SKCTF Writeup

原创

弱弱的小白～ 于 2018-12-14 19:15:51 发布 1260 收藏 1

分类专栏： writeup 文章标签： tcf

本文链接：https://blog.csdn.net/weixin_43848306/article/details/84990867

签到题

请打开微信关注，发送give me flag，即可获得。

Encode

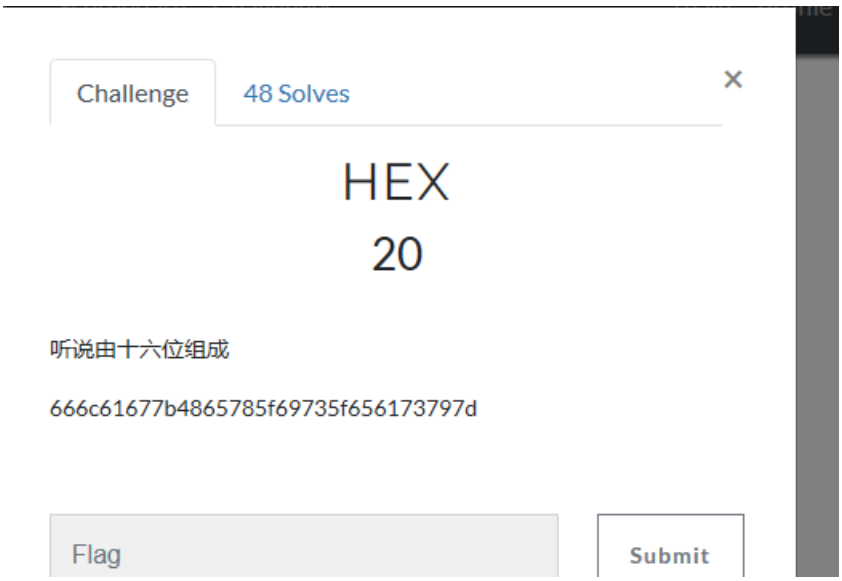
1.ACSCLL

首先看到这类题，我们肯定是要使用ASCLL的（这么明显的提示大家肯定一眼就能看出来），我们可以对照Ascii码表一一寻找，或者自己编写一段代码来实现，再或者简单地通过部分简单的解码网站来实现（如…这个就不列举了）

这里放上自己写的吧

```
#include <stdio.h>
int main ()
{
   int n;
   while(scanf("%d",&n)!=000)
   {
      printf("%c",n);
   }
}
```

2.HEX



这个上面有小暗示（听说由十六位组成），这不是16位嘛，这就好办了，还是两种办法，一种自己写代码实现，另一种就是在线的转换
（https://www.bejson.com/convert/ox2str/）
第二种推荐实在编不出来在使用
flag{Hex_is_easy}

3.Escape
我们进来后会发现有一个txt文件在等着我们，我们就肯定开心的点开啊，但是发现有一个字符串在等着，仔细观察发现这个是肯定是url解码啊，然后就解决了，这个不知道怎么写代码解决，就只推荐（http://tool.chinaz.com/tools/urlencode.aspx） 这个网址来解决下吧，flag{do_not_Escape}
4.jsfuck
题目上写的很明显了，就是jsfuck，只需要点开，将内容复制下来，如果你使用的是google浏览器的话，打开F12，点击console按下Ctrl+v加回车就完事了；如果没有的话，那就http://discogscounter.getfreehosting.co.uk/js-noalnum.php?ckattempt=1&i=1，这个网址解决问题吧。
flag{it_is_js?}

Misc

1.Ez密码

这个题是对考察zip文件解压的，上面题目里给出的信息有密码是**1.八位 2.是全数字. 3.十七年后的日子**
我在这里使用的是暴力破解，借助了工具ziperello

