

ctf_show misc入门

原创

臧有点  已于 2022-01-23 16:19:03 修改  177  收藏

分类专栏: [ctf_show](#) 文章标签: [经验分享](#)

于 2022-01-22 14:52:40 首次发布

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/weixin_52873955/article/details/122504877

版权



[ctf_show](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

图片篇(基础操作)

misc1

打开图片 看到flag

misc2

压缩包打开是txt文档, 提示图片题 将文件格式改为jpg

打开图片 显示flag

misc3

通过bpg软件打开图片即可

misc4

解压文件 有六个txt文档 打开是乱码 通过winhex打开 查看表头 修改文档后缀名

图片篇(信息附加)

misc5

winhex打开 flag在尾部

misc6

跟上一题类似

misc7

跟上一题一样

misc8

foremost分离图片 得到flag

misc9

通过winhex打开 ctrl+f 查找字符串 找到flag

misc10

foremost没有将图片分离 binwalk -e 此时同目录下会出现文件 打开查看flag

misc11

常规操作一遍后 没什么发现 看了大佬的wp IDAT块的问题 跟上题类似 但是binwalk解不出来

101模板一直出错 用tweakpng 删掉第一个IDAT 再打开图片flag就有了

misc12

一番操作后，没思路 看wp 通过测试删除前八个idat （这里真不懂 还是写的少）

misc13

winhex打开图片查看源码 查找flag没找到，搜c根据提示在图片末尾 所以最后一个是flag

flag字符串中间有间隔，这是一个提示，通过代码将其提取再转换为字符串得到flag

```
str="631A74B96685738668AA6F4B77B07B213114655333A5655432346578642534DD38EF66AB35103195381F628237BA6545347C32  
flag=""  
for i in range(0,len(str),4):  
    flag+=str[i]  
    flag+=str[i+1]  
print(flag)
```

misc14

binwalk过一遍 发现最后有个jpg数据块

通过010打开图片 搜索FF D8 有三个 将最后一个数据提取 另存为图片 打开图片看到flag

misc15

直接010打开图片搜索flag就可以

misc16

010打开搜索flag没有 binwalk -e打开DD4

misc17

zsteg检测图片中有隐藏的数据 读取出来 binwalk分离数据 打开图片查看flag

misc18

图片属性详细信息都有

misc19

通过[网站](#)图片详细信息

misc20

跟上一题同种做法

misc21

序列号	686578285826597329
-----	--------------------

直接提交flag不对 转换为字符串提示hex () X跟Y

X分辨率	3902939465
Y分辨率	2371618619
PageName	https://ctf.show/
X定位	1082452817
Y定位	2980145261
目标Printer	ctfshow{} CSDN @臧有点

将X Y 四组数据分开转换为十六进制 连接提交flag

misc22

用exiftool查看略缩图得到flag

生成image.raw的缩略图thumbnail.jpg

```
exiftool -b -ThumbnailImage image.raw > thumbnail.jpg
```

misc23

exiftool查看图片信息

```
History Action : ctfshow {}, UnixTimestamp, DECTIMEA, getFlag
```

时间戳 转换为16进制 得到flag

```
History When : 1997:09:22 02:17:02+08:00, 2055:07:15 12:14:48+08:00, 2038:05:05 16:50:45+08:00, 1984:08:03 18:41:46+08:00
```

四组数据分开转换 直接转换不对

misc41

010搜索F001高亮显示 就能看出来flag

```
ctfshow{fcbd427caf4a52f1147ab44346cd1cdd}
```