BUUCTF-Misc-No.5

原创

水星Sur 于 2020-07-04 16:25:26 发布 1137 收藏 1

分类专栏： BUUCTF Misc Python 文章标签： python 信息安全

本文链接：https://blog.csdn.net/pone2233/article/details/107126086


BUUCTF 同时被 3 个专栏收录

21 篇文章 2 订阅

订阅专栏


Misc

22 篇文章 0 订阅

订阅专栏


Python

5 篇文章 0 订阅

订阅专栏

文章目录

比赛信息

内心os（蛮重要的）

Misc：

[BSidesSF2019]zippy | SOLVED |

[ACTF新生赛2020]明文攻击 | SOLVED |

[GKCTF2020]Pokémon | SOLVED |

[GWCTF2019]huyao | SOLVED |

[SCTF2019]电单车 | SOLVED |

[GKCTF2020]code obfuscation | SOLVED |

[GKCTF2020]Harley Quinn | SOLVED |

[SUCTF2018]followme | SOLVED |

voip | SOLVED |

BJD&DAS CTF 2020 | Questionnaire | SOLVED |

BJD&DAS CTF 2020 | /bin/cat 2 | SOLVED |

[*CTF2019]otaku | SOLVED |

[UTCTF2020]docx | SOLVED |

[UTCTF2020]basic-forensics | SOLVED |

[UTCTF2020]zero | SOLVED |

比赛信息

比赛地址：Buuctf靶场

内心os（蛮重要的）

对不起我就是鸽子本精Σ(っ °Д °;)っ呜呜呜

Misc：

[BSidesSF2019]zippy | SOLVED |

下载，使用foremost，分离得到一个压缩包，

发现是带锁的

，发现了zip的密码

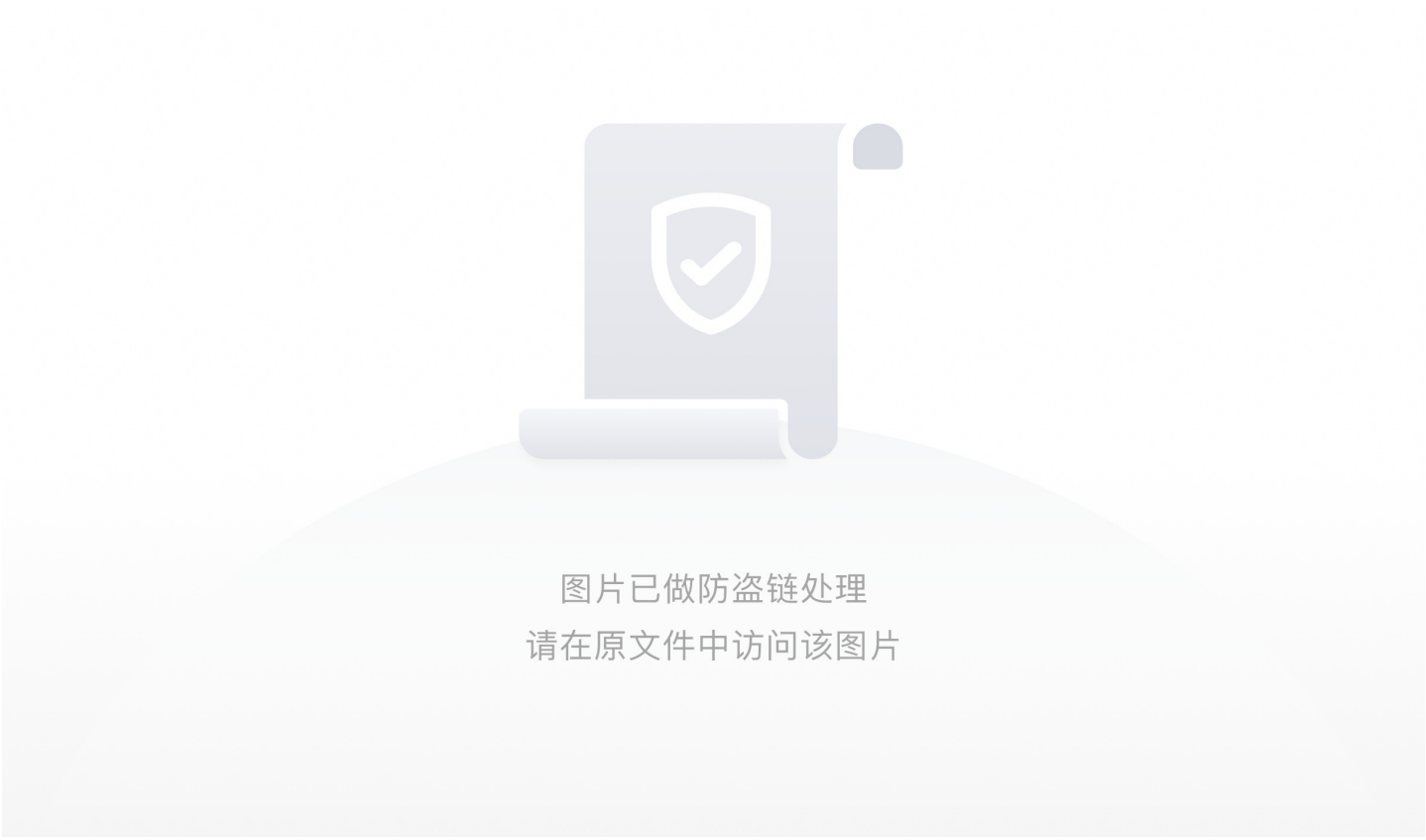
```
unzip -P supercomplexpassword flag.zip
```


```
CTF{this_flag_is_your_flag}
```

