攻防世界CRYPTO *4 writeup

原创

Sprint#51264 于 2020-08-01 20:20:46 发布 185 收藏

分类专栏： CRYPTO

本文链接：https://blog.csdn.net/qq_45837896/article/details/107726437

版权

CRYPTO 专栏收录该内容

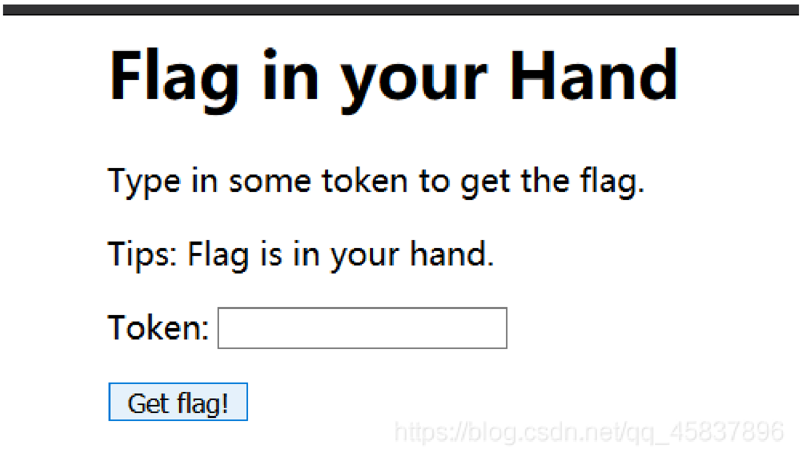
4 篇文章 0 订阅

订阅专栏

CRYPTO第四周

1.flag_in_your_hand

下载得到两个附件，打开index.html进入网页



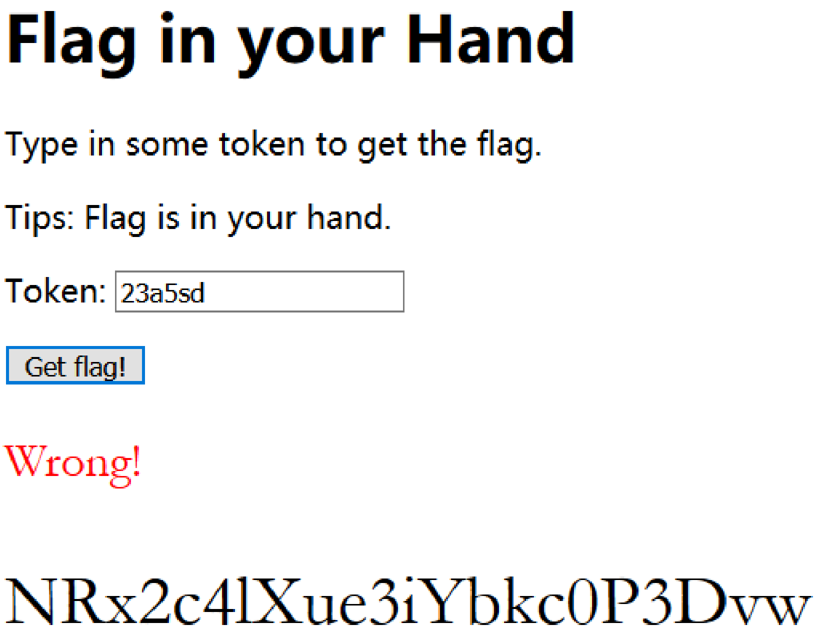
Flag in your Hand

Type in some token to get the flag.

Tips: Flag is in your hand.

Token:

要求我输入一个token获取flag，输入不同的数字会显示不同的字符串并提示我输入错误



Flag in your Hand

Type in some token to get the flag.

