2021-05-6 CTF Misc buu oj day7 6道题

原创

LiNa_llnA_741 于 2021-05-06 23:22:48 发布 56 收藏

分类专栏： ctf

本文链接：https://blog.csdn.net/LiNa_llnA_741/article/details/116357990

这里写目录标题

九连环
类型
图片文件
解题
面具下的flag
webshell后门
类型
文件
解题
被劫持的神秘礼物
类型
文件
解题
刷新过的图片
类型
图片文件
解题
snake
类型
图片文件
解题
梅花香之苦寒来
类型
图片文件
解题

九连环

类型

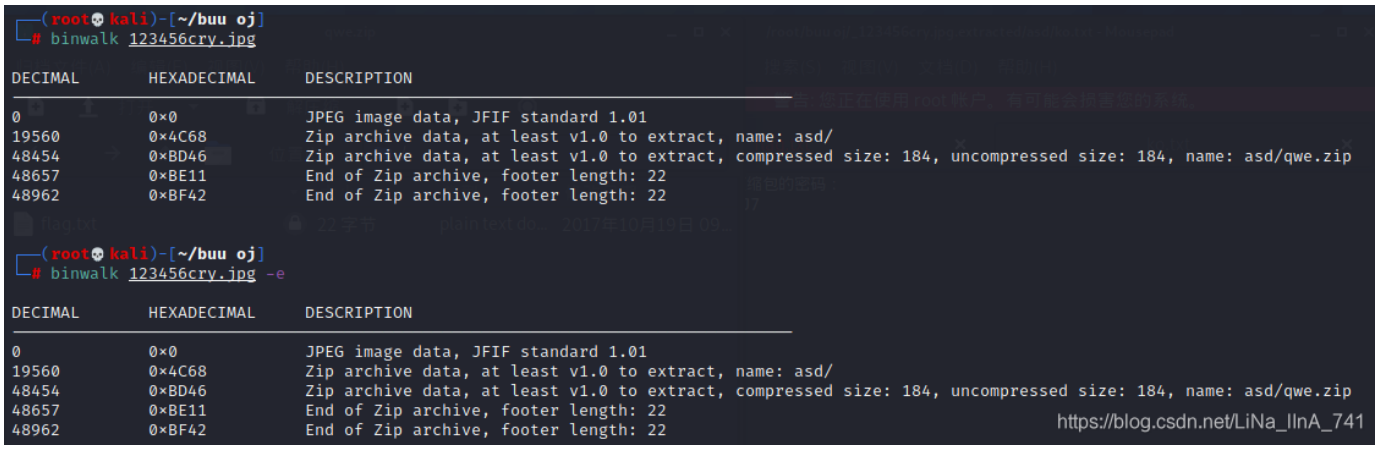
jpg图片分析

图片文件

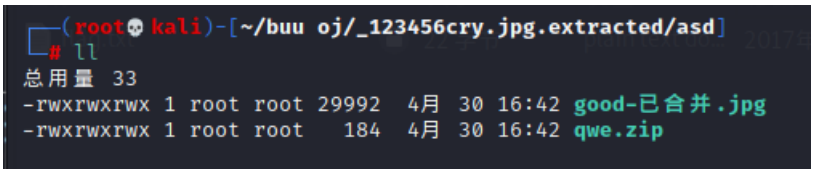
123456cry.jpg

解题

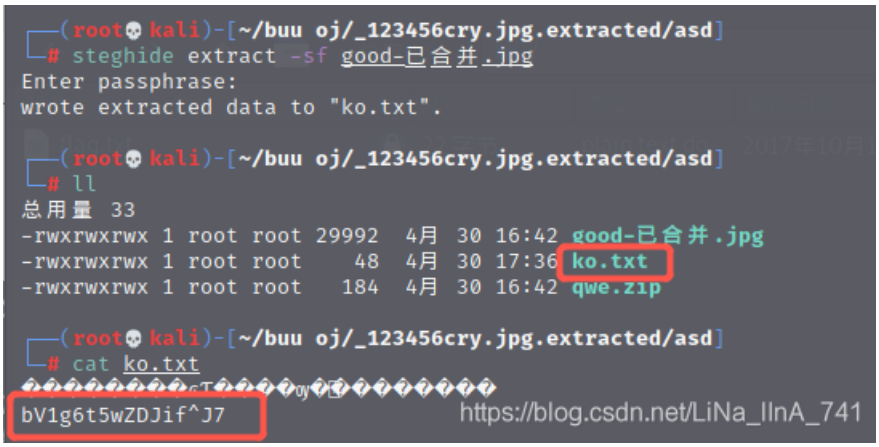
1. 据说是伪加密（文件目录加密而全局目录未加密），但是经过基础检查，用binwalk分析是可以zip文件的：