然后对文件进行解压，会发现：咦只有一个jpg文件，我的flag那？这是我们需要打开属性，查看详细信息，会发现flag藏在这里，真皮


备注 flag{exif_is_easy}
来源
作者
拍摄日期 2016/3/10 7:49
程序名称 Adobe Photoshop CC 2014 (Windows)
获取日期
版权
图像
图像 ID
分辨率 2560 x 1600
宽度 2560 像素
高度 1600 像素
水平分辨率 300 dpi
垂直分辨率 300 dpi
位深度 24
压缩
分辨率单位 2
颜色表示 sRGB
删除属性和个人信息
确定
取消
应用(A)

2.小猪佩奇

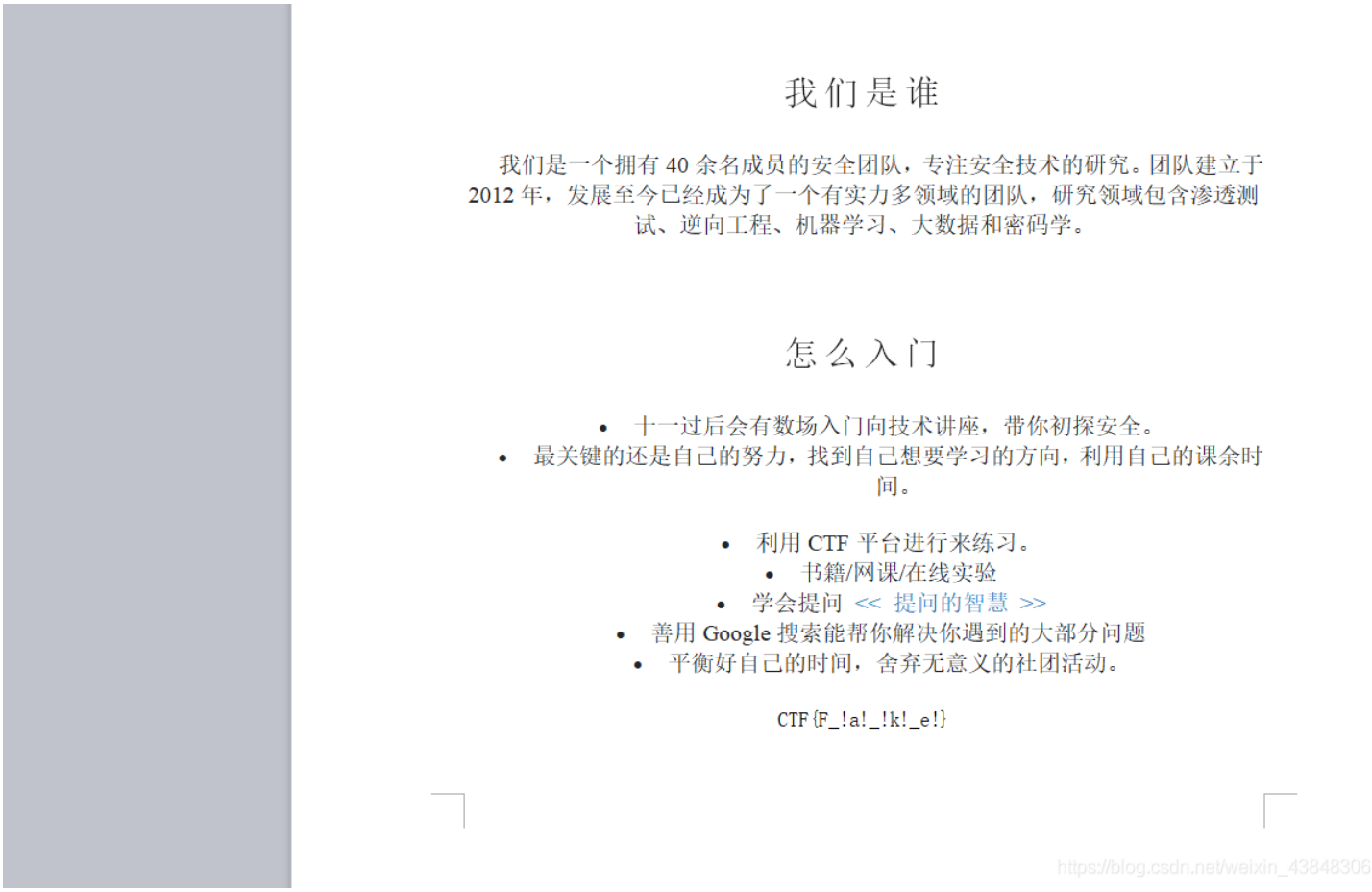

StegSolve 1.3 by Caesum
File Analyse Help
Blue plane 0

这个题目需要用到一个叫做stegolove的神奇工具，同时你需要有java的环境，当一切准备就绪后，打开我们社会人的图片，点箭头知道出现二维码，扫一扫即得flag