[ACTF新生赛2020]明文攻击 | SOLVED |

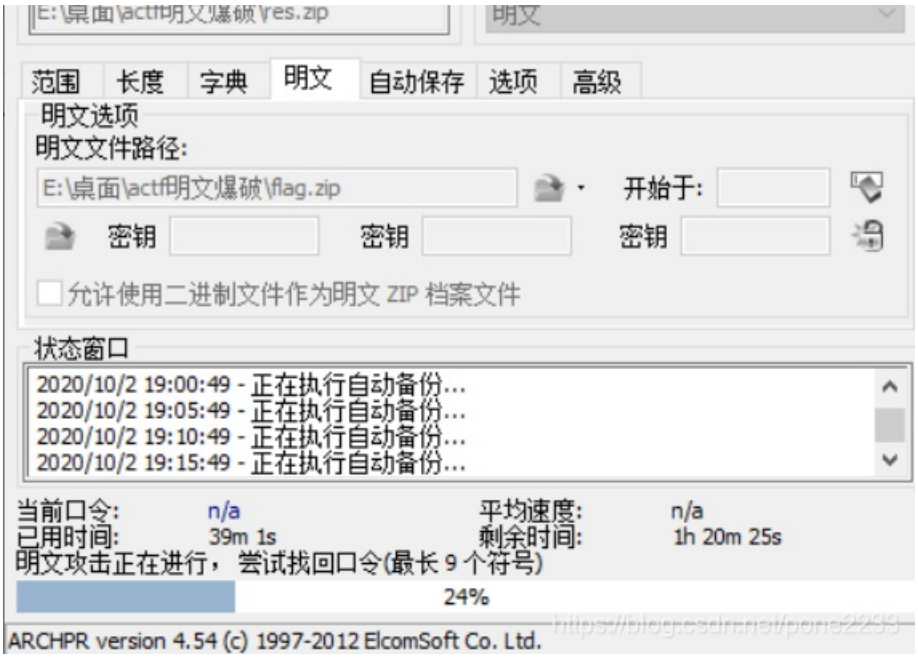
下载解压，发现一个带锁的zip和一张图片，图片放进winhex

最下面发现一个zip就少了一个pk头

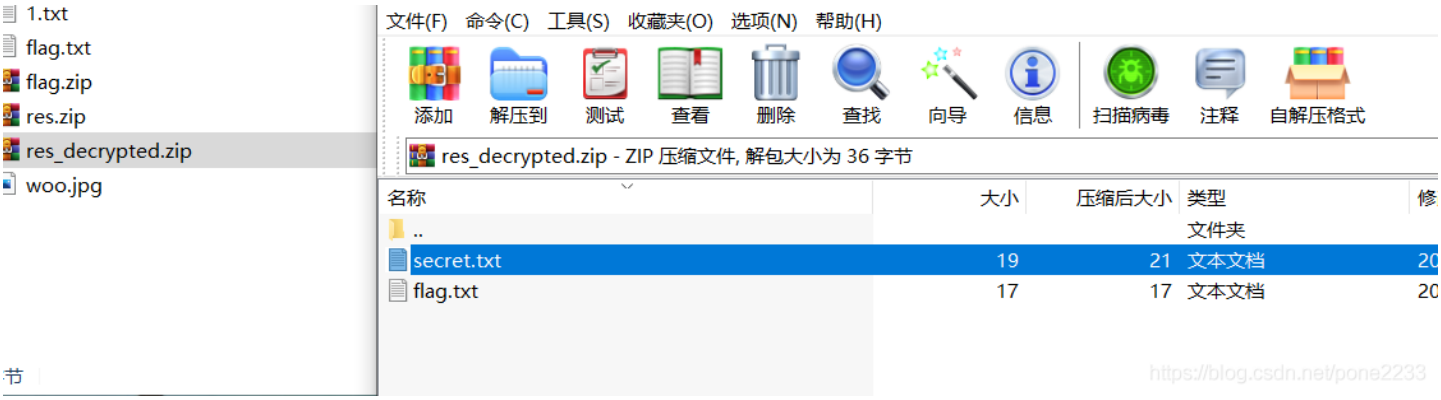


到这一步我们了解一下明文爆破的必要条件

重要的还是CRC要一致，接下来我们就可以进行使用软件跑一下



大概跑了30分钟，可能很短就可以了，我这时候去吃个饭回来点击停止按钮他会有一个保存页面弹出，保存一下就有无密码的zip了



flag就出来拉

```
ACTF{3te9_nbb_ahh8}
```

[GKCTF2020]Pokémon | SOLVED |

下载软件，在下载一个模拟器，走到103街道就能看到flag
我推荐使用金手指呦~


```
flag{PokEmon_14_CutE}
```

[GWCTF2019]huyao | SOLVED |

一看2张png，一看就是盲水印，

```
python decode.py --original <原始图像文件> --image <图像文件> --result <结果文件>
```

然后发现了这个


```
flag{BWM_1s_c00l}
```

[SCTF2019]电单车 | SOLVED |

这个找到文献资料

然后flag 是地址嘛，就是中间那段

```
01110100101010100110
flag{01110100101010100110}
```

[GKCTF2020]code obfuscation | SOLVED |

首先他给我们一个二维码，我们修复一下

> 扫描得到
> base(gkctf)

从二维码中分离出了rar

给了一个提示，看看刚刚扫描到的。

用base58就得到了rar的密码

> CfjxaPF