2. 解压后的文件又看到一个图片和一个加密的zip压缩包，压缩包里面和asd文件夹里一样，都是一张图片“good-已合并.jpg”和一个带flag.txt的“qwe”压缩包：



3. 基础检查“good-已合并.jpg”并未发现异常，这里下载了一个新的隐写查看工具steghide，看一下steghide制作图种，是将一个txt文件嵌入到jpg文件中，这道题是相反操作，`steghide extract -sf good-已合并.jpg`把txt文本提取出来，得到ko.txt打开后看到压缩包密码：bV1g6t5wZDJif^J7



4. 解压缩得到flag：flag{1RTo8w@&4nK@z*XL}

面具下的flag

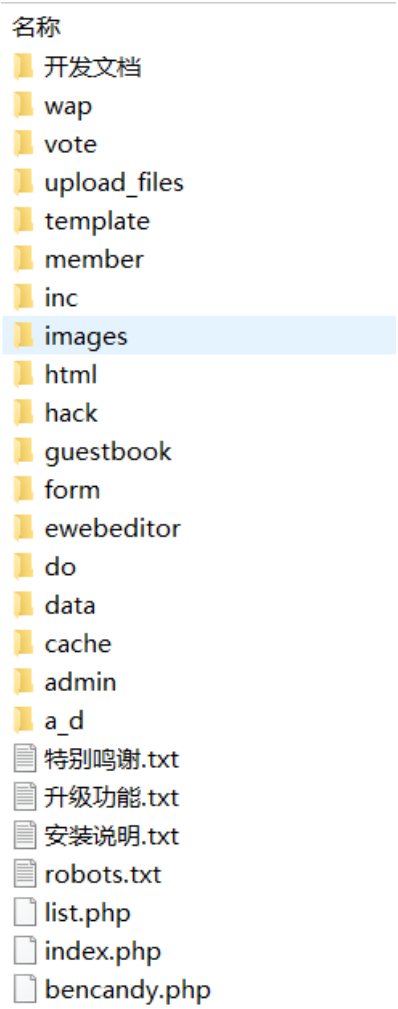
关键文件解压不出来，研究中。。。

webshell后门

类型

webshell后门分析

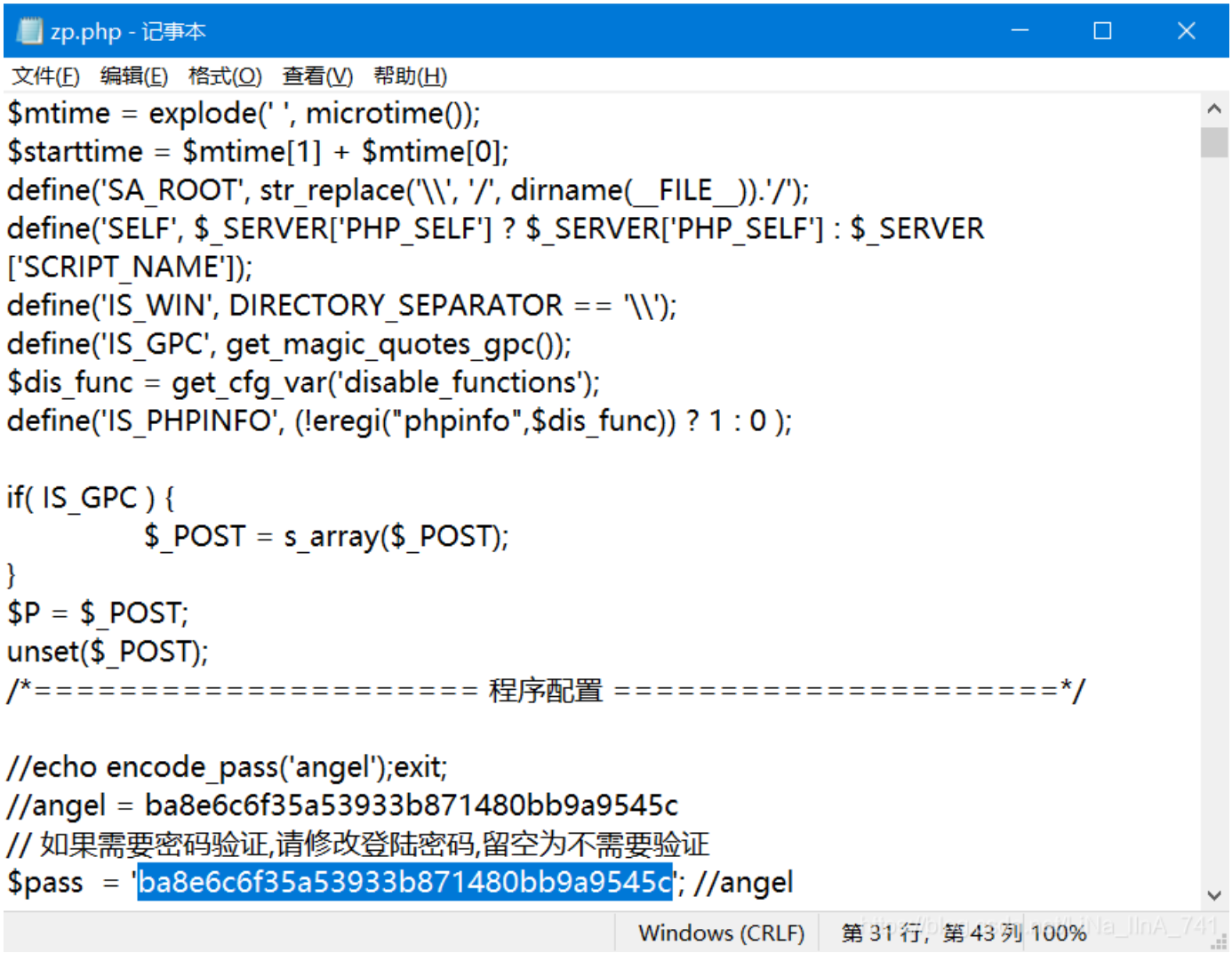
文件


名称
开发文档
wap
vote
upload_files
template
member
inc
images
html
hack
guestbook
form
ewebeditor
do
data
cache
admin
a_d
特别鸣谢.txt
升级功能.txt
安装说明.txt
robots.txt
list.php
index.php
bencandy.php

解题

复习题，同day6后门查杀解压后D盾查杀解压文件目录，发现可疑文件，搜索pass得到flag：

flag{ba8e6c6f35a53933b871480bb9a9545c}



被劫持的神秘礼物

类型

流量包分析

文件

gift.pcapng

解题

1. wireshark打开文件，追踪http流（题目中说找到账号密码，账号密码一般都是http请求中提交的），账号名为admina，密码为adminb

Wireshark · 追踪 HTTP 流 (tcp.stream eq 0) · gift.pcapng

```
POST /index.php?r=member/index/login HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
Referer: http://192.168.60.123/index.php?r=member/index/login
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 192.168.60.123
Content-Length: 129
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: PHPSESSID=ubkh99eqgp4apge0n5stkimna4

name=admina&word=adminb&cooktime=0&checkcode=5129&returnurl=http%3A%2F%2F192.168.60.123%2Findex.p
hp%3Fr%3Ddefault%2Findex%2FindexHTTP/1.1 302 Found
Date: Wed, 03 Dec 2014 05:51:53 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Centent-Type: text/html;charset=UTF-8
Pragma: no-cache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Set-Cookie:
yx_auth=da73XtTCqWpRWN%2Fi54TTa1mwjLXu6IffS392Ux2o4RQXYyF08uwKAN0Teu8LaeOHr07AdsDITqLLmrc6lItPgiq
V5BA6J3Q4Mw; path=/
location: http://192.168.60.123/index.php?r=default/index/index
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```


2. 拼接后用kali linux命令 `echo -n adminaadminb|openssl md5`
   回显flag：flag{1d240aafe21a86afc11f38a45b541a49}