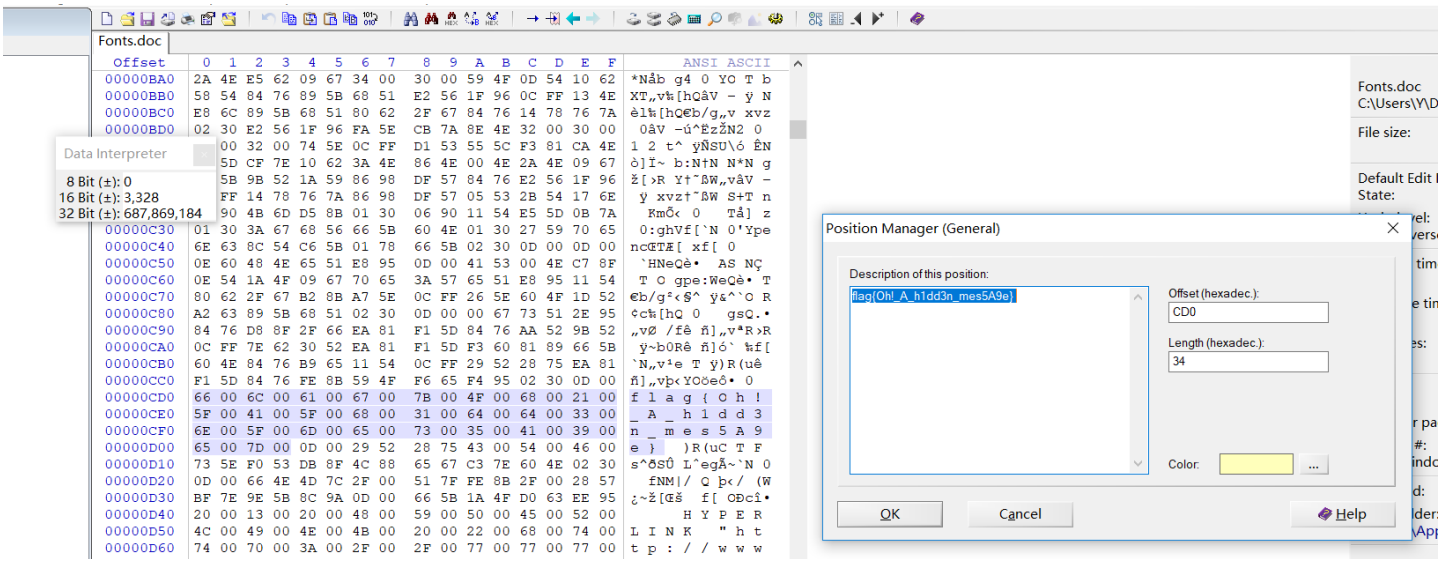
flag{lsb_is_easy}

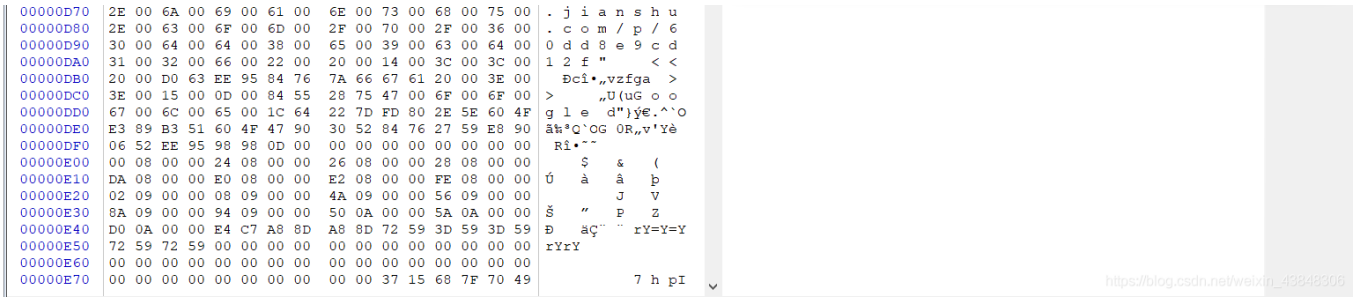
3.Fonts

这个将文件夹下载后发现没有任何的异常



这个时候我们就需要清楚分析工具来操作一下

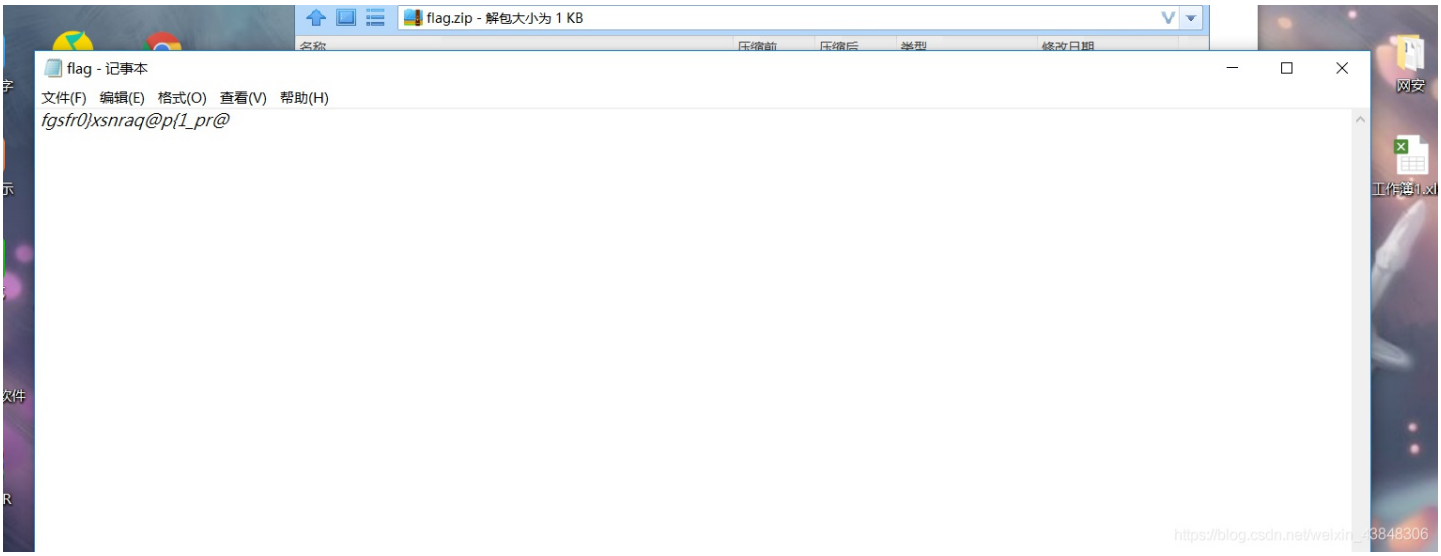




点开就会得到flag

6.ZipWithCrypto

这个题目的话你会下载下来发现有个压缩包（好像听说这个有解压密码，但是貌似我的没有哎，可能是因为解压工具原因），总之打开后会发现一个字符串

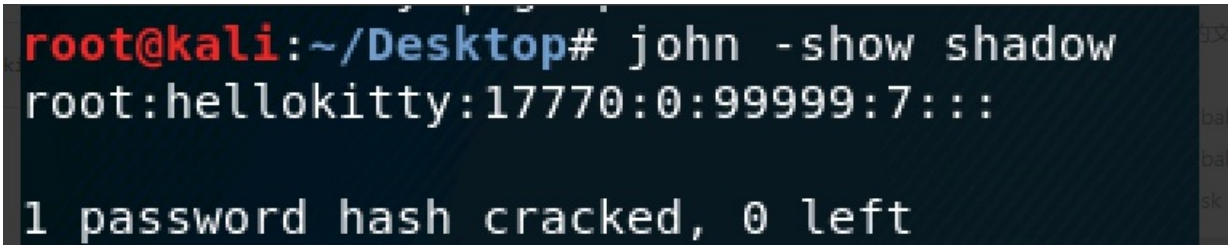


表示看到密码有点蒙，但是看到里面有“{}”类的，但是没有组合起来，自然就想到了栅栏，就用栅栏跑一下，考虑到密码是skctf开头的，{}位就要有5个字，因此就将移位码确定到3，将得到的密码再用凯撒跑下就得到flag了

7.Crack it

打开后会发现一个字符串：root:6HRMJoyGA$26Flgg6CU0bGUOfqFB0Qo9AE2LRZxG8N3H.3BK8t49wGlYbkFbxVFtGOZqVlq3qQ6k0oetDbn2aVzdhuVQ6US.:17770:0:99999:7:::