解压下来一个png一个1文件

1文件打开一看就是js加密，我们解密一下就是这样了送上解密网站https://tool.lu/js

然后打开png


```
import string
s = "$Bn$Ai$An$Ac$Al$Au$Ad$Ae$Bk$Cc$As$At$Ad$Ai$Ao$By$Ah$Ce$Ai$An$At$Bk$Am$Aa$Ai$An$Bs$Bt$Cn$Ap$Ar$Ai$An$At$Bs$B
m$Aw$Dd$Al$Ac$Da$Am$Ae$Cl$De$Ao$Cl$Dj$Ak$Ac$At$Df$Bm$Bt$Cb$Ar$Ae$At$Au$Ar$An$Bk$Da$Cb$Cp"
ll = s.split('$')
list1 = ['Bk','Bm','Bn','Bs','Bt','By','Cb','Cc','Ce','Cl','Cn','Cp',
'Da','Db','Dc','Dd','De','Df','Dg','Dh','Di','Dj']
list2 = [' ','"','#','(',')','.','','<','>','_','{','}','0','1','2','3','4','5','6','7','8','9']
list3 = []
list4 = []
s = string.ascii_lowercase
for i in s:
 list3.append('A%s'%i)
 list4.append(i)
#print(list3,'\n',list4)

t = ''
for i in range(0,len(ll)):
 for j in range(0,len(list1)):
  if ll[i]==list1[j]:
   t += list2[j]
 for k in range(0,len(list3)):
  if ll[i]==list3[k]:
   t +=list4[k]
print(t)
```

