**cyi WRITEUP**

## 个人信息

个人名称：cyi

个人排名：51

## 解题情况

### 请粘贴个人排名截图和答题情况截图：

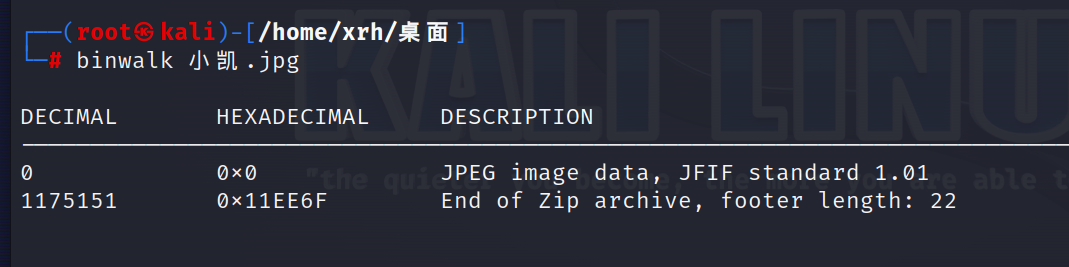


## 解题过程

### 题目序号 谁偷吃了我的外卖

### 操作内容：

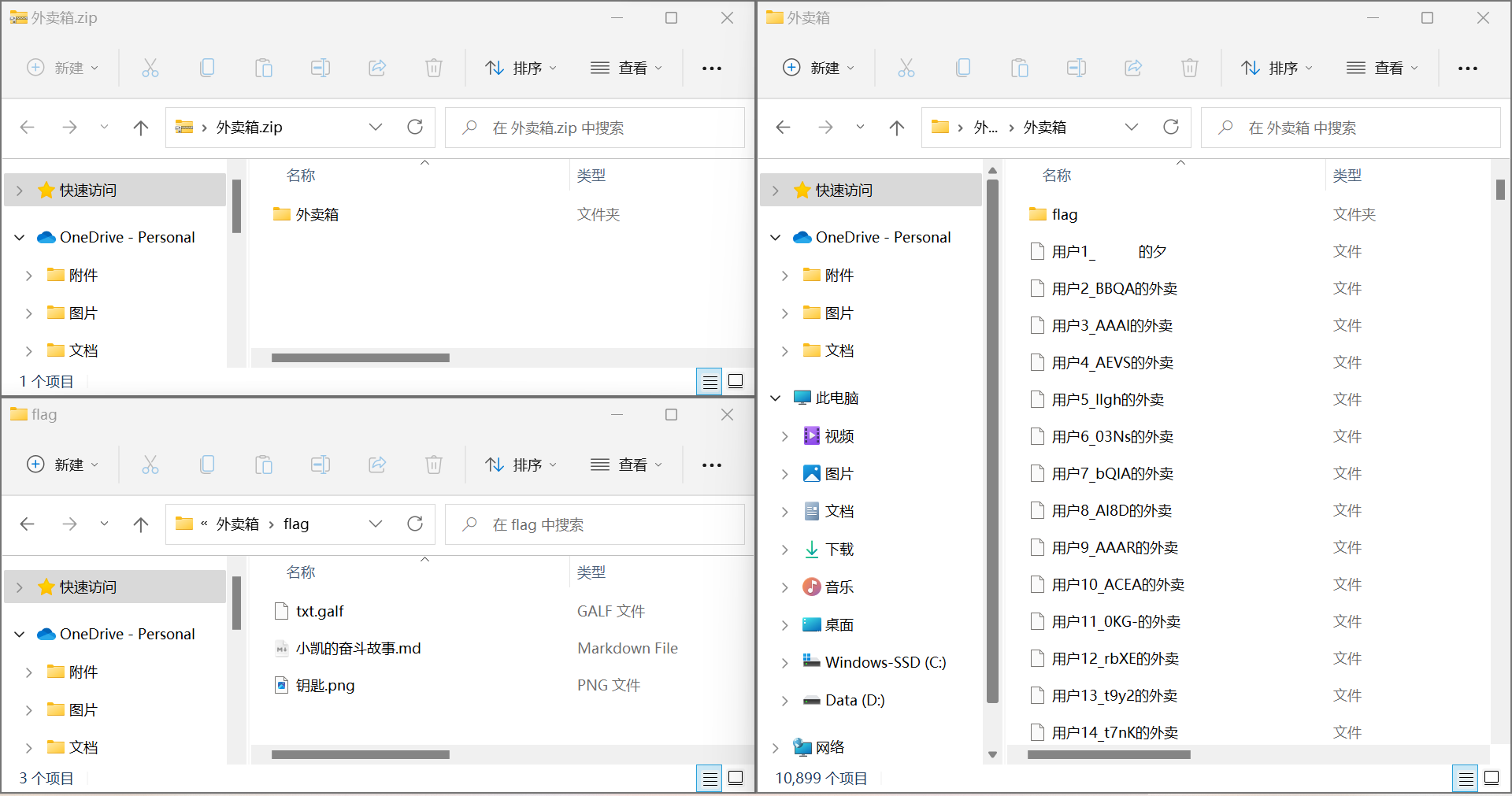
Winhex查看了一下，发现最后有个标志，直接binwalk+foremost



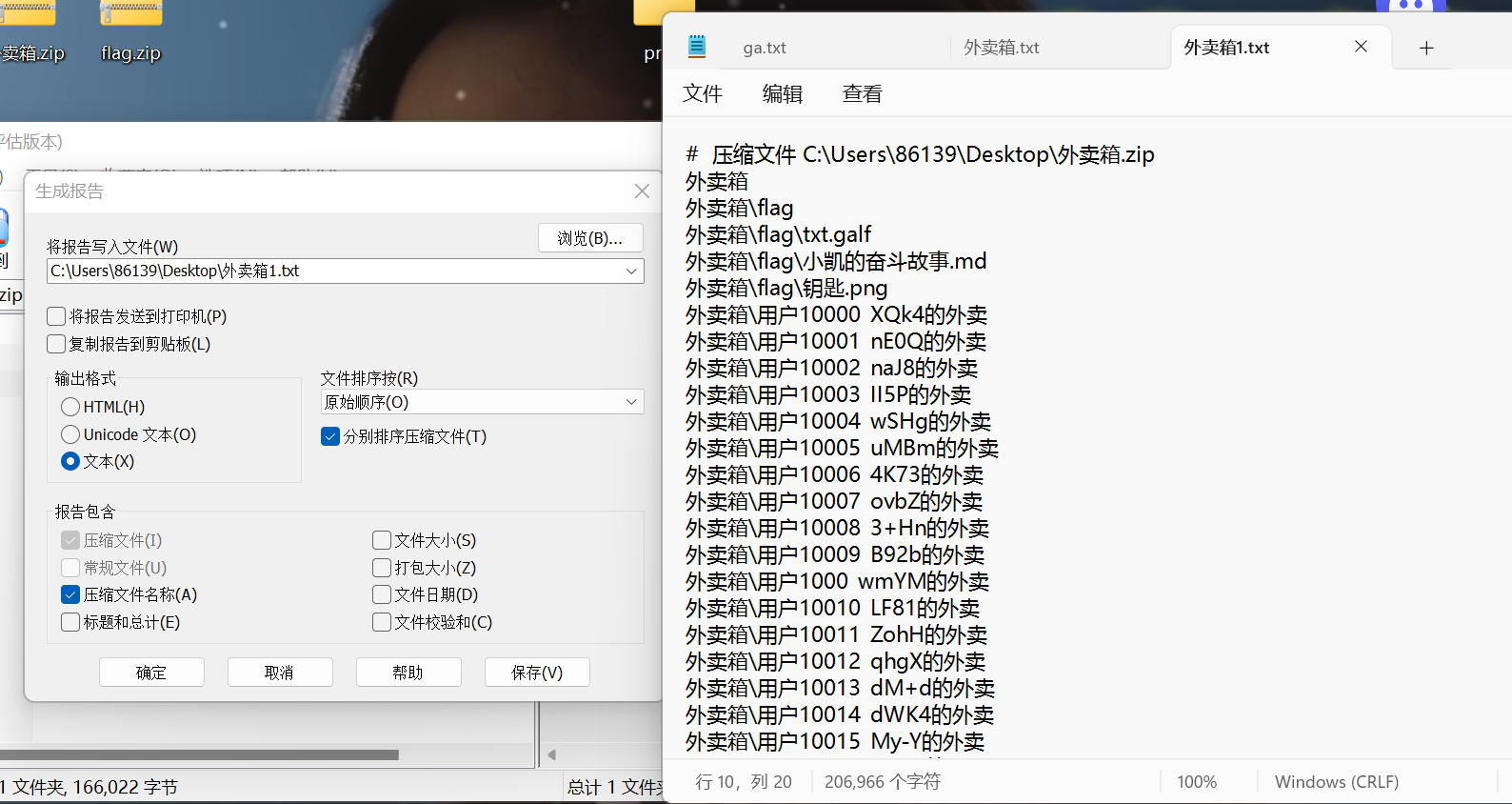
提取出一个压缩包



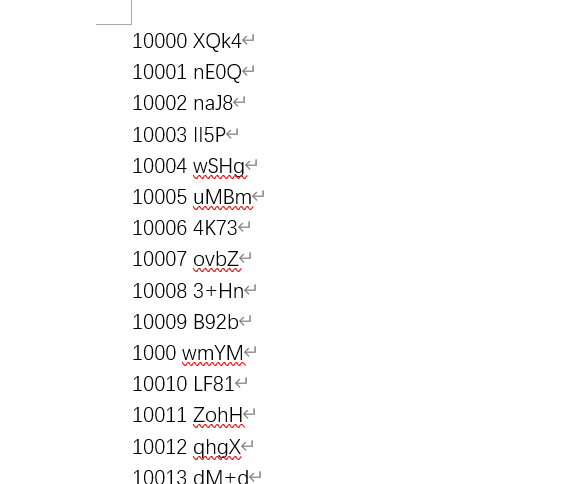
给了段注释，不知道什么用



本身还以为缺的用户1缺的四字符加上bumai（卜卖）爆破密码呢，结果爆不出，拉到最后发现==，就提一下文件名

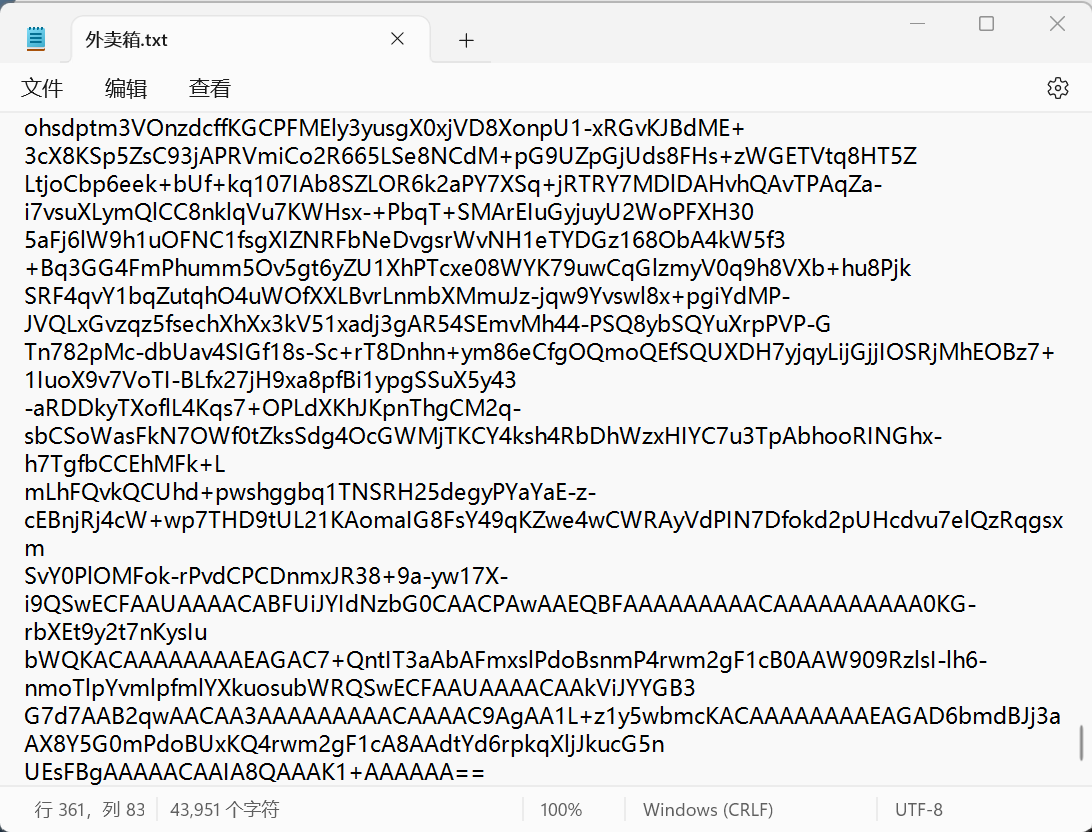


