BUUCTF WP

原创

「已注销」 于 2020-04-25 18:20:43 发布 1005 收藏 2

分类专栏： CTFWP 文章标签： wp

本文链接：https://blog.csdn.net/qq_45808659/article/details/105753923

版权

CTFWP 专栏收录该内容

8 篇文章 0 订阅

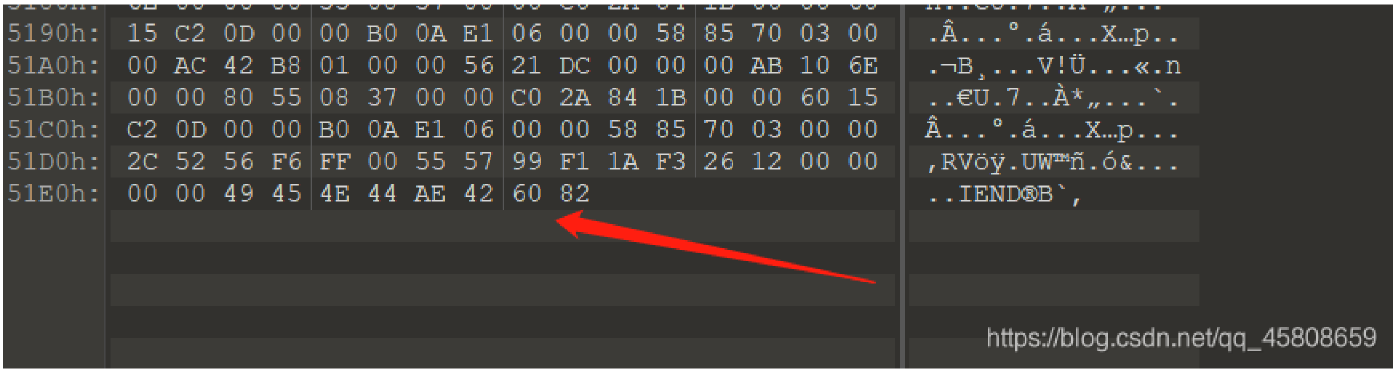
订阅专栏

MISC

最简单

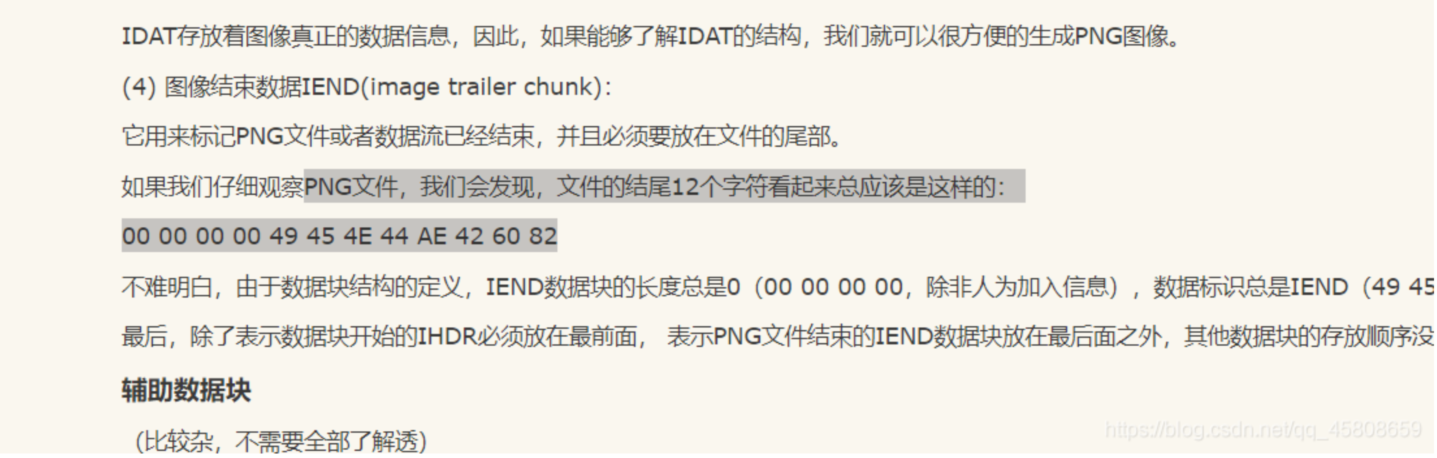
首先使用winrar修复伪加密

查看文件尾，发现是png结尾



```
5190h:  15 C2 0D 00 00 B0 0A E1 06 00 00 58 85 70 03 00   .Â...°.á...X…p..
51A0h:  00 AC 42 B8 01 00 00 56 21 DC 00 00 00 AB 10 6E   .¬B¸...V!Ü...«.n
51B0h:  00 00 80 55 08 37 00 00 C0 2A 84 1B 00 00 60 15   ..€U.7..À*„...`.
51C0h:  C2 0D 00 00 B0 0A E1 06 00 00 58 85 70 03 00 00   Â...°.á...X…p...
51D0h:  2C 52 56 F6 FF 00 55 57 99 F1 1A F3 26 12 00 00   ,RVöÿ.UW™ñ.ó&...
51E0h:  00 00 49 45 4E 44 AE 42 60 82                     ..IEND®B`‚
```