得到flag{w3lc0me_4o_9kct5}

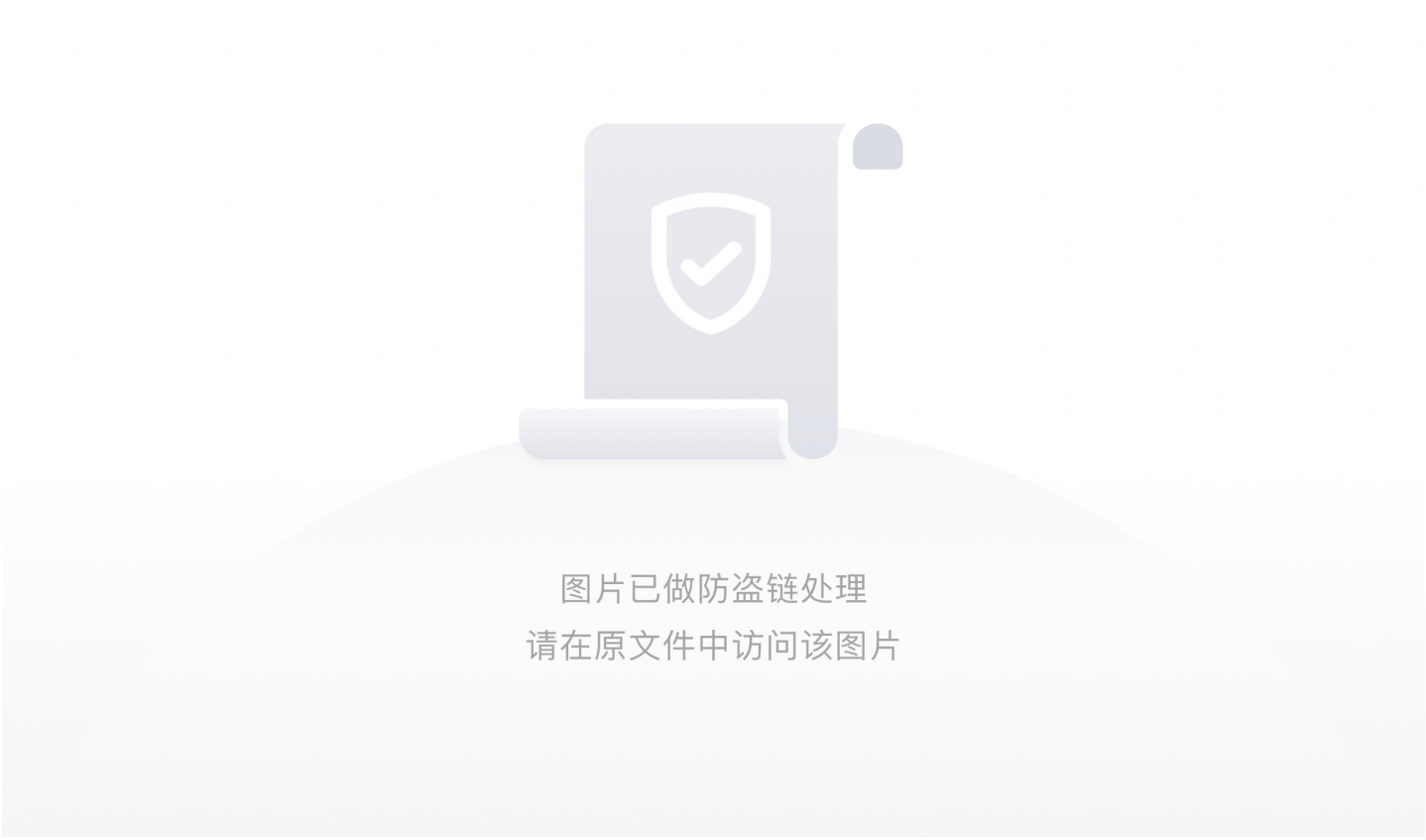
[GKCTF2020]Harley Quinn | SOLVED |

解压文件看到一个音乐，和图片，看见他的详细

知道了要听到最后面，似乎听到了按键电话的声音，然后使用之前看到大佬使用的软件点我呦，记住这个软件，最好删除其他杂音，就单独取出音频

就获得了，#22283334447777338866#

用9键盘打一下



ctfisfun,然后百度一下zip中的

最终得到了宝藏


```
flag{Pudd1n!!_y0u_F1nd_m3!}
```

[SUCTF2018]followme | SOLVED |

下载文件，然后最基础到处http

发现登录信息，从这一步大致猜到，是密码就是flag，可是有很多图片可以，都保存一一分析

最终找不到，有用的，最后就看http，最后找到了flag

