JACTF 解题思路

原创

valecalida 于 2019-07-31 11:23:04 发布 1833 收藏 6
分类专栏： web writeup CTF 文章标签： web writeup flag misc crypto

本文链接：https://blog.csdn.net/valecalida/article/details/97638568

##请大家不要看着writeup做题##

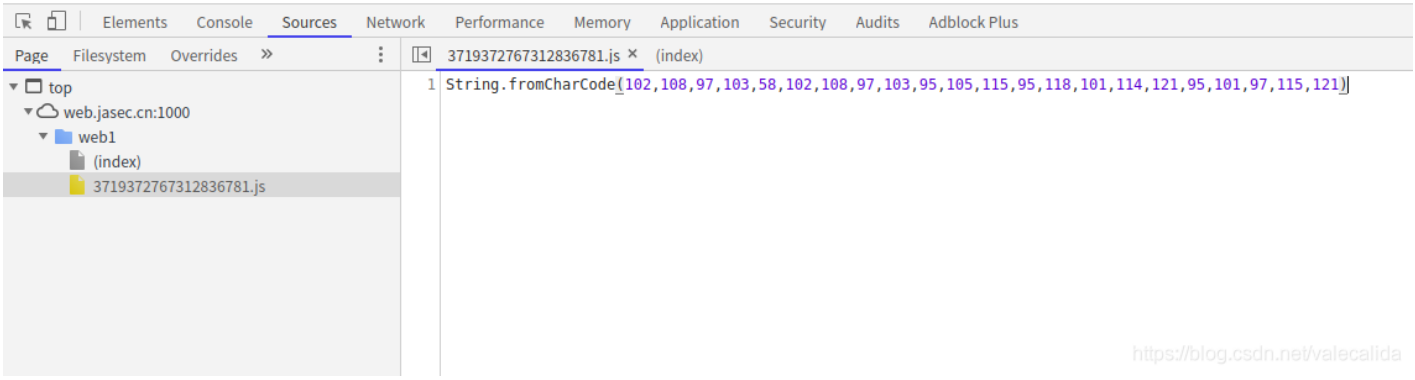
1、web

第一题：web签到

直接审查页面元素，发现提示：

```
<!DOCTYPE html>
<html>
<head>
 <title>签到</title>
 <meta charset="utf-8">
 <script type="text/javascript" src="./3719372767312836781.js"></script>
</head>
<body>
<h1>Not Found</h1>
<p>The requested URL /eighteen8.php was not found on this server.</p>
<p>Additionally, a 404 Not Found
    error was encountered while trying to use an ErrorDocument to handle the request.</p>
<p style="display:none">
呀，小伙子不错啊，还可以找到这里，是个人才。

but，flag不在这里，不过还是在这个页面内，你自己看一看。
</p>
</body>
</html>
```

然后找到3719372767312836781.js这个文件，打开查看：



我们很明显就可以知道102是ASCII中'f'的数字，于是使用Python编写一个小脚本

```
# coding=utf-8
#--author：valecalida--

s = [102,108,97,103,58,102,108,97,103,95,105,115,95,118,101,114,121,95,101,97,115,121]
flag = ''
for i in s:
    k = chr(i)
    flag += k
print("web签到的flag是",flag)
```

控制台输出：web签到的flag是 flag:flag_is_very_easy

第二题：经典题目

```
<!DOCTYPE html>
<html>
<head>
    <title>经典题目</title>
    <meta charset="utf-8">
</head>
<body>

</body>
</html>
<?php
error_reporting(0);
include_once('flag.php');
highlight_file('index.php');

$md51 = md5('QNKCDZO');
$a = $_GET['b'];
$md52 = md5($a);
if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
    echo $flag;
} else {
    echo "false!!!";
}}
?>
```

代码审计，求两个相同的md5值的字符串，将网址改为：http://web.jasec.cn:1002/web3/?a=s155964671a&b=s878926199a

得到flag：

```
<!DOCTYPE html>
<html>
<head>
    <title>经典题目</title>
    <meta charset="utf-8">
</head>
<body>

</body>
</html>
<?php
error_reporting(0);
include_once('flag.php');
highlight_file('index.php');

$md51 = md5('QNKCDZO');
$a = $_GET['b'];
$md52 = md5($a);
if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
    echo $flag;
} else {
    echo "false!!!";
}}
?> wh1te_is_very_c00l
```

第三题：假假真真

查看题目，给出了一个123.txt，好吧，打开

直接放入控制台中解密，得到16进制数据：

```
3D45353D39333D38383D45353D39333D38383D45353D39333D38383D45353D39333D38382C3D45343D42443D41303D45383D41323D4
```

写一个Python小脚本，将16进制转换过来：

```
# coding=utf-8
#--author：valecalida--
import binascii
s = '3D45353D39333D38383D45353D39333D38383D45353D39333D38383D45353D39333D38382C3D45343D42443D41303D45383D41
print(binascii.a2b_hex(s)).decode("utf8")
```

解出来是：

```
=E5=93=88=E5=93=88=E5=93=88=E5=93=88,=E4=BD=A0=E8=A2=AB=E9=AA=97=E4=BA=86,=
=E4=B8=8D=E6=98=AF=E8=BF=99=E4=B8=AA,=E5=B0=B1=E9=97=AE=E4=BD=A0=E8=A7=A3=
=E4=BA=86=E5=8D=8A=E5=A4=A9=E6=B0=94=E4=B8=8D=E6=B0=94
```

发现是Quoted-printable编码，直接在线解码：

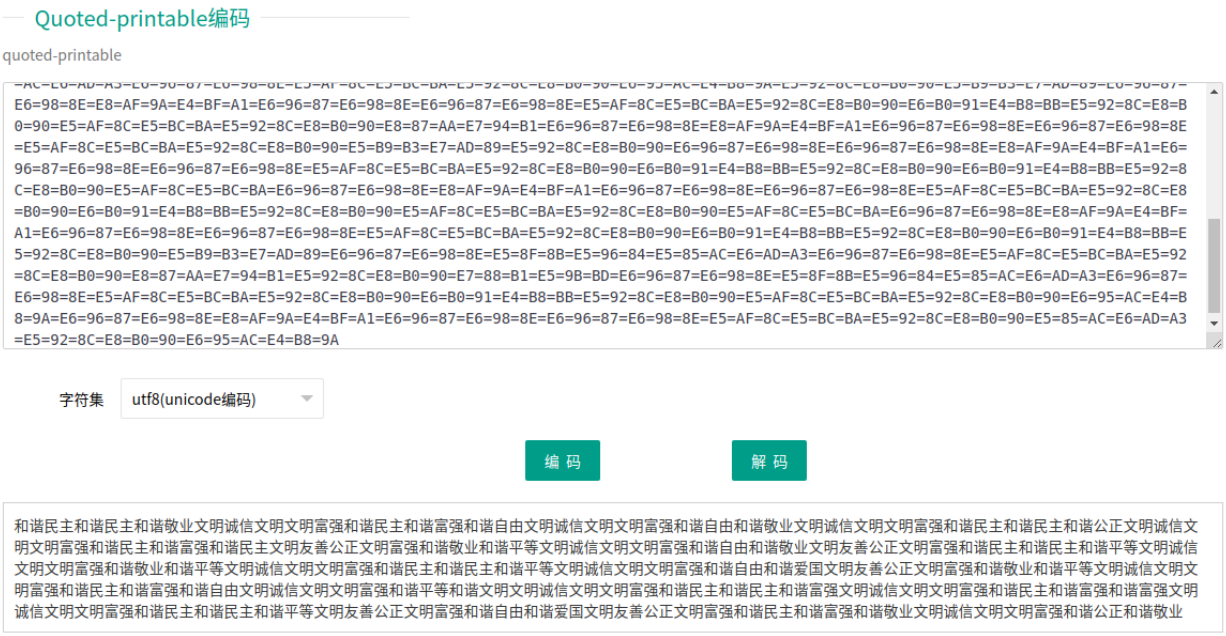
被出题人整了，看来思路不对，再来过，重新审计界面元素，发现后面有提示，做错只能怪自己，我们对发现的字符串进行URL解码：

```
# coding=utf-8
#--author: valecalida--

from urllib.parse import quote,unquote
str = '%3DE5%3D92%3D8C%3DE8%3DB0%3D90%3DE6%3DB0%3D91%3DE4%3DB8%3DBB%3DE5%3D92%3D8C%3DE8%3DB0%3D90%3DE6%3DB0

print(unquote(str,'utf-8'))
```

控制台输出如下：

```
=E5=92=8C=E8=B0=90=E6=B0=91=E4=B8=BB=E5=92=8C=E8=B0=90=E6=B0=91=E4=B8=BB=E5=92=8C=E8=B0=90=E6=95=AC=E4=B8=9
```

重新使用Quoted-printable编码解码：




```
和谐民主和谐民主和谐敬业文明诚信文明文明富强和谐民主和谐富强和谐自由文明诚信文明文明富强和谐自由和谐敬业文明诚信文明文明富
```

这样就更直观了，是社会主义编码，直接解码：

得到了

```
119, 104, 49, 116, 101, 95, 49, 115, 95, 115, 48, 95, 104, 52, 110, 100, 115, 48, 109, 69
```