png知识参考https://www.cnblogs.com/senior-engineer/p/9548347.html



IDAT存放着图像真正的数据信息，因此，如果能够了解IDAT的结构，我们就可以很方便的生成PNG图像。

(4) 图像结束数据IEND(image trailer chunk)：

它用来标记PNG文件或者数据流已经结束，并且必须要放在文件的尾部。

如果我们仔细观察PNG文件，我们会发现，文件的结尾12个字符看起来总应该是这样的：

00 00 00 00 49 45 4E 44 AE 42 60 82

不难明白，由于数据块结构的定义，IEND数据块的长度总是0（00 00 00 00，除非人为加入信息），数据标识总是IEND（49 45

最后，除了表示数据块开始的IHDR必须放在最前面， 表示PNG文件结束的IEND数据块放在最后面之外，其他数据块的存放顺序没

辅助数据块

（比较杂，不需要全部了解透）

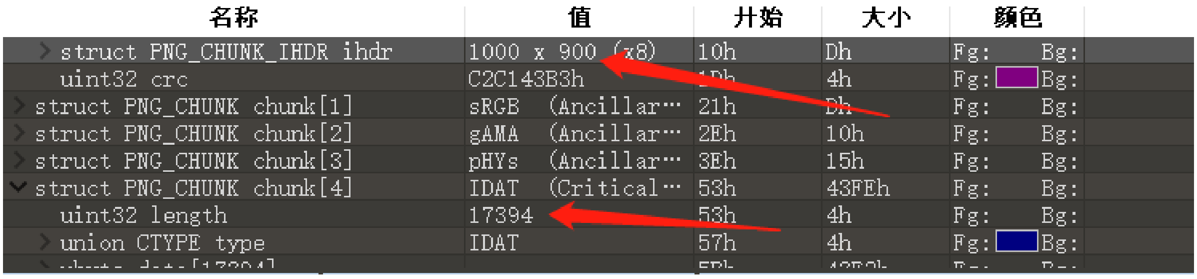
https://blog.csdn.net/qq_45808659

更改文件尾得到图片后使用16进制转字符串得到flag

十六进制转字符串网站：**https://www.sojson.com/hexadecimal.htm**

Misc-A_Beautiful_Picture-DreamerJack.png

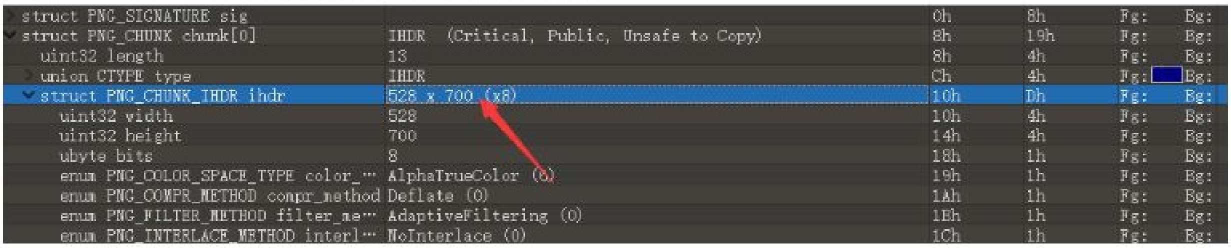
使用010打开图片，发现长高不对应大小，修改高度后即可得到flag



名称	值	开始	大小	颜色
struct PNG_CHUNK_IHDR ihdr	1000 x 900 (x8)	10h	Dh	Fg: Bg:
uint32 crc	C2C143B3h	1Dh	4h	Fg: 🟪 Bg:
struct PNG_CHUNK chunk[1]	sRGB (Ancillar…	21h	Dh	Fg: Bg:
struct PNG_CHUNK chunk[2]	gAMA (Ancillar…	2Eh	10h	Fg: Bg:
struct PNG_CHUNK chunk[3]	pHYs (Ancillar…	3Eh	15h	Fg: Bg:
struct PNG_CHUNK chunk[4]	IDAT (Critical…	53h	43FEh	Fg: Bg:
uint32 length	17394	53h	4h	Fg: Bg:
union CTYPE type	IDAT	57h	4h	Fg: 🟦 Bg:

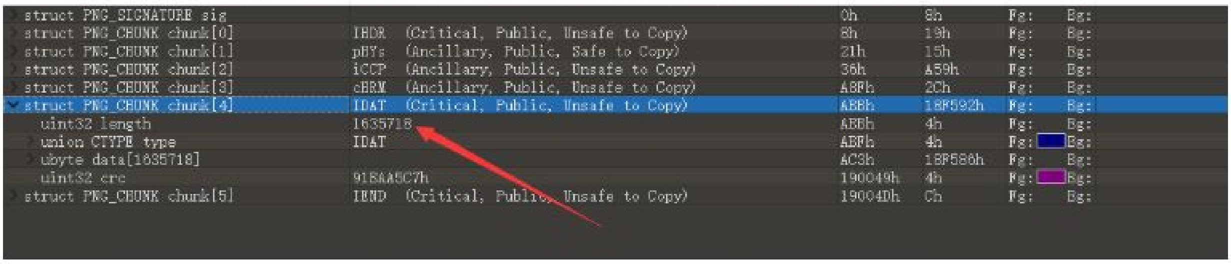
判断图片高度隐写

例题：判断图片高度隐写的方法



```
struct PNG_SIGNATURE sig                                                0h     8h    Fg:   Bg:
struct PNG_CHUNK chunk[0]             IHDR  (Critical, Public, Unsafe to Copy)  8h     19h   Fg:   Bg:
  uint32 length                       13                                8h     4h    Fg:   Bg:
  union CTYPE type                    IHDR                              Ch     4h    Fg:   Bg:
  struct PNG_CHUNK_IHDR ihdr          528 x 700 (x8)                    10h    Dh    Fg:   Bg:
    uint32 width                      528                               10h    4h    Fg:   Bg:
    uint32 height                     700                               14h    4h    Fg:   Bg:
    ubyte bits                        8                                 18h    1h    Fg:   Bg:
    enum PNG_COLOR_SPACE_TYPE color_… AlphaTrueColor (6)                19h    1h    Fg:   Bg:
    enum PNG_COMPR_METHOD compr_method Deflate (0)                      1Ah    1h    Fg:   Bg:
    enum PNG_FILTER_METHOD filter_me… AdaptiveFiltering (0)             1Bh    1h    Fg:   Bg:
    enum PNG_INTERLACE_METHOD interl… NoInterlace (0)                   1Ch    1h    Fg:   Bg:
```

计算图片的大小应该是528*700*3(RGB图像通常每像素3字节)=1108800

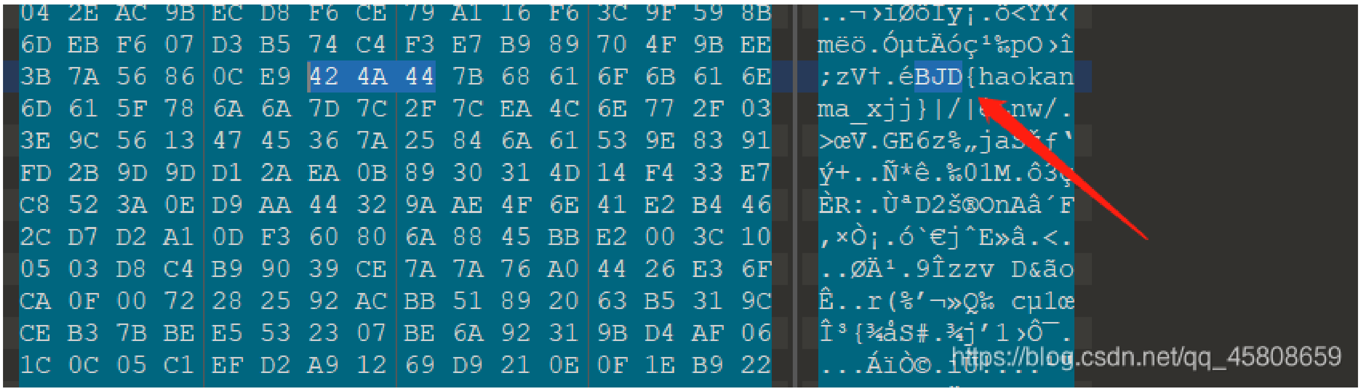


```
struct PNG_SIGNATURE sig                                                        0h       8h       Fg:   Bg:
struct PNG_CHUNK chunk[0]    IHDR  (Critical, Public, Unsafe to Copy)           8h       19h      Fg:   Bg:
struct PNG_CHUNK chunk[1]    pHYs  (Ancillary, Public, Safe to Copy)            21h      15h      Fg:   Bg:
struct PNG_CHUNK chunk[2]    iCCP  (Ancillary, Public, Unsafe to Copy)          36h      A59h     Fg:   Bg:
struct PNG_CHUNK chunk[3]    cHRM  (Ancillary, Public, Unsafe to Copy)          A8Fh     2Ch      Fg:   Bg:
struct PNG_CHUNK chunk[4]    IDAT  (Critical, Public, Unsafe to Copy)           ABBh     18F592h  Fg:   Bg:
  uint32 length              1635718                                            ABBh     4h       Fg:   Bg:
  union CTYPE type           IDAT                                               ABFh     4h       Fg:   Bg:
  ubyte data[1635718]                                                           AC3h     18F586h  Fg:   Bg:
  uint32 crc                 918AA5C7h                                          190049h  4h       Fg:   Bg:
struct PNG_CHUNK chunk[5]    IEND  (Critical, Public, Unsafe to Copy)           19004Dh  Ch       Fg:   Bg:
```