Winrar提取文件名，word删除多余字节，但还不是有序的



排序一下

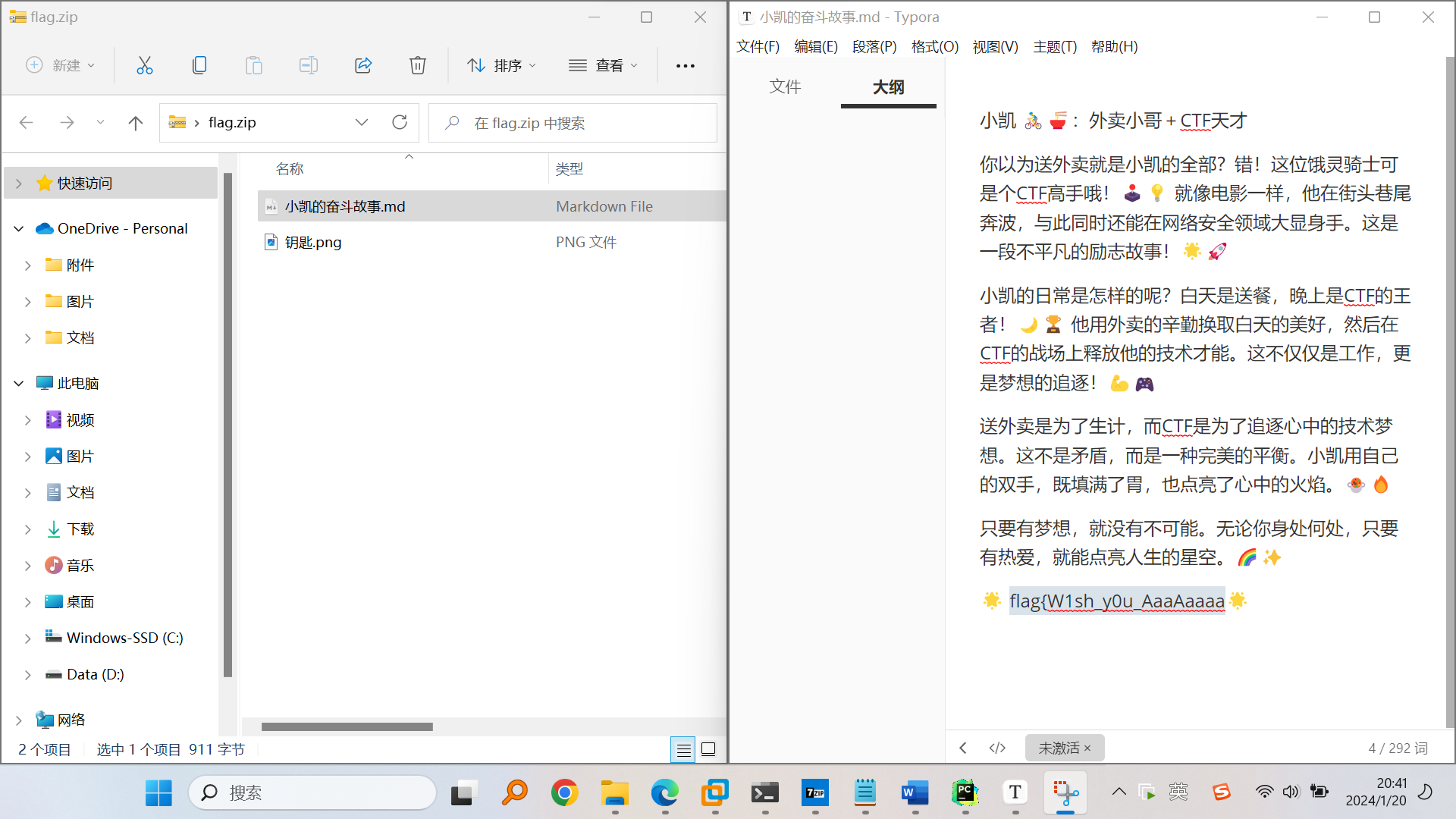
|  |
| --- |
| #include <bits/stdc++.h> using namespace std; int main(){  map<int,string>map1;  while(1){  int int1;  string string2;  cin >> int1 >> string2;  map1[int1] = string2;  if(int1==0) break;  }  map<int,string> sortedMap(map1.begin(),map1.end());  string ans="";  for(int i=1;i<=10898;i++){  ans+=sortedMap[i];  }  cout<<ans;  return 0; } |