```
┌──(root💀kali)-[~]
└─# echo -n adminaadminb|openssl md5
(stdin)= 1d240aafe21a86afc11f38a45b541a49
```

刷新过的图片

类型

jpg图片分析

图片文件

Misc.jpg

解题

题目提示刷新，找到隐写工具F5-Steganography

下载后打开F5-Steganography文件夹，执行命令 `java Extract /...(文件路径)/Misc.jpg`

```
┌──(root💀kali)-[~/buu oj]
└─# cd F5-steganography

┌──(root💀kali)-[~/buu oj/F5-steganography]
└─# java Extract /root/buu\ oj/Misc.jpg
```

```
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Huffman decoding starts
Permutation starts
309504 indices shuffled
Extraction starts
Length of embedded file: 190 bytes
(1, 31, 5) code used

┌──(root💀kali)-[~/buu oj/F5-steganography]
└─# ll
总用量 261
-rwxrwxrwx 1 root root    213  5月   6 13:05 bin.noise
drwxrwxrwx 1 root root   4096  5月   6 13:05 crypt
-rwxrwxrwx 1 root root     94  5月   6 13:05 d
-rwxrwxrwx 1 root root     62  5月   6 13:05 d.bat
-rwxrwxrwx 1 root root    109  5月   6 13:05 e
-rwxrwxrwx 1 root root    103  5月   6 13:05 e.bat
-rwxrwxrwx 1 root root   4685  5月   6 13:05 Embed.class
-rwxrwxrwx 1 root root   5250  5月   6 13:05 Embed.java
-rwxrwxrwx 1 root root   4227  5月   6 13:05 Extract.class
-rwxrwxrwx 1 root root   5941  5月   6 13:05 Extract.java
-rwxrwxrwx 1 root root  18007  5月   6 13:05 gpl.txt
drwxrwxrwx 1 root root      0  5月   6 13:05 image
drwxrwxrwx 1 root root   4096  5月   6 13:05 james
drwxrwxrwx 1 root root      0  5月   6 13:05 java
-rwxrwxrwx 1 root root    316  5月   6 13:05 license.txt
-rwxrwxrwx 1 root root 188706  5月   6 13:05 lopez.bmp
-rwxrwxrwx 1 root root    373  5月   6 13:05 Makefile
-rwxrwxrwx 1 root root     63  5月   6 13:05 ms_d.bat
-rwxrwxrwx 1 root root    104  5月   6 13:05 ms_e.bat
drwxrwxrwx 1 root root   4096  5月   6 13:05 output
-rwxrwxrwx 1 root root    190  5月   6 13:08 output.txt
-rwxrwxrwx 1 root root   1975  5月   6 13:05 readme.md
```


binwalk输出文件发现该文件为zip文件，提取后得到flag：flag{96efd0a2037d06f34199e921079778ee}

```
┌──(root💀kali)-[~/buu oj/F5-steganography]
└─# binwalk output.txt

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed size: 40, uncompressed size: 38, name: flag.txt
168           0xA8            End of Zip archive, footer length: 22

┌──(root💀kali)-[~/buu oj/F5-steganography]
└─# binwalk output.txt -e

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed size: 40, uncompressed size: 38, name: flag.txt
168           0xA8            End of Zip archive, footer length: 22
```



```
drwxrwxrwx 1 root root      0  5月   6 13:05 image
drwxrwxrwx 1 root root   4096  5月   6 13:05 james
drwxrwxrwx 1 root root      0  5月   6 13:05 java
-rwxrwxrwx 1 root root    316  5月   6 13:05 license.txt
-rwxrwxrwx 1 root root 188706  5月   6 13:05 lopez.bmp
-rwxrwxrwx 1 root root    373  5月   6 13:05 Makefile
-rwxrwxrwx 1 root root     63  5月   6 13:05 ms_d.bat
-rwxrwxrwx 1 root root    104  5月   6 13:05 ms_e.bat
drwxrwxrwx 1 root root   4096  5月   6 13:05 ortega
-rwxrwxrwx 1 root root    190  5月   6 13:08 output.txt
drwxrwxrwx 1 root root      0  5月   6 13:09 _output.txt.extracted
-rwxrwxrwx 1 root root   1975  5月   6 13:05 readme.md
drwxrwxrwx 1 root root      0  5月   6 13:05 sun