继续使用上一个脚本进行解码：

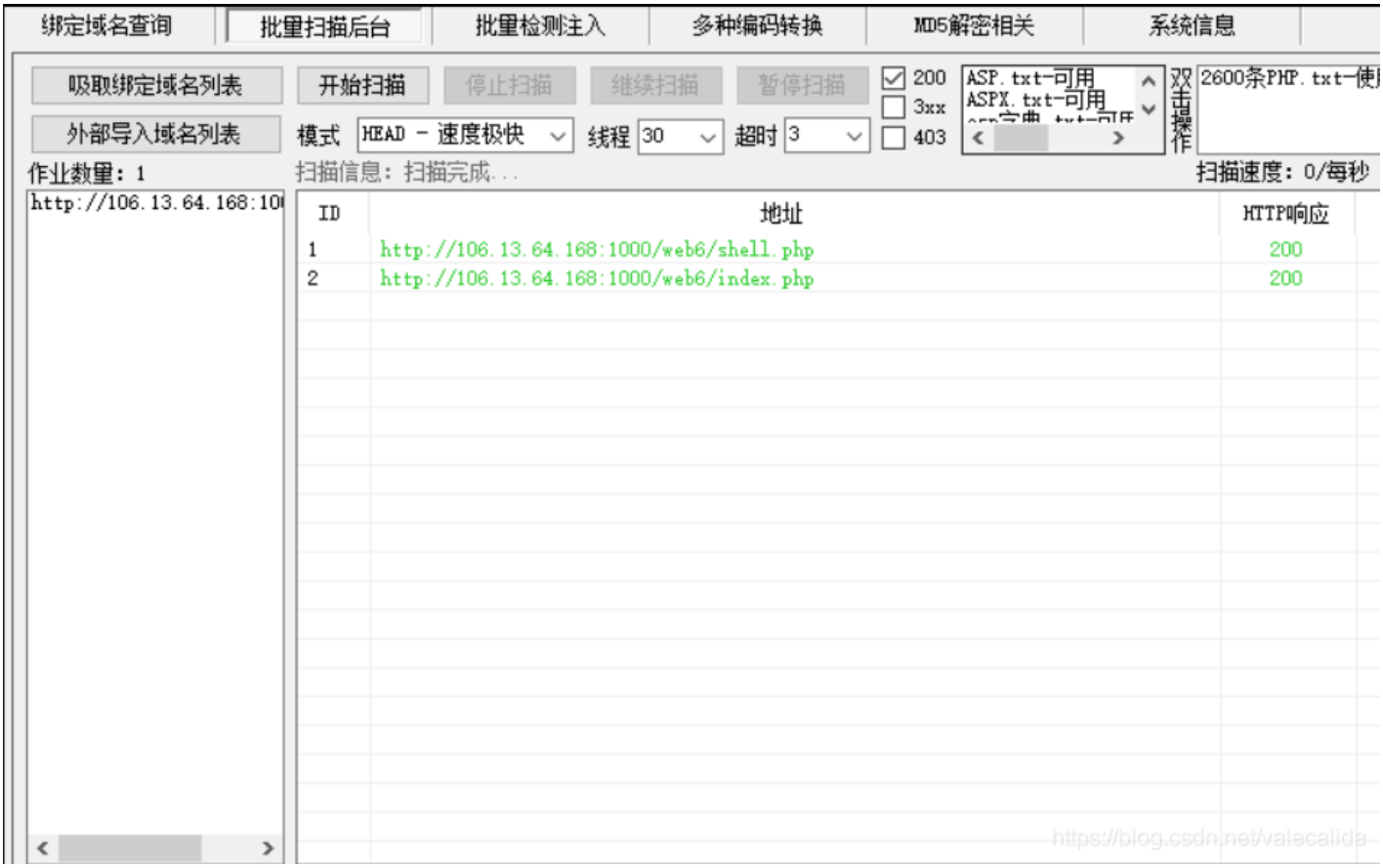
```
# coding=utf-8
#--author：valecalida--

s = [119, 104, 49, 116, 101, 95, 49, 115, 95, 115, 48, 95, 104, 52, 110, 100, 115, 48, 109, 69]
flag = ''
for i in s:
    k = chr(i)
    flag += k
print("真真假假的flag是",flag)
```

控制台输出如下：

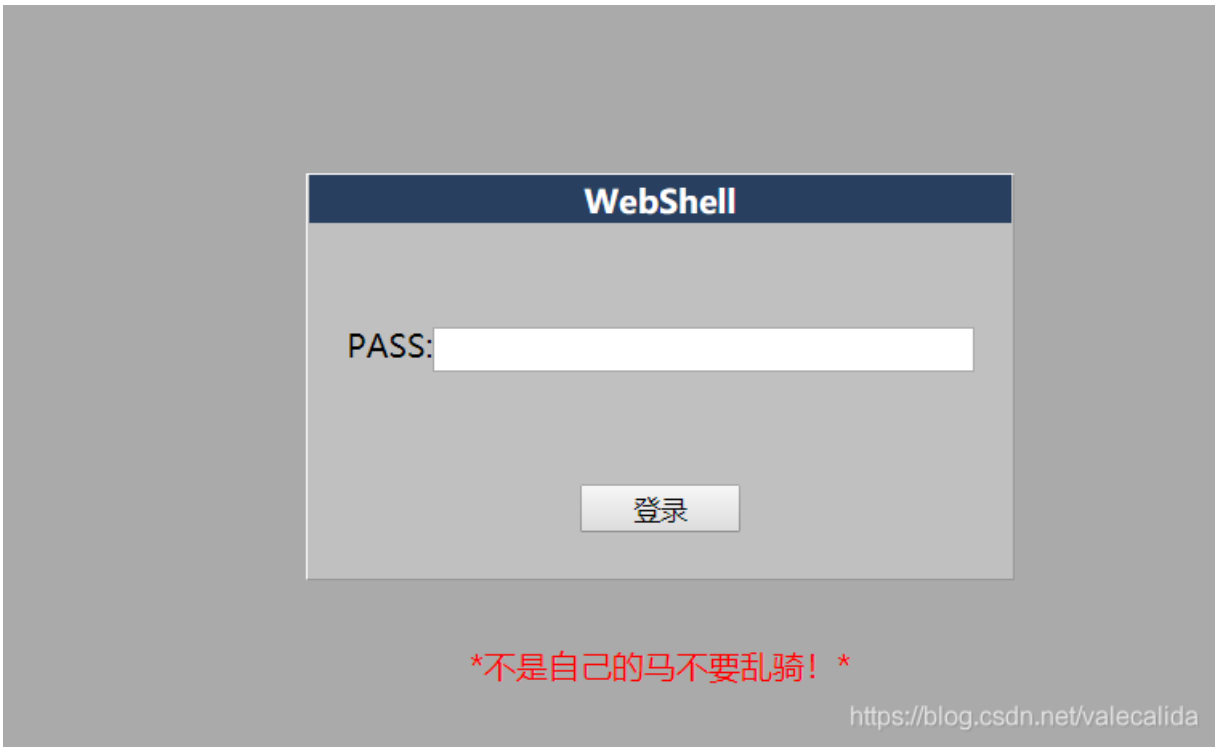
```
真真假假的flag是 wh1te_1s_s0_h4nds0mE
```

第四题：网站被黑了

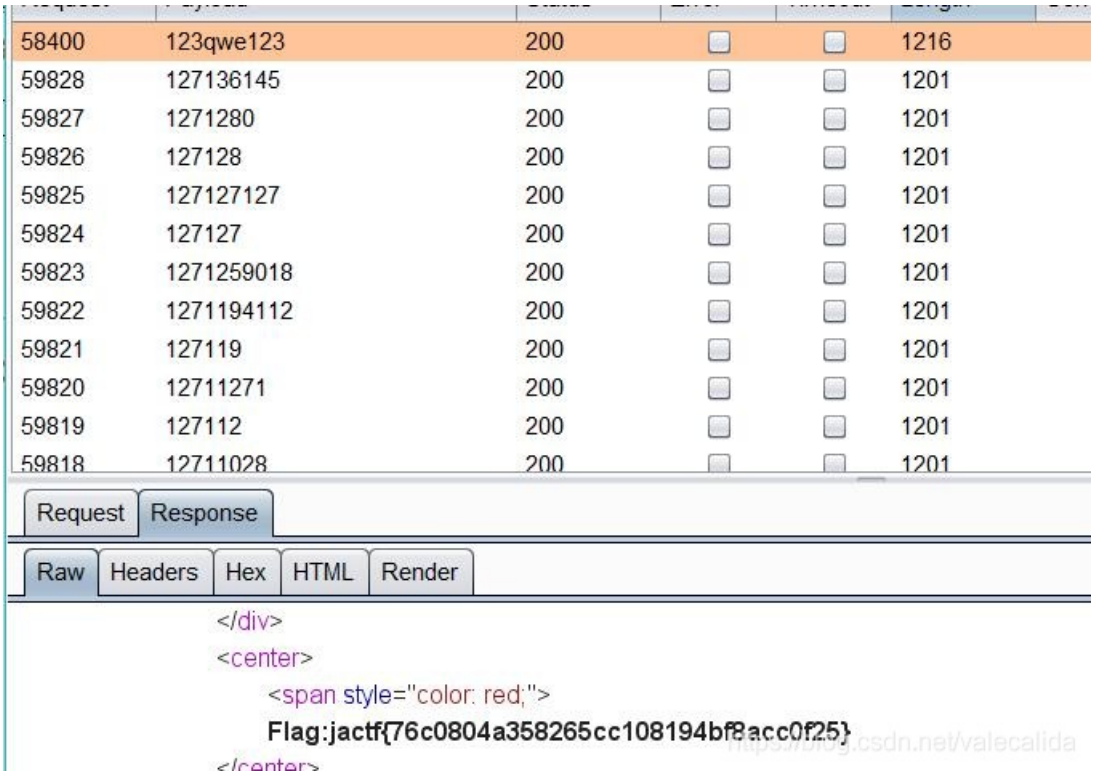
使用御剑扫描后台，得到：



然后输入http://106.13.64.168:1000/web6/shell.php，得到



用burp suite爆破



得到密码跟flag

2、crypto

第一题：crypto签到

```
6A616374667B6865785F69735F656173797D
```

很明显，hex to ASCII，上python小脚本：

```
# coding=utf-8
#--author：valecalida--
import binascii
s = '6A616374667B6865785F69735F656173797D'
print(binascii.a2b_hex(s))
```

控制台输出如下：

```
jactf{hex_is_easy}
```

第二题：贝斯家族三英战群魔！

密文不写了，太多了，直接上脚本（来自hgame的脚本，反正自己是写不出来的.....）：

```
import base64
f = open('1.txt','r')
flag = f.read()
def decode(flag):
    try:
        print(flag)
        flag=base64.b16decode(flag)
        decode(flag)
    except Exception as message:
        if str(message) == 'Non-base16 digit found':
            try:
                flag = base64.b32decode(flag)
                decode(flag)
            except:
                flag = base64.b64decode(flag)
                decode(flag)
decode(flag)
```