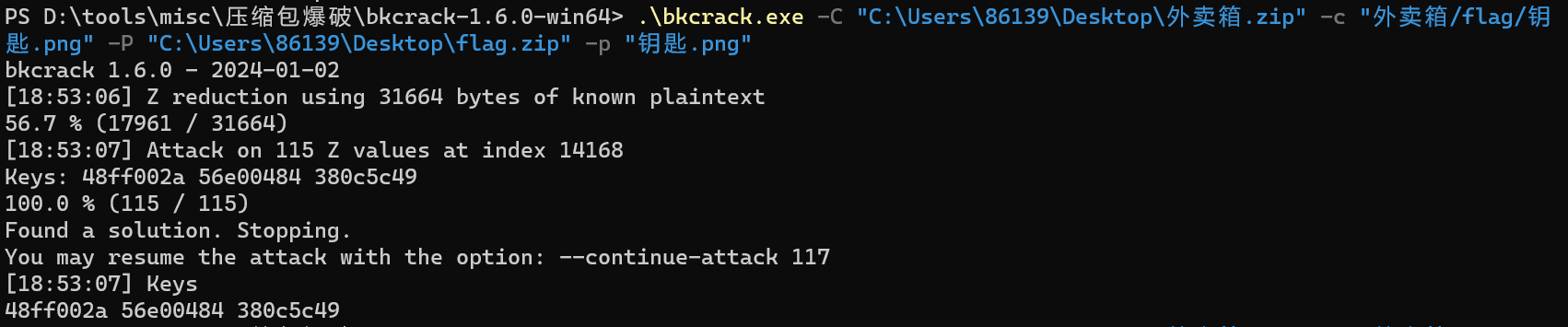
看着这串，感觉像base64，base64解码一下

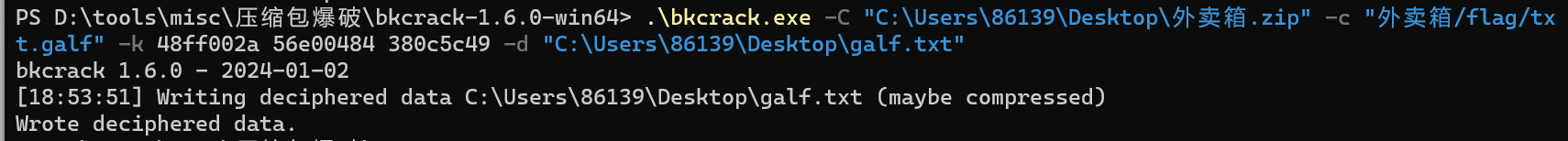
|  |
| --- |
| import base64  with open(路径, 'rb') as file:  data = file.read()  encoded\_data = base64.b64decode(data)  with open(保存路径, 'wb') as file:  file.write(encoded\_data) |

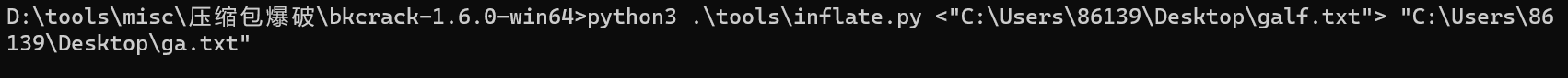
Winhex看到前面，zip头缺了，补一下打开，发现打不开，懵逼ing，突然想起前面的的注释，-=/，尝试把-和/替换再补一下