┌──(root💀kali)-[~/buu oj/F5-steganography]
└─# cd _output.txt.extracted

┌──(root💀kali)-[~/buu oj/F5-steganography/_output.txt.extracted]
└─# ll
总用量 1
-rwxrwxrwx 1 root root 190  5月   6 13:09 0.zip
-rwxrwxrwx 1 root root  38  5月   6 13:09 flag.txt

┌──(root💀kali)-[~/buu oj/F5-steganography/_output.txt.extracted]
└─# cat flag.txt
flag{96efd0a2037d06f34199e921079778ee}
```

snake

类型

jpg图片分析

图片文件

snake.jpg

解题

1. 常规检查，binwalk解压，得到两个文件cipher、key

```
┌──(root💀kali)-[~/buu oj/snake]
└─# binwalk snake.jpg -e

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
2925          0xB6D           Copyright string: "Copyright Apple Inc., 2015"
278260        0x43EF4         Zip archive data, at least v1.0 to extract, compressed size: 82, uncompressed size: 82, name: key
278375        0x43F67         Zip archive data, at least v1.0 to extract, compressed size: 48, uncompressed size: 48, name: cipher
278632        0x44068         End of Zip archive, footer length: 22
```

2. key可以直接打开，看到内容为base64编码，解码后得到一句话：What is Nicki Minaj's favorite song that refers to snakes?（百度查这句话出来的全是实验吧的writeup）所以key是anaconda。

```
┌──(root💀kali)-[~/buu oj/snake/_snake.jpg.extracted]
└─# ll
总用量 2
-rwxrwxrwx 1 root root 394  5月   6 13:48 43EF4.zip
-rwxrwxrwx 1 root root  48  1月   3  2016 cipher
-rwxrwxrwx 1 root root  82  1月   3  2016 key

