GKCTF：MISCwp

原创

FW_ENJOEY 于 2021-06-29 22:53:43 发布 131 收藏 2

分类专栏： 比赛题 CTF_MISC_Writeup

本文链接：https://blog.csdn.net/qq_46230755/article/details/118345652

比赛题 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏

CTF_MISC_Writeup

24 篇文章 2 订阅

订阅专栏

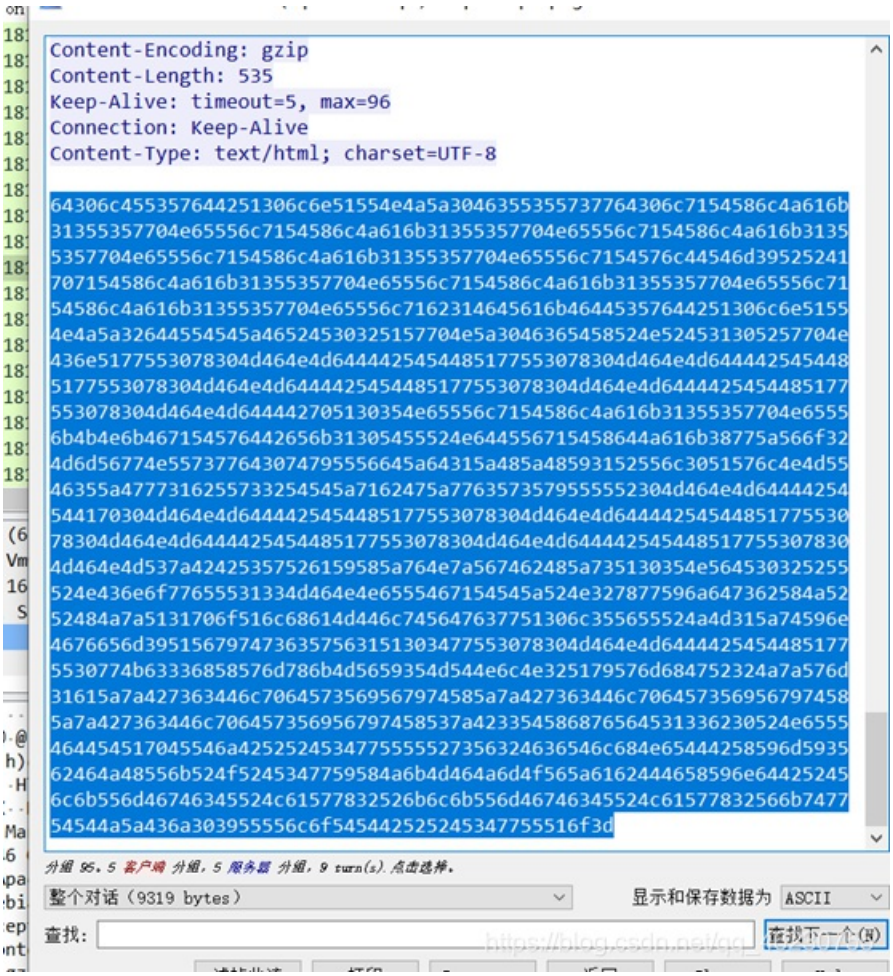
说实话挺开心的，这算是我第一次一个人比赛AK掉了全部MISC，虽然题目比较简单，在被强网杯暴虐之后做DAS的这些题目感觉还是很友好的。抱着玩玩的心态没想到可以凭借misc拿到一个优秀奖，还是蛮开心的，CTF越来越卷了，希望自己还能再打下去吧，最后，套宝，爸爸爱你。 ---- 肘子战队