但是IDAT模块的数值比它大，所以可以判定原图片的高度或者宽度被改小

xiaojiejie.jpg

在kali使用identify、exfitool查看数据都得到信息，用010打开后CTRL+F搜索BJD或者CTF尝试，flag得到



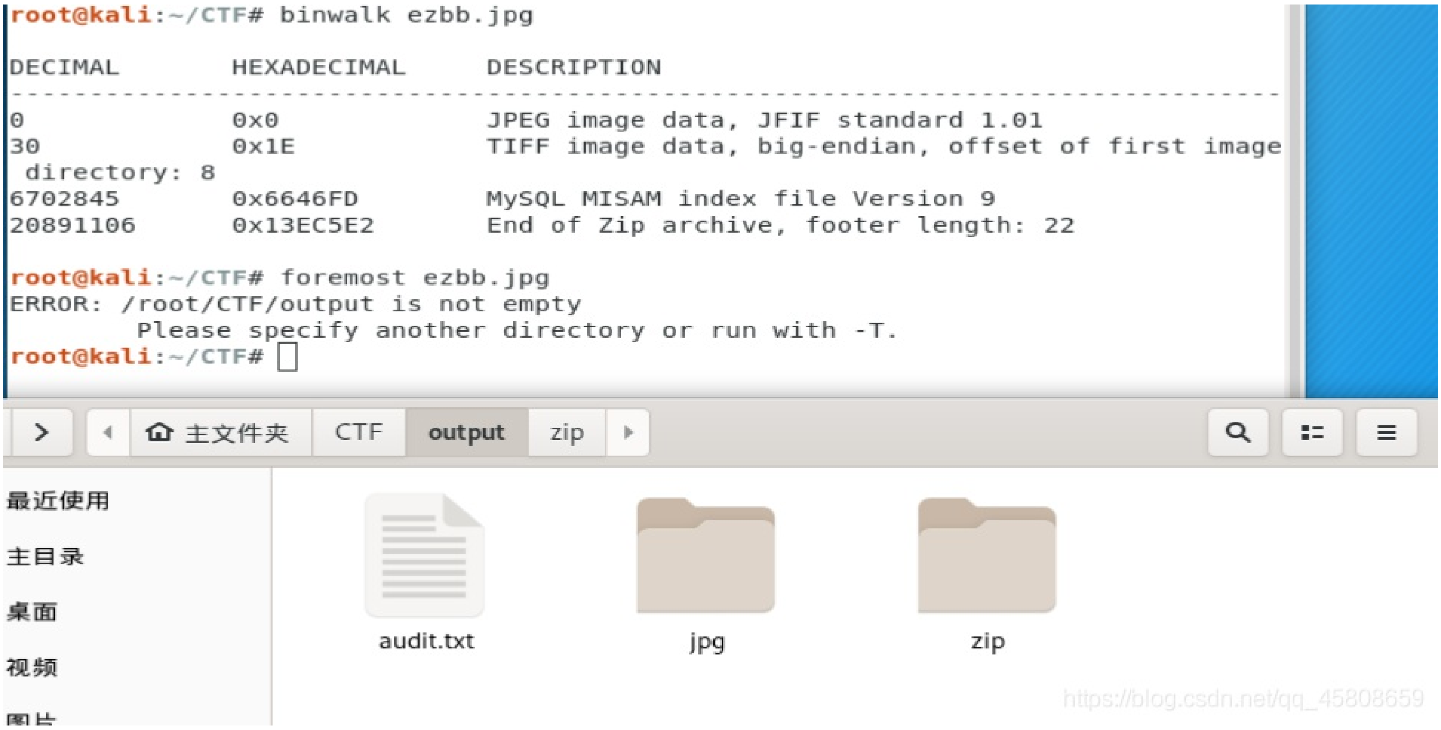
```
04 2E AC 9B EC D8 F6 CE 79 A1 16 F6 3C 9F 59 8B   ..¬›ìØöÎy¡.ö<ŸY‹
6D EB F6 07 D3 B5 74 C4 F3 E7 B9 89 70 4F 9B EE   mëö.ÓµtÄóç¹‰pO›î
3B 7A 56 86 0C E9 42 4A 44 7B 68 61 6F 6B 61 6E   ;zV†.éBJD{haokan
6D 61 5F 78 6A 6A 7D 7C 2F 7C EA 4C 6E 77 2F 03   ma_xjj}|/|êLnw/.
3E 9C 56 13 47 45 36 7A 25 84 6A 61 53 9E 83 91   >œV.GE6z%„jaSžƒ'
FD 2B 9D 9D D1 2A EA 0B 89 30 31 4D 14 F4 33 E7   ý+..Ñ*ê.‰01M.ô3ç
C8 52 3A 0E D9 AA 44 32 9A AE 4F 6E 41 E2 B4 46   ÈR:.ÙªD2š®OnAâ´F
2C D7 D2 A1 0D F3 60 80 6A 88 45 BB E2 00 3C 10   ,×Ò¡.ó`€jˆE»â.<.
05 03 D8 C4 B9 90 39 CE 7A 7A 76 A0 44 26 E3 6F   ..ØÄ¹.9Îzzv D&ão
CA 0F 00 72 28 25 92 AC BB 51 89 20 63 B5 31 9C   Ê..r(%’¬»Q‰ cµ1œ
CE B3 7B BE E5 53 23 07 BE 6A 92 31 9B D4 AF 06   Î³{¾åS#.¾j’1›Ô¯.
1C 0C 05 C1 EF D2 A9 12 69 D9 21 0E 0F 1E B9 22   ...ÁïÒ©.iÙ!...¹"
```

EASYBABA

花花 (ˇᴗˇ❀)