┌──(root💀kali)-[~/buu oj/snake/_snake.jpg.extracted]
└─# more key
V2hhdCBpcyBOaWNraSBNaW5haidzIGZhdm9yaXRlIHNvbmcgdGhhdCByZWZlcnMgdG8gc25ha2VzPwo=
```

Base64 在线解码、编码

常规Base64 | CSS Base64 | DES加密/解密 | 3DES加密/解密 | AES加密/解密 | RSA加密/解密

点击关闭

V2hhdCBpcyBOaWNraSBNaW5haidzIGZhdm9yaXRlIHNvbmcgdGhhdCByZWZlcnMgdG8gc25ha2VzPwo=

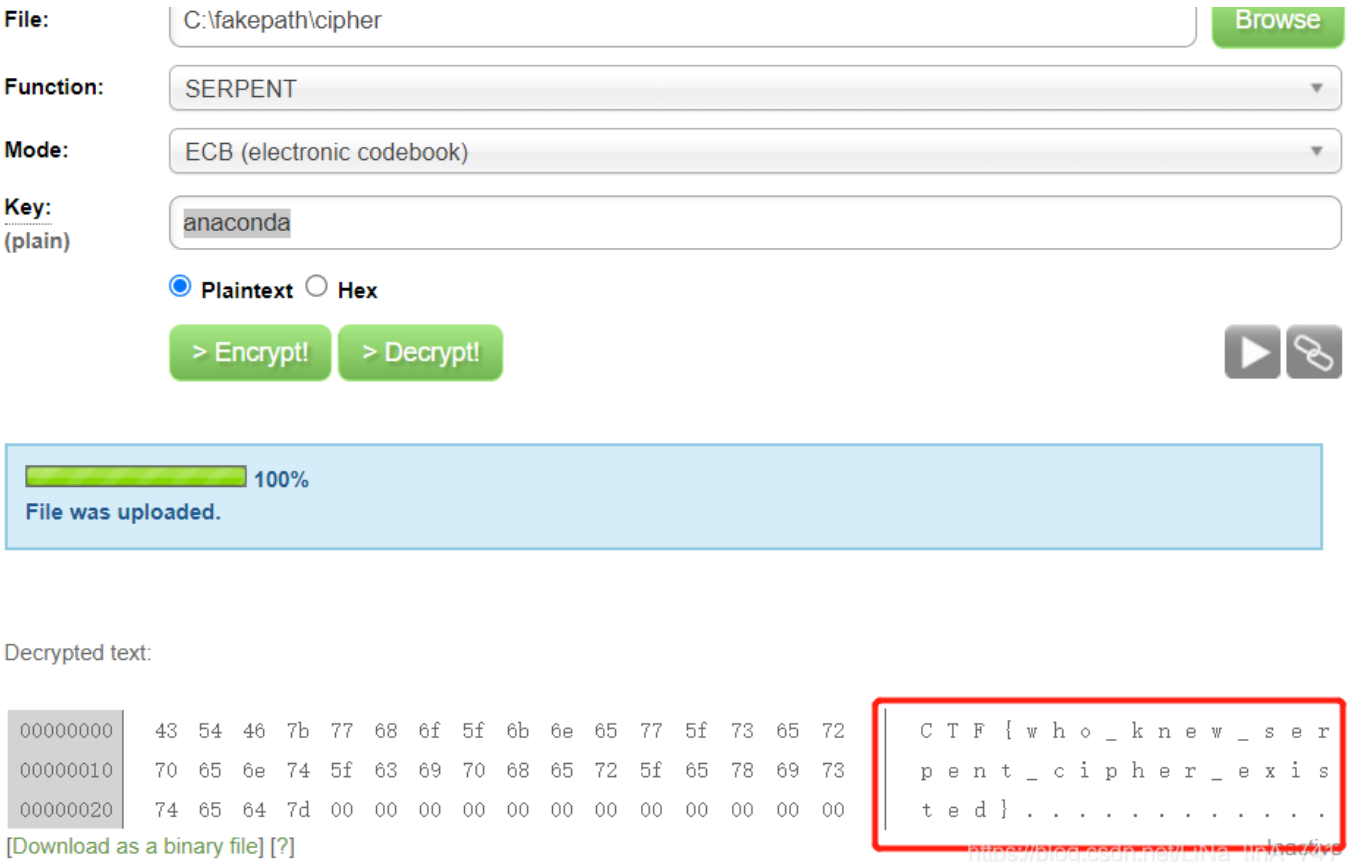
编码源格式：文本 Hex 解码结果：自动检测 中文编码：UTF-8 编码 解码

What is Nicki Minaj's favorite song that refers to snakes?