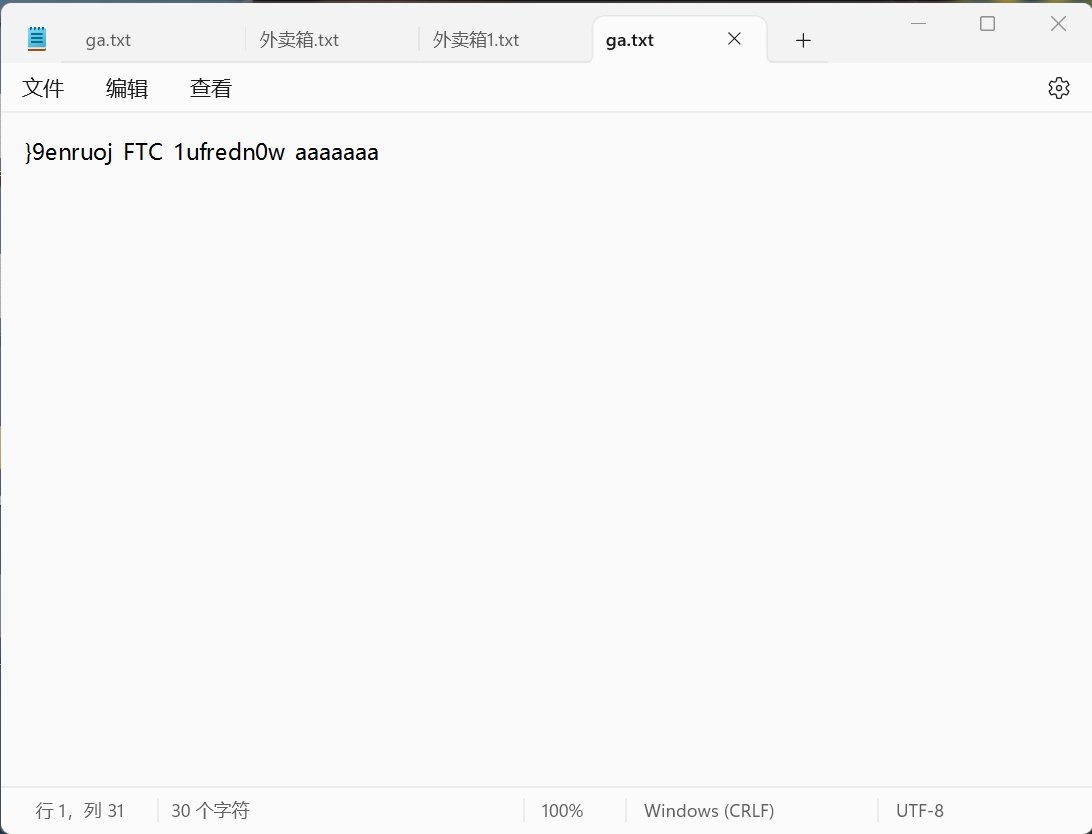


拿到前半段flag，然后就很明显了，明文攻击，bkcrack一下









再反转一下字符

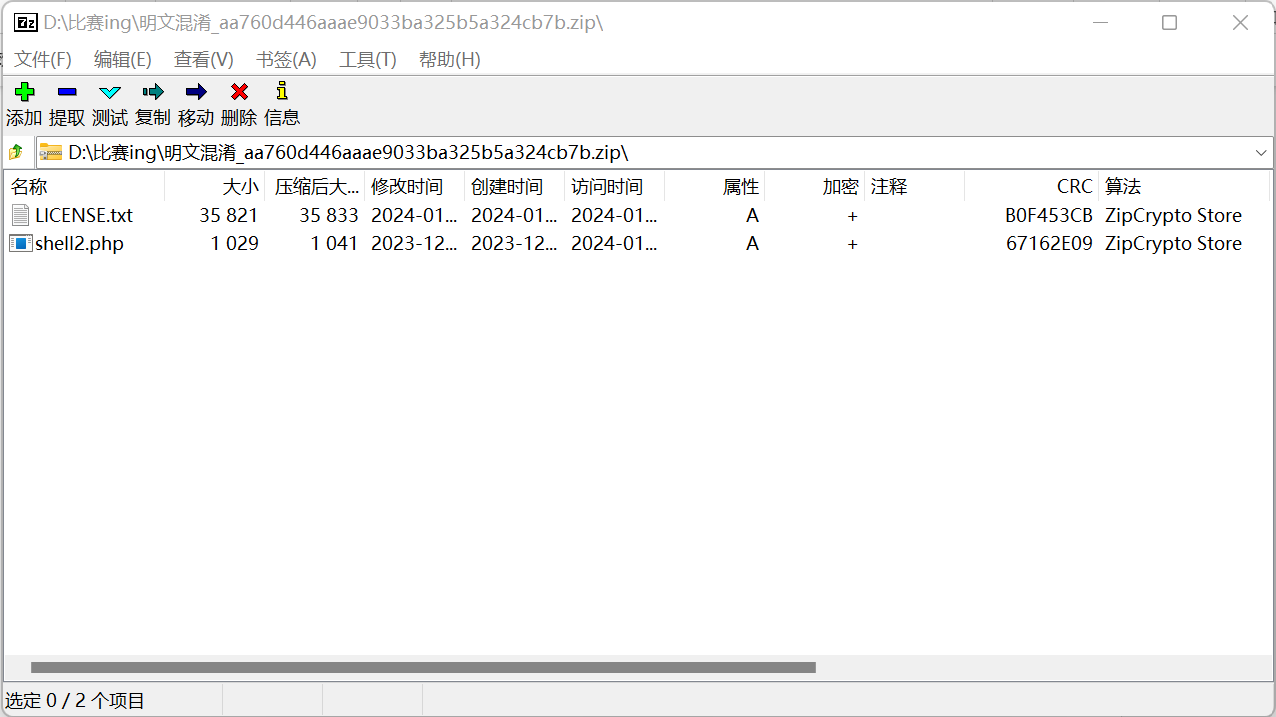
### flag值：

flag{W1sh\_y0u\_AaaAaaaaaaaaaaa\_w0nderfu1\_CTF\_journe9}

### 题目序号 明文混淆

### 操作内容：

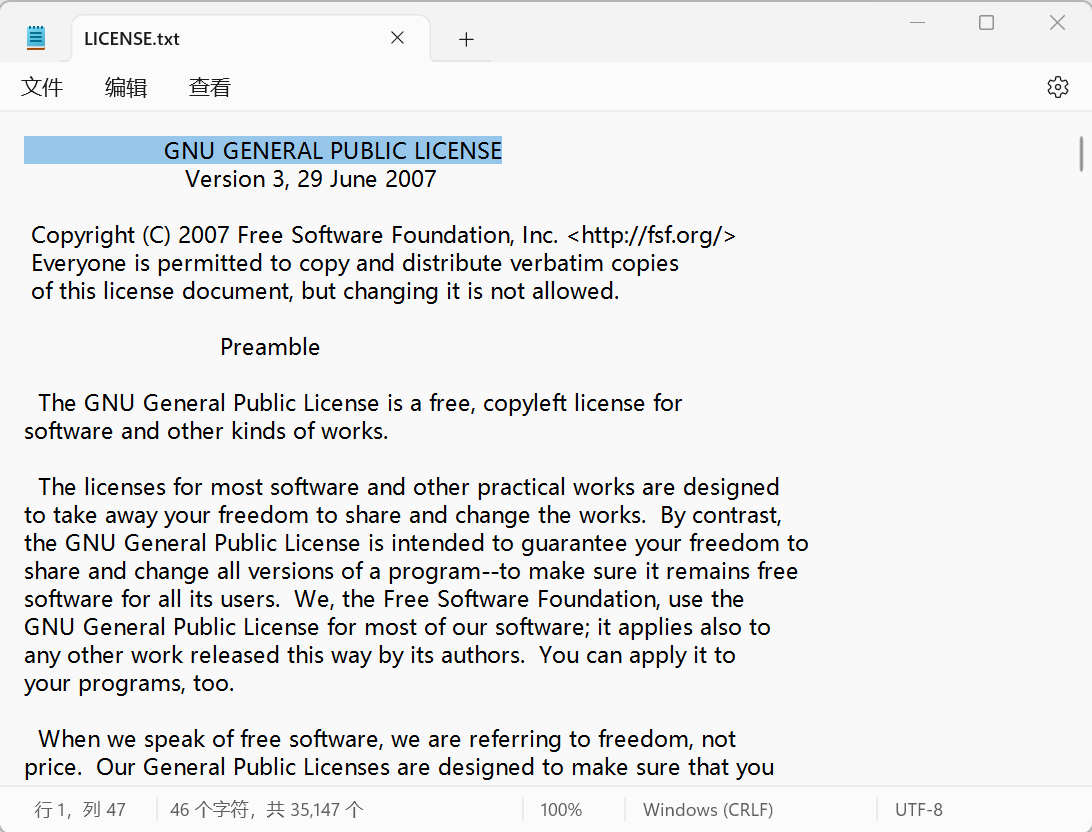
给了一个加密压缩包，加密算法zipcrypro store，很有明文攻击的味道



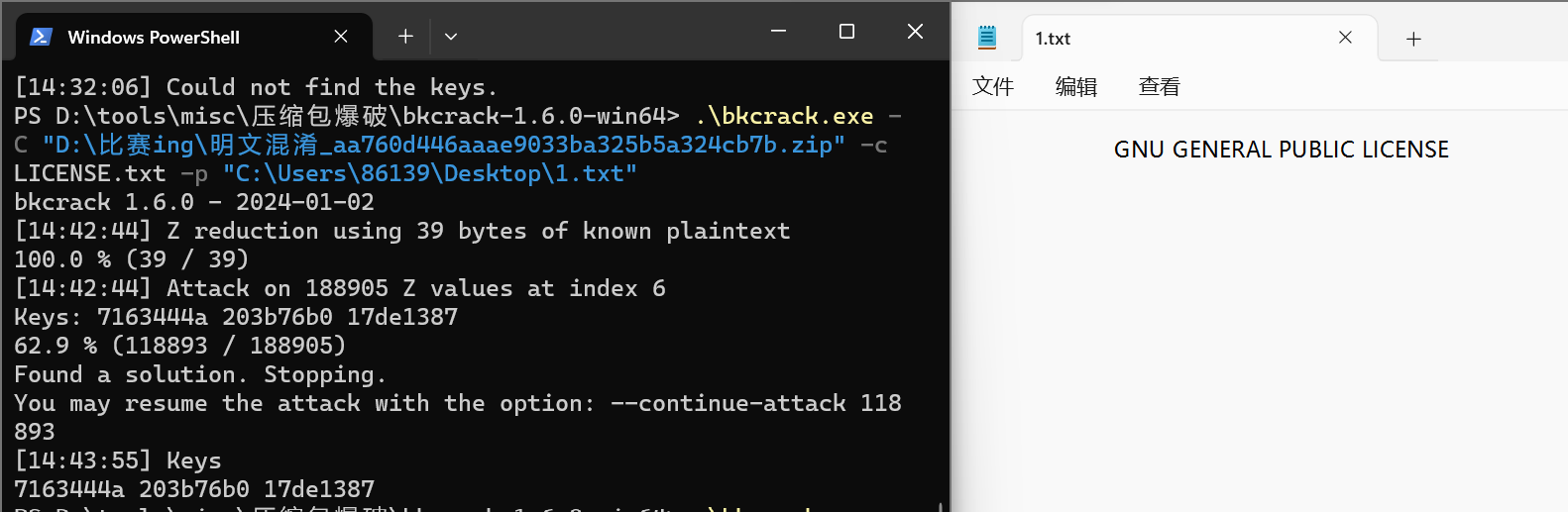
Shell2.php资源管理器说是jb的，我就拿了phpstorm文件的license前面的固定字节The following files can be redistributed under the license below:去爆破，没爆出来，注意到这个license大小，我就试着能不能找到一样大小的license

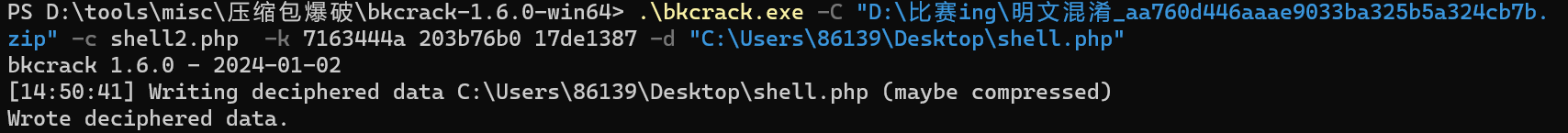


找到一个，下载了下来，但crc码不一样，bkcrack不出来，心灰意冷之时，打开发现原来有公共license

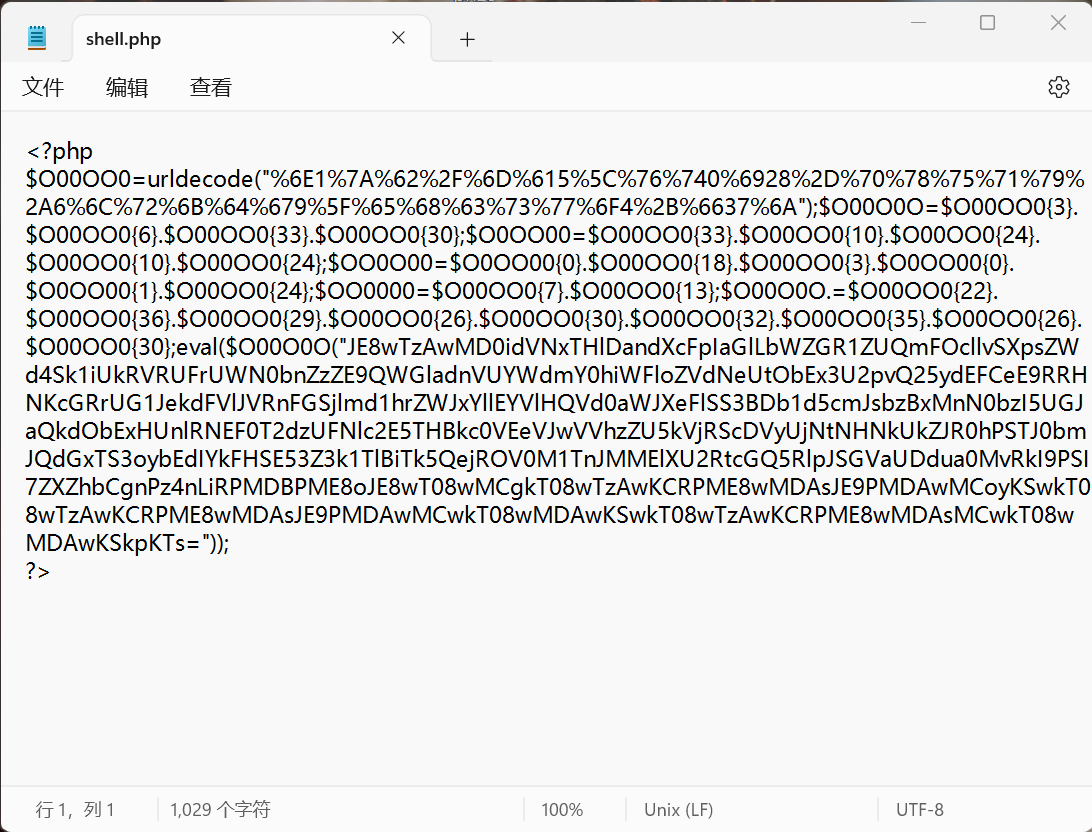


Bkcrack一下



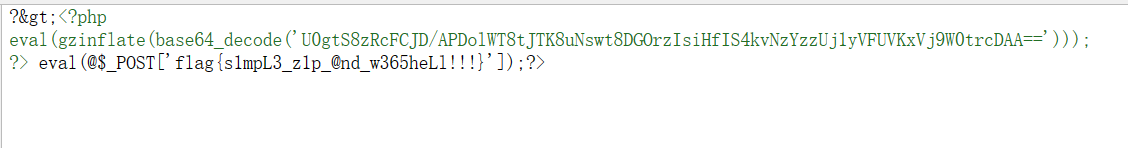


得到shell.php



一个微盾php解密

|  |
| --- |
| <?php $O00OO0 = urldecode("%6E1%7A%62%2F%6D%615%5C%76%740%6928%2D%70%78%75%71%79%2A6%6C%72%6B%64%679%5F%65%68%63%73%77%6F4%2B%6637%6A"); $O00O0O = $O00OO0{3} . $O00OO0{6} . $O00OO0{33} . $O00OO0{30}; $O0OO00 = $O00OO0{33} . $O00OO0{10} . $O00OO0{24} . $O00OO0{10} . $O00OO0{24}; $OO0O00 = $O0OO00{0} . $O00OO0{18} . $O00OO0{3} . $O0OO00{0} . $O0OO00{1} . $O00OO0{24}; $OO0000 = $O00OO0{7} . $O00OO0{13}; $O00O0O .= $O00OO0{22} . $O00OO0{36} . $O00OO0{29} . $O00OO0{26} . $O00OO0{30} . $O00OO0{32} . $O00OO0{35} . $O00OO0{26} . $O00OO0{30}; //eval($O00O0O(""));  $O0O000 = "uSqLyCjwWpZHhiKmfFGVTBaNrYoIzlegxJMbRDUEAkQctnvsdOPXiZvuTagfcHbXYheWMyKNlLwSjoCnrtABxOQDsJpdkPmIzGEVRUFqFJ9fwXkebqbYDaYGAWtibWxYRKpCoWyrblo0q2sto29PbZBGNlLGRyQ4AtOgsPSesa9LpdsEDyRpUXseNdV4Rp5rR3m4sdRFIGHOI2tnbPtlSKz2lGHbAGHNwgy5NPbNNPz4NWC5NrL0IWSdmpd9FZIHeZP7nkC/FB=="; echo (htmlspecialchars('?>') . $O00O0O($O0OO00($OO0O00($O0O000, $OO0000 \* 2), $OO0O00($O0O000, $OO0000, $OO0000), $OO0O00($O0O000, 0, $OO0000))));  echo gzinflate(base64\_decode('U0gtS8zRcFCJD/APDolWT8tJTK8uNswt8DGOrzIsiHfIS4kvNzYzzUj1yVFUVKxVj9W0trcDAA=='))  ?> |



