

香山杯CTF WP

原创

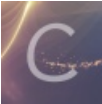
带头_小弟 于 2021-11-15 22:14:22 发布 3689 收藏 6

分类专栏: CTF 文章标签: 安全

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_45862372/article/details/121344447

版权



CTF 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

香山杯CTF WP

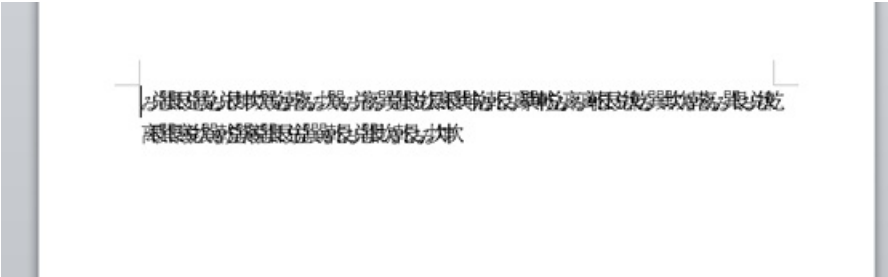
MISC

- 你悟了吗
- qrcode
- miao
- babyrgb
- brokenpassword
- 总结

MISC

你悟了吗

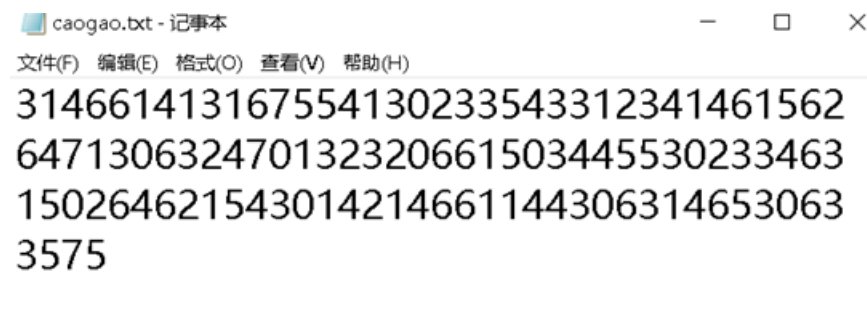
拿到.rtf文件打开



全选复制粘贴到txt里面

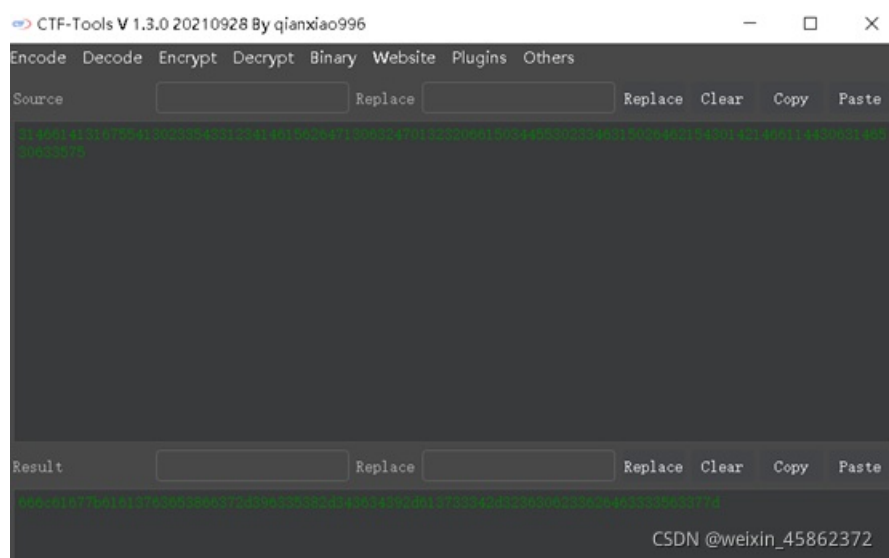
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
震兑巽艮艮兑巽兑震兑艮坤坎坎巽兑震乾离震震
坎巽震震兑离震巽兑巽艮兑坎艮离艮巽坤兑震乾
艮震离巽坤乾兑震离震离乾艮艮兑坎乾震巽巽坎
坎震乾离震震巽艮震兑坎乾离艮巽艮离兑坎巽震
乾兑巽离兑巽艮艮兑兑巽巽震乾艮震兑巽艮坎震