套宝yyds

- 签到
- 你知道apng吗
- 银杏岛の奇妙冒险
- FireFox Forensics
- excel 骚操作
- 0.03

签到

利用wireshark观察http流



然后hex解码一下

然后base64解一下

文本倒序一下

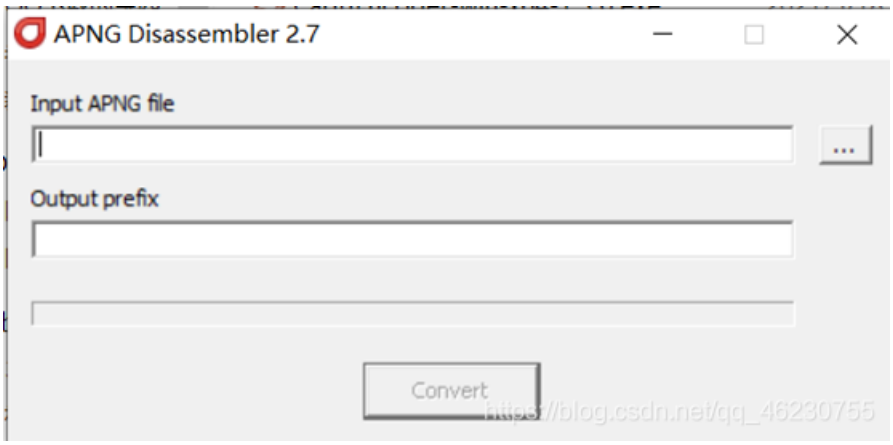
在进行一次base64

猜测后得到flag

```
flag{Welc0me_GkC4F_m1siCCCCCC!}
```

你知道apng吗

利用apng软件分离



然后得到许多图片
发现4张图片里面有比较奇怪的二维码
然后10的在Red通道里面

02的用ps拉伸一下扫描
剩下两个直接用微信扫的。

```
flag{a3c7e4e5-9b9d-ad20-0327-288a235370ea}
```

银杏岛の奇妙冒险

玩mc可太有意思了，进去里面，
先找那个男人，聊天聊完从屋子旁边拿到一把弓箭。然后和她老妈说完话，就去干boss了，前两个boss我神箭手直接射死。re爹卡了我好久，自己来就算了还带一堆小弟，我小小盾牌防不住啊。然后就很不爽去网上找语句附魔

/give @p diamond_sword 1 0 {ench:[{id:16,lvl:32767}]}
然后就去干掉对手，
最后的

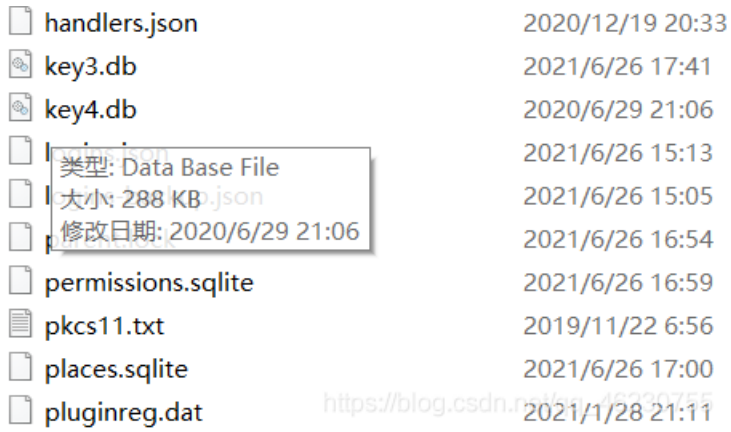
part 1 w3lc0me_ part 2 291 -95 67	part 2 t0_9kctf_ part 3 324 -190 79	part 3 2021_ part 4 362 -144 69	Part 4 Check_1n 恭喜你， 完成签到， 武运昌隆。

（可能讲的过程不是很清楚毕竟很早做了，现在才写的wp，应该是非预期了，因为我看到那个石中剑，然后老头钓鱼的那个，给了我个鱼竿，还让我钓河豚，水里毛都没有，我碰了个装置然后说水有毒，我一下水就毒死，难道河豚竟是我自己？）