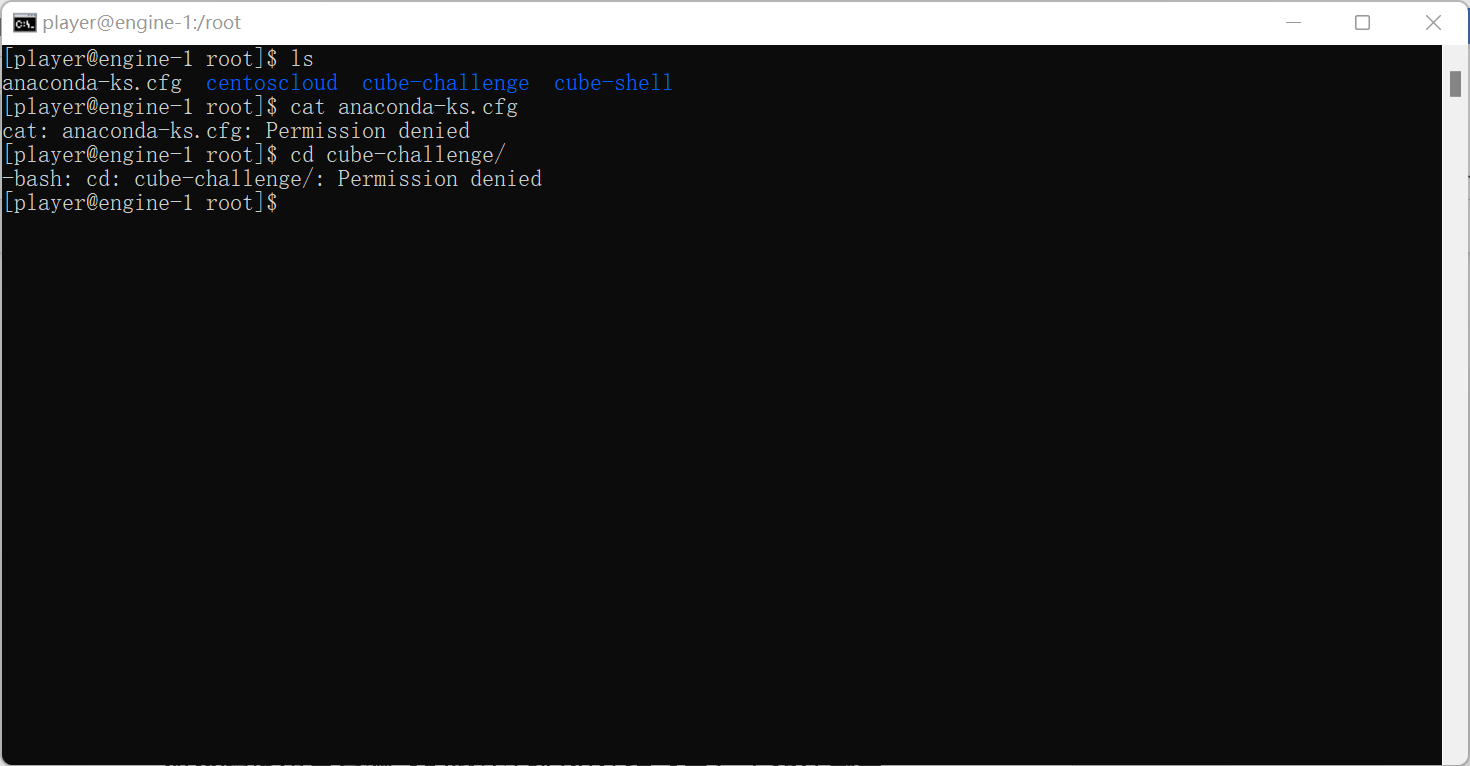
### flag值：

flag{s1mpL3\_z1p\_@nd\_w365heLl!!!}

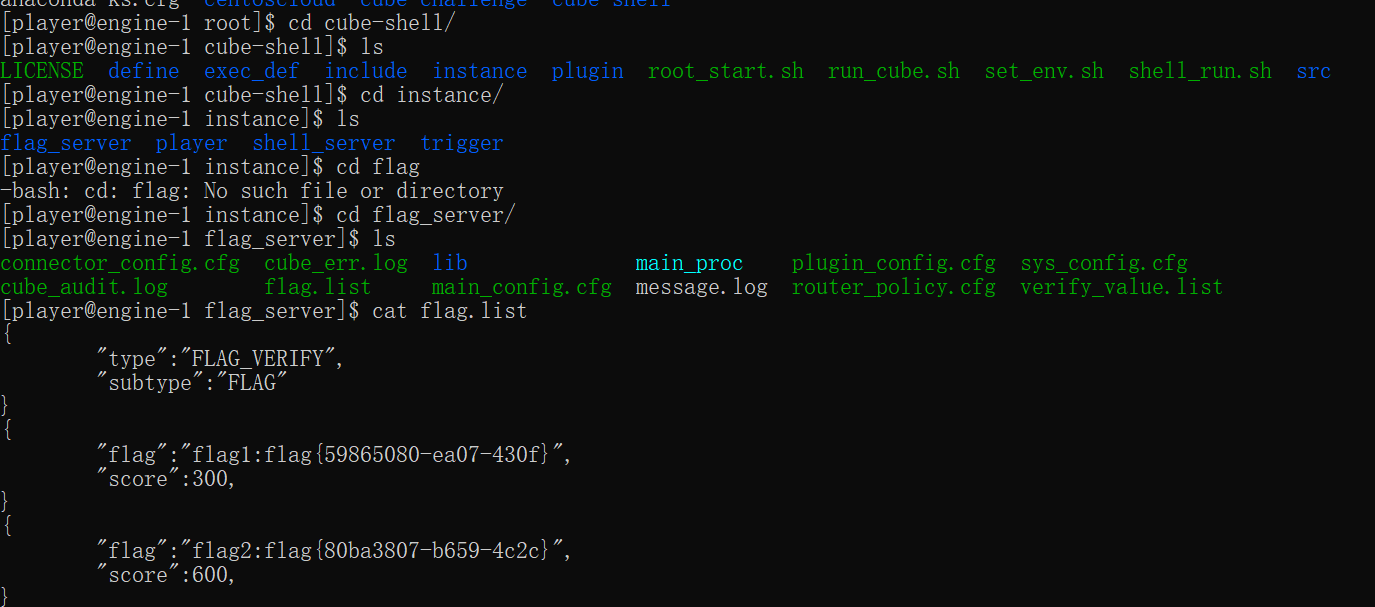
### 题目序号 基于挑战码的双向认证1

### 操作内容：

非预期了，来自web手（虽没做出来web）的瞎玩，发现有权限进root，两个没权限，一个云服



进实例



### flag值：

flag{59865080-ea07-430f}