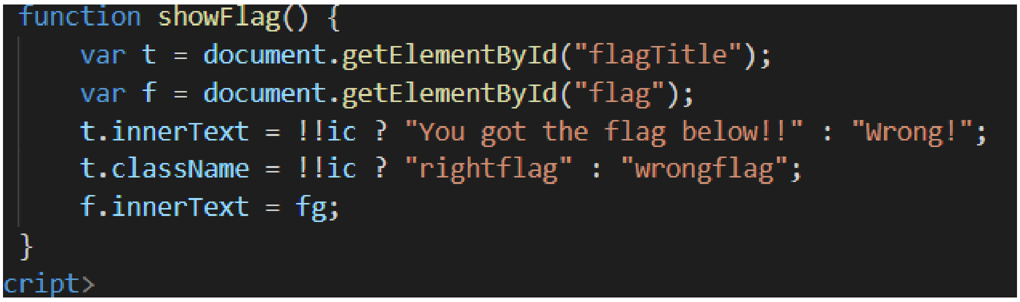
Tips: Flag is in your hand.

Token: 23a5sd

Wrong!

NRx2c4lXue3iYbkc0P3Dvw

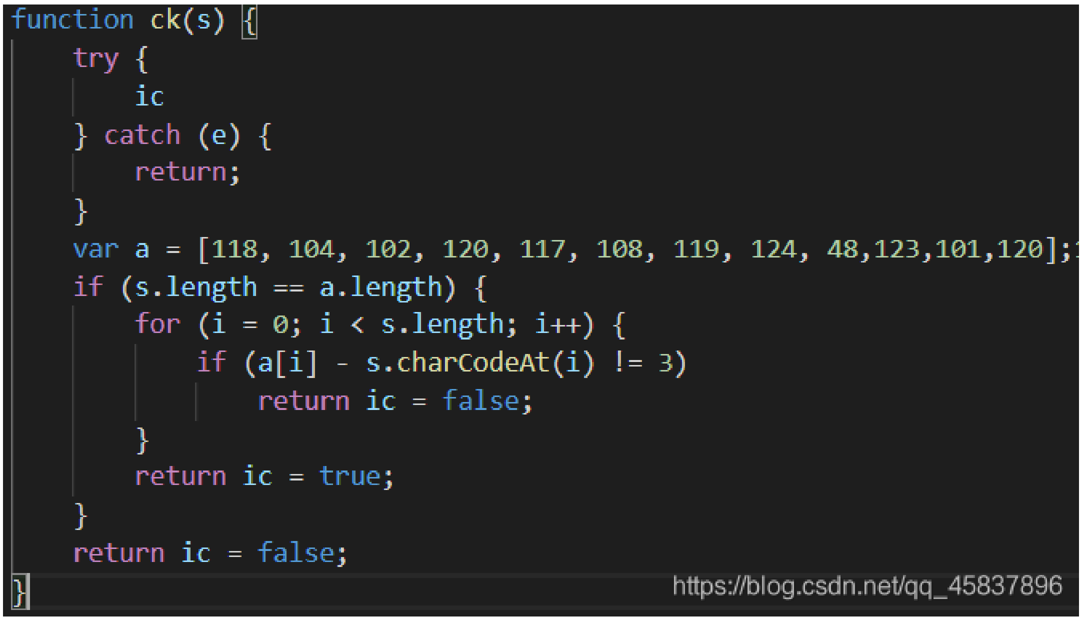
于是查看index源代码，发现了这么一段



```
function showFlag() {
    var t = document.getElementById("flagTitle");
    var f = document.getElementById("flag");
    t.innerText = !!ic ? "You got the flag below!!" : "Wrong!";
    t.className = !!ic ? "rightflag" : "wrongflag";
    f.innerText = fg;
}
cript>
```

