

# Writeup - CTF - MISC - 练习平台 (123.206.31.85)

转载

[weixin\\_34049948](#) 于 2017-11-14 23:08:00 发布 182 收藏

文章标签: [python 网络](#)

原文链接: <http://www.cnblogs.com/virgin-forest/p/7835317.html>

版权

## 这是一张单纯的照片??

题目

1574 Solves

### 这是一张单纯的图片??

30

<http://120.24.86.145:8002/misc/1.jpg>

FLAG在哪里??

Key

SUBMIT



用txt打开图片,在最下面发现一串HTML转义序列

```
&#107;&#101;&#121;&#123;&#121;&#111;&#117;&#32;&#97;&#114;&#101;&#32;&#114;&#105;&#103;&#116;
```

把转义序列放到网页中就可以看到flag

```
key{you are right}
```

## 隐写2

# 隐写2

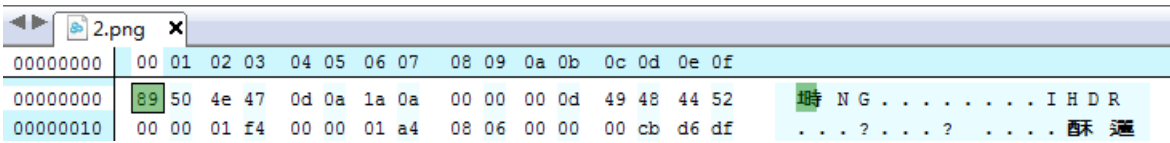
40

2.rar

Key

SUBMIT

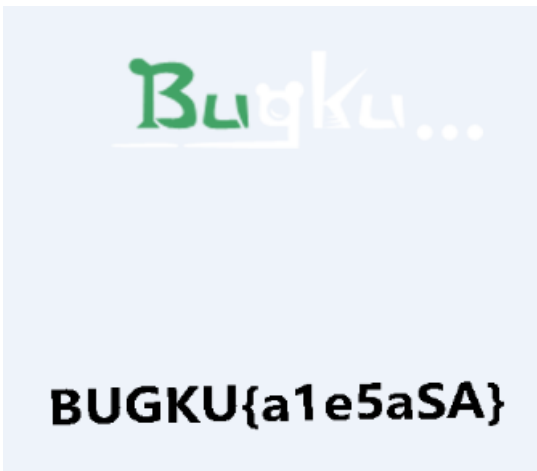
2.rar下载下来之后，里面有一个图片文件2.png，想到PNG隐写，用Hex Workshop打开



00 00 01 F4 表示图片的宽度

00 00 01 A1 表示图片的高度

加大图片的高度，获取到flag



telnet

题目

1159 Solves

×

## telnet

50

<http://120.24.86.145:8002/misc/telnet/1.zip>

key格式flag{xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx}

Key

SUBMIT

1.zip下载下来解压出来networking.pcap

用wireshark打开，根据题目提示查看telnet协议

一个个找下去，在第41个数据包找到flag

No.	Time	Source	Destination	Protocol	Length	Info
40	18.418931	192.168.221.128	192.168.221.164	TCP	60	23->1146 [ACK]
41	18.423632	192.168.221.128	192.168.221.164	TELNET	92	Telnet Data .
42	18.439232	192.168.221.164	192.168.221.128	TCP	60	23->1146 [ACK]

▶ Frame 41: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
▶ Ethernet II, Src: Vmware_84:86:5f (00:0c:29:84:86:5f), Dst: Vmware_26:7e:0e (00:0c:29:26:7e:0e)
▶ Internet Protocol Version 4, Src: 192.168.221.128, Dst: 192.168.221.164
▶ Transmission Control Protocol, Src Port: 1146, Dst Port: 23, Seq: 83, Ack: 124, Len: 38
▶ Telnet
Data: flag{d316759c281bf925d600be698a4973d5}

有一张图片，还单纯吗??