给imagin师傅征婚

打开是一张图片。查看图片大小发现为19M，使用binwalk分离文件

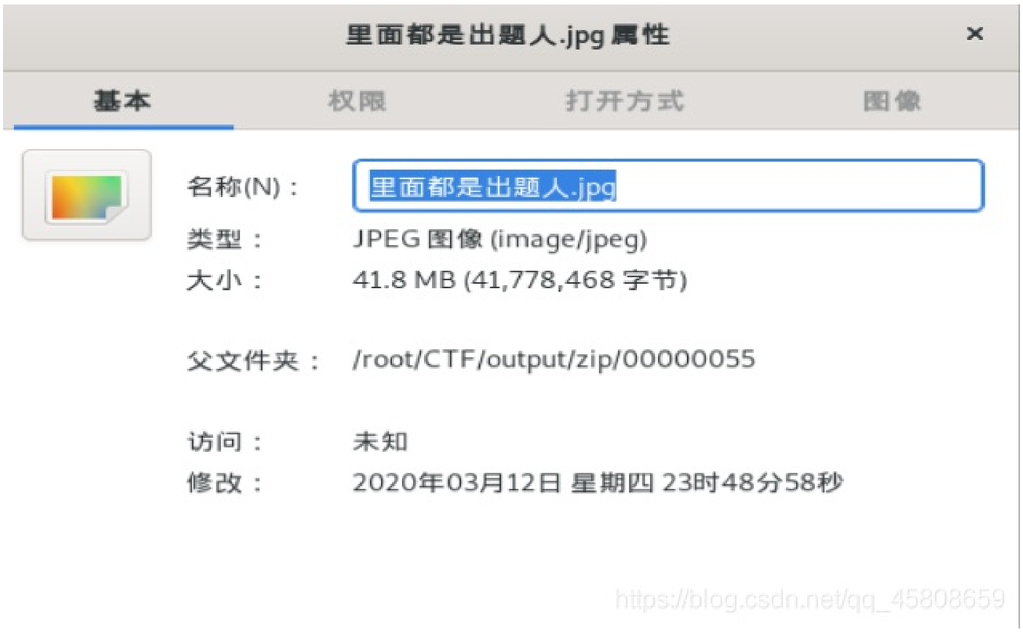


```
root@kali:~/CTF# binwalk ezbb.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image
 directory: 8
6702845       0x6646FD        MySQL MISAM index file Version 9
20891106      0x13EC5E2       End of Zip archive, footer length: 22

root@kali:~/CTF# foremost ezbb.jpg
ERROR: /root/CTF/output is not empty
        Please specify another directory or run with -T.
root@kali:~/CTF# 
```

得到一个压缩包，将压缩包打开后里面有个图片，大小为40M，而且图片无法显示



里面都是出题人.jpg 属性

名称(N)：里面都是出题人.jpg

类型：JPEG 图像 (image/jpeg)

大小：41.8 MB (41,778,468 字节)

父文件夹：/root/CTF/output/zip/00000055

访问：未知

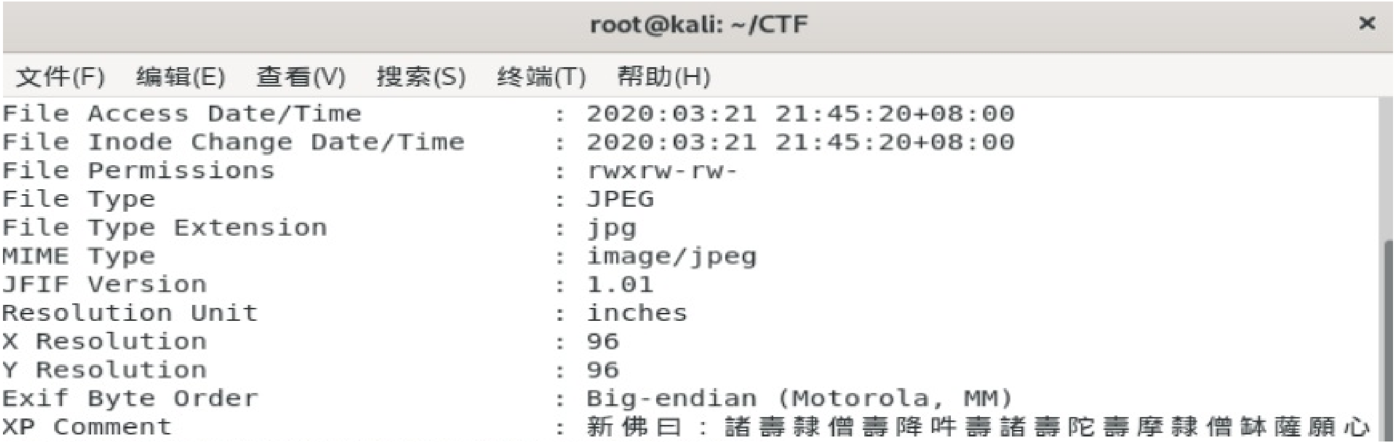
修改：2020年03月12日 星期四 23时48分58秒

使用exiftool查看，发现是movie，格式为avi

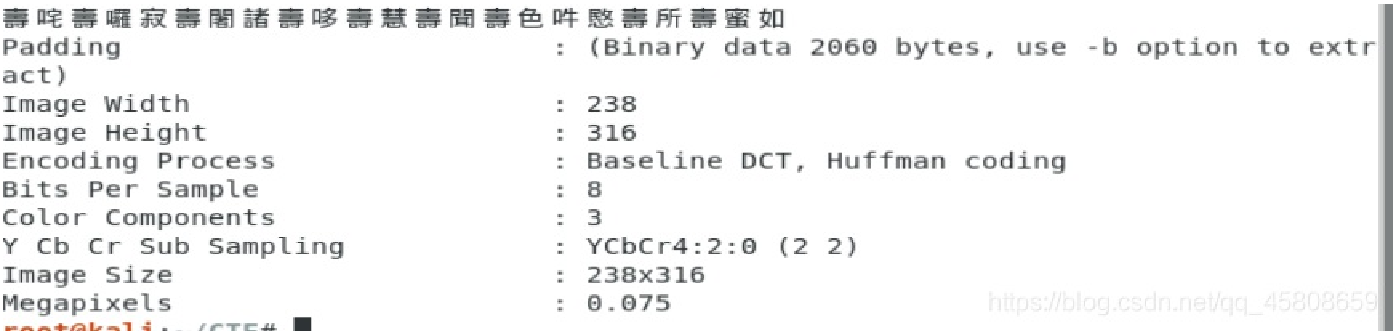
共四张，扫码后得到6167696E5F6C 6F76655F59 424A447B696D 316E677D
尝试用16进制转字符串，更改一下顺序即可得到flag