要求是ic必须正确，然后才能获取flag。

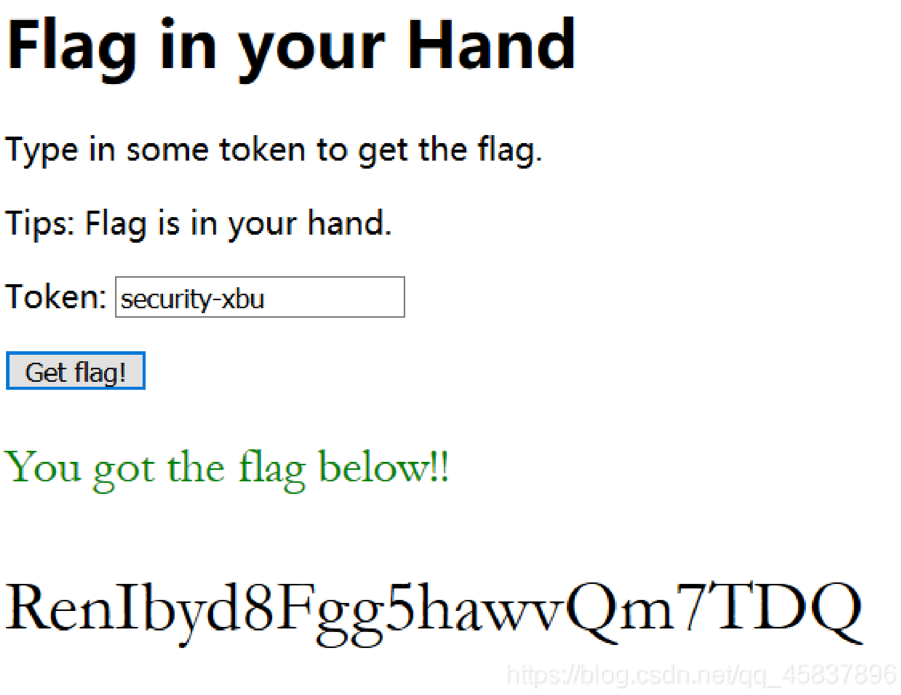
又进入到script-min.js中进行查看，找到了与ic相关的函数



```
function ck(s) {
    try {
        ic
    } catch (e) {
        return;
    }
    var a = [118, 104, 102, 120, 117, 108, 119, 124, 48,123,101,120];
    if (s.length == a.length) {
        for (i = 0; i < s.length; i++) {
            if (a[i] - s.charCodeAt(i) != 3)
                return ic = false;
        }
        return ic = true;
    }
    return ic = false;
}
```

说是要求传进来的s每个字符都要比a组中的对应字符小3，不然ic就false，于是把a中各数减3并通过ascll转换得

security-xbu
输入获取flag


Flag in your Hand

Type in some token to get the flag.

Tips: Flag is in your hand.

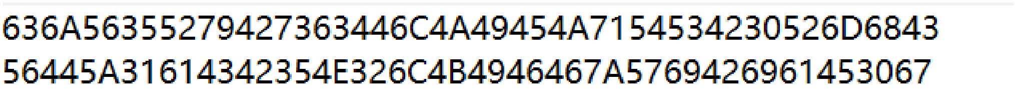
Token: security-xbu

You got the flag below!!