仔细观察会发现这个是查看shadow的，打开kali使用john直接破解就行



然后就找到了，***flag{hellokitty}***

8.啊哒

这个题目中发现图中有隐藏文件，需要借助神器kali，打开kali，打开终端使用binwalk，发现有隐藏文件，使用foremost将他分离，将会在out中发现隐藏文件flag是个被压缩的txt文件，呀比，这可怎么办？没有任何提示，发现题目中也没有提示（so暴力破解也是不可能了），没办法就只好回头了，点开图片详细信息，发现里面有神秘的字符

ada.jpg 属性

这不是base16嘛，解密后发现啊呀，好有规律的数字

就这样得到了解压密码，打开后发现了flag **flag{3XiF_iNf0rM@ti0n}**

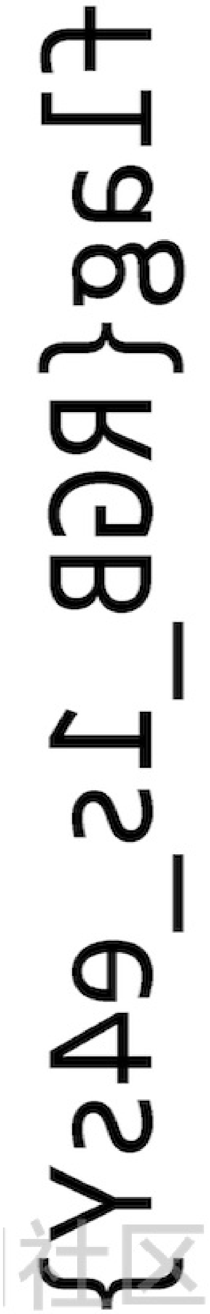
9.***basic***

打开后我们会发现是一个txt文件，打开后发现是一组组图像点，很容易就会想到python像素问题，讲到这里就要敲敲小黑板了：好好学**python**

这里直接用python跑下

代码如下：

```
# coding=utf-8
from PIL import Image
import re
pic = Image.new("RGB",(150,900))
f = open('C:/Users/Y/Desktop/网安/0/basic.txt','r')
imlist = []
for i in f.readlines():
    i = re.sub('[( )\n]', '', i)
    imlist.append(i)
    i=0
    for x in range(0,150):
        for y in range(0,900):
            s = imlist[i].split(',')
            pic.putpixel([x, y], (int(s[0]), int(s[1]), int(s[2])))
            i += 1
            print(135000 - i)
            pic.show()
            pic.save("flag.png")
```