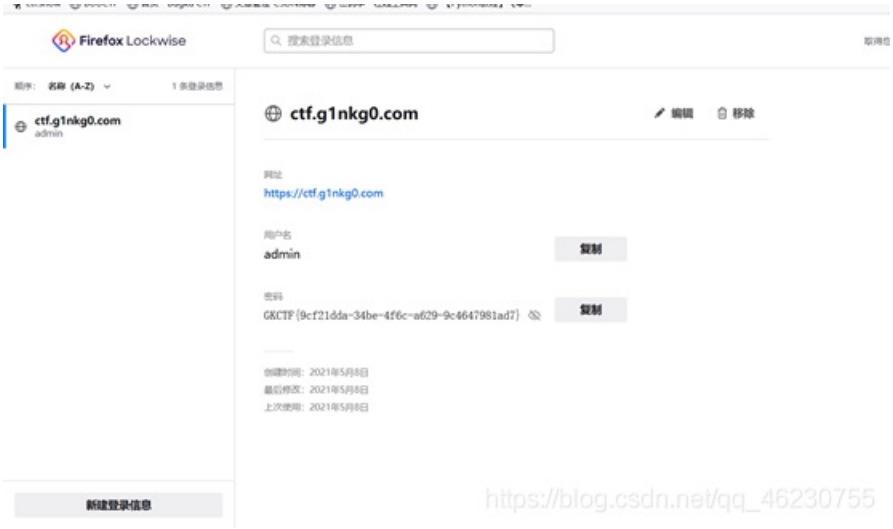
```
GKCTF{w3lc0me_t0_9kctf_2021_Check_1n}
```

FireFox Forensics

把两个文件，放到火狐的文件夹中



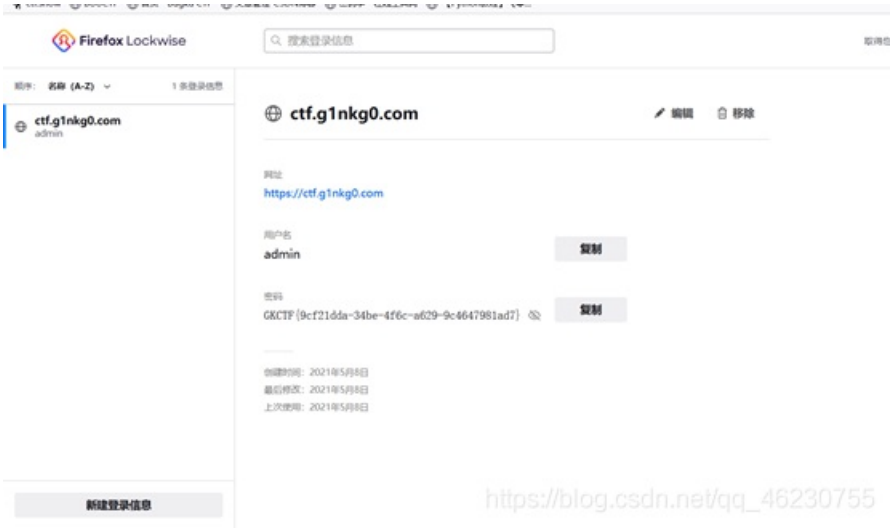
替换一下，然后直接住火狐浏览器里面查看




```
GKCTF{9cf21dda-34be-4f6c-a629-9c4647981ad7}
```

