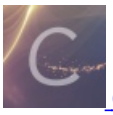
香山杯CTF WP

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

本文链接：https://blog.csdn.net/weixin_45862372/article/details/121344447

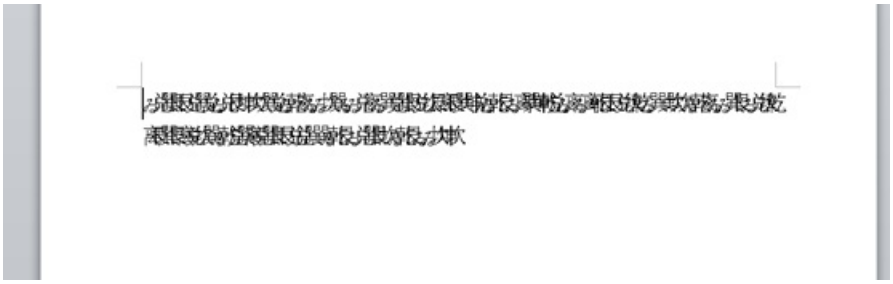


香山杯CTF WP

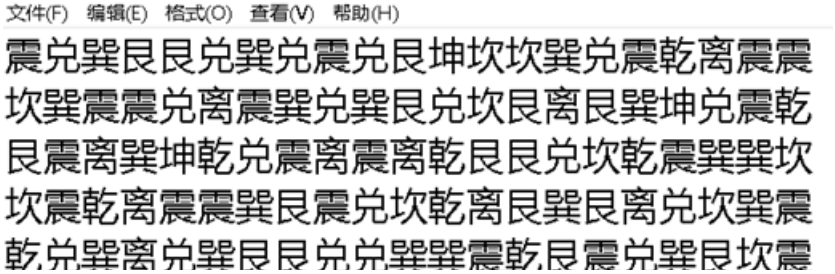
MISC

你悟了吗

拿到.rtf文件打开

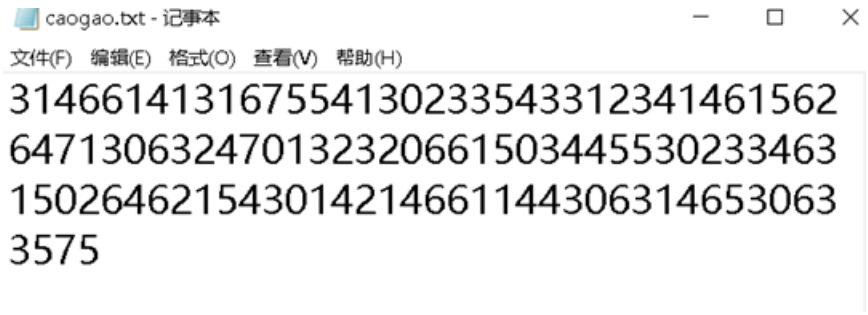


全选复制粘贴到txt里面

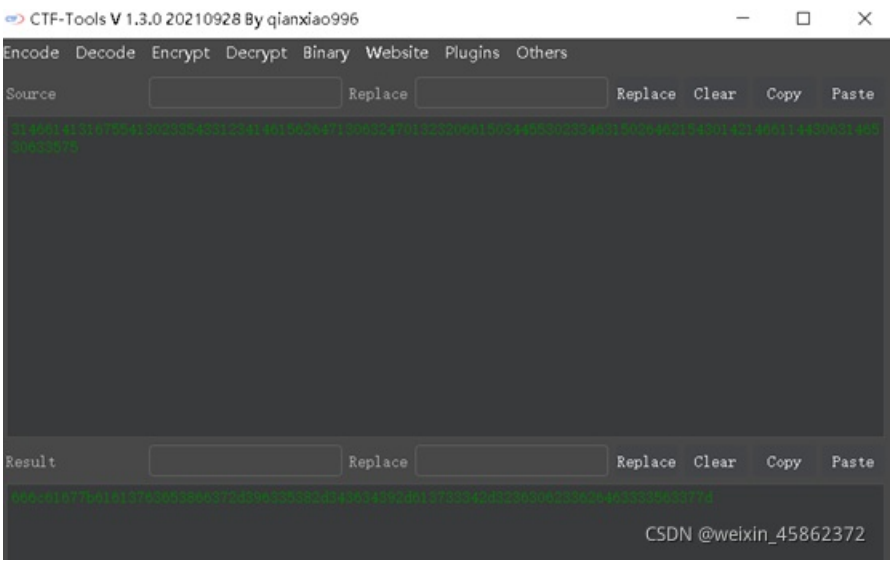


乾艮震震坎坤坎

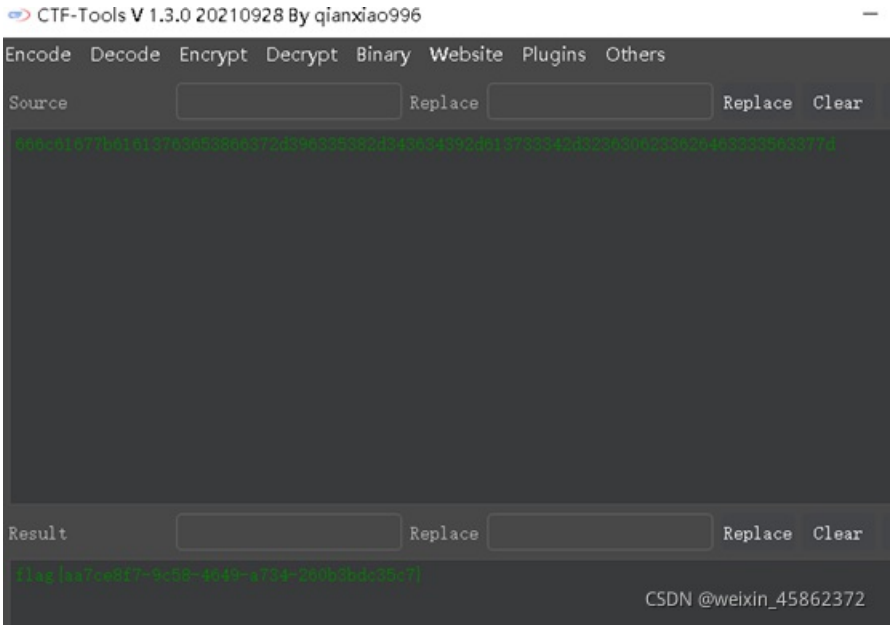
根据提示为先天八卦，乾-0、兑-1、离-2、震-3、巽-4、坎-5、艮-6、坤-7。一个一个替换，得到一堆8进制数