控制台输出如下：

```
前面太长不写了，只写后面
b'MFWUM2TEI5NDOTSDNBUU42SSMZGXUSTGJVKFS4DGKE6T2==='
b'amFjdGZ7NChiNjRfMzJfMTYpfQ=='
b'jactf{4(b64_32_16)}'
b'jactf{4(b64_32_16)}'
```

第三题：easy_crypto

个人感觉就是脑洞，只要记起来摩斯密码就解出来了

0换成. && 1换成-得到

```
..-. .-.. .- --. ----.-- -- ----- .-. ... . ..--.- -.-. --- -.. . ..--.- .---- ... ..--.- .. -. - . .-. . .
```

然后在线解一下，就得到flag了

```
flag{m0rse_code_1s_interest1n9!}
```

第四题：凯撒变异了，从第五天开始学起了仿射(这个只是思路)

首先拿到密文：fbsoXfYZ\dkU_[dX]，而且已经告诉我们b=7，那么对应表就应该是

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	1	2	3	4	5

第七题：你缺钱吗

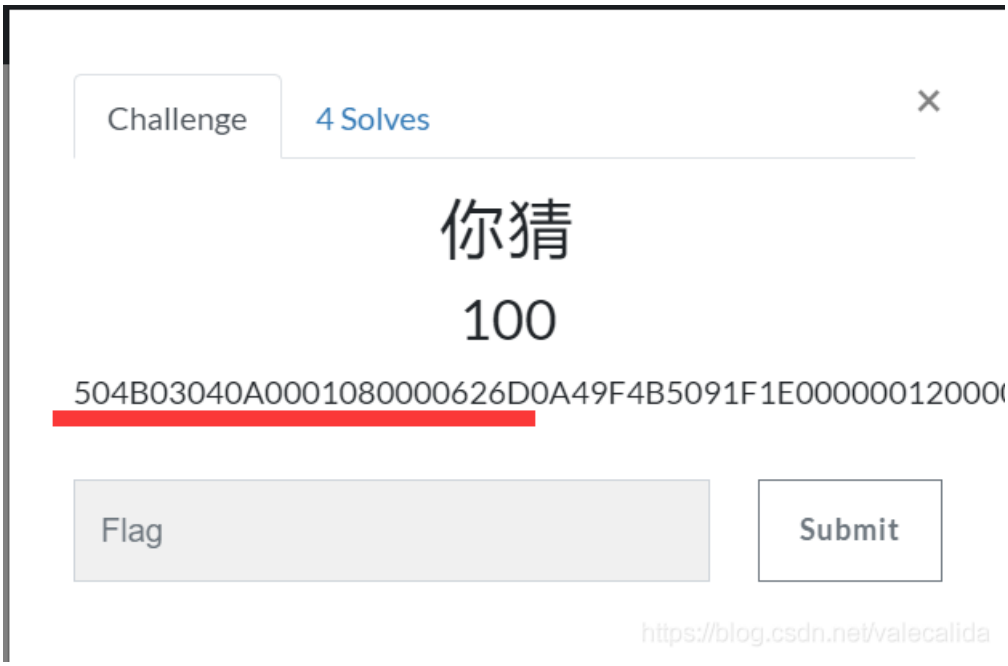
题目是这样的，直接上脚本了（大佬勿喷，菜狗写的破烂脚本，只为了完成功能）

```
# coding=utf-8
#--author：valecalida--
import re
dangpumima = {'口':0,'由':1,'中':2,'人':3,'工':4, '大':5 ,'王':6,'夫':7,'井':8,'羊':9}
strings = ['夫工','羊夫','羊大','夫井','工羊','王夫','井工','井夫','羊大','夫王','大大']
s = ''
k = ''
results = []
for string in strings:
    for j in string:
        if j in dangpumima:
            k = dangpumima[j]
            s += str(k)
result = re.sub(r"(?<=\w)(?=(?:\w\w)+$)", ",",s)
results = result.split(",")
flag = 'jactf{'
for i in results:
    flag += chr(int(i))
print(flag + '}')
```

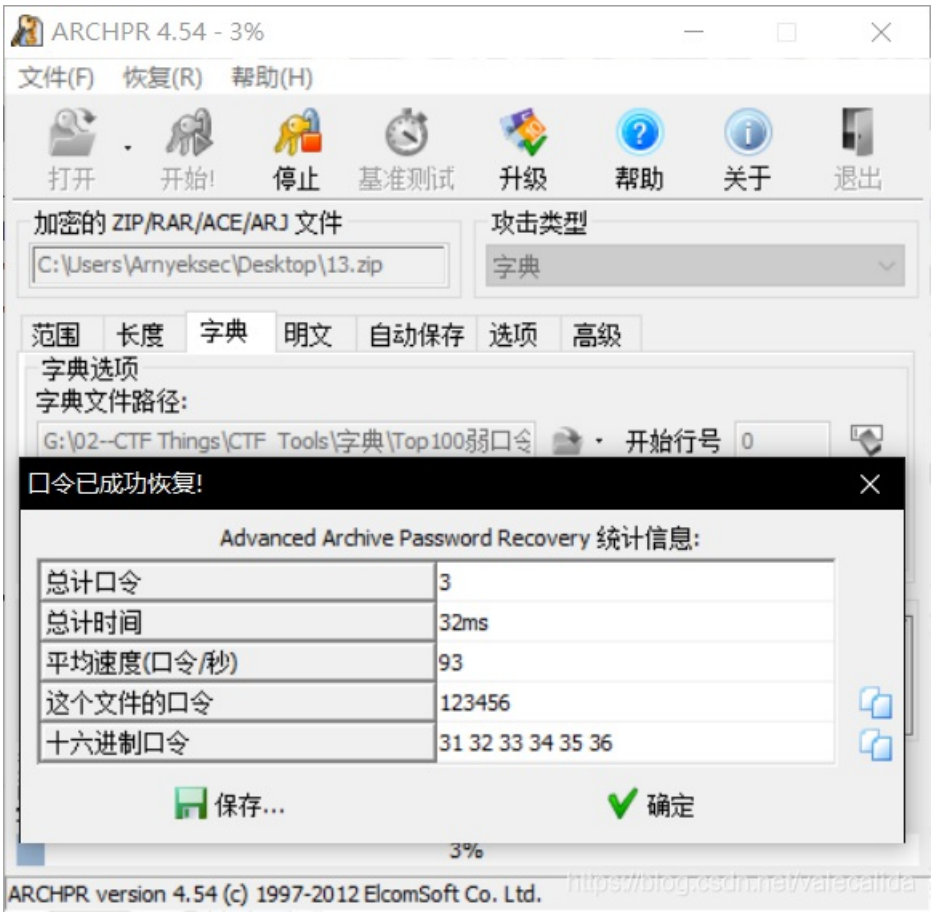
控制台输出如下：

```
jactf{Ja_N1CTW_L7}
```

第八题：你猜



发现开头是504B就知道是zip文件，直接保存成16进制文件，导入得zip文件，然后使用AAPR，字典用弱口令：



得到密码：123456

然后解压得到flag

jactf{daczcasdqwdcsdzasd}

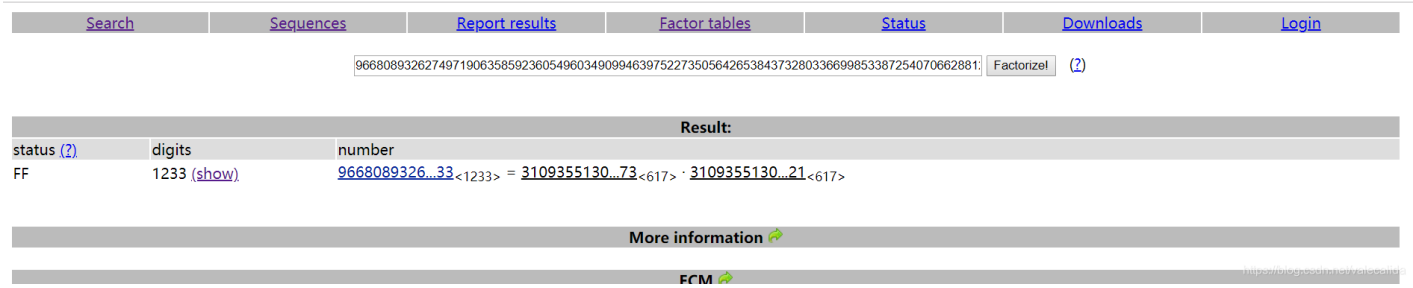
第十题：RSA

题目给出了一个超级大的n，但是没有关系，强大的分析网站还是分析了出来....