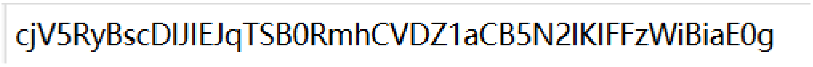
RenIbyd8Fgg5hawvQm7TDQ

2.告诉你个秘密（脑洞）

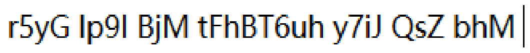
下载题目附件打开发现这么两行


636A56355279427363446C4A49454A7154534230526D6843
56445A31614342354E326C4B4946467A576942696145306

根据其格式猜测是16进制，进行转换得


cjV5RyBscDlJIEJqTSB0RmhCVDZ1aCB5N2lKIFFzWiBiaE0g

转出这么一串字符串，尝试着用base64解码


r5yG lp9I BjM tFhBT6uh y7iJ QsZ bhM

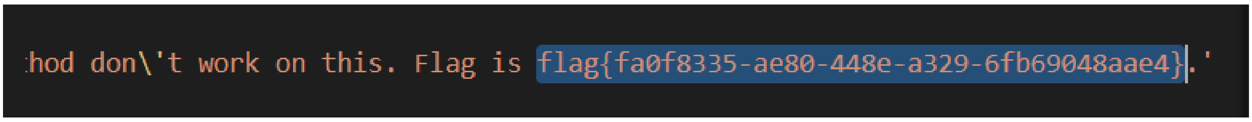
解出一个见都没见过的几个码，但是却没有解错，是有规律可循的，每几个字符隔一个空格，属实蒙圈，看了别人的writeup，发现是从键盘上找奥妙，它们分别都围着一个另一个字符！！

```
TONGYUAN
```