> SUCTF{password_is_not_weak}

voip | SOLVED |

下载文件，百度一下，知道了这个通话数据

看到RTP

分析一下

在这一段有非常清楚的几个单词就是flag了

```
9001IVR
报上flag
flag{9001IVR}
```

BJD&DAS CTF 2020 | Questionnaire | SOLVED |

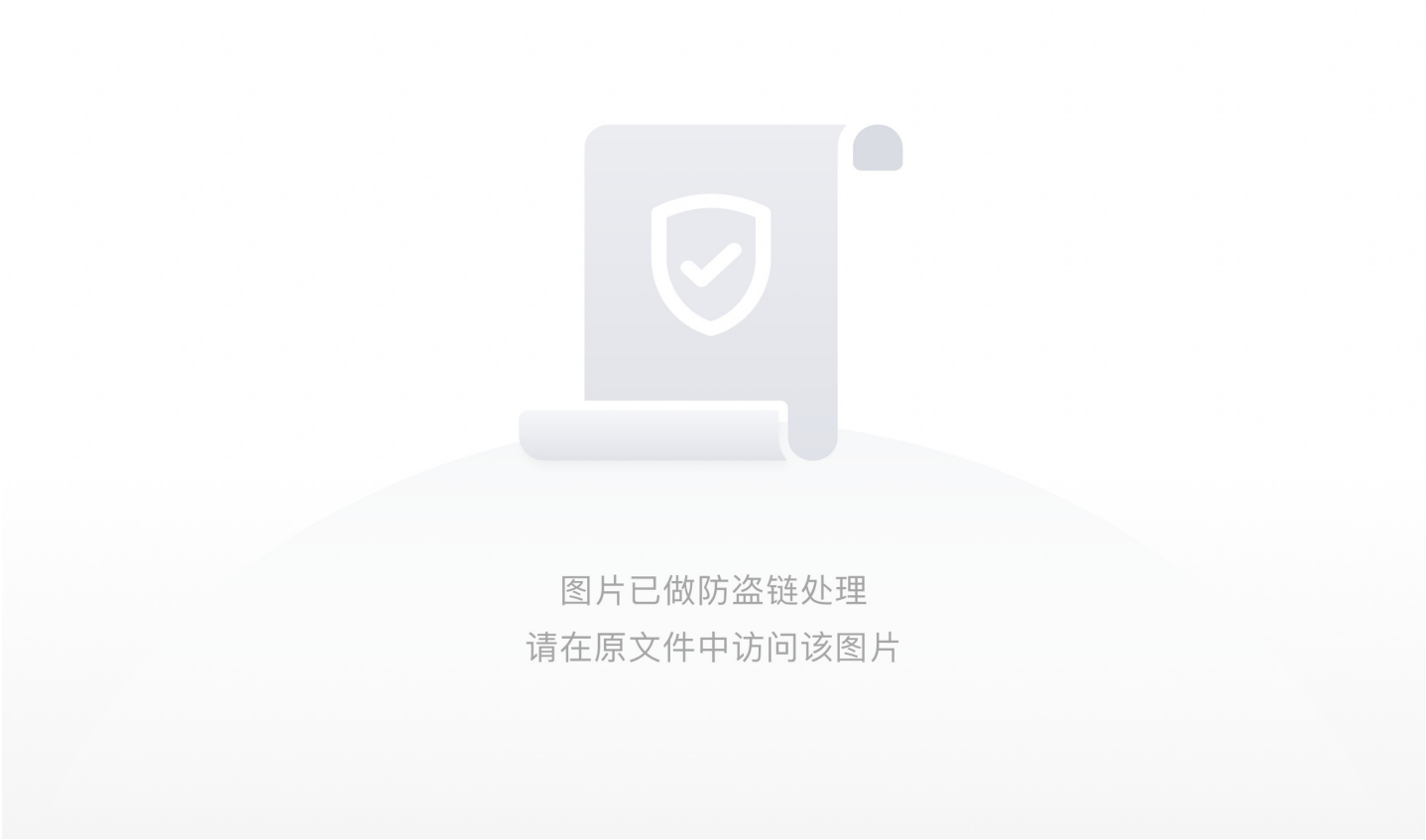
需要翻墙，打开源码一看

输入正确的地名就有一小段的flag

```
d41d8cd98f00b204e9800998ecf8427e
```

BJD&DAS CTF 2020 | /bin/cat 2 | SOLVED |

打开图片发现颜色有些不一样，然后调一下色



扫码结果

```
m1ao~miao~mi@o~Mia0~m!aO~m1a0~~~
md5
9b84eb9e7107ffafebeb1000e8c05322
```