圣火昭昭

使用exiftool打开得到信息，使用新与佛论禅解密，得到gemlovecom，后听出题人说去掉com

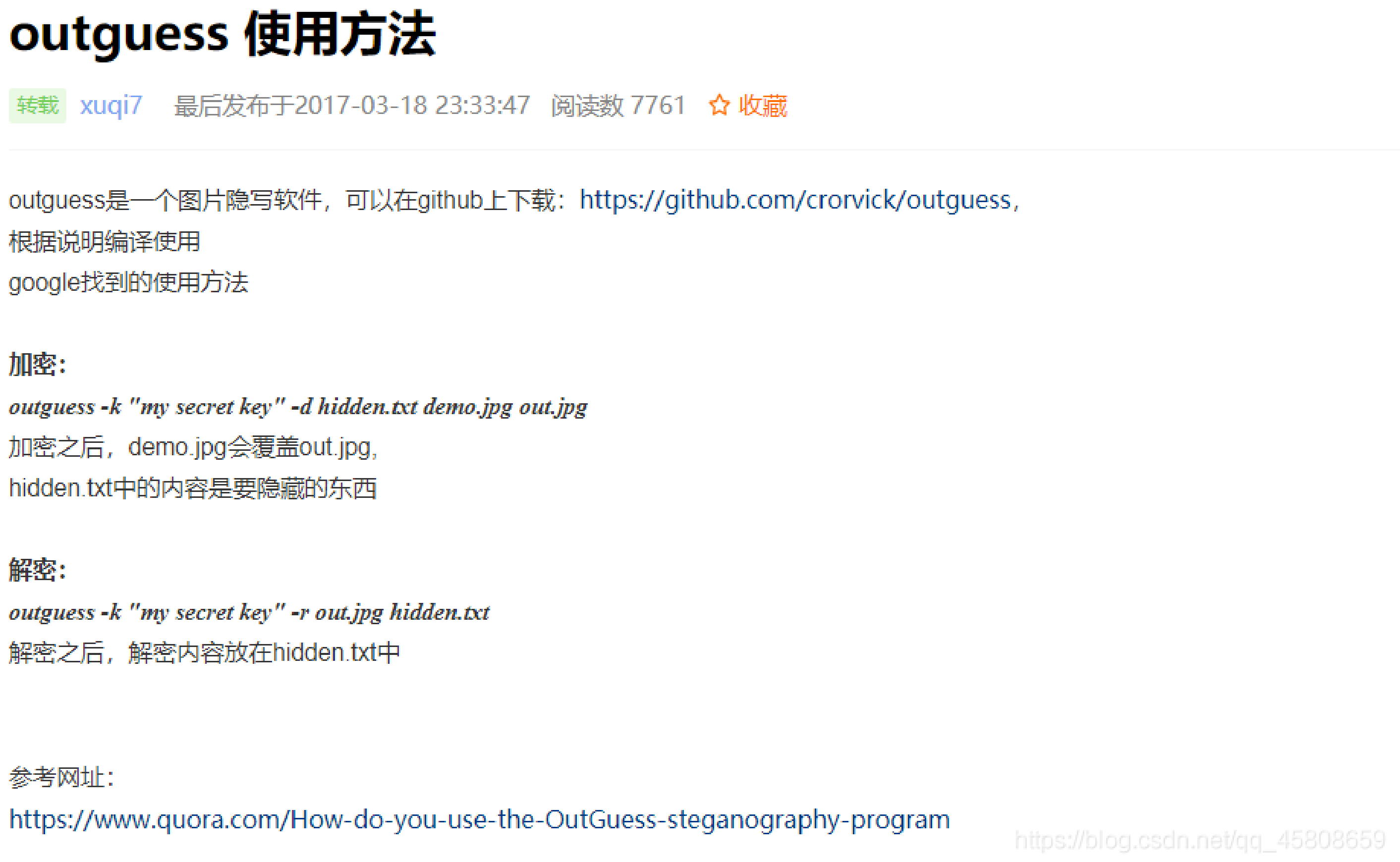


```
File Access Date/Time           : 2020:03:21 21:45:20+08:00
File Inode Change Date/Time     : 2020:03:21 21:45:20+08:00
File Permissions                : rwxrw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 96
Y Resolution                    : 96
Exif Byte Order                 : Big-endian (Motorola, MM)
XP Comment                      : 新佛曰：諸壽隸僧壽降吽壽諸壽陀壽摩隸僧缽薩願心
```



```
壽咤壽喔寂壽閣諸壽哆壽慧壽閘壽色吽愍壽所壽蜜如
Padding                          : (Binary data 2060 bytes, use -b option to extr
act)
Image Width                      : 238
Image Height                     : 316
Encoding Process                 : Baseline DCT, Huffman coding
Bits Per Sample                  : 8
Color Components                 : 3
Y Cb Cr Sub Sampling             : YCbCr4:2:0 (2 2)
Image Size                       : 238x316
Megapixels                       : 0.075
root@kali:~/CTF#
```

后知道要使用outguess，在kali安装



outguess 使用方法

转载 xuqi7 最后发布于2017-03-18 23:33:47 阅读数 7761 ☆ 收藏

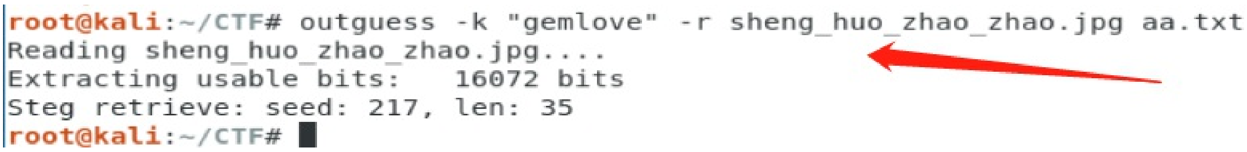
outguess是一个图片隐写软件，可以在github上下载：https://github.com/crorvick/outguess，
根据说明编译使用
google找到的使用方法

加密：
outguess -k "my secret key" -d hidden.txt demo.jpg out.jpg
加密之后，demo.jpg会覆盖out.jpg，
hidden.txt中的内容是要隐藏的东西

解密：
outguess -k "my secret key" -r out.jpg hidden.txt
解密之后，解密内容放在hidden.txt中

参考网址：
https://www.quora.com/How-do-you-use-the-OutGuess-steganography-program

按照格式输入outguess -k “gemlove” -r sheng_huo_zhao_zhao.jpg aa.txt，即可得到flag



```
root@kali:~/CTF# outguess -k "gemlove" -r sheng_huo_zhao_zhao.jpg aa.txt
Reading sheng_huo_zhao_zhao.jpg....
Extracting usable bits:   16072 bits
Steg retrieve: seed: 217, len: 35
root@kali:~/CTF#
```