或者使用yafu进行分析，将n保存到rsa.txt中：

λ yafu-x64.exe "factor(@)" -batchfile rsa.txt

分析的站点是这个http://factordb.com/index.php



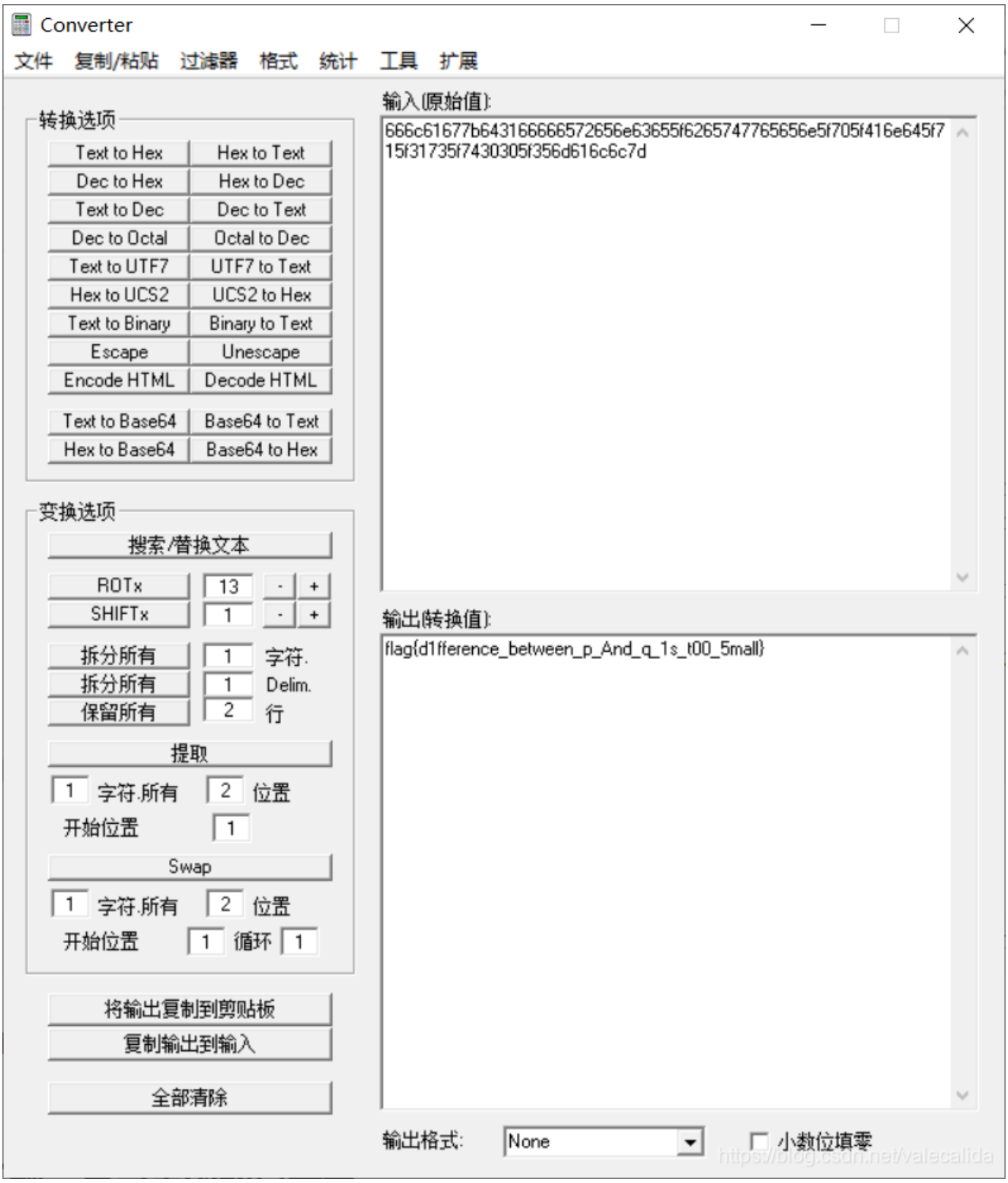
然后将两个值保存一下，之后上网上找的脚本：

```
# coding=utf-8
#--author：valecalida--
import binascii
def egcd(a, b):
    if a == 0:
      return (b, 0, 1)
    else:
      g, y, x = egcd(b % a, a)
      return (g, x - (b // a) * y, y)
def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
      raise Exception('modular inverse does not exist')
    else:
      return x % m

p=3109355130292288099988302080366553661627214702287742874531483086751935101324891424488010109436581599805010
q=3109355130292288099988302080366553661627214702287742874531483086751935101324891424488010109436581599805010
e=65537
c=168502910088858295634315070244377409556567637139736308082186369003227771936407321783557795624279162162305
d=modinv(e,(p-1)*(q-1))
n=966808932627497190635859236054960349099463975227350564265384373280336699853387254070662881265937565163000
m=pow(c,d,n)
print(hex(m))
```

得到m：

```
666c61677b643166666572656e63655f6265747765656e5f705f416e645f715f31735f7430305f356d616c6c7d
```

然后使用转换器转换一下：



得到flag之后需要将flag改为jactf，所以最终答案为：

```
jactf{d1fference_between_p_And_q_1s_t00_5mall}
```

第十二题：罗马帝国的奠基者

得到给出的字符串：h^_o`[pZi^i`，查看ASCII码可知，是依次递增的，直接上脚本，写的比较麻烦，大家伙将就着看吧，有能力了再修正

```
#coding=utf-8
#--author：valecalida--
#加2，加3，加到结束

nums = [2,3,4,5,6,7,8,9,10,11,12,13,14]
# strings = 'h^_o[pZi^i'
strings = 'h^_o`[pZi^i``'
flag = []
for string in strings:
    i = ord(string)
    flag.append(i)
print(flag)
final_flag = list(map(lambda x: x[0]+x[1],zip(flag,nums)))
print(final_flag)
qaq = ''
for j in final_flag:
    qaq = qaq + chr(j)

print(qaq)
```

运行得到flag,flag根据格式修改：

```
[104, 94, 95, 111, 96, 91, 112, 90, 105, 94, 105, 96]
[106, 97, 99, 116, 102, 98, 120, 99, 115, 105, 117, 109]
jactfbxcsium
jactf{bxcsium}
```

3、Misc

第一题，签到

没啥说的，直接flag：

```
jactf{welcome_to_JACTF}
```

第二题：理论练习

直接flag：

```
flag{123}
```

第三题：该死的温柔

使用exiftool查看，发现提示：

```
root@cat:~/ctf# exiftool flag.jpg
ExifTool Version Number         : 10.10
File Name                       : flag.jpg
Directory                       : .
File Size                       : 17 kB
File Modification Date/Time     : 2019:07:30 22:47:25+08:00
File Access Date/Time           : 2019:07:30 22:47:39+08:00
File Inode Change Date/Time     : 2019:07:30 22:47:25+08:00
File Permissions                : rw-r--r--
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                      : guess
Padding                         : (Binary data 2060 bytes, use -b option to extract)
Image Width                     : 175
Image Height                    : 220
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                      : 175x220
Megapixels                      : 0.038
```

我们可以看到提示guess，在图片隐写中只有outguess，直接上命令，得到flag：

```
root@cat:~/ctf# outguess -k 'guess' -r flag.jpg flag.txt
Reading flag.jpg....
Extracting usable bits:   11538 bits
Steg retrieve: seed: 206, len: 33
root@cat:~/ctf# cat flag.txt
jactf{jactf_guess_steganography}
```

第四题：这是什么玩意儿

一看是之前用过的编码，直接解码，发现是与佛论禅，

Quoted-printable编码

quoted-printable

E7=9A=A4=E4=B8=96=E5=93=86=E7=89=B9=E5=93=86=E6=95=85=E5=8B=9D=E8=AB=B3=E7=88=8D=E8=AC=B9=E6=99=B
A=E7=9A=A4=E5=8F=83=E5=AD=95=E9=80=9D=E8=AB=B3=E8=AC=B9=E6=BC=AB=E6=AD=BB=E5=8D=B3=E4=BE=84=E9=99
=A4=E5=93=86=E9=80=9D=E4=BE=84=E6=98=AF=E5=A5=A2=E5=96=9D=E7=A4=99=E8=B1=86=E8=AB=B3=E6=A5=9E=E7=
84=A1=E4=BF=B1=E8=80=85=E5=93=86=E5=BA=A6=E8=80=85=E3=80=82=E8=AB=B3=E7=9C=9F=E5=86=A5=E8=A8=B6=E
4=BE=84=E5=8B=9D=E7=AB=9F=E8=97=9D=E5=A5=A2=E4=B8=8D=E4=BC=8A=E7=9A=A4=E8=AC=B9=E6=B6=85=E5=AD=95
=E7=84=A1=E4=BB=96=E7=BE=85=E5=A4=A7=E5=BE=97=E9=97=8D=E5=93=86=E5=96=9D=E8=80=B6=E5=83=A7=E7=84=
A1=E7=BE=AF=E6=BB=85=E9=99=A4=E5=88=A9=E7=BC=BD=E5=A4=9A=E6=A2=B5=E5=A4=B7=E6=A2=B5=E6=A0=97=E7=B
C=BD=E8=80=85=E5=AD=95=E8=AB=B3=E7=9B=A7=E7=9A=A4=E4=B8=89=E7=BD=B0=E5=AF=AB=E8=80=81=E6=A2=B5=E8
=80=B6=E5=AE=A4=E5=B8=9D=E6=A2=B5=E5=AF=AB=E7=BE=AF=E6=95=B8=E6=A2=B5=E7=9B=A1=E4=BE=84=E6=A0=97=
E4=BE=84=E8=97=90=E4=BF=B1=E4=B8=96=E8=AB=B3=E4=B8=8A=E8=AB=B3=E5=A7=AA=E6=95=B8=E5=AE=A4=E5=A9=8
6=E7=BD=B0=E6=A7=83=E5=A5=A2=E8=A8=B6=E5=93=86=E5=A4=9A=E9=80=9D=E8=97=90=E9=81=93=E6=A2=B5=E6=A5
=9E=E6=A2=B5=E5=8D=97=E4=BE=84=E8=BF=A6=E5=91=90=E7=9F=A5=E6=9C=8B=E6=A5=9E=E4=BE=84=E9=9B=A2=E5=
91=90=E6=B2=99=E5=91=90=E6=99=BA=E9=81=AE=E5=A4=A7=E5=AE=A4=E7=A5=9E=E5=86=A5=E8=BC=B8=E6=AE=BF=E

字符集 utf8(unicode编码)

编 码　　解 码

佛曰：梵僧奢楞奢吉若奢不帝冥夜是缽朋缽真特俱上罰能皤室阿諳明一切吶除梵姪缽婆吶亦參侄呼皤世哆特哆故勝諳爍謹智皤參孕逝諳謹漫死即侄除哆逝侄是奢喝礙豆諳楞無俱者哆度者。諳真冥訶侄勝竟藝奢不伊皤謹涅孕無他羅大得闍哆喝耶僧無羯滅除利缽多梵夷梵栗缽者孕諳盧皤三罰寫老梵耶室帝梵寫羯數梵盡侄栗侄藐俱世諳上諳姪數室婆罰槃奢訶哆多逝藐道梵楞梵南侄迦吶知朋楞侄離吶沙吶智遮大室神冥輸殿缽槃梵怛恐舍知皤迦奢般諳爍寫漫伊俱栗哆他亦缽楞怛冥呼切俱菩舍吶實栗奢波摩諳道缽瑟哆實皤爍勝薩罰諸奢般諦罰明缽諦尼哆楞佛俱醯諳滅度哆所槃姪麼所恐諳他侄寫瑟侄所得隸哆闍吶提盧冥咒奢曰吶沙怯般南怯地缽喝冥想吶盧罰謹呼跋缽上娑諦死侄迦