[*CTF2019]otaku | SOLVED |

解压zip，发现有一个带锁的，还是伪加密，不过我推荐是同binwalk -e 分离，拒绝一切花里胡哨。

打开flag

是一个加密的，看来要在word 中找到密文，这一段无论无何都无法复制，我这边使用格式刷，直接复制到txt中

然后就可以明文爆破了，（PS：这里有一些问题，不能用UTF-8的编码要用，GBK，就默认使用ANSI就行了。）然后就可以爆破了

> My_waifu

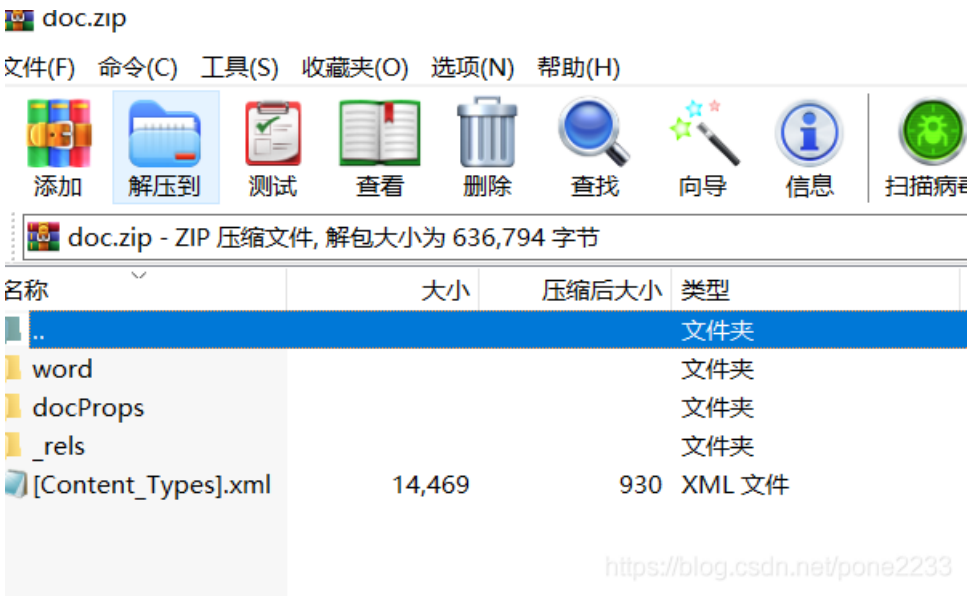
得到了zip密码了

在看图软件中用LSB找到了flag，或者使用很方便的隐写工具也行这个是下载地址哦


```
*ctf{vI0l3t_Ev3rg@RdeN}
```

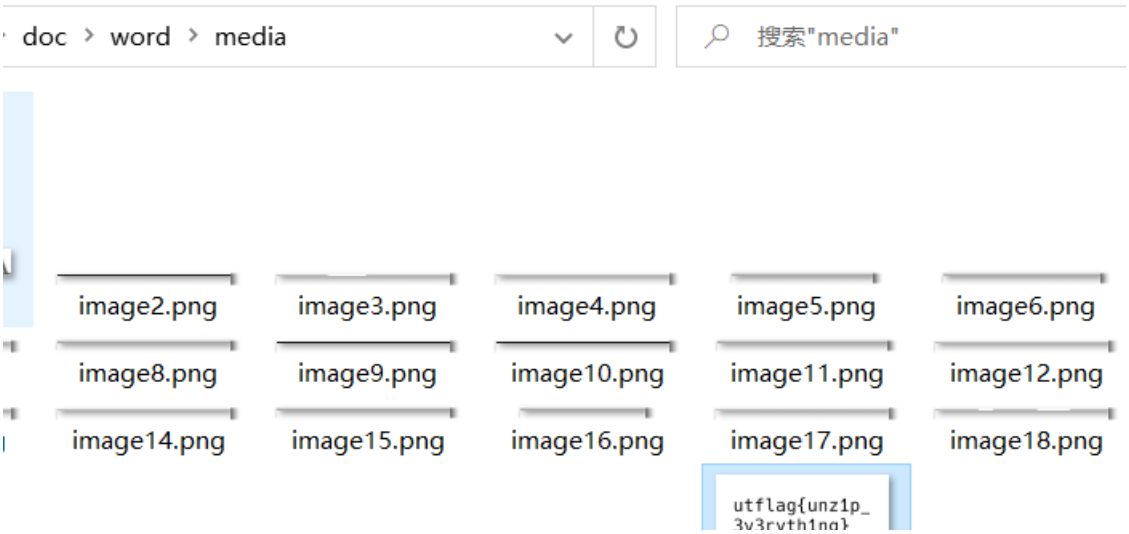
[UTCTF2020]docx | SOLVED |

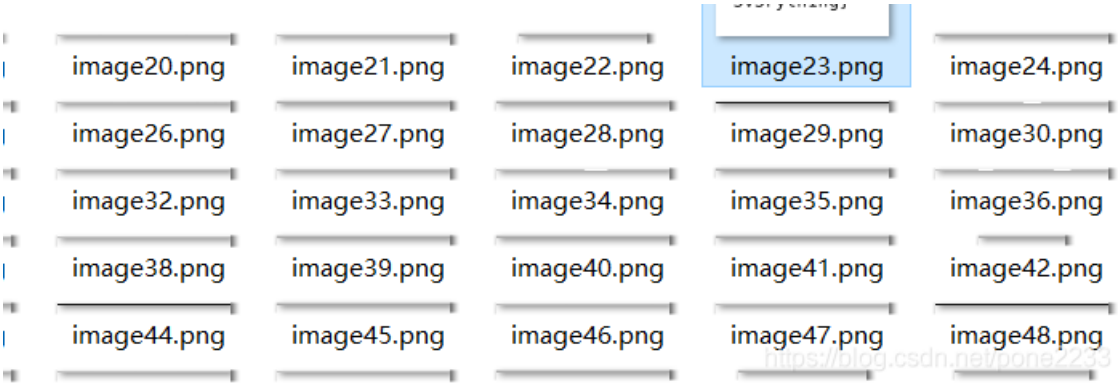
下载文件，然后docx 文件里面搜不到flag，我们就直接修改他的后缀名docx改成zip