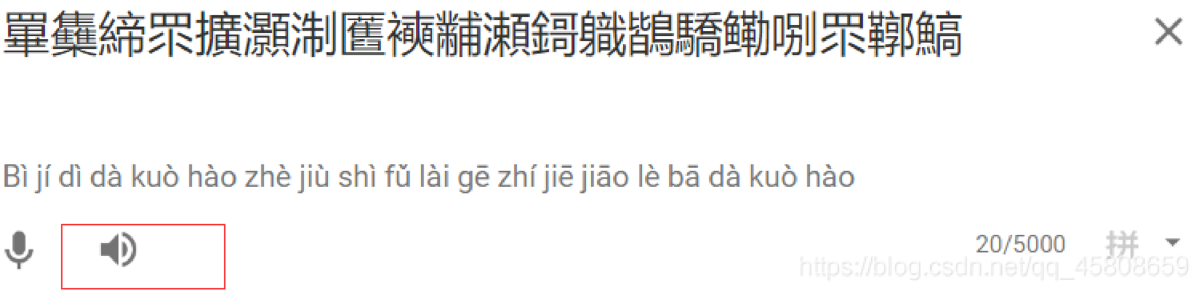
CRYPTO

签到题

base64解密
QkpEe1czbGMwbWVfVDBfQkpEQ1RGfQ==

老文盲了

罼襲締眔擴灝淛匶襫黼瀬鎶軄鶛驕鰳哵眔鞹鰝

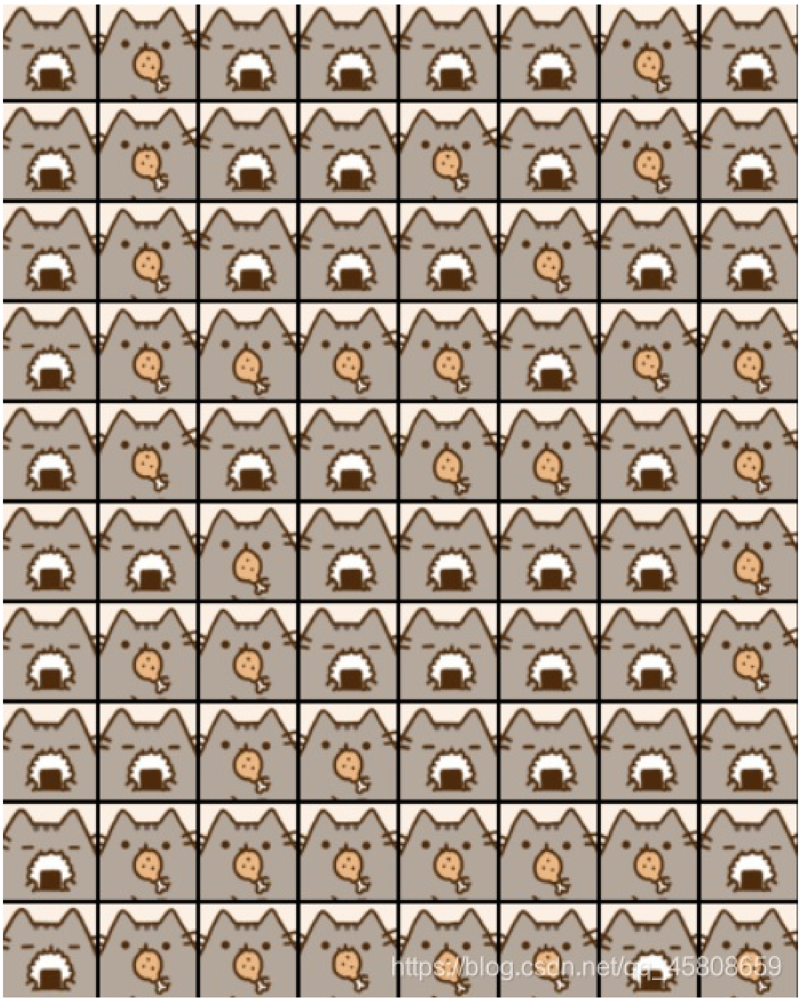


罼襲締眔擴灝淛匶襫黼瀬鎶軄鶛驕鰳哵眔鞹鰝

Bì jí dì dà kuò hào zhè jiù shì fǔ lài gē zhí jiē jiāo lè bā dà kuò hào

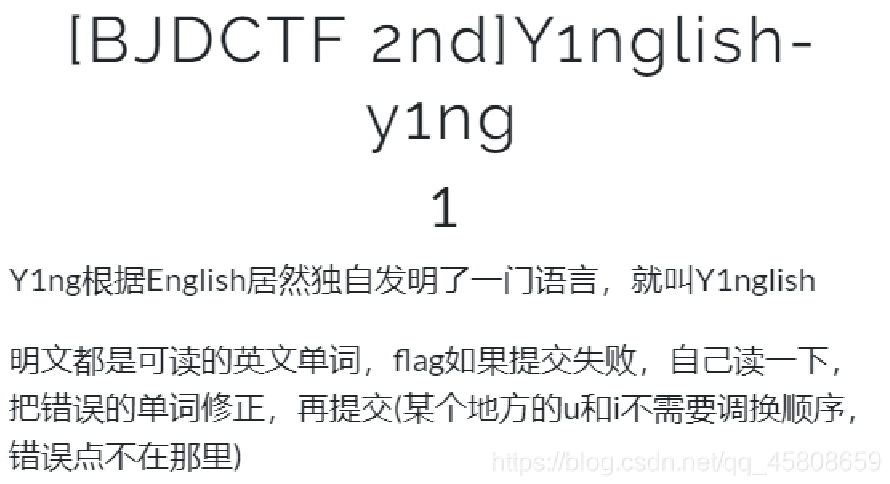
根据拼音即可知道flag为flag{淛匶襫黼瀬鎶軄鶛驕鰳哵}

cat_flag



将饭团为0，鸡腿为1，得到
0100001001001010010001000111101101001101001000010110000100110000011111001111101
将二进制转换为字符串** http://www.txttool.com/wenben_binarystr.asp ** 即可得到flag
Y1nglish
Nkbaslk ds sef aslckdqdqst. Sef aslckdqdqst qo lzqtbw usf ufkoplkt zth oscpslsfko. Dpkfk zfk uqjk dwcko su dscqao qt dpqo aslckdqdqst, kzap su npqap qo jkfw mzoqa. Qu wse zfk qtdkfkodkh qt tkdnsfw okaefqdw, nkbaslk ds czfdqaqczdk. Bkd lk dkbb wse z odsfw.
Q nzo pzjqtv hqttkf zd z fkodzefztd npkt Pzffw Odkkbk azlk qt, pk qo z lzcztkok ufsl lzczt med tsn pk qo tsd bqjqtv qt lzczt, lzwmk Pzffw qot'd z lzcztkok tzlk med pk qo fkzbbw z lzcztkok. Pzffw nsfwkh qt z bznwkf'o suuqak wkzfo zvs, med pk qo tsn nsfwqtv zd z mztw. Pk vkdo z vssh ozbzfw, med pk zbnzwo msffsno lstkw ufsl pqo ufqktho zth tkjkf czwo qd mzaw. Pzffw ozn lk zth azlk zthozdzd

dpk ozlk dzmbk. Pk pzo tkjkf msffsnkh lstkw ufsl lk. Npqbk pk nzo kzdqtv, Q zowkh pql ds bkth lk &2. Ds lw oefcfqok, pk vzjk lk dpk lstkw qllkhqzdkbw. ‘Q pzjk tkjkf msfffsnkh ztw lstkw ufsl wse,’ Pzffw ozqh,‘os tsn wse azt czw usf lw hqttkf!’ Tsn q nqbb vqjk wse npzd wse nztd.
MIH{cwdp0t_Mfed3_u0fa3_sF_geqcgeqc_ZQ_Af4aw}



