ctfshow 第二届月饼杯 misc部分writeup

原创

AshMOB 于 2021-11-12 16:45:39 发布 2729 收藏

分类专栏： ctf比赛wp 文章标签： 安全

本文链接：https://blog.csdn.net/ashMOB/article/details/121291312

ctfshow 第二届月饼杯 misc部分writeup

说是部分其实就一道

月饼起义

下载得到一个损坏的zip

利用binwalk或者bandizip自带的修复都能得到一个hint.txt，解压后猜测是零宽隐写，去

Unicode Steganography with Zero-Width Characters (330k.github.io)

这解密能得到一个hint提示170

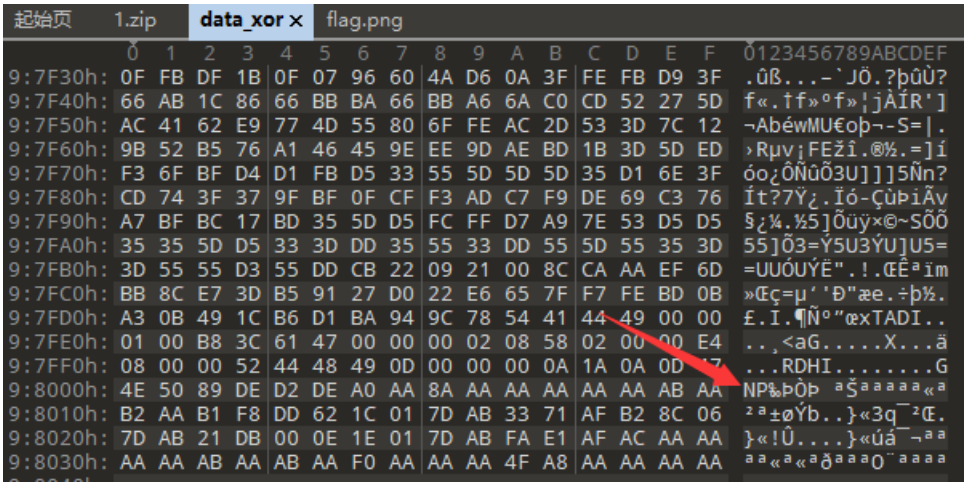
猜测原来的zip文件中还有文件，接着猜是应该要对该zip的16进制进行异或计算（经验与积累，不过我是看wp才知道的）

这一步有的师傅直接用010editer的工具—>十六进制运算—>二进制异或，选择无符号数异或170即可。

但是有的师傅是利用python来进行异或的，实际使用发现可能是python2的脚本，于是我改了一下让python3也能用了

```
#异或的脚本
f = open("data", "rb")
d=f.read(999999)
f = open("data_xor", "ab")
for i in d:
    e = i ^ 170
    t=e.to_bytes(1,"big")
    f.write(t)
f.close()
```

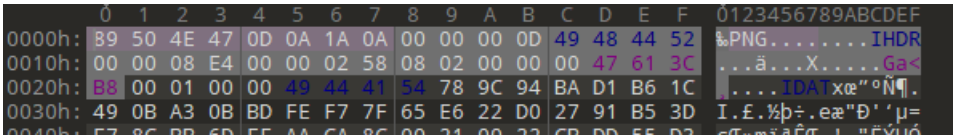
在010editer中看到文件尾有个GNP



于是将整个十六进制逆转一下

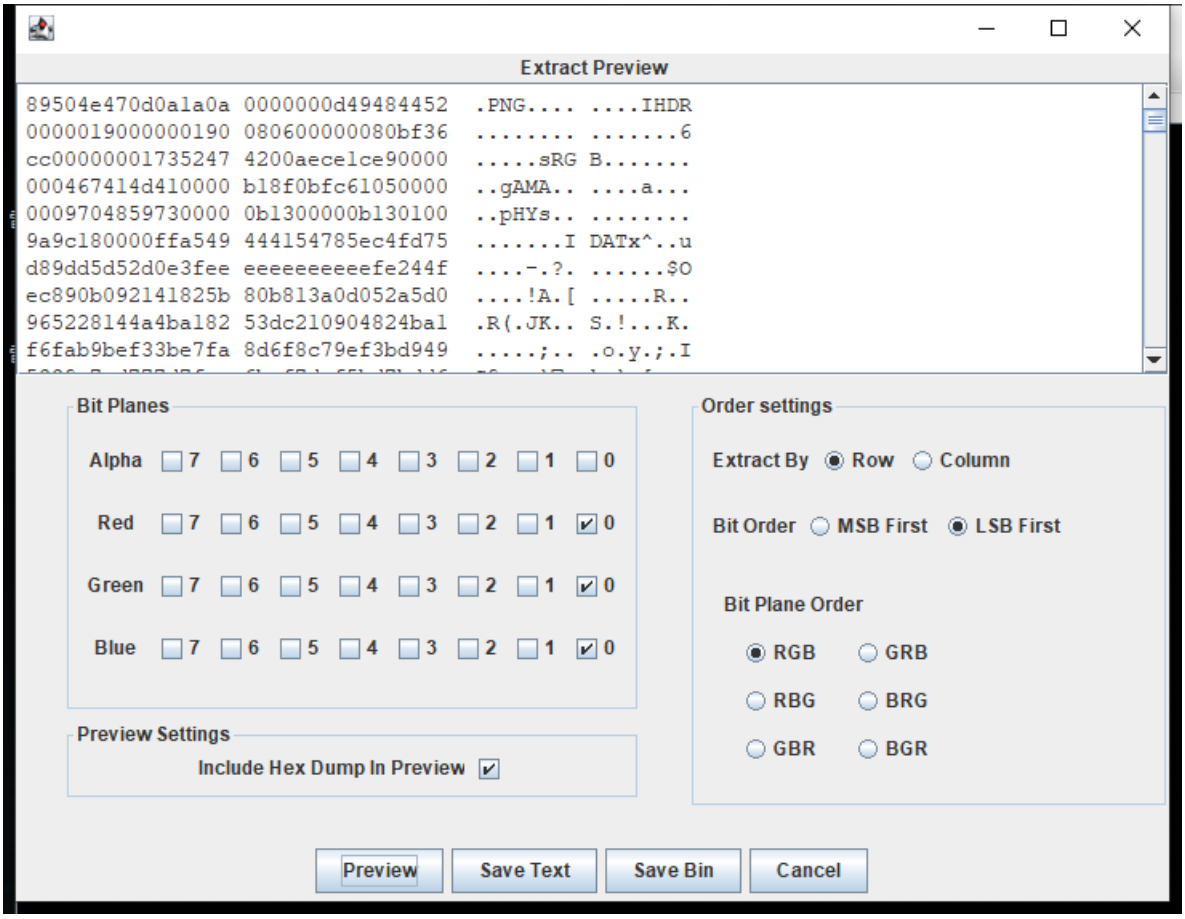
```
f=open("data_xor","rb")
d=f.read(9999999)
d=d[::-1]
f=open("flag.png","wb")
f.write(d)
f.close()
```