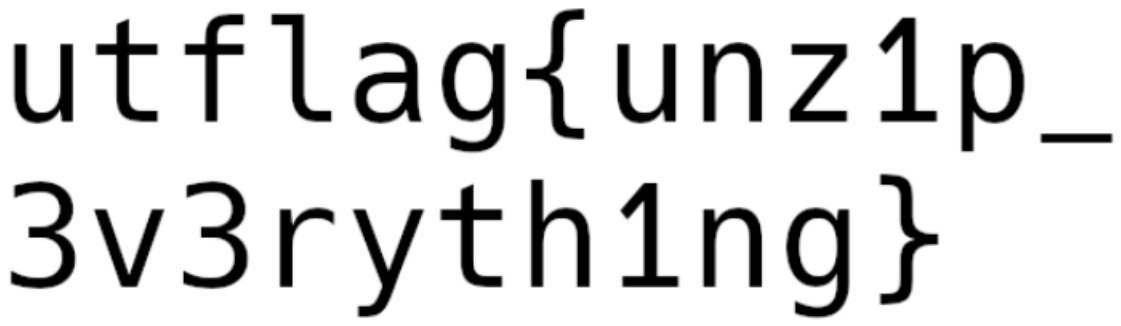


在所有文件中搜索flag

啥也没有，在文件夹中图片，找到了



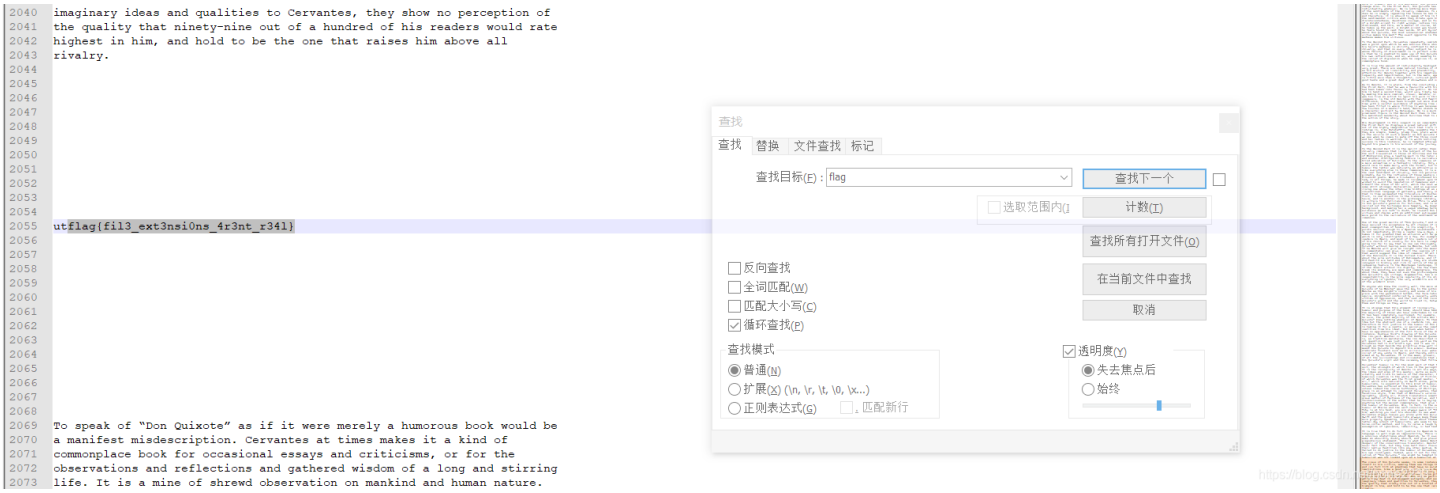




> flag{unz1p_3v3ryth1ng}

[UTCTF2020]basic-forensics | SOLVED |

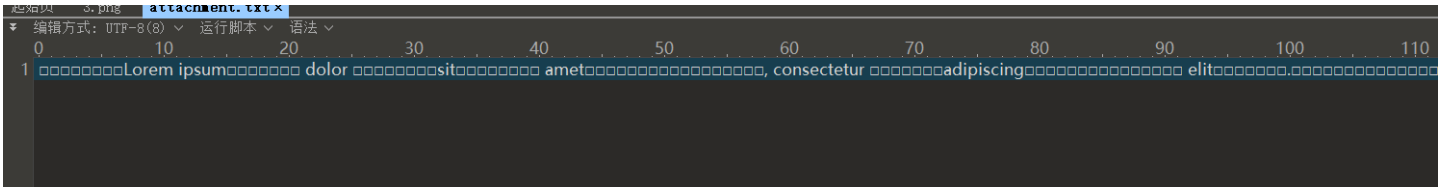
下载，发现打不开，然后拖进winhex发现就是普通的文本，然后查找一下就发现了



