

XCTF-MISC-新手区：ext3

原创

1stPeak 于 2019-12-03 15:46:45 发布 1766 收藏 6

分类专栏：CTF刷题 文章标签：XCTF

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/qq_41617034/article/details/103350213

版权



[CTF刷题 专栏收录该内容](#)

87 篇文章 22 订阅

订阅专栏

题目：

ext3 70 最佳Writeup由**hackcat**提供

难度系数： ★★1.0

题目来源： [bugku](#)

题目描述：今天是菜狗的生日，他收到了一个linux系统光盘

题目场景：暂无

题目附件： [附件1](#)

题目已答对

分享wp点赞赚金币哦 [马上去写](#)

https://blog.csdn.net/qq_41617034 [查看全部评论](#)

我们下载附件1，看看里面有什么

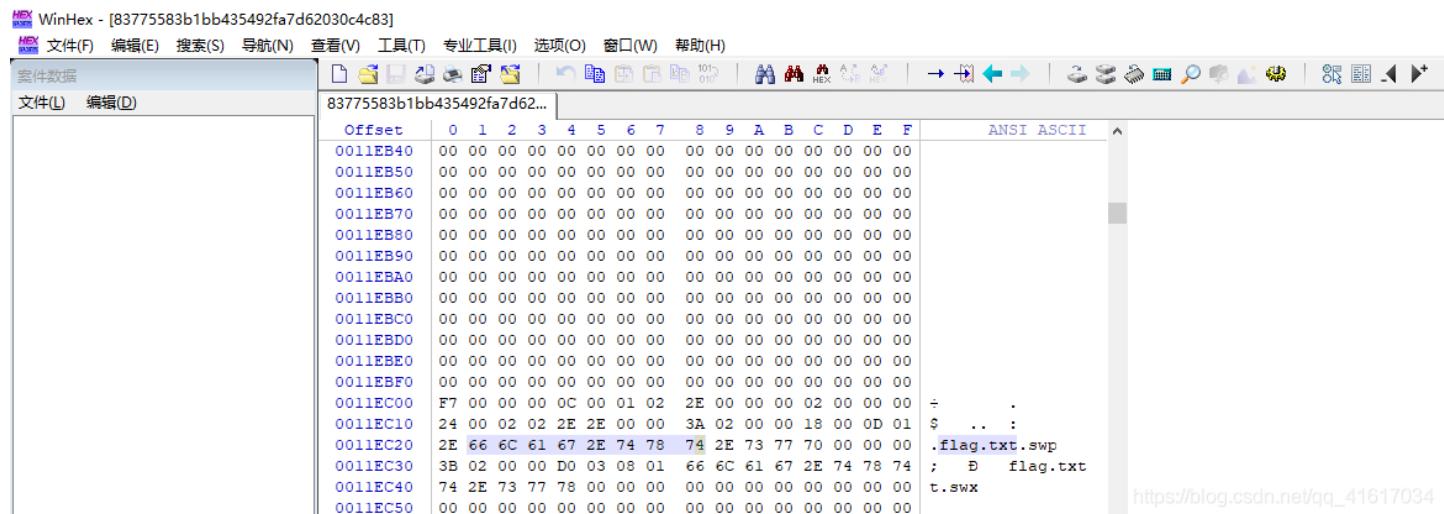
发现上图所示的一个文件，总共有两种解决方案：

1、放入Winhex

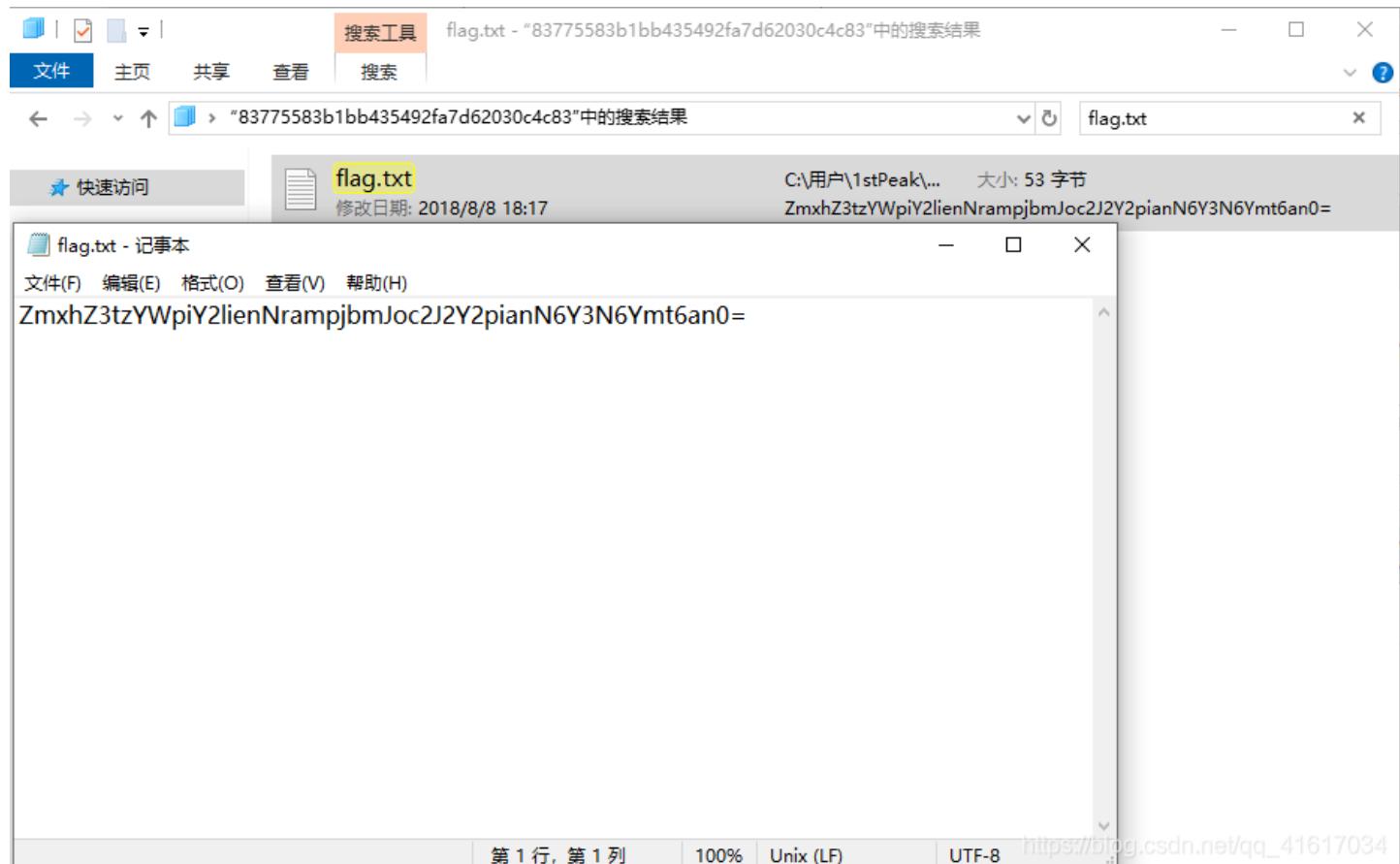
2、根据题目ext3，可以使用Linux进行挂载（ext3是一个日志文件系统，常用于Linux操作系统）

方案一：

将文件直接放入Winhex，找到flag.txt，但是我们如何打开呢？



此时，我们可以尝试，将目标文件后缀改为zip，进行解压，从而得到文件中的flag.txt文件



发现flag.txt中的数据被base64加密了，我们进行解密

The screenshot shows an online Base64 decoder. The input field contains the base64 encoded flag: 'ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0='. The output field shows the decoded result: 'flag(sajbcibzskijcnbhsbvc|bjjszcszbkzj)'. There is also a '解密Base64' button.

成功获得到flag。

方案二：

将目标文件放入kali中进行挂载

将目标文件放入linux中，可以使用默认/mnt、目录进行挂载，也可以自行创建一个目录

这里我创建一个xctf-misc目录，之后将目标文件挂载到这个目录里面

```
[root@localhost 1stpeak]# mkdir xctf-misc
[root@localhost 1stpeak]# ls
83775583b1bb435492fa7d62030c4c83 公共 视频 文档 音乐
xctf-misc 模板 图片 下载 桌面
[root@localhost 1stpeak]# mount 83775583b1bb435492fa7d62030c4c83 xctf-misc/
[root@localhost 1stpeak]# cd xctf-misc/