题目

742 Solves

×

## 又一张图片，还单纯吗??

60

<http://120.24.86.145:8002/misc/2.jpg>

好像和上一个有点不一样

Key

SUBMIT



用binwalk检测发现还有一张图片

```
root@kali:~/图片# binwalk 2.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, EXIF standard
12	0xC	TIFF image data, big-endian, offset of first image directory: 8
13017	0x32D9	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#> <rdf:Description rdf:about="" xmlns:photoshop="http://ns.adobe.com/photoshop/1.0/" xmlns
158792	0x26C48	JPEG image data, JFIF standard 1.02
158822	0x26C66	TIFF image data, big-endian, offset of first image directory: 8
159124	0x26D94	JPEG image data, JFIF standard 1.02
162196	0x27994	JPEG image data, JFIF standard 1.02
164186	0x2815A	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#> <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:xap="htt
168370	0x291B2	Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"

把图片提取出来，就是flag

flag{NSCTF\_e6532a34928a3d1dadd0b049d5a3cc57}

多种办法解决

## 多种方法解决

60


在做题过程中你会得到一个二维码图片

<http://120.24.86.145:8002/misc/3.zip>

Key

SUBMIT

3.zip解压出来一个KEY.exe，打开的时候报错，用记事本打开看一下



```
KEY.exe - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
data:image/jpeg;base64,iVBORw0KGgoAAAANSUheEUgAAAIUAAACFCAYAAAB12js8AAAAAXNSR0I
sMAAA7DAcdvqGQAAArZSURBVHhe7ZKBitxIFgTv/396Tx564G1UouicKg19hwPCDcrMJ9m7/7n45z
+3pnDp9yF7tneQvvmcZu/21f78zhU+5i9yxv4T3T200/7eud680T2H3LCft01/ae9Z1To+23pPvXf
+PIndt5ywT3dp71mfOTXafku6f/2uD09i9y0n7NNd2nvWZ06Ntt+S71+/68MJc5000SWpcyxnFjJ
+vDCXOTtDklqXMnsZxy33LCPiVtbpKUX7/rwwlzk7Q5JalzJ7GcWN9ywj41bW6S1F+/68MJc5000S
L+DcXOTtDklqXMnsZxy33LCPiVtbpKUX7/rwwlzk7Q5JalzJ7GcWN9ywj41bW6S1F+/68MJc5000S
```

看到jpg和base64，想到base64转图片

还原生成的Base64编码为图片：



扫二维码得到flag

KEY{dca57f966e4e4e31fd5b15417da63269}

猜？

猜？

60

<http://120.24.86.145:8002/misc/cai/QQ20170221-132626.png>

flag格式key{某人名字全拼}

Key

SUBMIT



我还没有特殊的识别方式，百度识图走一波

[刘亦菲清新雅致大片古韵弥漫似画中人- 中国日报网](#)



刘亦菲清新雅致大片古韵弥漫似画中人-中国日报网  
[www.chinadaily.com.cn](http://www.chinadaily.com.cn)

key{liuyifei}

宽带信息泄露

题目

698 Solves

×

## 宽带信息泄露

60

flag格式：

flag{宽带用户名}

conf.bin

Key

SUBMIT

bin文件用RouterPassView读取 链接：<http://pan.baidu.com/s/1c20HHpm> 密码：ojed



```
<Name val=pppoe_eth1_d />
<Uptime val=671521 />
<Username val=053700357621 />
<Password val=210265 />
```

flag{053700357621}

## 图片又隐写

题目

3 Solves

×

## 图片又隐写

60

Welcome\_....

Key

SUBMIT



想拿到flag？心の中ないいくつかB数かの？

看到图片直接扔binwalk，得到一个zip文件

zip文件解压出来一个flag.rar和提示.jpg

**告诉你们一个秘密，密码是3个数哦。**

查理曼：

查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。

雅典娜：

女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。

兰斯洛特，

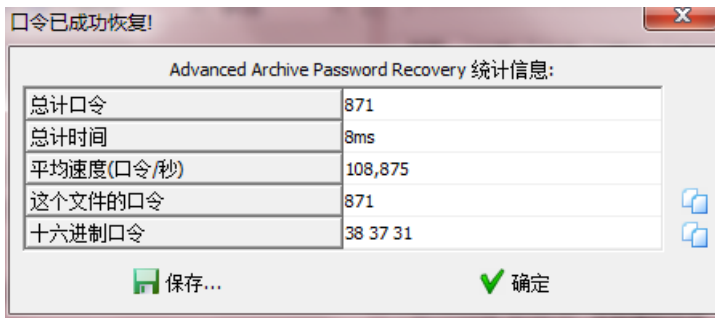
英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。

Hint:

其实斗地主挺好玩的。

虽然提示了，但是我并不会去猜的，还是爆破简单粗暴





解压出来3.jpg



在文件末尾发现