### 题目序号 基于挑战码的双向认证2

### 操作内容：

和上面一样

### flag值：

flag{80ba3807-b659-4c2c}

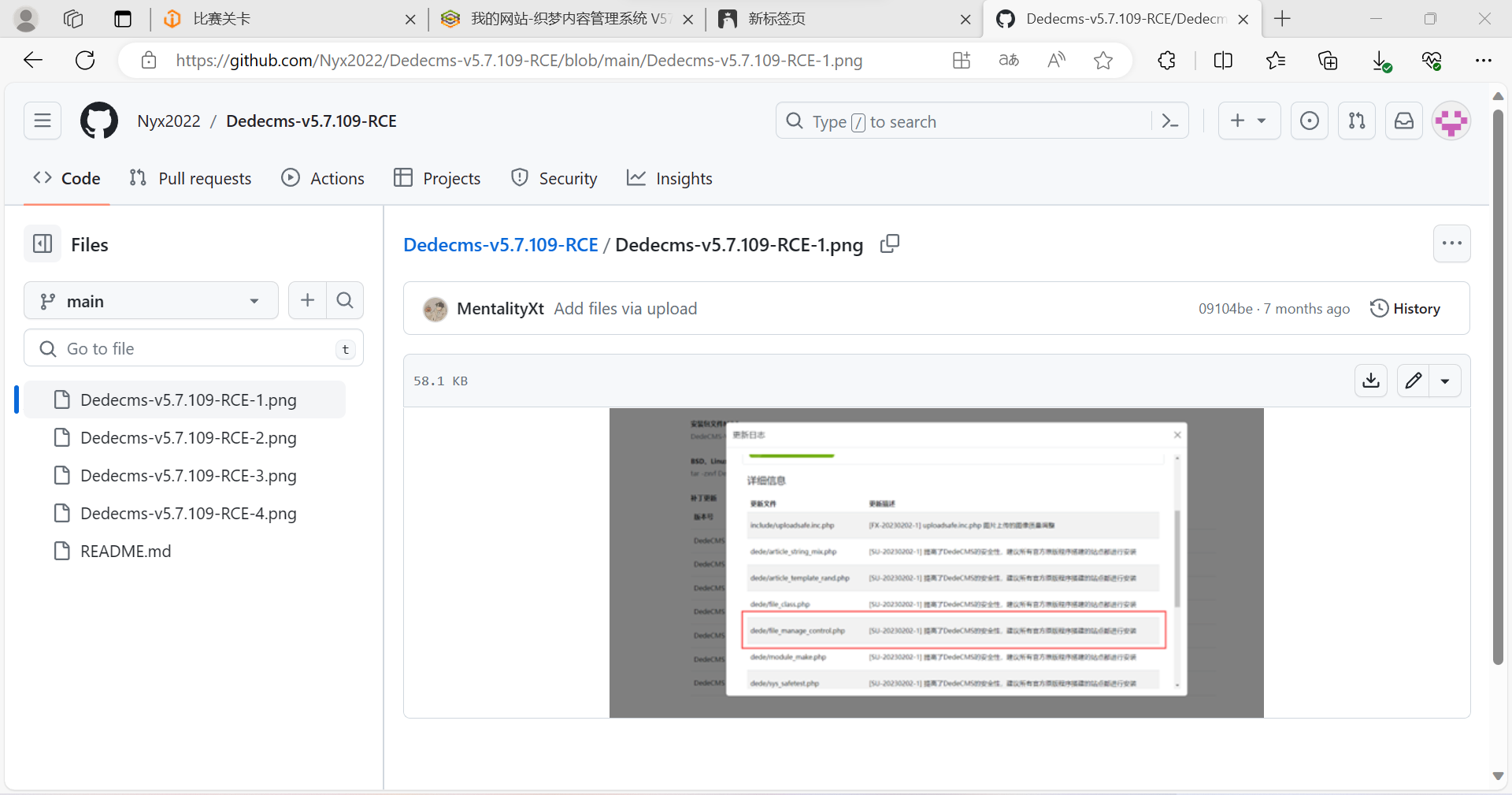
### 题目序号 ezdede

### 操作内容：

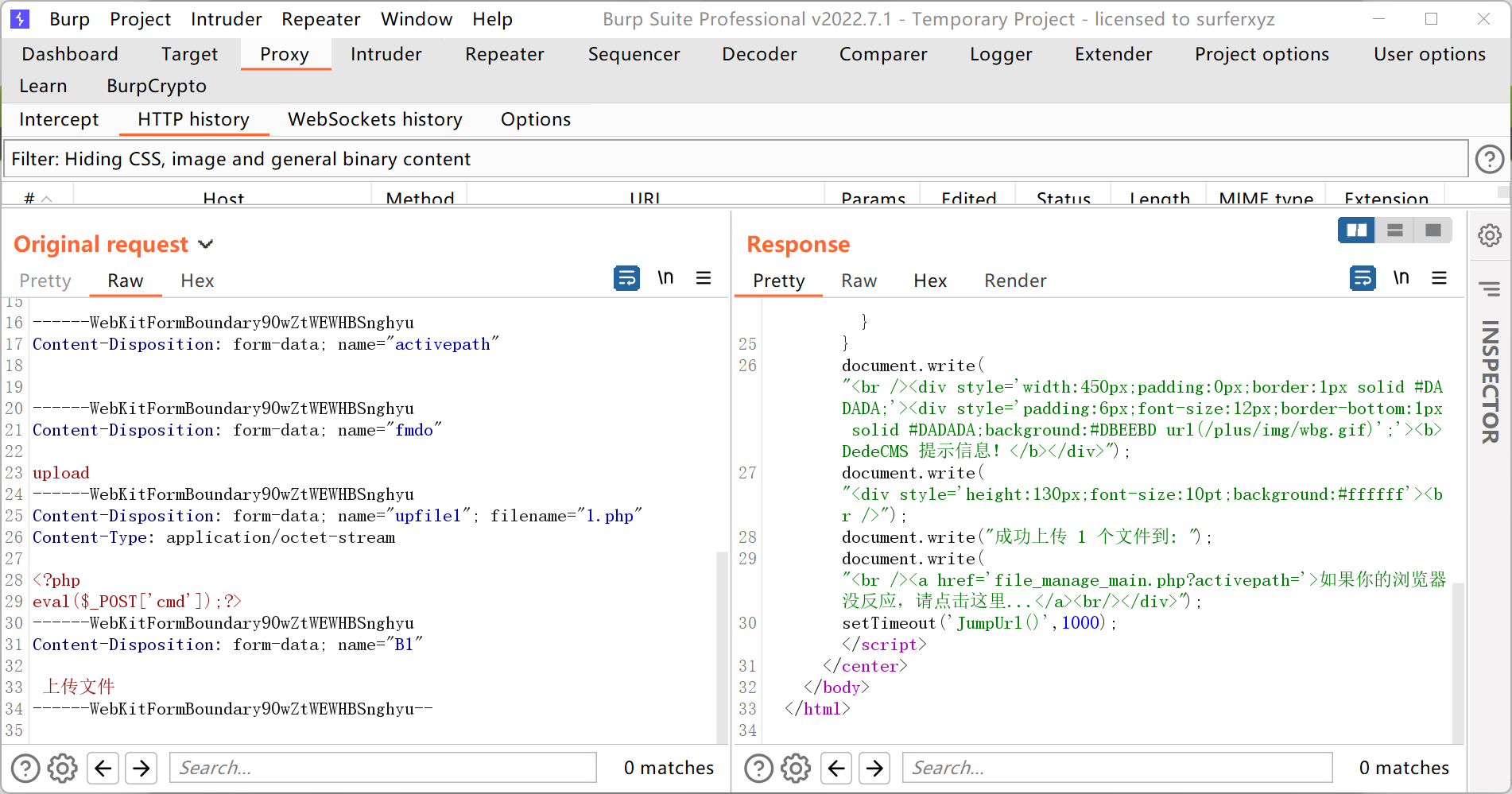
开始一直在注这个search界面，网上也有sql注入，结果没注出来，算了，关注一下公众号吧。