[root@localhost xctf-misc]# ls
02CdWGSxGPX.bin  8A2MFawD4  ix1EMRHRpIc2    n          r
0GY1l            8DQFirm0D  j6uLMX        NgzQPW      Raf3SYj
0h3a5            8HhWfV9nK1  jE           Nv          rhZE1LZ6g
0l               8nwg       jj           o           Ruc9
0qsd             8RxQG4bvd  KxEQM        07avZhikgKgbF  RZTOGd
0wDq5            FinD       LG6F          o8          scripts
0Xs              fm         Lh           00oOs      sdb.cramfs
1                g          LlC6Z0zrgy.bin  orcA       sn
2X              gtj       L00J8        oSx2p      SPaK812sYN
3                h          lost+found   OT          SrZzhSAj
3J              H          LvUGM        poiuy7Xdb  t
44aAm            H2Zj8FNbu  lWIRfzP     px6u       T
4A              hdi7      m           Q          TFGVOSwYd.txt
6JR3            hYuPvID   m9V0lIaElz   qkCN8
6wUaZE1vbsW   i          MiU         QmUY1d
7H7geL1S5      imgLDPt4BY  Mnuc        QQY3sF63w
[root@localhost xctf-misc]# find / -name flag.txt
/home/1stpeak/xctf-misc/07avZhikgKgbF/flag.txt
[root@localhost xctf-misc]# cd 07avZhikgKgbF/
[root@localhost 07avZhikgKgbF]# ls
flag.txt
[root@localhost 07avZhikgKgbF]# cat flag.txt
ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=
[root@localhost 07avZhikgKgbF]#
```

发现flag是进行base64加密的，这时，我们将base64进行解密

Base64:

解密 Base64:

解密
Base64



创作打卡挑战赛 >

赢取流量/现金/CSDN周边激励大奖