```
f1@g{eTB1IEFyZSBhIGhAY2t1ciE=}
```

将base64解码，flag补齐

```
flag{you Are a h@cker!}
```

linux??????

题目 774 Solves

linux ??????

80

<http://120.24.86.145:8002/misc/1.tar.gz>

linux基础问题哟

Key

SUBMIT

压缩包下载下来，解压，里面有一个flag文件，记事本打开，搜索flag没有，搜索key GET!

linux? 不存在的...

```
key{feb81d3834e2423c9903f4755464060b}
```

# 中国菜刀，不再web里？

题目 519 Solves ×

## 中国菜刀，不再web里？

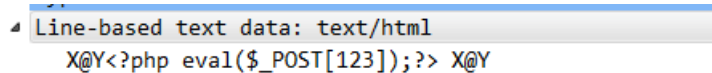
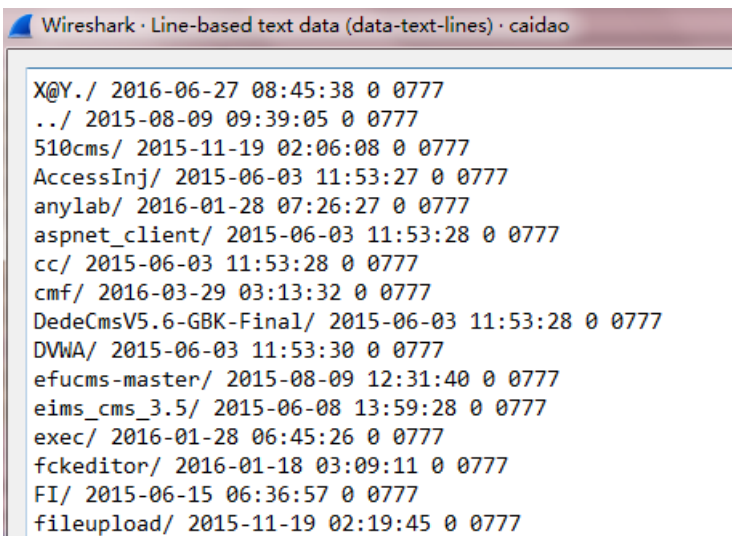
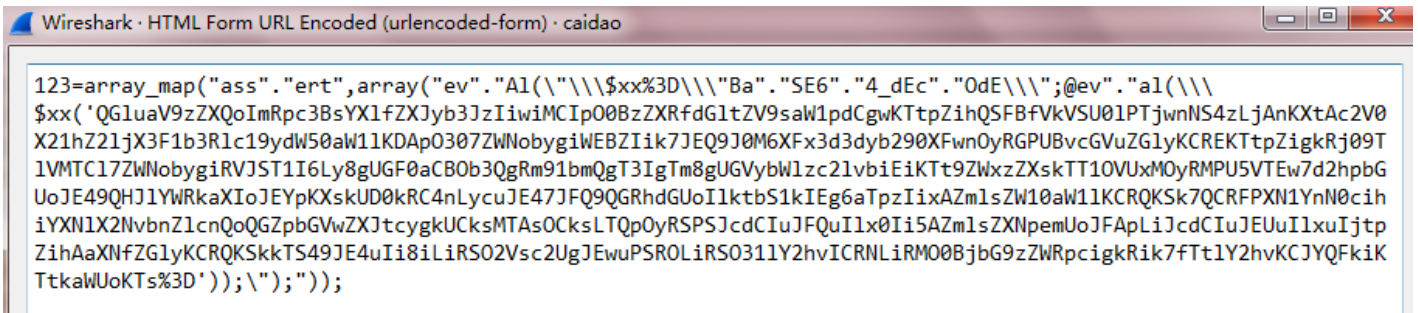
80

国产神器

<http://120.24.86.145:8002/misc/caidao.zip>

解压出来caidao.pcapng，用wireshark打开

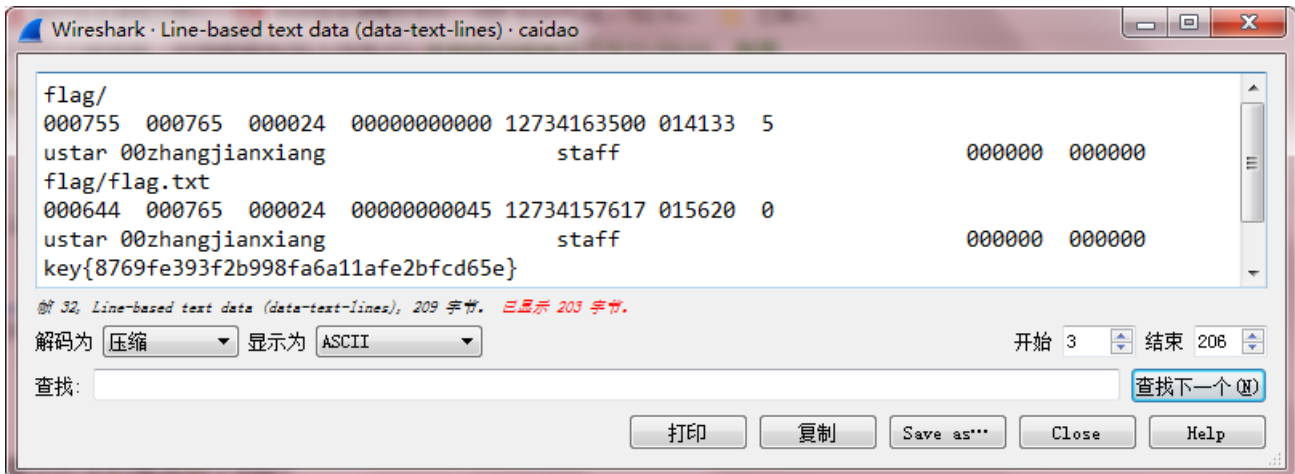
数据包都是菜刀的操作



可以看出在头和尾添加了X@Y

在最后一个HTTP数据包看到了传过来了一个文件

把头和尾的X@Y去掉，解码为压缩



## 这么多数据包

题目 288 Solves

### 这么多数据包

80

这么多数据包找找吧，先找到getshell的流

CTF.pcapn...

Key

SUBMIT

打开数据包，前面都是一些扫描端口的操作，往下到5542已经getshell

追踪TCP数据流，发现s4cr4t.txt

```
C:\>type s4cr4t.txt
type s4cr4t.txt
Q0NURntkb195b3VfbG1rZV9zbnlmZmVyfQ==
```

base64解码

CCTF{do\_you\_like\_sniffer}

## 再来一道隐写

题目 422 Solves ×

### 再来一道隐写

80

58d54bd3...

Key

SUBMIT

解压出来一张PNG，尝试高度，获得flag



想蹭网先解开密码

## 想蹭网先解开密码

100

flag格式：flag{你破解的WiFi密码}

tips：密码为手机号，为了不为你，大佬特地让我悄悄地把前七位告诉你

1391040\*\*

Goodluck!!

感谢@NewBee

wif.cap

Key

SUBMIT

用wireshark打开，WiFi认证过程重点在WPA的四次握手包，找到EAPOL握手协议，另存为  
根据题目提示，写字典

```
#include<stdio.h>
int main()
{
    int i,j,k,l;
    FILE *fp=NULL;
    fp=fopen("words.txt","w");
    for(i=0;i<=9;i++)
    {
        for(j=0;j<=9;j++)
        {
            for(k=0;k<=9;k++)
            {
                for(l=0;l<=9;l++)
                {
                    fprintf(fp,"1391040%d%d%d\n",i,j,k,l);
                }
            }
        }
    }
    fclose(fp);
}
```

使用aircrack-ng爆破密码

```
root@kali:~/下载# aircrack-ng wifi.pcap -w words.txt
Opening wifi.pcap
Read 4257 packets.