当前编码：[Ascii]
数据长度：59 Bytes
插件数：16，耗时：1ms

3. serpent在线解密上传cipher文件，输入key后解密得flag：flag{who_knew_serpent_cipher_existed}

Input type: File



梅花香之苦寒来

类型

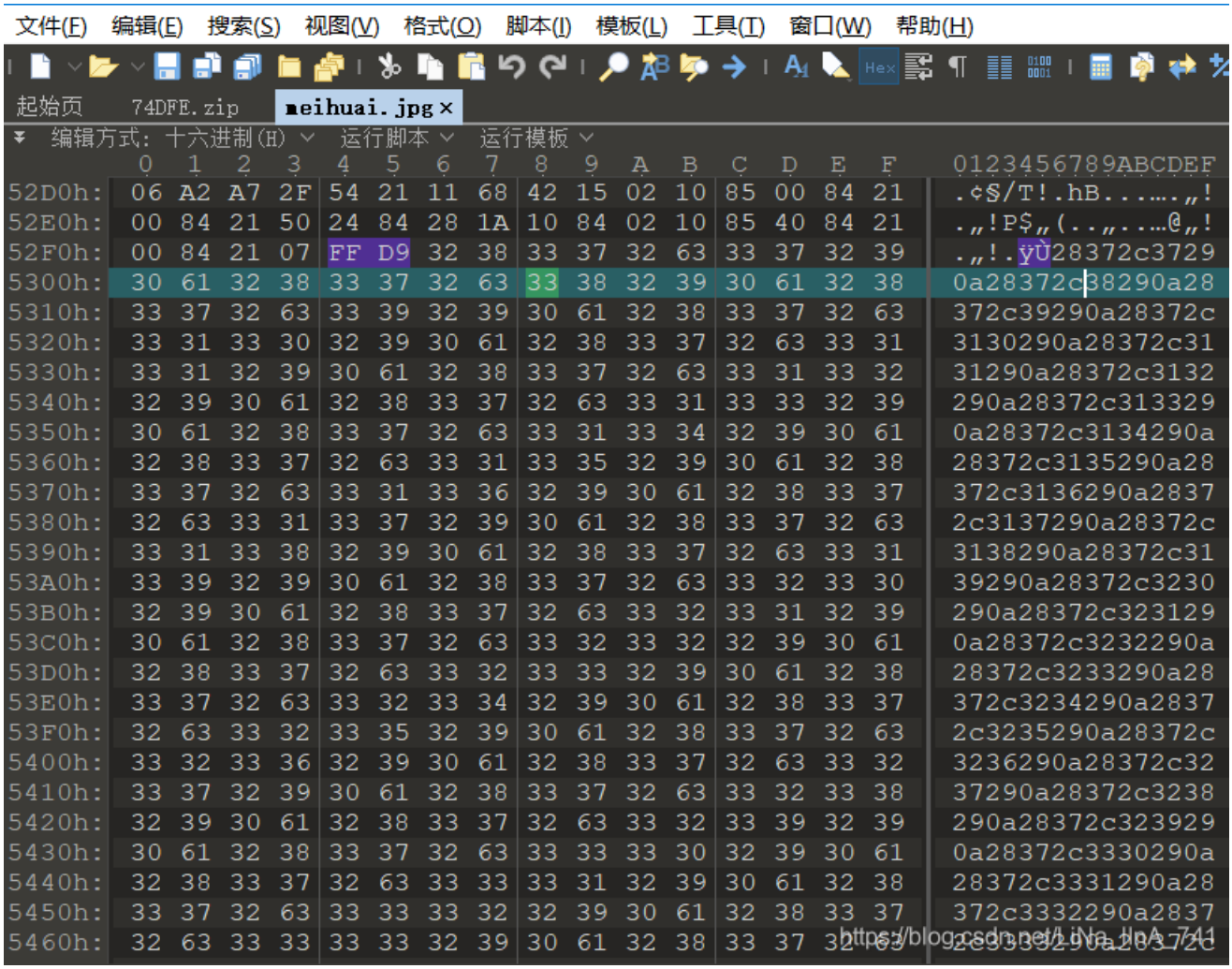
jpg图片分析

图片文件

meihuai.jpg

解题

1. 图片内容“图穷匕见”，基础检查用010Editor打开搜索jpg文件尾FF D9，后面全是数字字母，取出来两位转个ascii码试试，28->‘(’，37->‘7’，2c->‘,’，29->‘)’，0a->回车，前五个16进制数字转换成ascii得到(7,7)：



2. 复制所有图片后数字保存为hex.txt文件，用python脚本转换成ascii.txt：