记住是大写

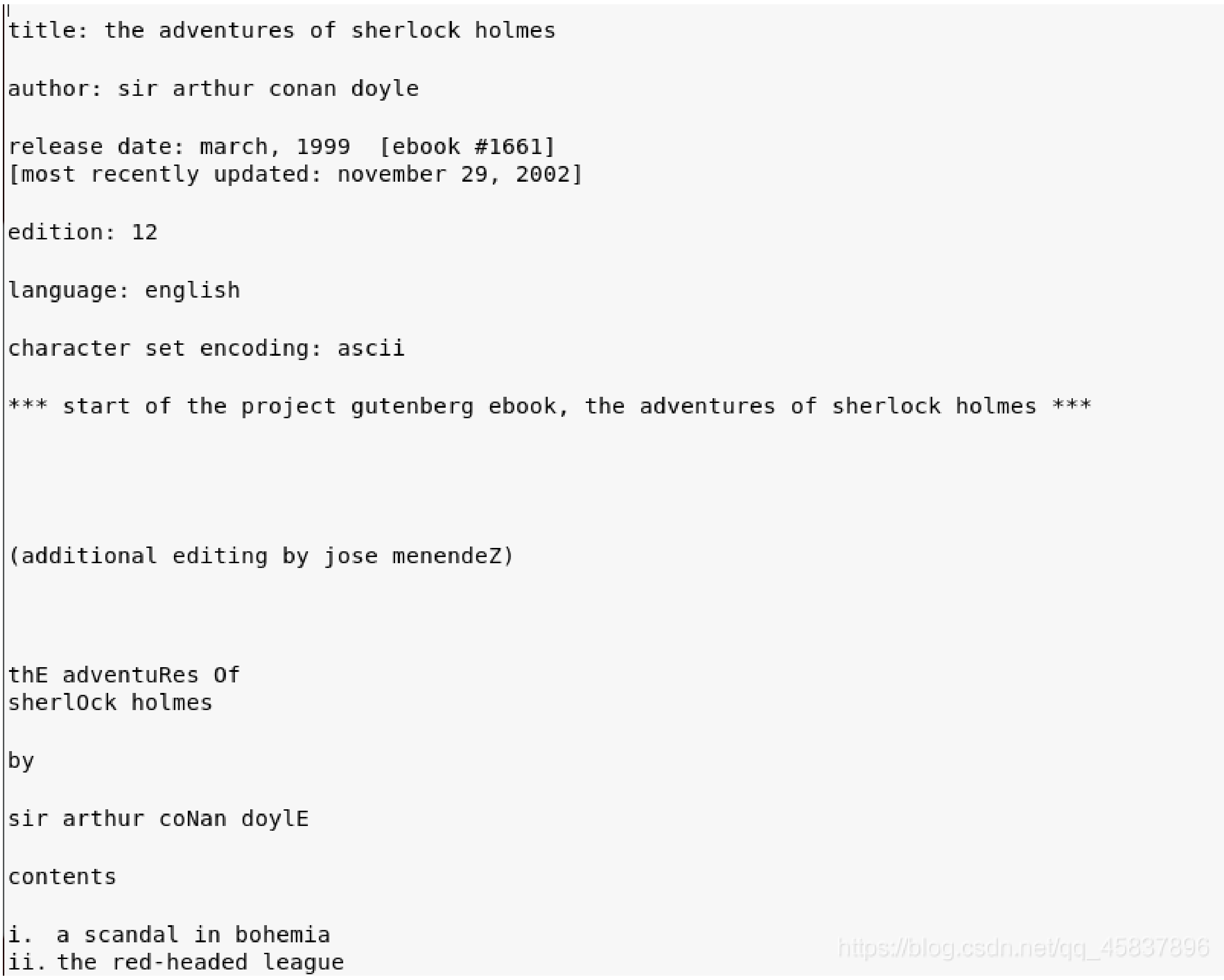
2+.Broadcast（送分）

解压打开task.py，还真就明文


```
:hod don\'t work on this. Flag is flag{fa0f8335-ae80-448e-a329-6fb69048aae4}.'
```

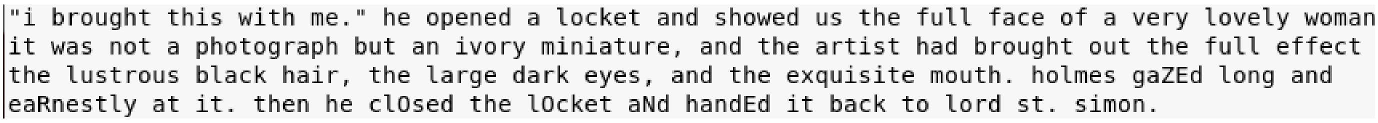
3.sherlock

通过附件下载到一本emm小说


```
title: the adventures of sherlock holmes

author: sir arthur conan doyle

release date: march, 1999  [ebook #1661]
[most recently updated: november 29, 2002]

edition: 12

language: english

character set encoding: ascii

*** start of the project gutenberg ebook, the adventures of sherlock holmes ***




(additional editing by jose menendeZ)



thE adventuRes Of
sherlOck holmes

by

sir arthur coNan doylE

contents

i.  a scandal in bohemia
ii. the red-headed league
```

神探夏洛克…

全文非常长，初次观察没有看出什么端倪，我以为会在文章末尾给出什么提示但是并没有，可是发现几处不一样


```
"i brought this with me." he opened a locket and showed us the full face of a very lovely woman
it was not a photograph but an ivory miniature, and the artist had brought out the full effect
the lustrous black hair, the large dark eyes, and the exquisite mouth. holmes gaZEd long and
eaRnestly at it. then he clOsed the lOcket aNd handEd it back to lord st. simon.
```

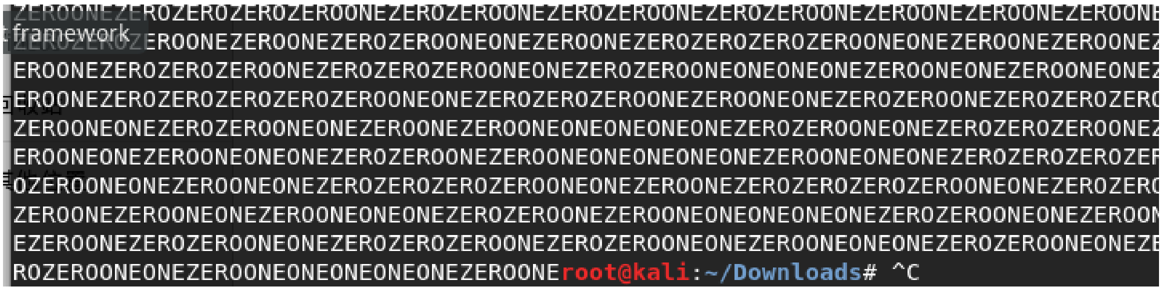
看到

有些字母大写，我把这几个拿出来拼一起以为会出现base64编码，发现拼出来的是ZEROONE,在再观察文章发现有很多处类似的，都是ZERO或者ONE，于是乎想到二进制，对整个文本的大写字符进行提取