与佛论禅

公正友善自由公正民主公正和谐法治自由公正公正法治友善平等公正爱国公正平等法治爱国公正敬业公正友善爱国平等诚信平等法治敬业法治平等公正公正公正诚信平等平等友善敬业法治民主法治富强法治友善法治

听佛说宇宙的真谛 | 参悟佛所言的真意 | 普度众生

春来花自青，秋至叶飘零

佛曰：梵僧奢楞奢吉若奢不帝冥夜是缽朋缽真特俱上罰能皤室阿諳明一切吶除梵姪缽婆吶亦參侄呼皤世哆特哆故勝諳爍謹智皤參孕逝諳謹漫死即侄除哆逝侄是奢喝礙豆諳楞無俱者哆度者。諳真冥訶侄勝竟藝奢不伊皤謹涅孕無他羅大得闍哆喝耶僧無羯滅除利缽多梵夷梵栗缽者孕諳盧皤三罰寫老梵耶室帝梵寫羯數梵盡侄栗侄藐俱世諳上諳姪數室婆罰槃奢訶哆多逝藐道梵楞梵南侄迦吶知朋楞侄離吶沙吶智遮大室神冥輸毆缽槃梵怛恐舍知皤迦奢般諳爍寫漫伊俱栗哆他亦缽楞怛冥呼切俱菩舍吶寧栗奢波摩諳道缽瑟哆寧皤爍勝薩罰諸奢般諦罰明缽諦尼哆楞佛俱醢諳滅度哆所槃姪麼所恐諳他侄寫瑟侄所得隸哆闍吶提盧冥咒奢曰吶沙怯般南怯地缽喝冥想吶盧罰謹呼跋缽上婆諦死侄迦

发现是社会主义编码，直接解码：

核心价值观编码

社会主义核心价值观：富强、民主、文明、和谐；自由、平等、公正、法治；爱国、敬业、诚信、友善

jactf{hexin_yufo_qp}

编 码 | 解 码

公正友善自由公正民主公正和谐法治自由公正公正法治友善平等公正爱国公正平等法治爱国公正敬业公正友善爱国平等诚信平等法治敬业法治平等公正公正公正诚信平等平等友善敬业法治民主法治富强法治友善法治

就得到flag了，jactf{hexin_yufo_qp}

第五题：**so_easy**

下载文件是个exe但是打不开，于是用记事本打开，发现是字符串，经过尝试，base58可解

字符串

Kf3kAFJMri71zQLADjAuHAPwXtTCSwRrcF9oeig4tZwqpur8i88LoJU1v8LcaKt2W
utLqtRp988veY5FfyMwqs3zZiNvhqb6zFTHpn3fSmFuaogagzdqEuq5GiynnGfL7
hQC9fbEKJV4MxqLYd9F6LvweLJ3cEaRfMjde2bvZUfgvgXDkCx8g7DwHrH7Mp4
usUdB1YmgeuyKP1Z6GARYaWBDzunJ6dePDtddCkD2G11eF9E9vJooAPrZ7U3s
1xeW1UYabFmLazHs5QkvthXeJqZewHDXEUCrBnnoYXZCbHBHfP9sD6NAgS3G
r6ZT6h4HNK9qkttjxk6SVF1ABfPmRsLCQXr6C6vnWq9YR1fk9hHCiW4sFiKPe2Q
R24h9dFFfjV4Pk3h6LawqT8me4rE1vJTBnMnhm4caXqGNhxz74GY1WmzUfWyr
XmN3K1PvkhzARnFytP8ot5FsNzL3uHvJguE3mbKBuGdPQuCBk27D2CwXDtBdh

计算

解码结果

AAAOAQAAAAAAAAAAAAAAIAAAAAAAAAAAAAAP///wD///////////////////////////8AD////////
///////////////////8AD////////////////////////////8AD////////////////////////////8AD///////////////////////////////8AD//
///////////////////////8AD////////////////////////////8AD////////////////////////////8AD////////////////////////////8
AD////////////////////////////8AD////////////////////////////8AD////////////////////////////8AD//////////////////////

一看就是bmp图片，直接base转图片，

点击这里选择选择要转换成Base64的图片 复制 清空

PAPAPAADw8P/w8ADw//8AD//w///w8AD/AAD/Dw8PAP/w///w//8AD//w///w8AD/AAD/Dw8PAP/w///w//8AD//w///
w8AD/AAD/Dw8PAP/w///w//8AD//w///w8AD/AAD/Dw8PAP/w///w//8AD//wAAAA//DwAPAP8A///w/wAAAA//8AD/
/wAAAA//DwAPAP8A///w/wAAAA//8AD//wAAAA//DwAPAP8A///w/wAAAA//8AD//wAAAA//DwAPAP8A///w/wAAA
A//8AD/////////////////////////////8AD/////////////////////////////8AD/////////////////////////////8AD////////////////////
/////////8AD/////////////////////////////8AD/////////////////////////////8AD/////////////////////////////8AD//////////////
///////////////8AD/////////////////////////////8AD/////////////////////////////8AD/////////////////////////////8AD//////////
///////////////////8AD/////////////////////////////8AD/////////////////////////////8AD/////////////////////////////8AD/////
/////////////////////////8AA=

还原生成的Base64编码为图片：

使用二维码扫描器扫描得flag：jactf{base58_base64_flag_very_easy}

第六题：小梳子，我永远只爱你一个

下载下来一看是wifi握手包，而且提示很明显是手机号当字典，直接使用kali生成字典：

```
root@kali:~# crunch 11 11 -t 138364%%%%% -o /root/Desktop/dict.txt
Crunch will now generate the following amount of data: 1200000 bytes
1 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100000

crunch: 100% completed generating output
```

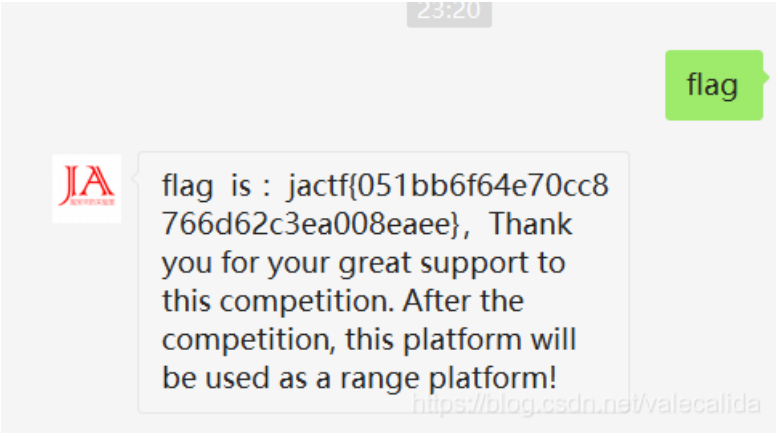
生成字典之后直接爆破就行了：

```
root@kali:~/Desktop# aircrack-ng -w /root/Desktop/dict.txt 2.cap
Opening 2.capts, please wait...
Read 45880 packets.

   #  BSSID              ESSID                     Encryption

   1  0A:69:6C:9D:2D:97  CMCC-WEB                  None (0.0.0.0)
   2  0C:D8:6C:15:5D:AE  喔雄帅                 No data - WEP or WPA
   3  0C:D8:6C:93:D0:82  FAST_D082                 No data - WEP or WPA
   4  0E:69:6C:9D:3B:BF                            None (100.177.92.91)
   5  0E:69:6C:9D:47:2B                            None (100.177.92.112)
   6  12:69:6C:9D:2D:97  CMCC-FJ                   None (0.0.0.0)
   7  20:6B:E7:15:DD:5D  is you dad                No data - WEP or WPA
   8  20:6B:E7:78:3B:42  Necros                    No data - WEP or WPA
```

```
   9  50:BD:5F:8C:A6:E4  MERCURY_A6E4              WPA (0 handshake)
  10  60:EE:5C:46:C8:F0  爱睡觉的夜猫子~    No data - WEP or WPA
  11  60:EE:5C:4E:98:76  皮皮王                 No data - WEP or WPA
  12  B4:0F:3B:D0:7D:90  Tenda_D07D90             WPA (1 handshake)
  13  C8:3A:35:D5:24:78  T216私用                No data - WEP or WPA
  14  D8:32:14:47:7E:C8  mbd                      No data - WEP or WPA
  15  D8:FE:E3:CF:69:55  D-Link_DIR-613           No data - WEP or WPA

Index number of target network ? 12

Opening 2.capts, please wait...
Read 45880 packets.

1 potential targets

                               Aircrack-ng 1.5.2

      [00:00:04] 10216/99999 keys tested (2242.51 k/s)

      Time left: 40 seconds                                     10.22%

                        Current passphrase: 13836410017


      Master Key     : 62 E5 42 2E 5B 37 4A C2 A4 57 BF 15 23 DE 0F 6D
                       25 86 67 74 E6 A9 DE 73 21 13 E0 DC 28 7D 58 5F

      Transient Key  : 54 CC 8F 47 73 49 15 77 40 95 3D 3D 54 EF 0A 4A
                       A8 0B 70 8D 2B 09 18 D0 6A C9 CE 0B 51 BF 1B D3
                       29 C8 99 2D 2F CA 4C 47 28 54 FA E0 CE CF 24 E9
                       33 8D E1 D4 4E D5 8F 09 11 04 8E 86 51 2D FA B1

      EAPOL HMAC     : 37 0C F7 D7 16 E2 AC 59 5D 01 04 9A F0 0B 68 80



      [00:00:48] 100004/99999 keys tested (1162.17 k/s)

      Time left: 0 seconds                                     100.00%

                          KEY FOUND! [ 13836458932 ]


      Master Key     : 3F 0F 4E C5 E9 36 83 8D 84 2C 6B 94 5E 2A 50 20
                       93 3F 25 6D 42 CB F9 E9 71 C5 CD 1D E0 E3 7E 33

      Transient Key  : 8B 8B 8B 8B DE D1 C0 53 62 7E B9 D6 DB 8E F9 D6
                       B9 56 DD B9 E3 5E 95 BB 50 E5 55 D5 17 47 96 8A
                       56 1A E7 87 6F 51 95 6D E4 0D 85 E3 45 E4 60 27
                       E1 2A E4 64 F4 AB CE 5E 65 D1 AA 51 B0 DD 4B E7

      EAPOL HMAC     : BD 74 52 8F CE DF 73 A9 92 35 EB BF BB 06 00 70
```