```
with open('hex.txt','r') as h:
 h = h.read()

tem = ''

f = open('ascii.txt','w'):
 for i in range(0,len(h),2):
  #h中每两个数字字符组成一个十六进制数，如‘0x28’，故步长为2，
  tem = '0x' + h[i] + h[i+1]
  tem = int(tem, base=16)
  #十六进制字符串转换成十进制整型
  print(chr(tem), end = '', file = f)
  #十进制整型转换成字符型即ascii码
f.close()
```

```
1  (7,7)
2  (7,8)
3  (7,9)
4  (7,10)
5  (7,11)
6  (7,12)
7  (7,13)
8  (7,14)
9  (7,15)
10 (7,16)
11 (7,17)
12 (7,18)
13 (7,19)
14 (7,20)
15 (7,21)
16 (7,22)
17 (7,23)
18 (7,24)
19 (7,25)
20 (7,26)
21 (7,27)
22 (7,28)
23 (7,29)
24 (7,30)
25 (7,31)
26 (7,32)
```

```
34996 (271,213)
34997 (271,214)
34998 (271,236)
34999 (271,237)
35000 (271,238)
35001 (271,239)
35002 (271,240)
35003 (271,241)
35004 (271,242)
35005 (271,243)
35006 (271,244)
35007 (271,245)
35008 (271,246)
35009 (271,247)
35010 (271,248)
35011 (271,249)
35012 (271,250)
35013 (271,265)
35014 (271,266)
35015 (271,267)
35016 (271,268)
35017 (271,269)
35018 (271,270)
35019 (271,271)
35020
```

3. 得到内容为坐标，可以用来作图，为了利用Kali Linux中画图工具GNUPLOT，修改ascii.txt格式，去掉左右括号，把横纵坐标中间逗号改用空格隔开，用python脚本：

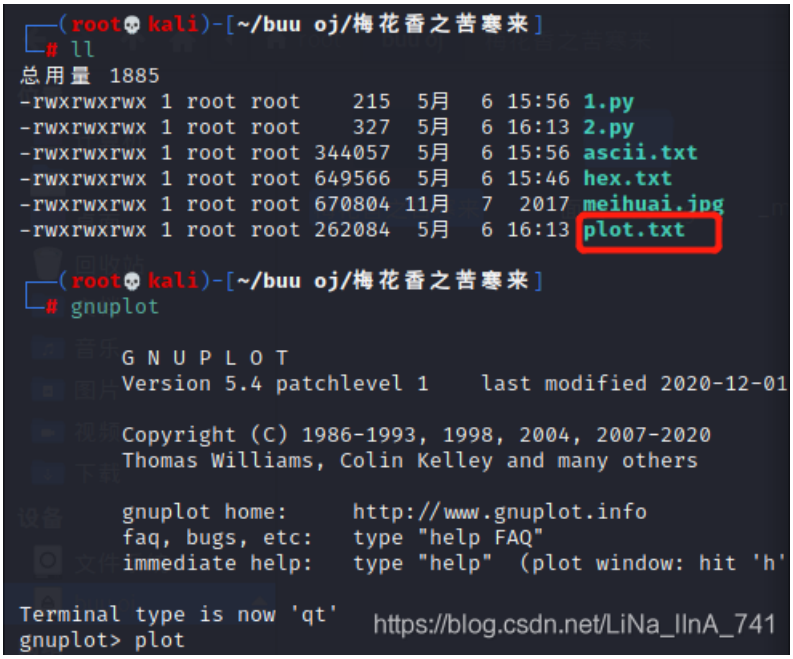
```
with open('ascii.txt','r') as a:
 a = a.read()
 a = a.split()
 #每个坐标分割为一组修改对象
tem = ''

f = open('plot.txt', 'w'):
 for i in range(0, len(a)):
  tem = a[i]
  tem = tem.lstrip('(')
  #去掉左括号'('
  tem = tem.rstrip(')')
  #去掉右括号')'
  for j in range(0, len(tem)):
   if (j==','):
    tem = tem[:j] + ' ' + tem[:j+1]
  #逗号改为空格
  print(tem, file = f)
f.close()
```

```
 1  7 7
 2  7 8
 3  7 9
 4  7 10
 5  7 11
 6  7 12
 7  7 13
 8  7 14
 9  7 15
10  7 16
11  7 17
12  7 18
13  7 19
14  7 20
15  7 21
16  7 22
17  7 23
18  7 24
19  7 25
20  7 26
21  7 27
22  7 28
23  7 29
24  7 30
25  7 31
26  7 32
27  7 33
```

```
34996  271 213
34997  271 214
34998  271 236
34999  271 237
35000  271 238
35001  271 239
35002  271 240
35003  271 241
35004  271 242
35005  271 243
35006  271 244
35007  271 245
35008  271 246
35009  271 247
35010  271 248
35011  271 249
35012  271 250
35013  271 265
35014  271 266
35015  271 267
35016  271 268
35017  271 269
35018  271 270
35019  271 271
35020
```

4. 到plot.txt所在目录下执行`gnuplot`，进入gnuplot后执行`plot “plot.txt”`得到二维码图片，扫码得到flag：flag{40fc0a979f759c8892f4dc045e28b820}



Free Online Barcode Reader

To get such results using ClearImage SDK use TBR Code 103.

If your **business** application needs barcode recognition capabilities,
email your technical questions to support@inliteresearch.com
email your sales inquiries to sales@inliteresearch.com

File: flag.png New File
Pages: 1 **Barcodes:** 1

Barcode: 1 of 1 **Type:** QR
Length: 38 **Rotation:** left
Module: 13.1pix **Rectangle:** {X=62,Y=74,Width=460,Height=470}

Page 1 of 1

```
flag{40fc0a979f759c8892f4dc045e28b820}
```

引用最后一题题目，“梅花香自苦寒来”，冲冲冲！