用到一个cat命令（学习点）

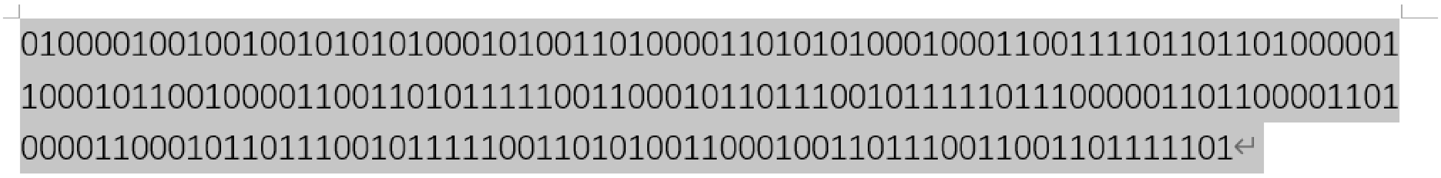
```
cat 1.txt | grep -Eo '[A-Z]' |tr -d '\n'
```

搜索出这样的结果



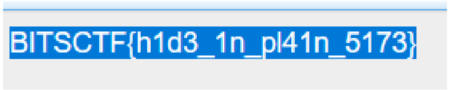
```
ZEROONEZEROZEROZEROZEROONEZEROZEROONEZEROZEROONEZEROZEROONEZEROONEZEROONEZEROONE
ZEROZEROZEROONEZEROONEZEROZEROONEONEZEROONEZEROZEROZEROZEROONEONEZEROONEZEROONEZ
EROONEZEROZEROZEROONEZEROZEROZEROONEONEZEROZEROONEONEONEONEZEROONEONEZEROONEONEZ
EROONEZEROZEROZEROZEROZEROONEONEZEROZEROZEROONEZEROONEONEZEROZEROONEZEROZEROZERO
ZEROONEONEZEROZEROONEONEZEROONEZEROONEONEONEONEONEZEROZEROONEONEZEROZEROZEROONEZ
EROONEONEZEROONEONEONEZEROZEROONEZEROONEONEONEONEONEZEROONEONEONEZEROZEROZEROZER
OZEROONEONEZEROONEONEZEROZEROZEROZEROONEONEZEROONEZEROZEROZEROZEROONEONEZEROZERO
ZEROONEZEROONEONEZEROONEONEONEZEROZEROONEZEROONEONEONEONEONEZEROZEROONEONEZEROON
EZEROONEZEROZEROONEONEZEROZEROZEROONEZEROZEROONEONEZEROONEONEONEZEROZEROONEONEZE
ROZEROONEONEZEROONEONEONEONEONEZEROONEroot@kali:~/Downloads# ^C
```

用word替换一下出二进制



```
010000100100100101010100010100110100001101010100010001100111101101101000001
100010110010000110011010111110011000101101110010111110111000001101100001101
000011000101101110010111110011010100110001001101110011001101111101
```