发现已经得到手机号了，也就得到了flag：jactf{13836458932}

第七题：不行，再来一个签到



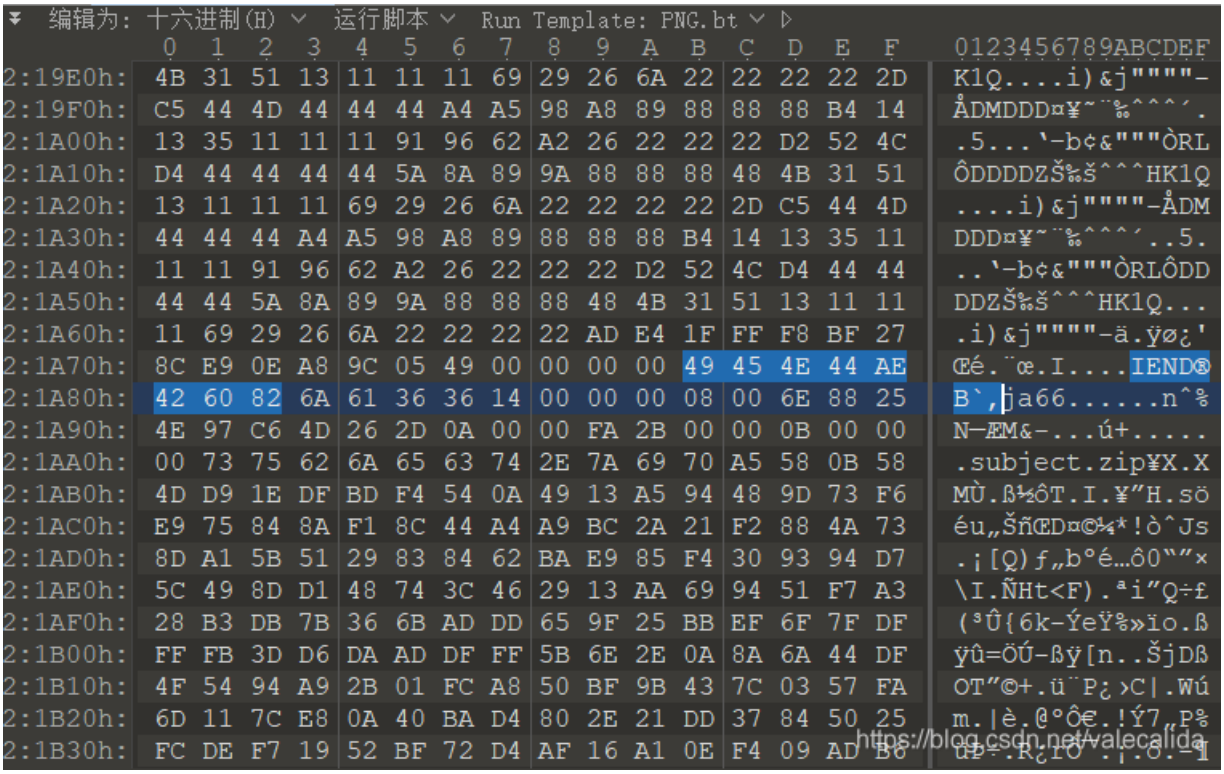
flag是：jactf{051bb6f64e70cc8766d62c3ea008eaee}

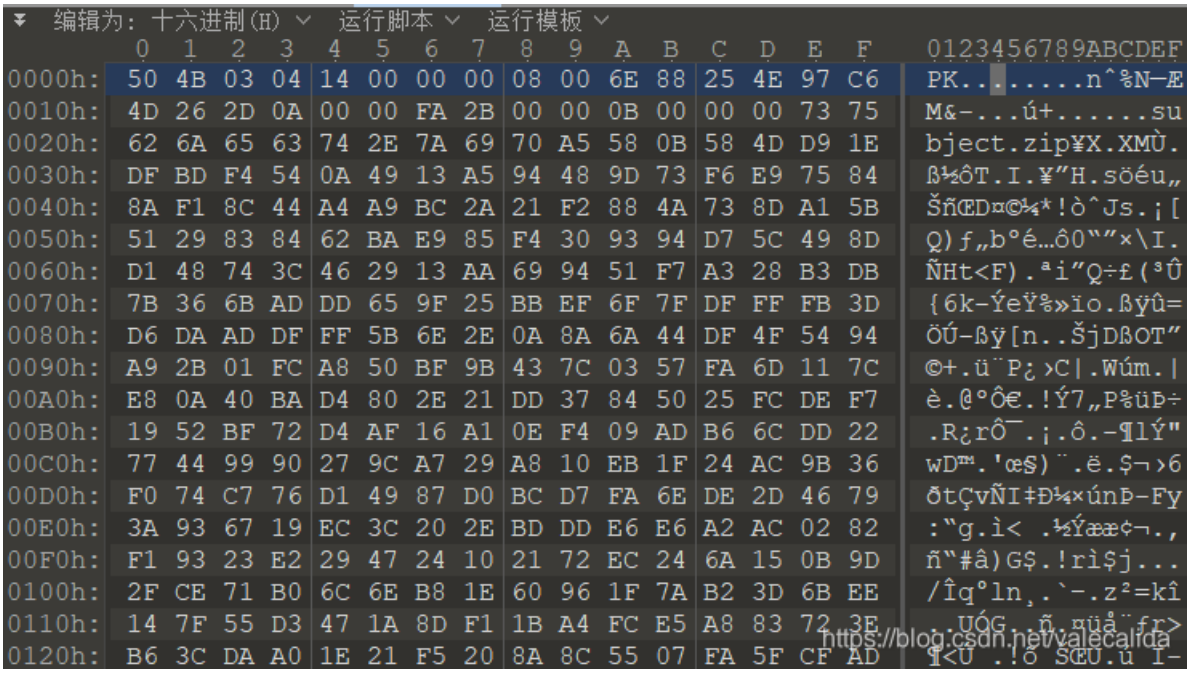
第八题：真的不是图片

直接拿到图片先分析下有么有隐藏文件，发现有个zip：

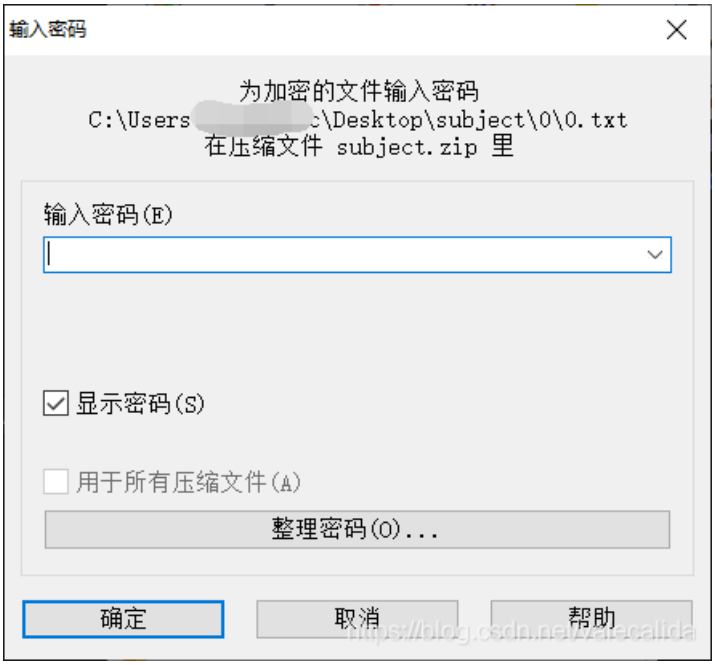
```
root@cat:~/ctf# binwalk misc.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 824 x 639, 8-bit/color RGB, non-interlaced
91            0x5B            Zlib compressed data, compressed
140598        0x22536         End of Zip archive

root@cat:~/ctf# file misc.png
misc.png: PNG image data, 824 x 639, 8-bit/color RGB, non-interlaced
```

查看这个图片，是个png，文件结尾为42 60 82，直接使用010editor分离，得到一个png，一个zip，





将zip解压出来发现变成了subject.zip，继续解压，发现需要密码了，



我们之前保存成压缩包的时候文件头部是ja66，很符合题目，把这个当作密码，发现解压成功，然后对里面所有的txt文档综合一下，一共有32个，肯定不能挨个写，上脚本：

```
#官方脚本
import base64
flag = ''
for i in range(32):
        f = open('./subject/' + str(i) +'/' + str(i) + '.txt','r')
        flag += f.read()
print(base64.b64decode(flag))
```

```
#自己写的脚本
#/usr/bin/env python3
# -*- coding: utf-8 -*-
#--author：valecalida--
import base64
import os
flag = ''
for filename in range(32):
    f = open('subject/' + str(filename) + '/' + (str(filename) + '.txt'))
    key = f.read()
    flag += key
print(base64.b64decode(flag))
```