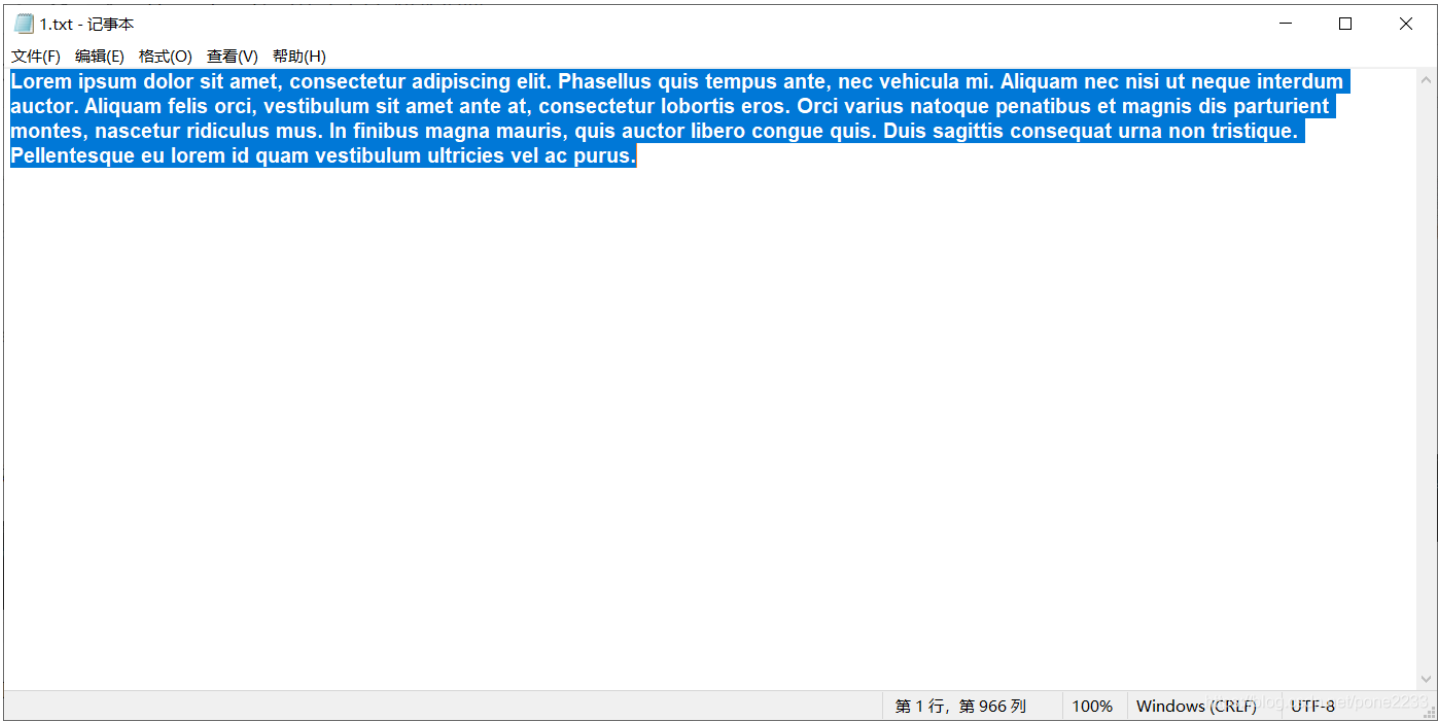
> flag{fil3_ext3nsi0ns_4r3nt_r34l}

[UTCTF2020]zero | SOLVED |

下载文件用010打开

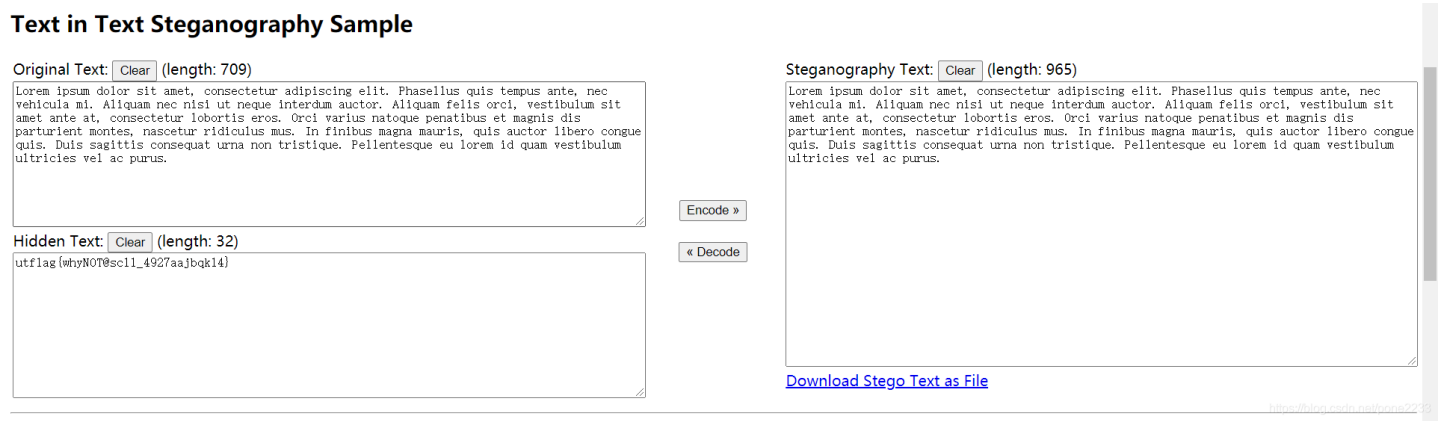


在打开txt对比



起初以为是字屏统计，然后发现不是，会报错，然后看看题目zero 是0？

百度一下，找不到，去github上面看到了一个关于零的加密，零宽度字符加密然后就有flag了



> flag{whyNOT@sc11_4927aajbqk14}

~~丸~~