转字符串得flag

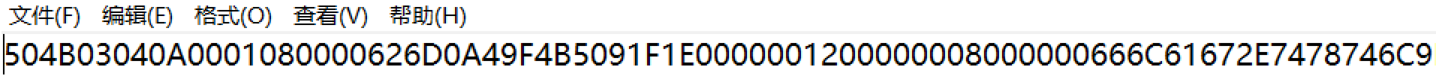


BITSCTF{h1d3_1n_pl41n_5173}

（amazing）

4.你猜猜

下载附件后得以下txt文本

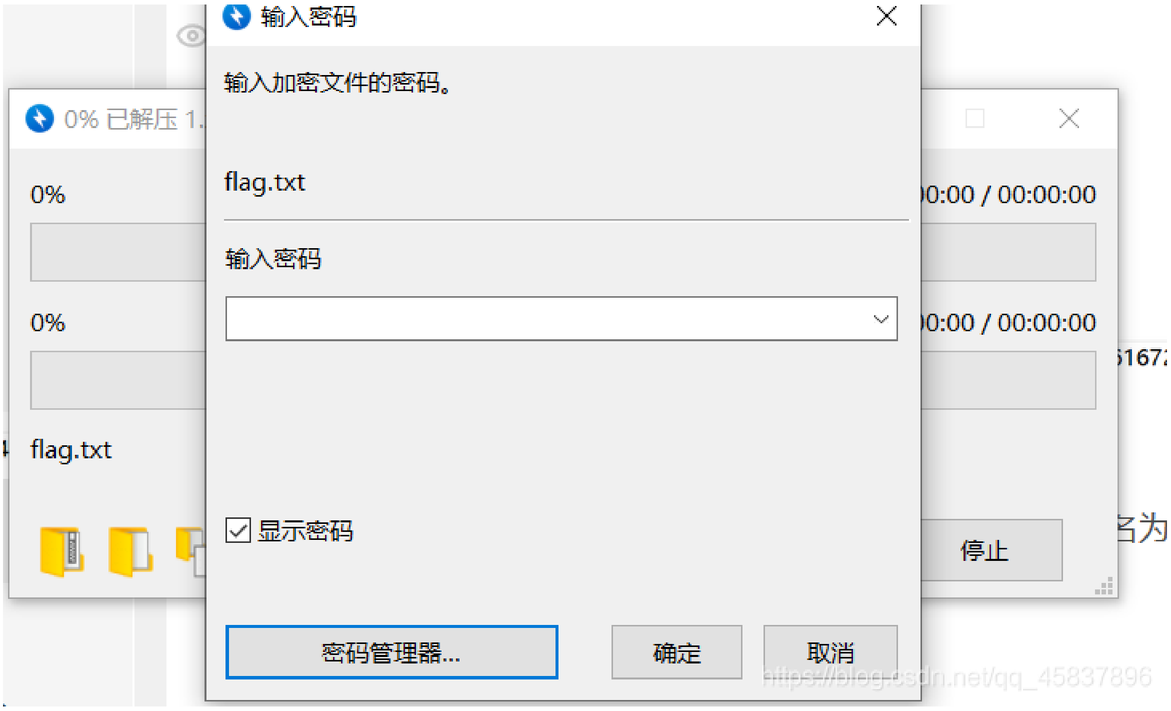


```
504B03040A0001080000626D0A49F4B5091F1E000000120000000800000666C61672E7478746C9
```

通过观察其形式注意到504B0304是一个zip的文件头

使用winhex新建文件并将文本中的文件hex复制进去，重新命名为.zip

解压发现需要密码

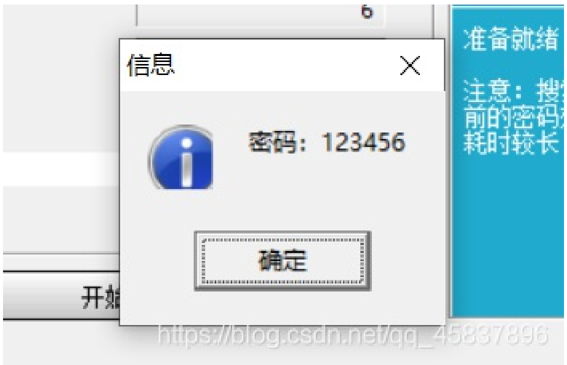


输入加密文件的密码。

flag.txt

输入密码

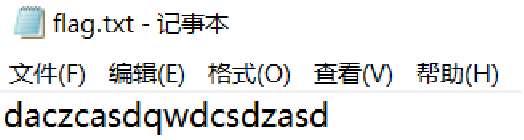
用到工具ziperello进行破解



密码：123456

ps：用组合密码算死了，所以用的数字检索，直接得到123456

进入flag.txt



daczcasdqwdcsdzasd

得到flag