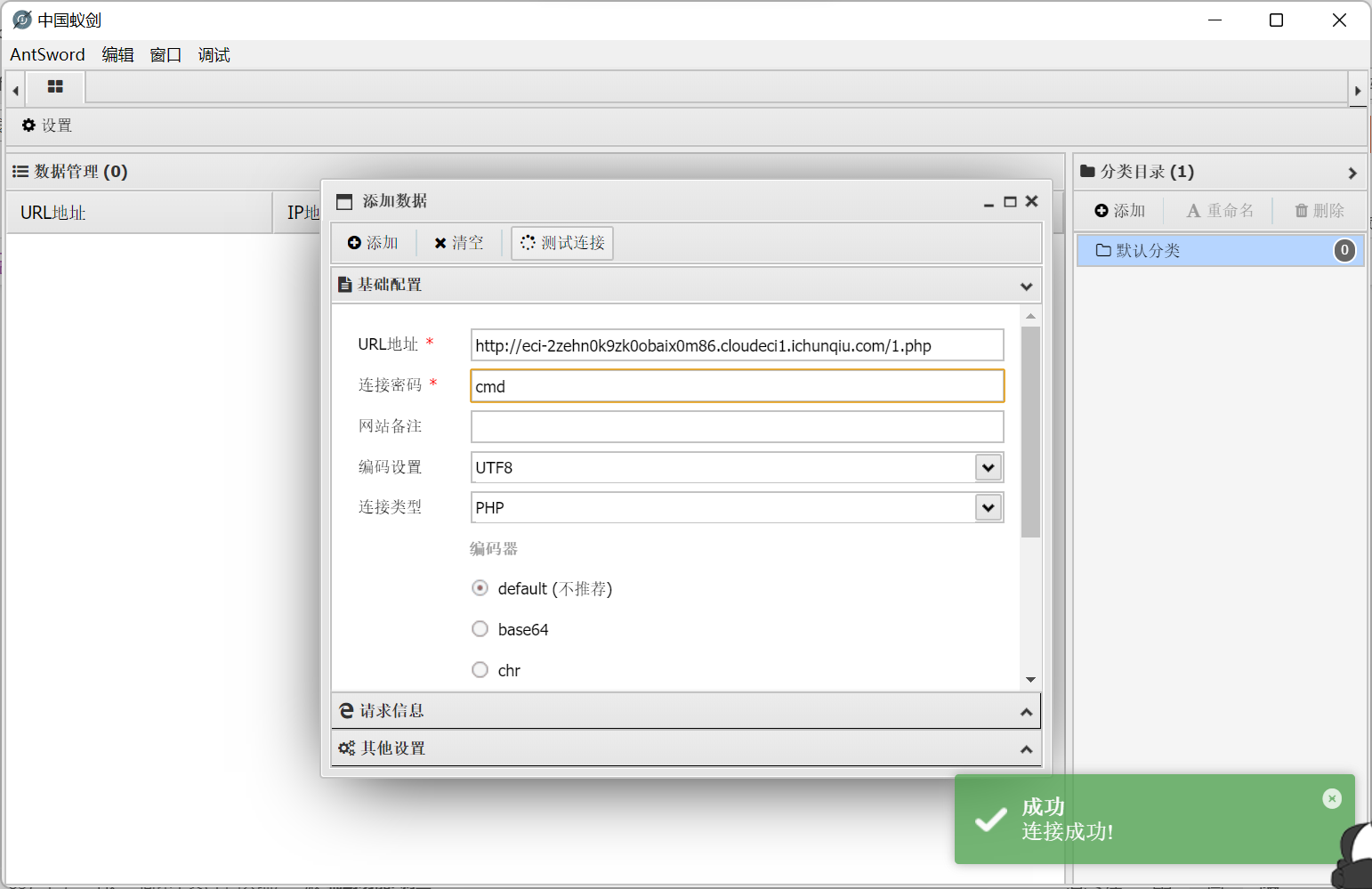


根据提示，进入后台，同时找到了一个rce文章

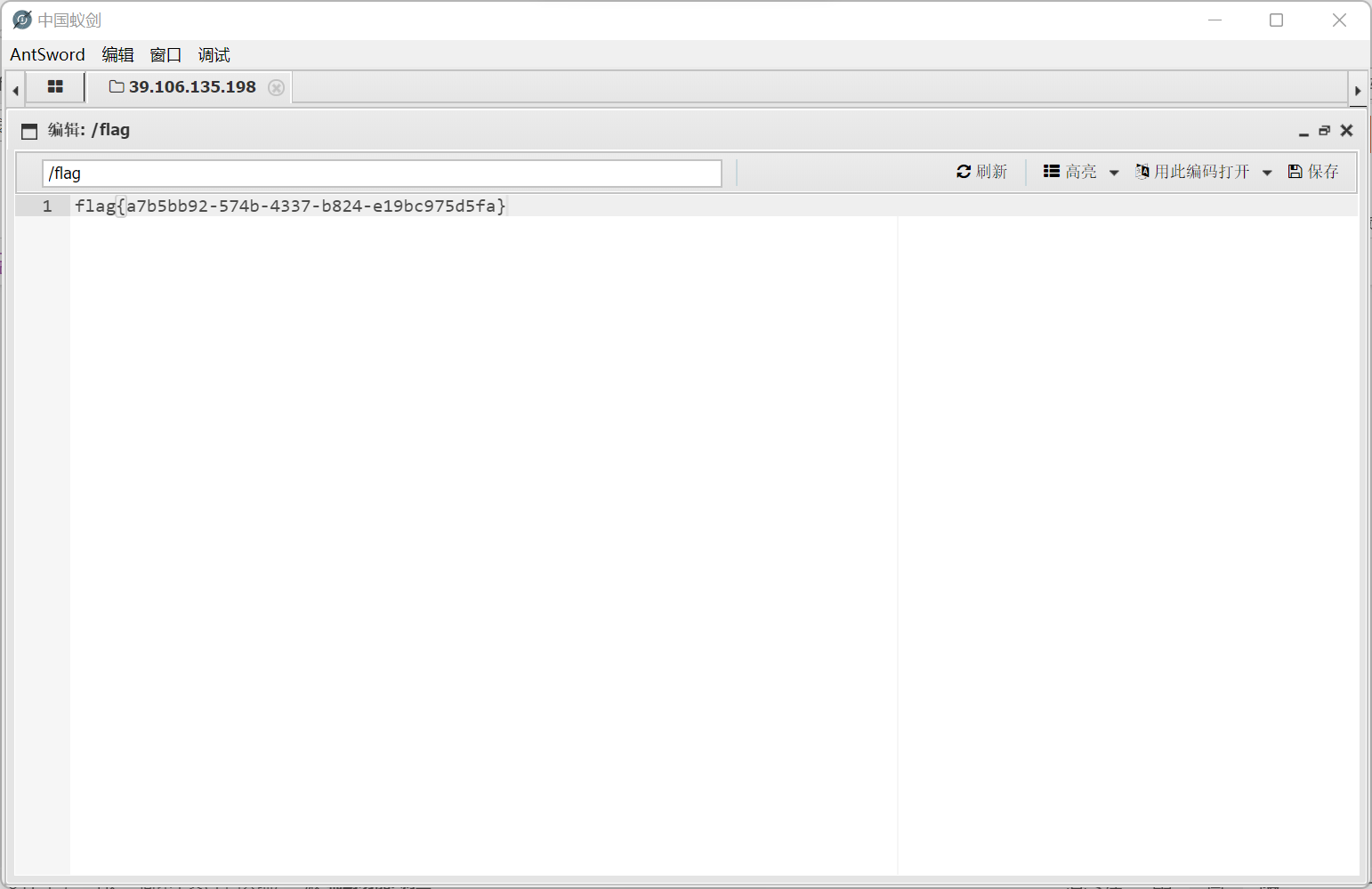
 

进入模块—文件管理器—文件上传





根目录下



### flag值：

flag{a7b5bb92-574b-4337-b824-e19bc975d5fa}

注：不是原来提交那个