# BSSID          ESSID          Encryption
1 3C:E5:A6:20:91:60 CATR           No data - WEP or WPA
2 3C:E5:A6:20:91:61 CATR-GUEST     None (10.2.28.31)
3 BC:F6:85:9E:4E:A3 D-Link_DIR-600A WPA (1 handshake)

Index number of target network ? 3
```

选择正确的目标网络，进行爆破

```
Aircrack-ng 1.2 rc4
[00:00:09] 7688/9999 keys tested (860.77 k/s)
Time left: 2 seconds                               76.89%
KEY FOUND! [ 13910407686 ]

Master Key   : C4 60 FE 8B 14 7D 58 00 91 D7 0A 9C 3C DE 44 69
              0B E1 CD 81 07 F8 28 DB EA 76 1E ED 81 A3 FF FD

Transient Key : 0D 88 B3 F4 BC A3 C9 D2 06 12 28 43 FF 5E 21 3E
              F5 23 8E 0B 7A 9F 25 59 E9 7C 86 1E 7A 78 E4 D4
              D3 62 CD DD 4D 87 80 EE B9 E1 16 91 4A 6E 3E 09
              1E CE 5E 62 38 3C 05 35 34 A6 EB 16 31 D8 CE 96

EAPOL HMAC   : 1C E7 D0 96 DE 87 93 56 88 1D 08 C8 B9 AA B3 B0
```

flag{13910407686}

## Linux基础1

题目 264 Solves ×

### Linux基础1

100

给你点提示吧：key的格式是KEY{}

题目地址：链接: <http://pan.baidu.com/s/1skJ6t7R> 密码: s7jy

brave.zip解压出来brave文件，放到linux里面strings打开，过滤一下KEY就找到了