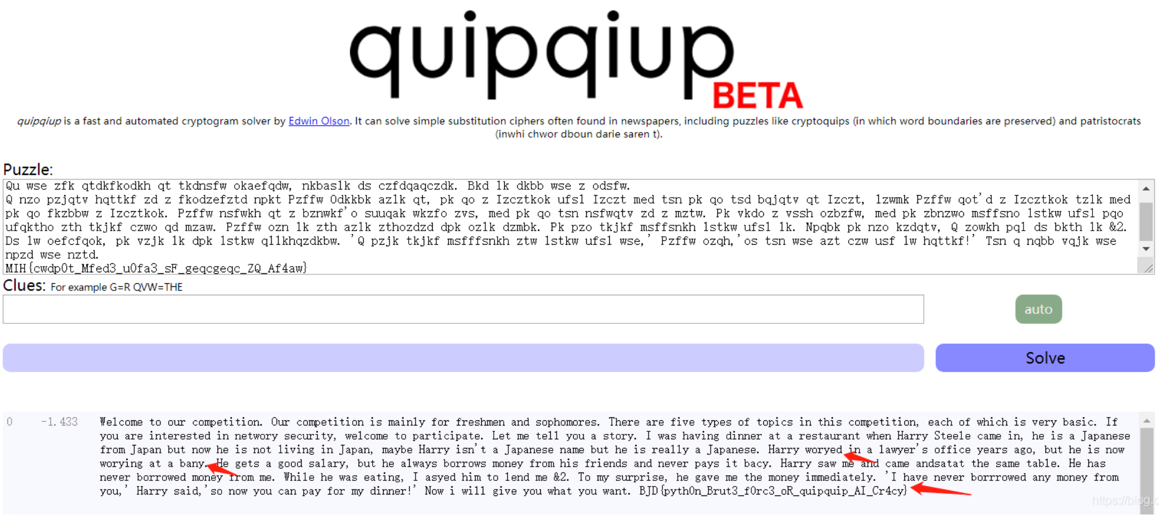
[BJDCTF 2nd]Y1nglish-y1ng

1

Y1ng根据English居然独自发明了一门语言，就叫Y1nglish

明文都是可读的英文单词，flag如果提交失败，自己读一下，把错误的单词修正，再提交(某个地方的u和i不需要调换顺序，错误点不在那里)

使用别人提供链接 ** https://quipqiup.com/ ** 得到



quipqiup is a fast and automated cryptogram solver by Edwin Olson. It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

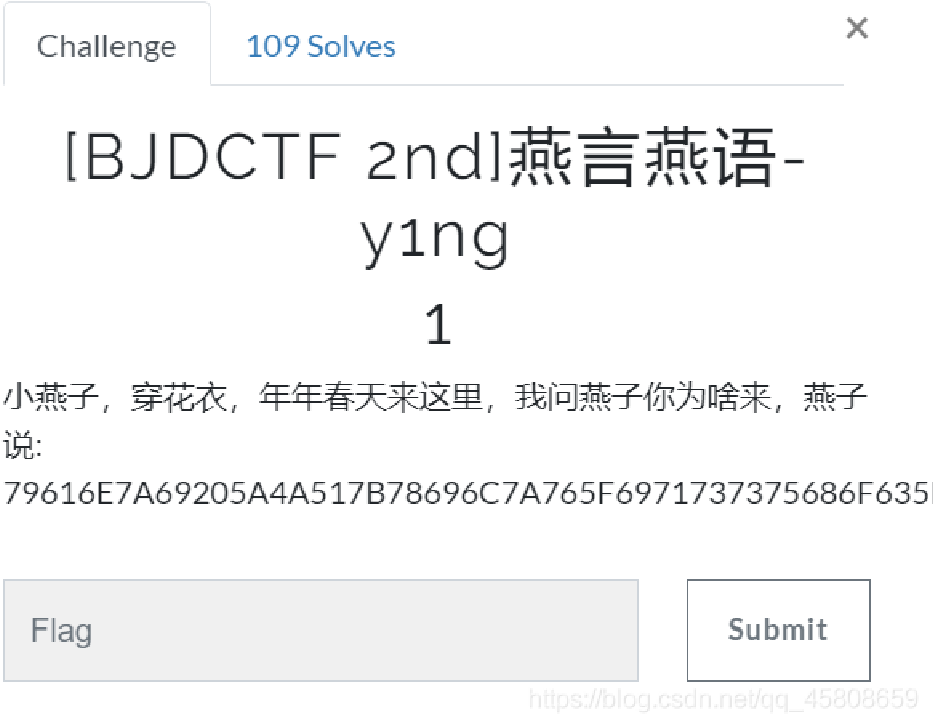
```
Qu wse zfk qtdkfkodkh qt tkdnsfw okaefqdw, nkbaslk ds czfdqaqczdk. Bkd lk dkbb wse z odsfw.
Q nzo pzjqtv hqttkf zd z fkodzefztd npkt Pzffw 0dkkbk azlk qt, pk qo z Izcztkok ufsl Izczt med tsn pk qo tsd bqjqtv qt Izczt, lzwmk Pzffw qot'd z Izcztkok tzlk med
pk qo fkzbbw z Izcztkok. Pzffw nsfwkh qt z bznwkf'o suuqak wkzfo zvs, med pk qo tsn nsfwqtv zd z mztw. Pk vkdo z vssh ozbzfw, med pk zbnzwo msffsno lstkw ufsl pqo
ufqktho zth tkjkf czwo qd mzaw. Pzffw ozn lk zth azlk zthozdzd dpk ozlk dzmbk. Pk pzo tkjkf msffsnkh lstkw ufsl lk. Npqbk pk nzo kzdqtv, Q zowkh pql ds bkth lk &2.
Ds lw oefcfqok, pk vzjk lk dpk lstkw qllkhqzdkbw. 'Q pzjk tkjkf msfffsnkh ztw lstkw ufsl wse,' Pzffw ozqh,'os tsn wse azt czw usf lw hqttkf!' Tsn q nqbb vqjk wse
npzd wse nztd.
MIH{cwdp0t_Mfed3_u0fa3_sF_geqcgeqc_ZQ_Af4aw}
```

Clues: For example G=R QVW=THE

```
0    -1.433   Welcome to our competition. Our competition is mainly for freshmen and sophomores. There are five types of topics in this competition, each of which is very basic. If
              you are interested in networy security, welcome to participate. Let me tell you a story. I was having dinner at a restaurant when Harry Steele came in, he is a Japanese
              from Japan but now he is not living in Japan, maybe Harry isn't a Japanese name but he is really a Japanese. Harry woryed in a lawyer's office years ago, but he is now
              worying at a bany. He gets a good salary, but he always borrows money from his friends and never pays it bacy. Harry saw me and came andsatat the same table. He has
              never borrowed money from me. While he was eating, I asyed him to lend me &2. To my surprise, he gave me the money immediately. 'I have never borrrowed any money from
              you,' Harry said,'so now you can pay for my dinner!' Now i will give you what you want. BJD{pyth0n_Brut3_f0rc3_oR_quipquip_AI_Cr4cy}
```