删减16进制文件头直到剩下这个

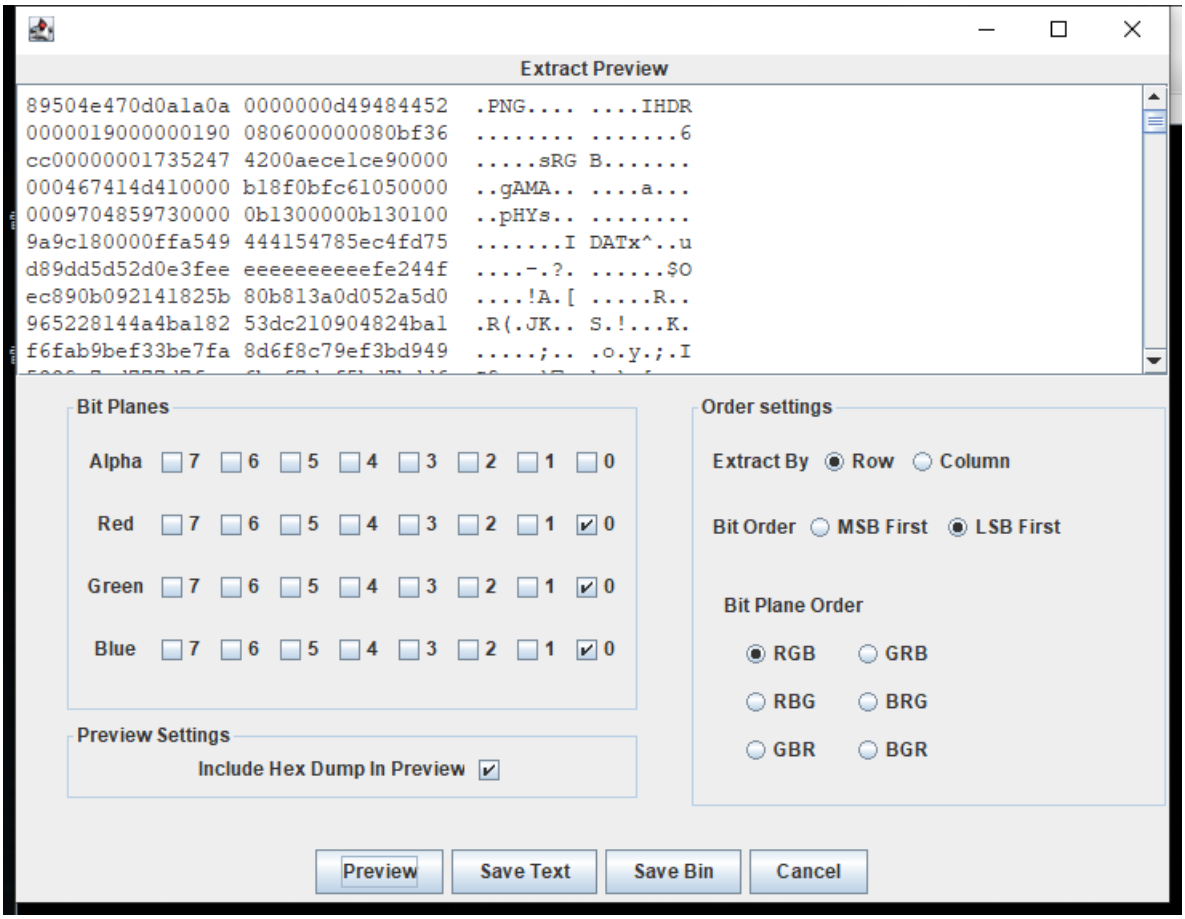


保存得到一个全黑的png文件

利用Stegsolve查看最低位



egsolve查看最低位



发现还有个png文件在里面，save bin得到该png文件即可看到flag