excel 骚操作

excel打开，然后发现存在1，利用execl自带的规则进行填充

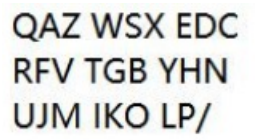


然后手机上用中国编码软件扫一下

```
flag{9ee0cb62-f443-4a72-e9a3-43c0b910757e}
```

0.03

利用ntfs隐写流得到密码本

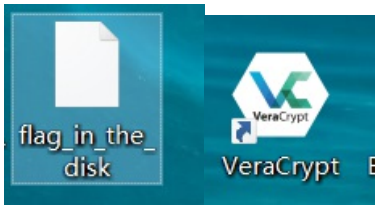


然后再sercet.txt里面有密文

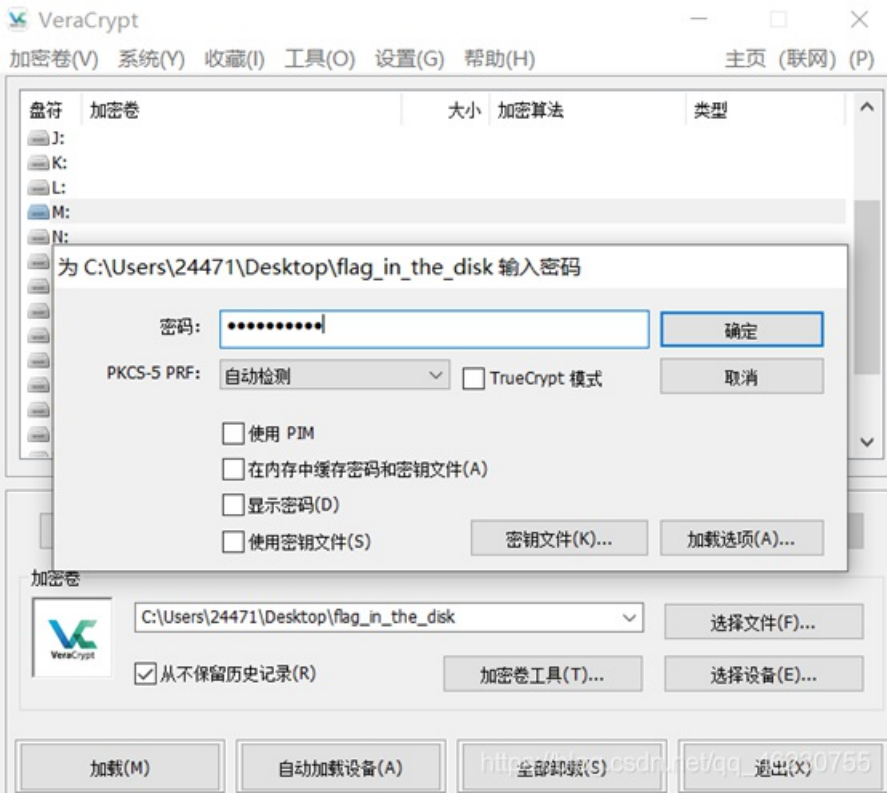
> do you believe that you get?
>
> 31122331331311212231231231311

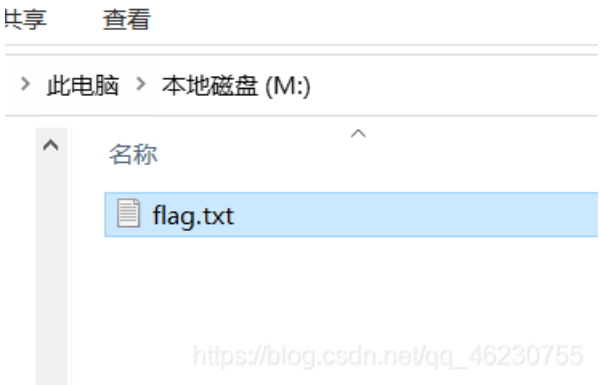
三分密码，简单分一下得到
E是第三组第一行第一个，因此类推

```
EBCCAFDDCE
```



把文件去掉zip后缀然后利用这个软件解密。
电子取证课刚好学到哈哈，运气好





然后看挂载磁盘里存在flag

```
flag{85ec0e23-ebbe-4fa7-9c8c-e8b743d0d85c}
```

[创作打卡挑战赛](#)
[赢取流量/现金/CSDN周边激励大奖](#)