```
root@kali:~/下载# strings brave | grep KEY
KEY{24f3627a86fc740a7f36ee2c7a1c124a}
KEY{}
```

## 细心的大象

题目

192 Solves

×

## 细心的大象

100

链接: <https://pan.baidu.com/s/1i5ehluj> 密码: gprt

Key

SUBMIT

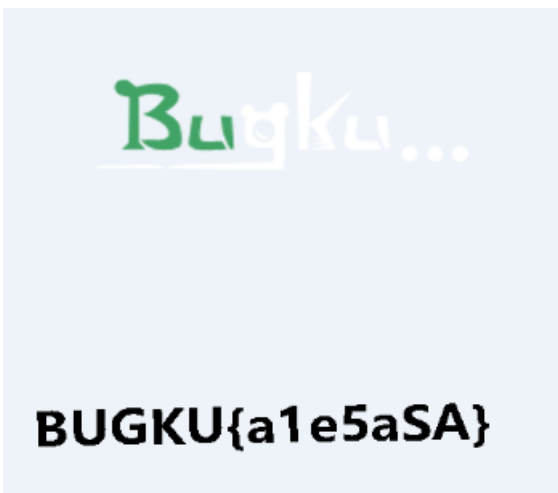
下载下来一个6.1M的1.jpg, 用binwalk检测发现有一个rar文件, 提取出来发现里面有一个2.png, 但是有密码

名称	大小	压缩后大小	类
..(上层目录)			
2.png *	17.26 KB	15.84 KB	P

并不想爆破, 于是找了一下有没有提示, 最后在1.jpg的详细信息中找到了一串base64



解密base64得到解压密码, 得到2.png, 尝试图片高度, 获得flag



账号被盗了

题目

15 Solves

×

## 账号被盗了

100

http://120.24.86.145:9001/

flag格式flag{QB充值卡密}