10.进制转换

这个题的话肯定还是代码直接跑吧，没发现什么辅助工具

```
import binascii

text = "d87 x65 x6c x63 o157 d109 o145 b100000 d116 b1101111 o40 x6b b1100101 b1101100 o141 d105 x62 d101 b1101001 d46 o40 d71 x69 d118 x65 x20 b1111001 o157 b1110101 d32 o141 d32 d102 o154 x61 x67 b100000 o141 d115 b100000 b1100001 d32 x67 o151 x66 d116 b101110 b100000 d32 d102 d108 d97 o147 d123 x31 b1100101 b110100 d98 d102 b111000 d49 b1100001 d54 b110011 x39 o64 o144 o145 d53 x61 b1100010 b1100011 o60 d48 o65 b1100001 x63 b110110 d101 o63 b111001 d97 d51 o70 d55 b1100010 d125 x20 b101110 x20 b1001000 d97 d118 o145 x20 d97 o40 d103 d111 d111 x64 d32 o164 b1101001 x6d o145 x7e"
solution = ''
text2 = text.split(' ')
for x in text2:
    print(x)
    if x[0] == 'b': #binary
        solution += chr(int(x[1:],2))
    elif x[0] == 'x': # hexadecimal
        solution += x[1:].decode("hex")
    elif x[0] == 'd': # decimal
        solution += chr(int(x[1:]))
    elif x[0] =='o': # octal
       solution += chr(int(x[1:],8))
print(solution)
```