8进制转16进制



再16进制转字符串得到flag



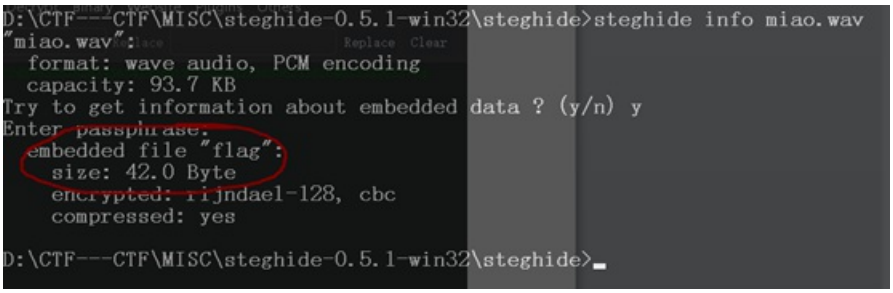
Flag值：flag{aa7ce8f7-9c58-4649-a734-260b3bdc35c7}

qrcode

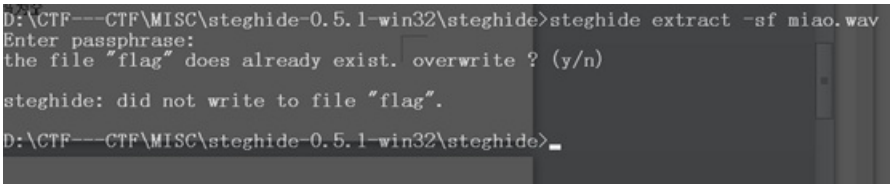
解法一：将16张图片放到word里面拼凑，先把四个角的图片位置确定，就是那4张带有方块的图，从每张图的边缘痕迹很容易看得出旁边的那种图是哪一张。完全可以手动拼。
解法二：montage可以实现拼图功能，montage *.png -tile 4x4 -geometry +0+0 test.png将16张图拼成一张完整的图，再用github上的一款神器将图片进行调整，https://github.com/Keytie21/gaps。
命令：gaps --image=test.png --generation=30 --population=300 --size=65
解法三：将文件名md5解密，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.



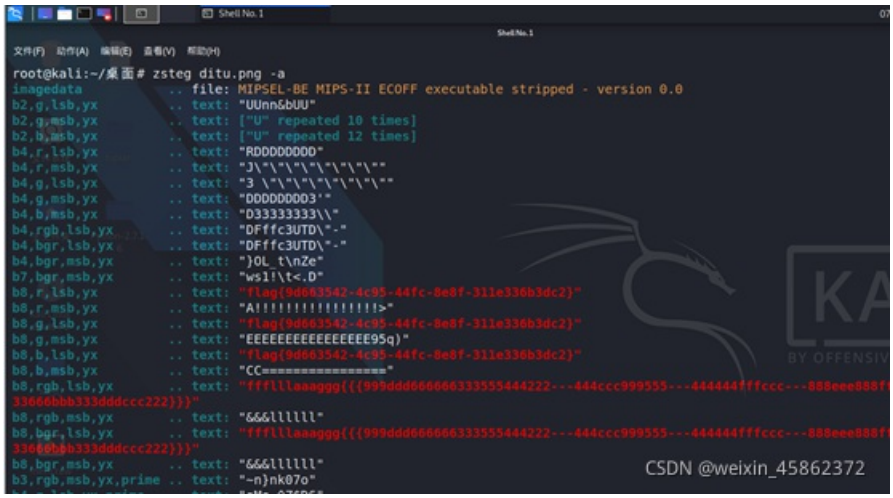
将隐写文件提取出来，密码为空



用txt打开就是flag
Flag值：flag{0f83ca08-c51c-4574-b2cd-bbdd786ae807}

babyrgb

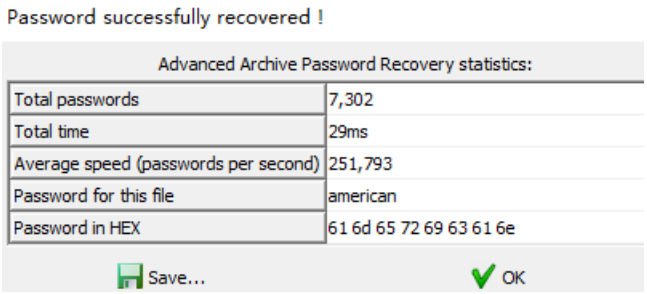
.DStore文件为苹果自带的文件，不用管，打开图片是中山市的地图，放到hxd里面查看是否有信息，无果，用stegsolve.jar打开，没看到异常，于是就用kali的zetsg打开看看是否为lsb隐写，即可看到flag



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



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。。。