根据提示为先天八卦，乾-0、兑-1、离-2、震-3、巽-4、坎-5、艮-6、坤-7。一个一个替换，得到一堆8进制数



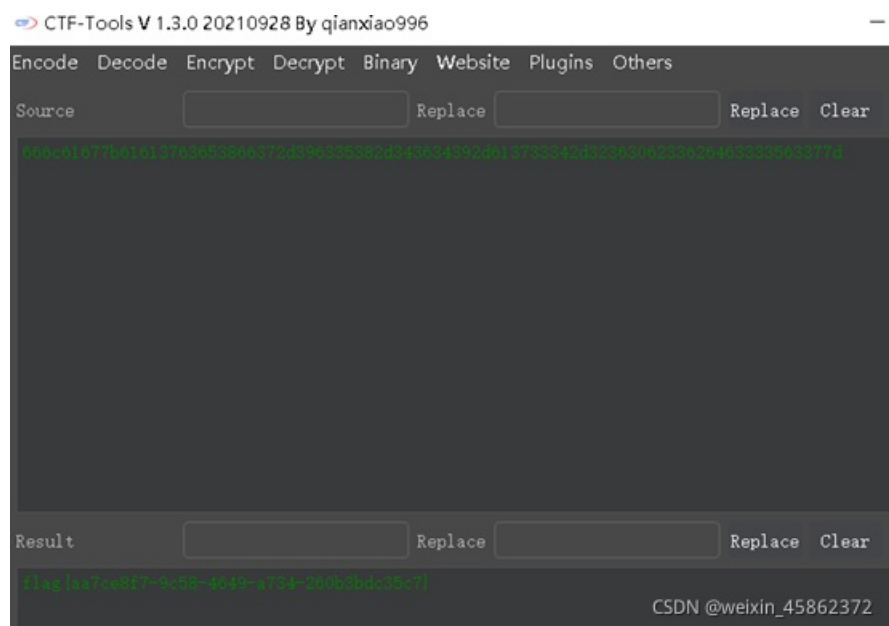
```
caogao.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
314661413167554130233543312341461562
647130632470132320661503445530233463
150264621543014214661144306314653063
3575
```

8进制转16进制



```
CTF-Tools V 1.3.0 20210928 By qianxiao996
Encode Decode Encrypt Decrypt Binary Website Plugins Others
Source [ ] Replace [ ] Replace Clear Copy Paste
3146614131675541302335433123414615626471306324701323206615034455302334631502646215430142146611443063146530633575
Result [ ] Replace [ ] Replace Clear Copy Paste
666c01677b026137636b386b372d396325382d386b34392d613753343d3266306233620463333563377d
CSDN @weixin_45862372
```

再16进制转字符串得到flag



```
CTF-Tools V 1.3.0 20210928 By qianxiao996
Encode Decode Encrypt Decrypt Binary Website Plugins Others
Source [ ] Replace [ ] Replace Clear
666c01677b026137636b386b372d396325382d386b34392d613753343d3266306233620463333563377d
Result [ ] Replace [ ] Replace Clear
[flag{aa7ce8f7-9c58-4649-a734-260b3bdc35c7}]
CSDN @weixin_45862372
```

Flag值: flag{aa7ce8f7-9c58-4649-a734-260b3bdc35c7}

解法一：将16张图片放到word里面拼凑，先把四个角的图片位置确定，就是那4张带有方块的图，从每张图的边缘痕迹很容易看出旁边的那种图是哪一张。完全可以手动拼。

解法二：montage可以实现拼图功能，montage *.png -tile 4x4 -geometry +0+0 test.png将16张图拼成一张完整的图，再用github上的一款神器将图片进行调整，<https://github.com/Keytie21/gaps>。