跑完就会在末尾找到flag

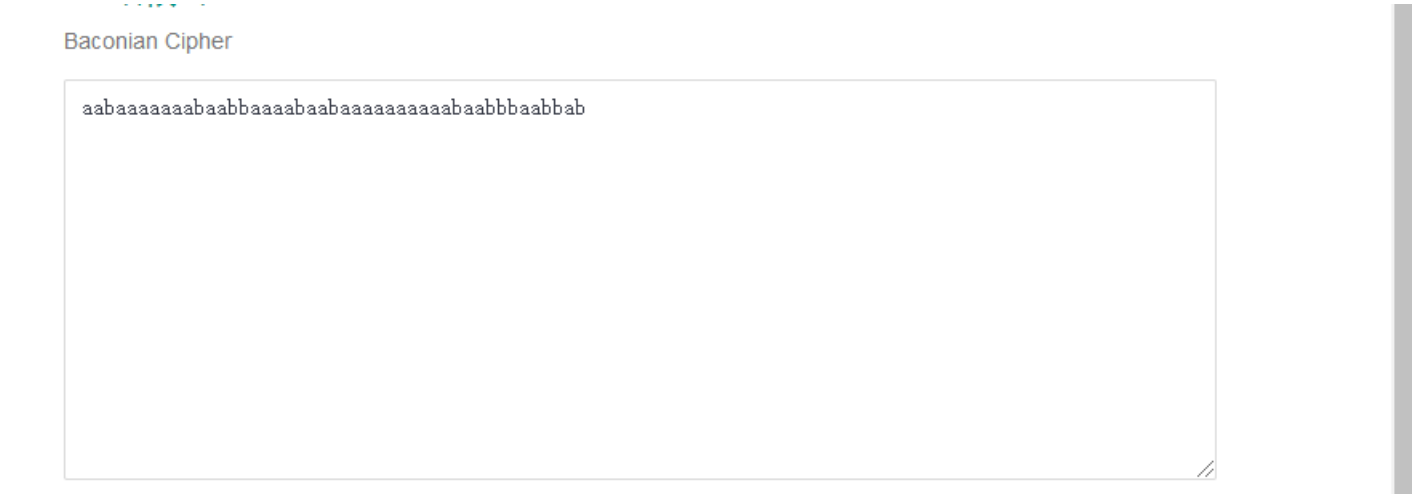
Crypto

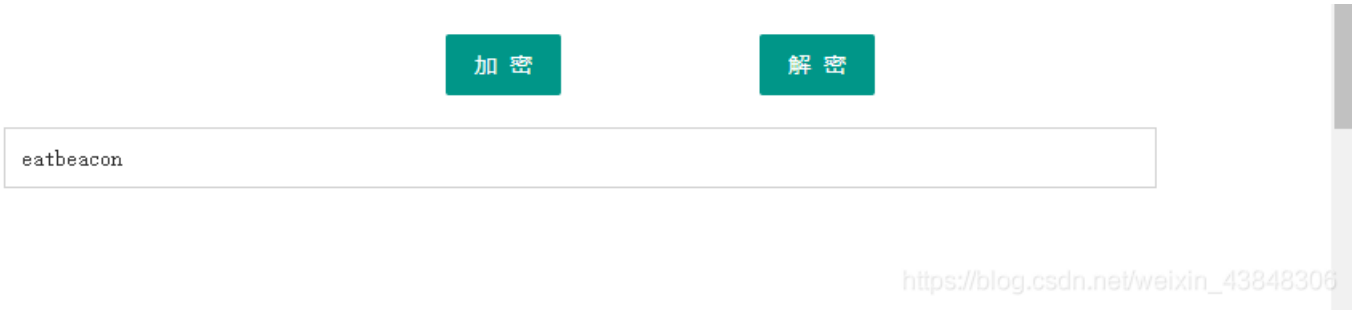
1.培根

培根烤肉可还行，直接打开找到aabaaaaaaaabaabbaaaabaabaaaaaaaaaaabaabbbaabbab

明显的培根啊，打开http://ctf.ssleye.com/baconian.html

直接破解





2.Base64

直接打开辅助网站http://www.ssleye.com/，直接解码

flag{base_64_32_16}

3.Caesar来啦

凯撒密码了解下（其实就是一个偏移）

会得到skctf{veni_vidi_vici.}

4.栅栏里的爱

栅栏密码了解下，解码后会得到

flag{jursytp_taon}_old_c

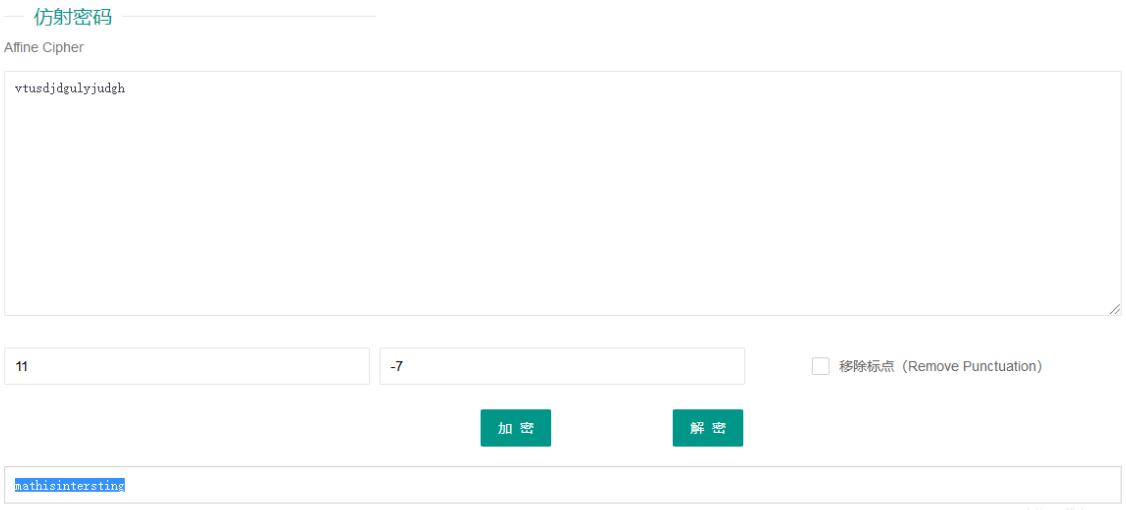
5.base一家

base一家嘛，那肯定有64、32、16啦，首先观察得到的字符是64的，那就肯定先64，解完发现是32的再解就是16，最后得到了flag

flag{fl4g_1_B4se_i3_V3ry_9ood}

6.仿射密码

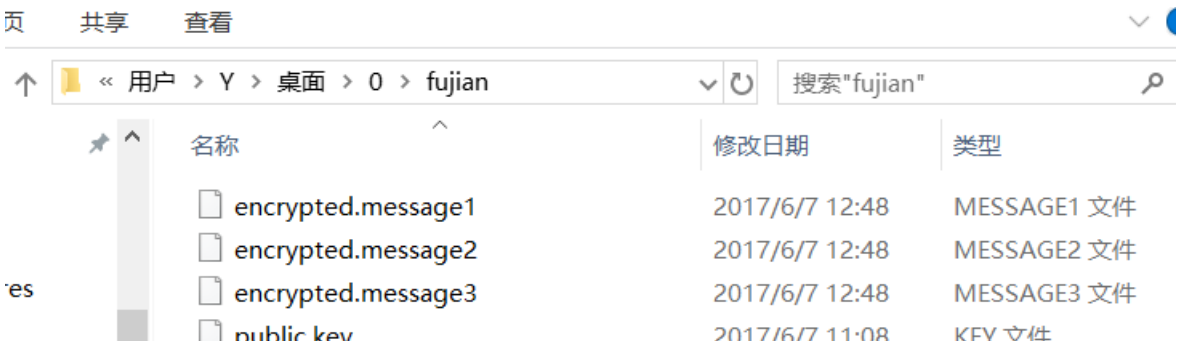
放射密码的话可以了解下工具http://ctf.ssleye.com/affine.html



mathisintersting，最后再加上flag{}。

7.RivestShamirAdleman

下载后就会压缩包，解压后会发现三个文件



看到是这个，就肯定得打开kali linux的openssl

```
Public-Key: (256 bit)
Modulus:
    00:d9:9e:95:22:96:a6:d9:60:df:c2:50:4a:ba:54:
    5b:94:42:d6:0a:7b:9e:93:0a:ff:45:1c:78:ec:55:
    d5:55:eb
Exponent: 65537 (0x10001)
Modulus=D99E952296A6D960DFC2504ABA545B9442D60A7B9E930AFF451C78EC55D555EB
