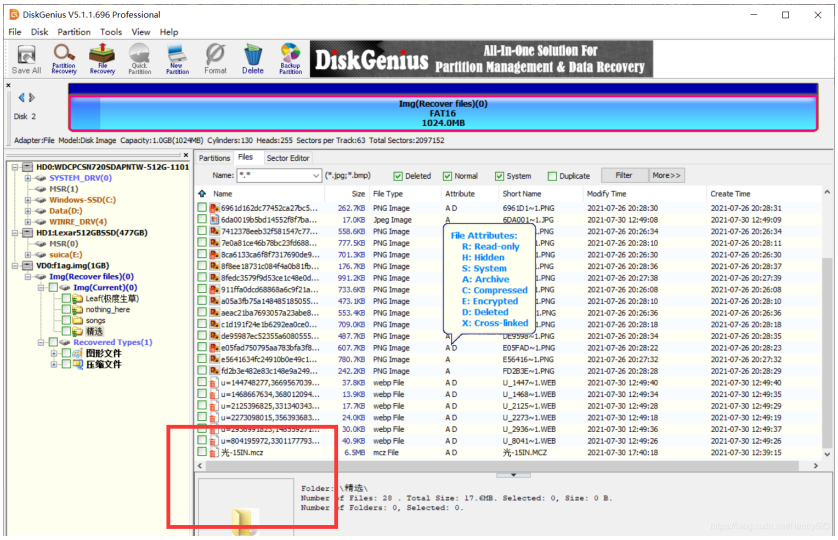
这玩意复盘复盘了一个多小时属实给我整麻了，，，

下载得到f1ag文件 解压得到f1ag.img

用DiskGenius加载（需要的可以找我要，，）

点击恢复文件

打开精选文件夹 找到后缀为.mcz的文件 导出来



搜索关键字：

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

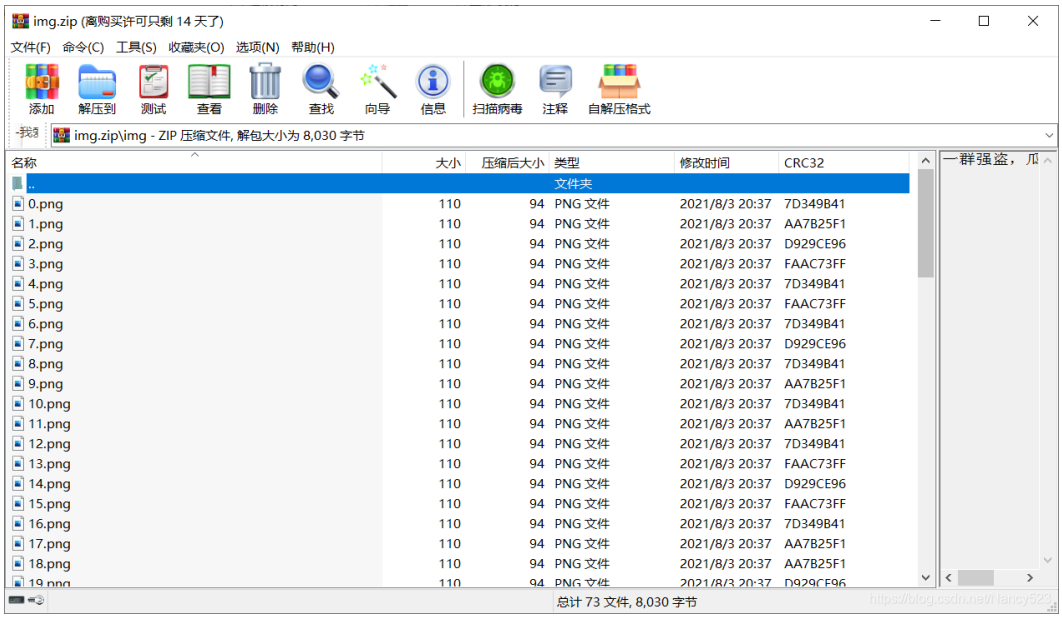
手撸flag：（你ctf届全是二刺猿）

> 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}