命令：gaps -image=test.png --generation=30 --population=300 --size=65

解法三：将文件名md5解密，即是图片的顺序

Flag值：flag{aa7ce8f7-9c58-4649-a734-260b3bdc35c7}

miao

Wav音频的隐写，先放到AU里面查看频谱，无果放到hxd.exe里面看看有无文件隐写，无果。用slienteyes打开，看看是否存在lsb隐写，无果。用steghide查看隐藏信息，发现flag文件。

```
D:\CTF---CTF\MISC\steghide-0.5.1-win32\steghide>steghide info miao.wav
"miao.wav":
  format: wave audio, PCM encoding
  capacity: 93.7 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "flag":
    size: 42.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
D:\CTF---CTF\MISC\steghide-0.5.1-win32\steghide>
```

将隐写文件提取出来，密码为空

```
D:\CTF---CTF\MISC\steghide-0.5.1-win32\steghide>steghide extract -sf miao.wav
Enter passphrase:
the file "flag" does already exist. overwrite ? (y/n)
steghide: did not write to file "flag".
D:\CTF---CTF\MISC\steghide-0.5.1-win32\steghide>
```

用txt打开就是flag

Flag值：flag{0f83ca08-c51c-4574-b2cd-bbdd786ae807}

babyrgb

.DStore文件为苹果自带的文件，不用管，打开图片是中山市的地图，放到hxd里面查看是否有信息，无果，用stegsolve.jar打开，没看到异常，于是就用kali的zetsg打开看看是否为lsb隐写，即可看到flag

```
root@kali:~/桌面# zsteg ditu.png -a
imagedata .. file: MIPS-EL BE MIPS-II ECOFF executable stripped - version 0.0
b2,g,lsb,yx .. text: "UUnn5bUU"
b2,g,msb,yx .. text: ["U" repeated 10 times]
b2,b,msb,yx .. text: ["U" repeated 12 times]
b4,r,lsb,yx .. text: "R000000000"
b4,r,msb,yx .. text: "3 \\"
b4,g,lsb,yx .. text: "D00000003\"
b4,b,msb,yx .. text: "D33333333\"
b4,rgb,lsb,yx .. text: "Dfffc3UTD\"
b4,bgr,lsb,yx .. text: "Dfffc3UTD\"
b4,bgr,msb,yx .. text: "J0L t'nZe"
b7,bgr,msb,yx .. text: "ws1\\t<.D"
b8,r,lsb,yx .. text: "flag(9d663542-4c95-44fc-8e8f-311e336b3dc2)"
b8,r,msb,yx .. text: "A!!!!!!!!!!!!!!>"
b8,g,lsb,yx .. text: "flag(9d663542-4c95-44fc-8e8f-311e336b3dc2)"
b8,g,msb,yx .. text: "EEEEEEEEEEEEEE95q)"
b8,b,lsb,yx .. text: "flag(9d663542-4c95-44fc-8e8f-311e336b3dc2)"
b8,b,msb,yx .. text: "CC=====
b8,rgb,lsb,yx .. text: "fffflllaaggg{{{999ddd060606333555444222---444ccc999555---444444ffffcc---888eee888f
33666bb333ddccc222}}}"
b8,rgb,msb,yx .. text: "666llllll"
b8,bgr,lsb,yx .. text: "fffflllaaggg{{{999ddd060606333555444222---444ccc999555---444444ffffcc---888eee888f
33666bb333ddccc222}}}"
b8,bgr,msb,yx .. text: "666llllll"
b3,rgb,msb,yx,prime .. text: "--n)nk07o"
```

Flag值：flag{9d663542-4c95-44fc-8e8f-311e336b3dc2}

brokenpassword

题目给了一个压缩包和一个1.txt，找不出1.txt里面有什么规律，从压缩包入手，爆破数字密码，无果，winhex分析不是伪加密，明文模式爆破无果，使用字典爆破，密码是american，打开flag.txt即可

Password successfully recovered !

Advanced Archive Password Recovery statistics:	
Total passwords	7,302
Total time	29ms
Average speed (passwords per second)	251,793
Password for this file	american
Password in HEX	61 6d 65 72 69 63 61 6e

 Save...  OK

Flag值：flag{5BAF2AB2-3C15-4B6D-9BC4-51BCC27B718E}

总结

本人misc混子选手，等了好几天的wp，发现没多少人写这个比赛的wp，于是决定记录一下，并希望其他大佬能把其他题的wp发出来学习学习。。。



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)