充值地址http://pay.qq.com/

一血有qb拿

Key

SUBMIT

好厉害的样子，不会，下一个

## MISC 图穷匕见

题目

286 Solves

×

## MISC 图穷匕见

110

作者：NIPC

paintpaint...

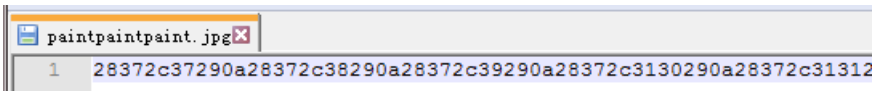
Key

SUBMIT

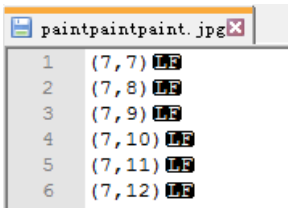


用txt打开，发现文件尾有东西，截取出来





用notepad++的插件 HEX转ASCII 得到35019个坐标



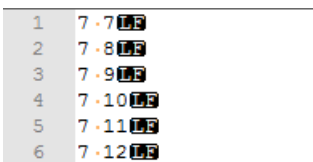
根据图片的详细信息的提示



应该是要把这些坐标转换为图形

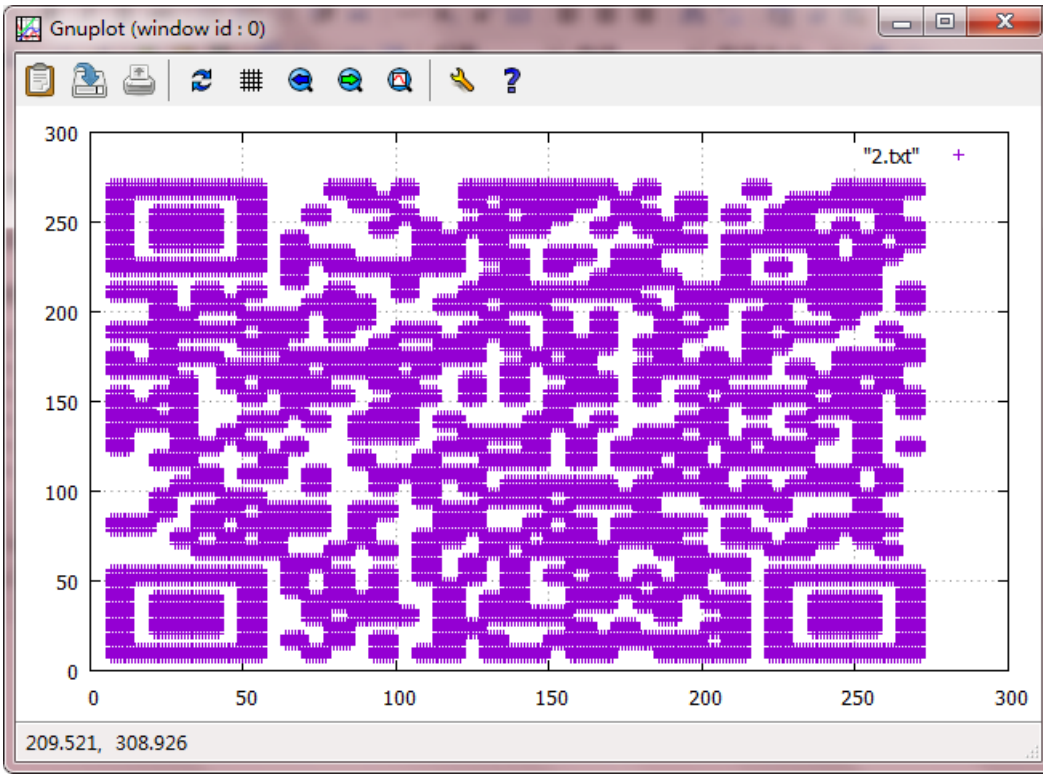
这里使用gnuplot 链接: <http://pan.baidu.com/s/1bpFCUyN> 密码: qt73

先把坐标转换为gnuplot识别的格式

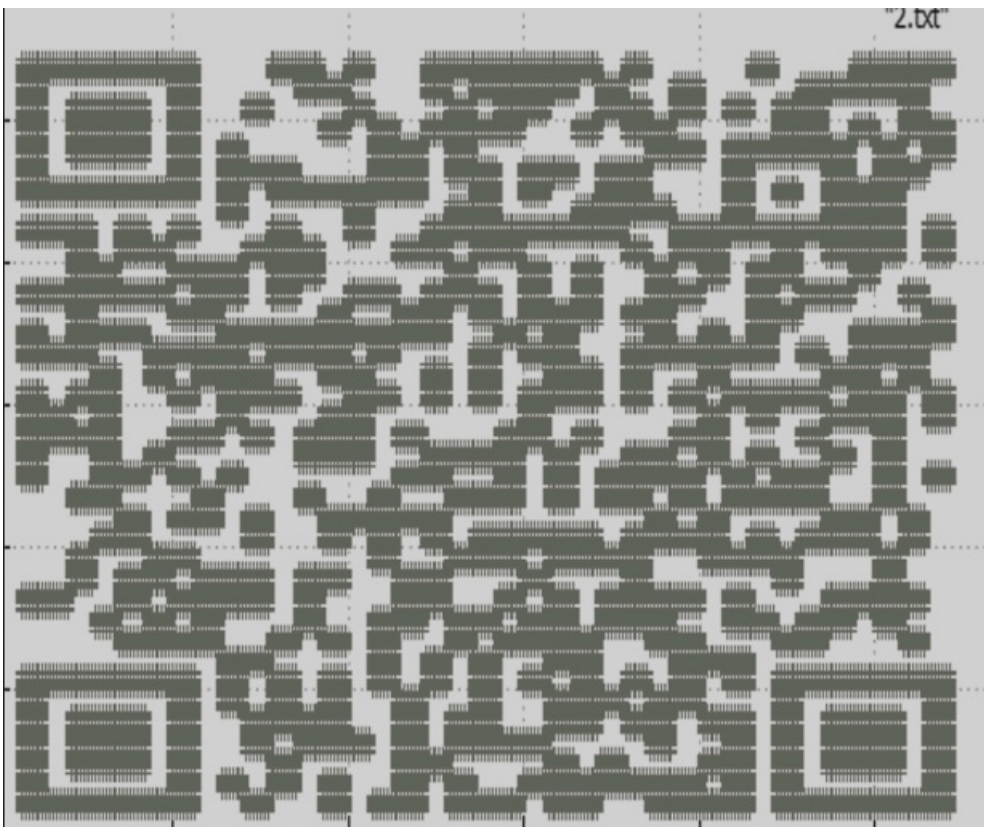