根据题目，可知题目中的k都被替换为了k，在得到的flag中有两个带y的单词，根据明文是可读的英文单词，将后面把那个y修改为k即可得到flag

燕言燕语

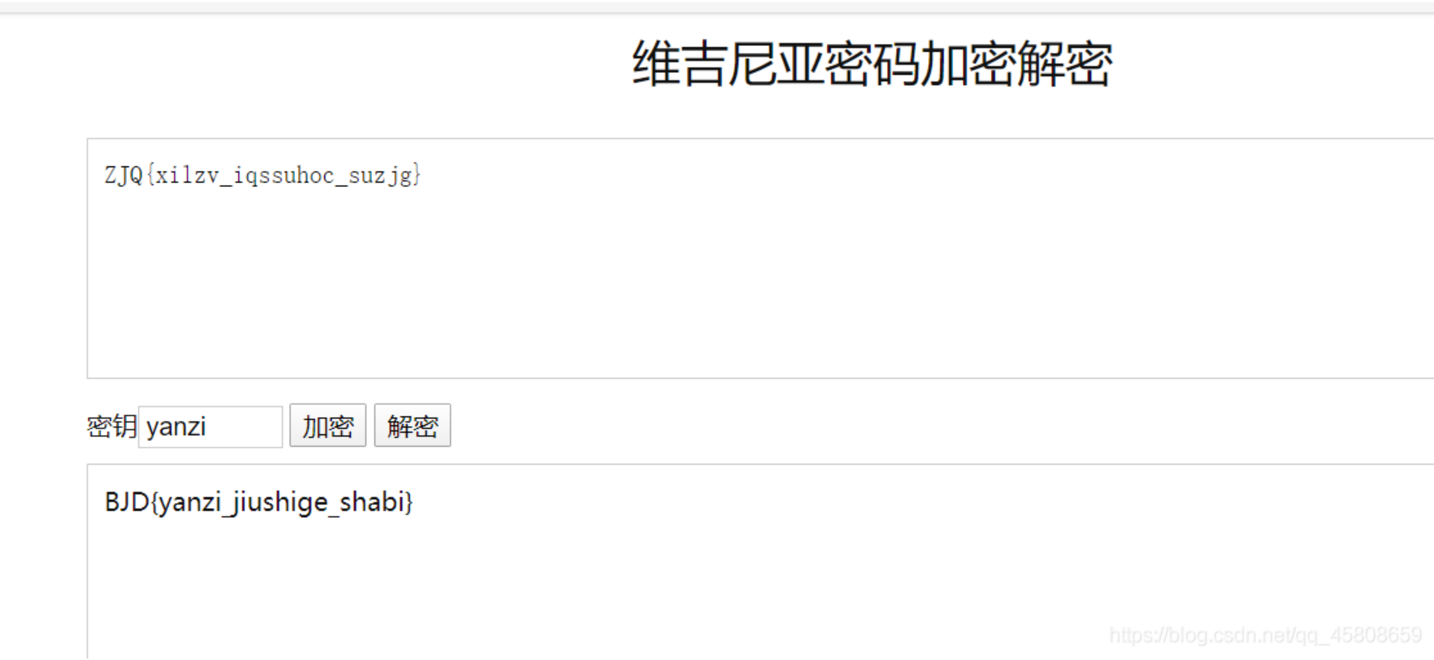


[BJDCTF 2nd]燕言燕语-y1ng

1

小燕子，穿花衣，年年春天来这里，我问燕子你为啥来，燕子说: 79616E7A69205A4A517B78696C7A765F6971737375686F635

79616E7A69205A4A517B78696C7A765F6971737375686F635F73757A6A677D20
十六进制转字符得到yanzi ZJQ{xilzv_iqssuhoc_suzjg} 提交flag不正确
yanzi为密钥，尝试密钥的加密方式



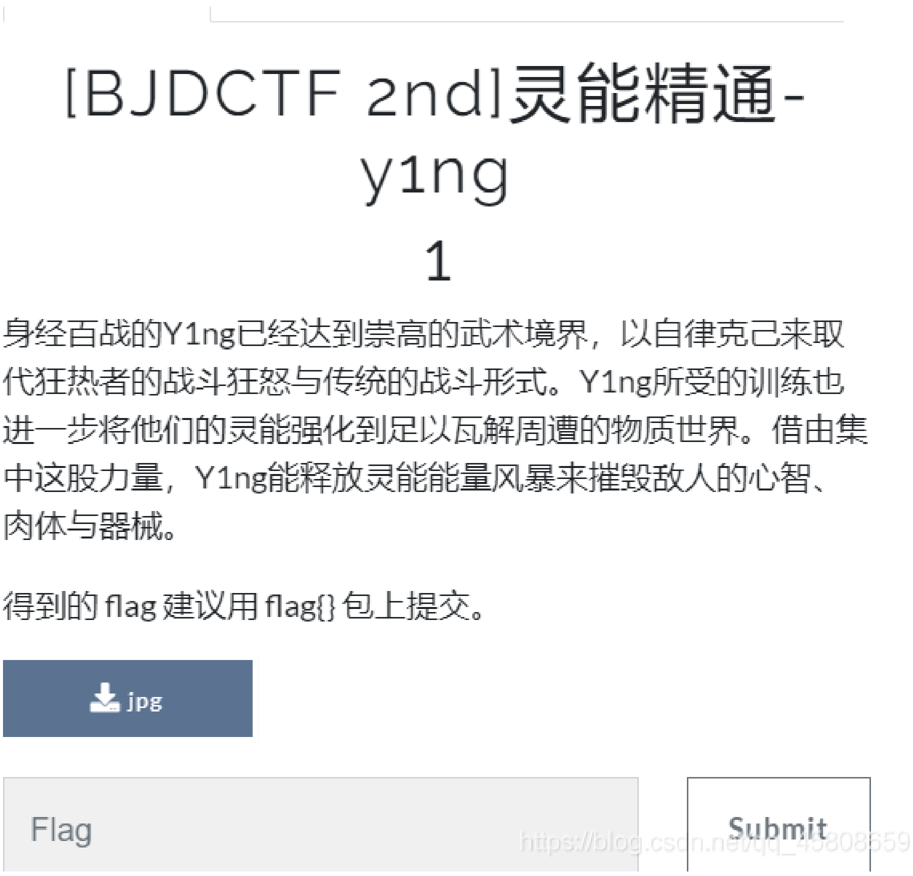
维吉尼亚密码加密解密

ZJQ{xilzv_iqssuhoc_suzjg}

密钥 yanzi

BJD{yanzi_jiushige_shabi}

灵能精通

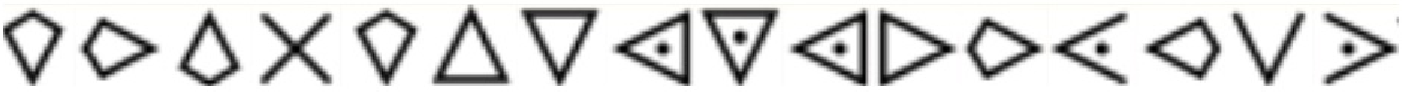


[BJDCTF 2nd]灵能精通-y1ng

1

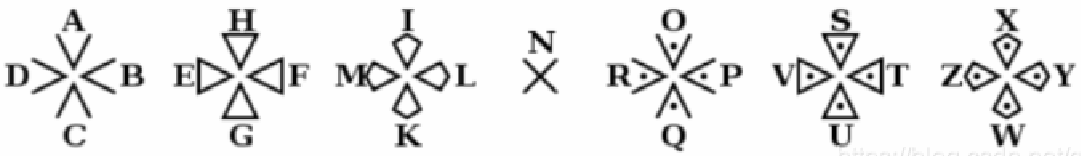
身经百战的Y1ng已经达到崇高的武术境界，以自律克己来取代狂热者的战斗狂怒与传统的战斗形式。Y1ng所受的训练也进一步将他们的灵能强化到足以瓦解周遭的物质世界。借由集中这股力量，Y1ng能释放灵能能量风暴来摧毁敌人的心智、肉体与器械。

得到的 flag 建议用 flag{} 包上提交。



圣堂武士密码(Templar Cipher)是共济会的“猪圈密码”的一个变种，一直被共济会圣殿骑士用。

明文字母和对应密文：



猪圈密码的变型圣堂武士密码
imknightstemplar