突然发现修改了脚本之后跟官方给的差不多。。。。，还是官方的最简单。。。

第九题：修补二维码

pass

第十题：隐写术

下载文件得到一个hello.exe，使用ida打开，使用shift + F12进入strings view找到ciphertext：
U2FsdGVkX19EEyvXloCK7ovgV04fyMsIci538oHlQnJ24ltaGk7oGrkoaYpU6L90

在Linux使用binwalk对这个文件进行分析。得到下面结果,后面有一个png图片：

```
root@cat:~/ctf# binwalk hello.exe

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Microsoft executable, portable (PE)
......
73757         0x1201D         Unix path: /crossdev/src/mingw-w64-v3-svn/mingw-w64-crt/crt
74581         0x12355         Unix path: /crossdev/src/mingw-w64-v3-svn/mingw-w64-crt/crt
77858         0x13022         Unix path: /crossdev/src/mingw-w64-v3-svn/mingw-w64-crt/crt
78562         0x132E2         Unix path: /crossdev/src/mingw-w64-v3-svn/mingw-w64-crt/crt
79517         0x1369D         Unix path: /crossdev/src/mingw-w64-v3-svn/mingw-w64-crt/crt
127581        0x1F25D         PNG image, 1890 x 1161, 8-bit/color RGB, non-interlaced
127672        0x1F2B8         Zlib compressed data, compressed
```

直接分离出来，修改高度04 89为 05 89得到key，0xA是10，在线aes解密得flag


```
flag:jactf{hey_y0u_are_right},
```

第十一题：你知道bitcoin吗

第十二题：怀疑人生

先解压出来三个文件，第一个文件暴力破解得到密码：password

解压得到字符串：

```
XHU2Nlx1NmNcdTYxXHU2N1x1N2JcdTY4XHU2MVx1NjNcdTZiXHU2NVx1NzI=
```

base64解码：

```
\u66\u6c\u61\u67\u7b\u68\u61\u63\u6b\u65\u72
```

unicode解码，得到第一部分flag：

```
flag{hacker
```

CTF2.jpg通过binwalk分离出一个压缩包，打开后是ook密码，直接解码

```
3oD54e
```

得到第二部分，第三部分是一个二维码，直接扫码得：

```
12580}
base58解码后是：misc
```

得到完整flag：

```
flag{hackermisc12580}
```

第十三题：玩拼图吗？

得到图片，然后拼起来

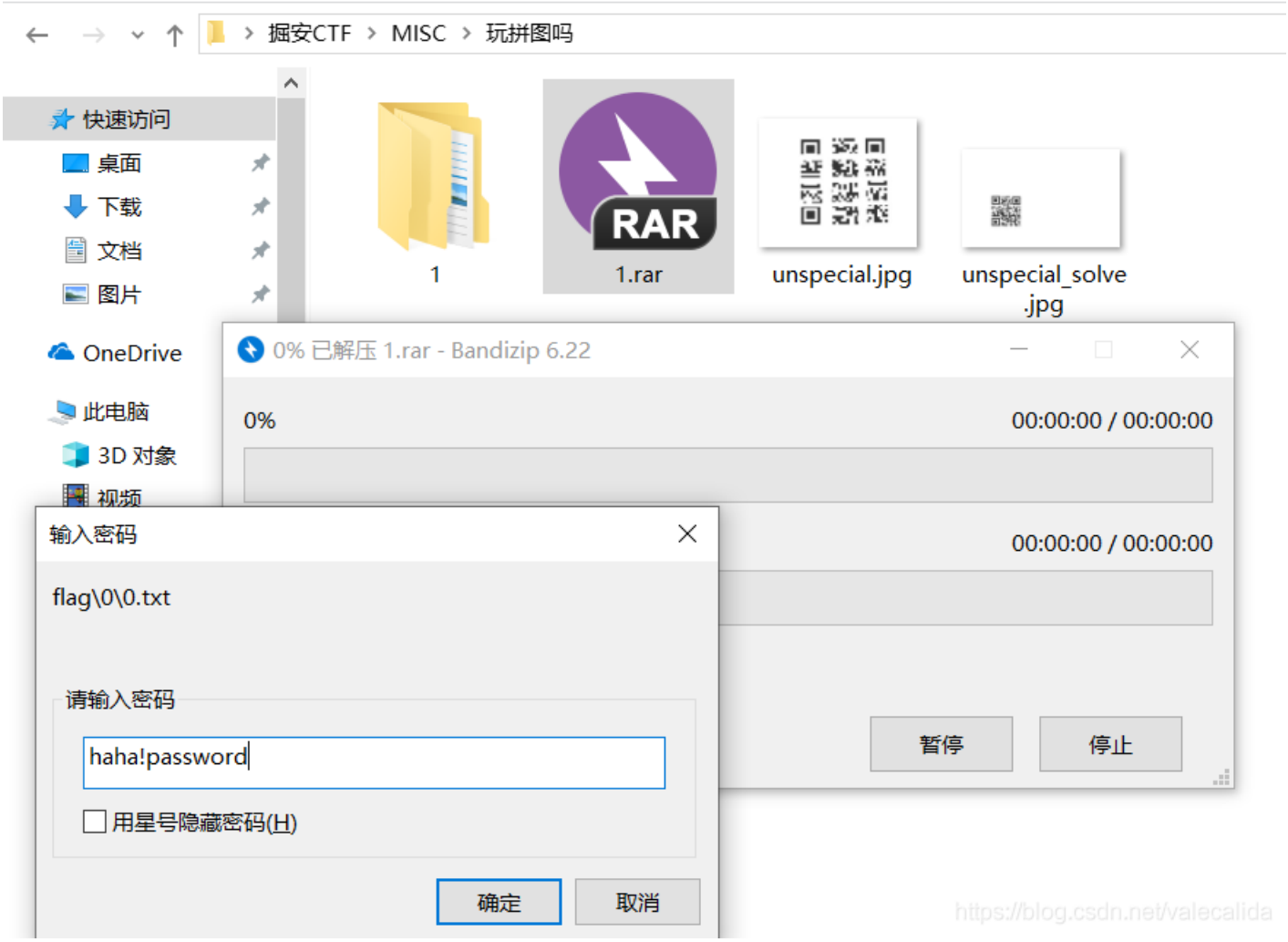
拼的不太好，中间还有条缝，不过已经不影响识别了


```
#base解码
>>> import base64
>>> s = 'aGFoYSFwYXNzd29yZA=='
>>> base64.b64decode(s)
b'haha!password'
```

得到密码之后分析一波原来的图片：

```
root@kali:~/Desktop# binwalk unspecial.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, EXIF standard
12            0xC             TIFF image data, big-endian, offset of first image directory: 8
48215         0xBC57          RAR archive data, version 5.x

root@kali:~/Desktop# dd if=unspecial.jpg of=1.rar skip=48215 bs=1
4537+0 records in
4537+0 records out
4537 bytes (4.5 kB, 4.4 KiB) copied, 0.033055 s, 137 kB/s
```

得到1.rar，解压出来



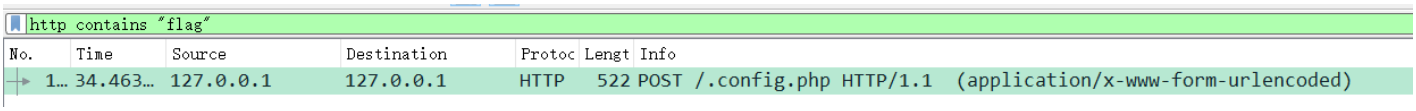
上脚本，得到flag

```
import base64
flag = ''
for i in range(30):
        f = open('./flag/' + str(i) +'/' + str(i) + '.txt','r')
        flag += f.read()

print(flag)
```

```
λ python solve.py
jactf{w0w_This_is_zhe_answer!}
```

第十八题：你对我网站做了什么

拿到流量包，直接用过滤：http contains "flag"



追踪流，得到字符串：eJxLy0lMrw6NTzPMS4n3TVWsBQAz4wXi

```
POST /.config.php HTTP/1.1
Host: www.cometohackme.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:48.0) Gecko/20100101 Firefox/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 30

k=cometohackme&c=cat /flag.txtHTTP/1.1 200 OK
Date: Mon, 09 Jul 2018 03:22:10 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 32
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

eJxLy0lMrw6NTzPMS4n3TVWsBQAz4wXi
```


编写python小脚本

```
import zlib
import base64
s = 'eJxLy0lMrw6NTzPMS4n3TVWsBQAz4wXi'
print(zlib.decompress(base64.b64decode(s)))
```

控制台输出如下：

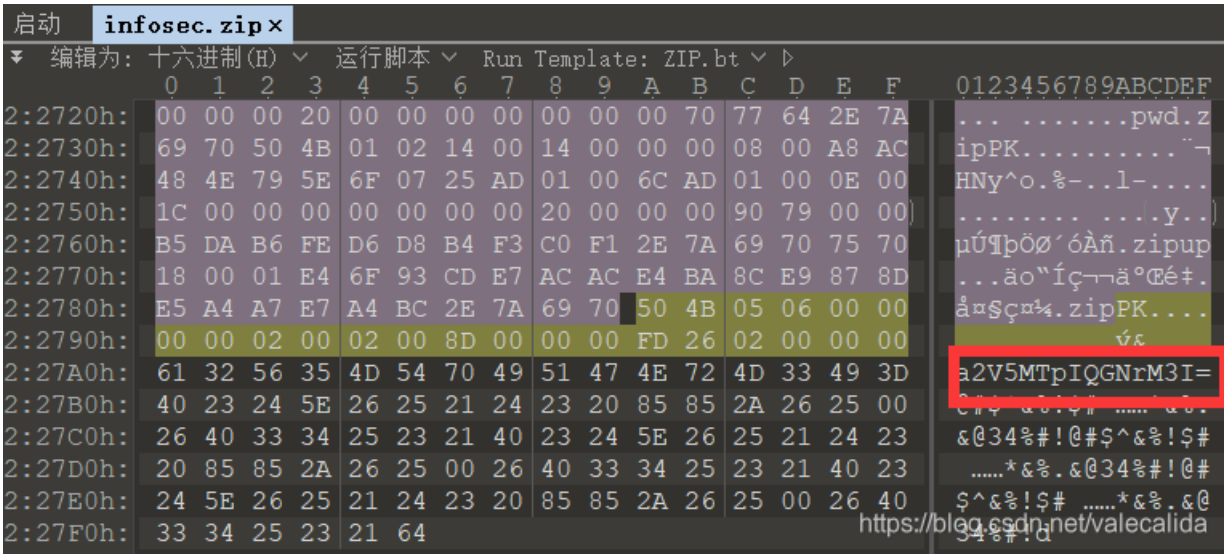
```
b'flag{U_f1nd_Me!}'
```

第十九题：春节三重礼 （这道题应该会下架，不建议大家看了）

使用zip伪加密解一下，发现接出来两个，将文件解压出来

```
C:\Users\valecalida\Desktop\掘安CTF\MISC\春节三重礼
λ java -jar ZipCenOp.jar r infosec.zip
success 2 flag(s) found
```