```
C:\Users\Administrator>gnuplot.exe
gnuplot> plot "xy.txt"
```

得到二维码



这种颜色识别不出来，暗化一下（我用的PS）



扫描得到flag

```
flag{40fc0a979f759c8892f4dc045e28b820}
```

## convert

题目 222 Solves ×

### convert

130

作者：NIPC

convert.txt

Key

SUBMIT

convert.txt打开是一串二进制，用python转十六进制（别人的代码）

```
# -*- coding: utf8 -*-
import binascii
file1=open('convert.txt')
s=file1.read()
file2=open('3.rar','wb')
s1=''

for i in range(0,len(s),8):
    #print (type(int(s[i:i+8],2)))
    if ((int(s[i:i+8],2))<= 15):
        print(hex(int(s[i:i+8],2)))
        s1=s1+'0'+hex(int(s[i:i+8],2)).replace('0x','')
        print (s1)
    else:
        s1+=hex(int(s[i:i+8],2)).replace('0x','')

print (s1)
file2.write(binascii.a2b_hex(s1))
```

解压出来key.jpg，用记事本打开，发现一串base64

```
Z m x h Z 3 s w M W E y N W V h M 2 Z k N j M 0 O W M 2 Z T Y z N W E x Z D A x O T Z I N z V m Y n 0 =
```

解密得到flag