另外通过观察10进制发现有信息附加：



使用base64解码得：

```
λ python
Python 3.7.2 (tags/v3.7.2:9a3ffc0492, Dec 23 2018, 23:09:28) [MSC v.1916 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import base64
>>> s = 'a2V5MTpIQGNrM3I='
>>> base64.b64decode(s)
b'key1:H@ck3r'
```

第二部分编写脚本从那20多个文件里对比出社会主义核心价值观编码，得到key2

第三部分修改png文件高度，有NTFS流附加得到key3

最终得到的三个key都没有用上，所以这道题可能会下架，这里记录一下思路

这里最终flag是：flag{md5(key1+key2+key3)}

3、逆向（Reverse）

1

2

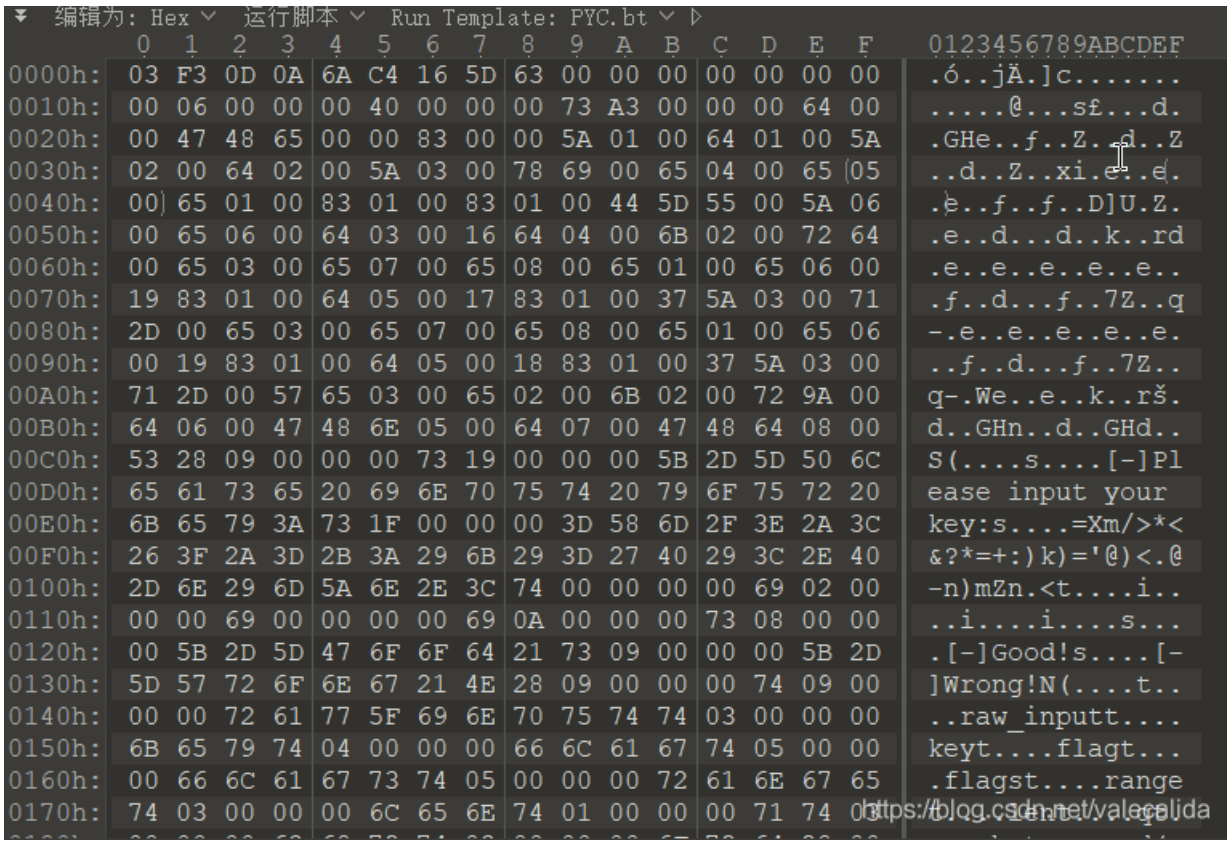
3

4

5

第六题、py

下载python_en.pyc到本地，直接使用在线反编译https://tool.lu/pyc/，失败，使用另外一个pyc文件与python_en.pyc文件进行比较，发现缺少了四个字节头：6A C4 16 5D，补全，再进行反编译，发现反编译成功：




```
#!/usr/bin/env python
# encoding: utf-8
print '[-]Please input your key:'
key = raw_input()
flag = "=Xm/>*<&?*=+:)k)='@)<.@-n)mZn.<"
flags = ''
for q in range(len(key)):
    if q % 2 == 0:
        flags += chr(ord(key[q]) + 10)
        continue
    flags += chr(ord(key[q]) - 10)

if flags == flag:
    print '[-]Good!'
else:
    print '[-]Wrong!'
```

这是一个python2版本写的代码，进行审计,我用了python3将他改了一下。然后写一个逆程序

```
flag = "=Xm/>*<&?*=+:)k)='@)<.@-n)mZn.<"
flags = ''
for i in range(len(flag)):
    if i % 2 == 0:
        flags += chr(ord(flag[i]) - 10)
        continue
    flags += chr(ord(flag[i]) + 10)
print(flags)
```

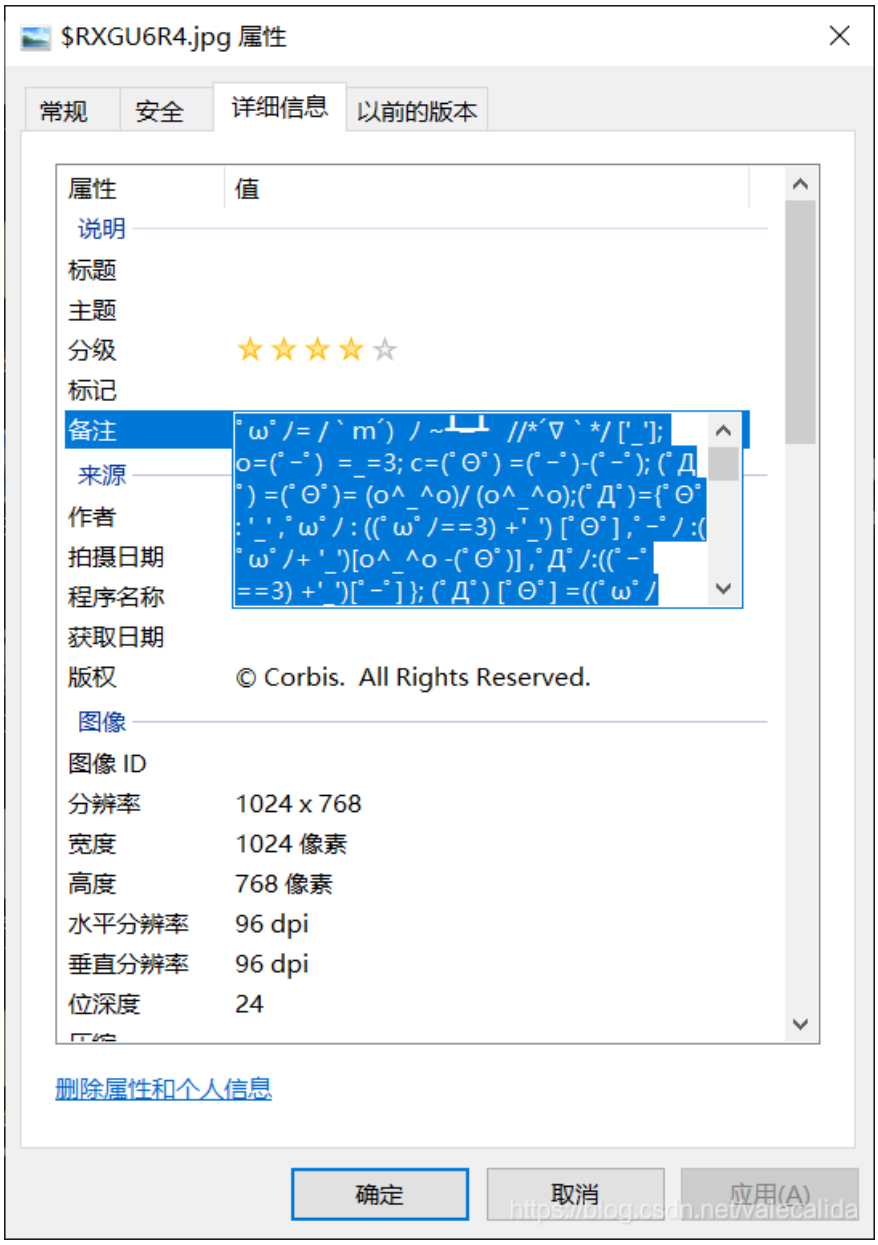
得到flag：3bc94420543503a331632867d3cdd82

本文将持续更新

第十二题、disk

下载下来，加载到diskgenius中，得到图片跟desktop.ini

复制出来，然后查看图片属性，得到提示：



是jjdecode/aadecode，解码得flag：

jjencode与aaencode解密

提交的时候需要将flag改成jactf