```
flag{01a25ea3fd6349c6e635a1d0196e75fb}
```

## 听首音乐

# 听首音乐

150

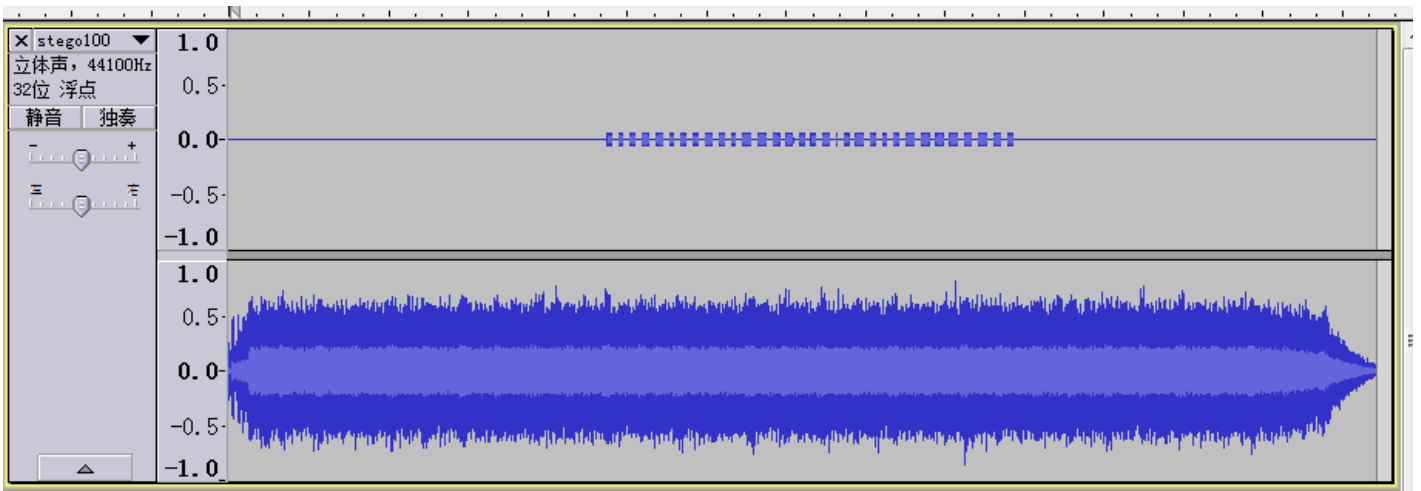
听首音乐放松放松吧~

下载地址：链接：<http://pan.baidu.com/s/1gfvezBI> 密码：y6gh

Key

SUBMIT

下载下来一个wav文件，用Audacity打开 链接：<http://pan.baidu.com/s/1skEoo9n> 密码：xuih



把莫尔斯电码取出来

```
.....
.....
```

解码得到flag

5BC925649CB0188F52E617D70929191C

好多数值

俄罗斯套娃

小明的电脑

## 好多压缩包

## 一个普通的压缩包

## 妹子的陌陌

题目 428 Solves ×

### 妹子的陌陌

300

想要妹子陌陌号吗？  
做题来拿吧

下载这个图片做题

<http://120.24.86.145:8002/misc/momo.jpg>

Key

SUBMIT

图片直接用binwalk检测，发现一个rar文件

```
root@kali:~/下载# binwalk momo.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
37340	0x91DC	RAR archive data, first volume type: MAIN_HEAD

取出来发现rar是加密的，不知道密码多大，并不想爆破

发现图片上有文字，尝试了一下密码，还真是



解压出来momo.txt





KEY{nitmzhen6}

就五层你能解开吗

转载于:<https://www.cnblogs.com/virgin-forest/p/7835317.html>



[创作打卡挑战赛](#) >  
[赢取流量/现金/CSDN周边激励大奖](#)