writing RSA key
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhANmelSKWptlg38JQSrpUW5RC1gp7npMK
/0UceOxV1VXrAgMBAAE=
-----END PUBLIC KEY-----
```


然后就看到e是Exponentialent的值，将Modulus转成10进制就得到n=，接着将n因式分解得到p、q。（此过程可以自己编程实现或者引用一下工具http://www.atool.org/quality_factor.php）；然后将得到的m,n，接着用python跑一下

```
#coding:utf-8
import gmpy
import rsa
p = 3028255367440967415185462127611943114 77
q = 3250455041864363462098773013201312779 83
n = 9843207927151313098126791905614916163189282270716717785883184169952177431089 1
e = 65537
d = int(gmpy.invert(e , (p-1) * (q-1)))
privatekey = rsa.PrivateKey(n , e , d , p , q)     #根据已知参数，计算私钥
with open("encrypted.message1" , "rb") as f:
    print(rsa.decrypt(f.read(), privatekey).decode())      #使用私钥对密文进行解密，并打印
with open("encrypted.message2" , "rb") as f:
    print(rsa.decrypt(f.read(), privatekey).decode())      #使用私钥对密文进行解密，并打印
with open("encrypted.message3" , "rb") as f:
    print(rsa.decrypt(f.read(), privatekey).decode())      #使用私钥对密文进行解密，并打印
```

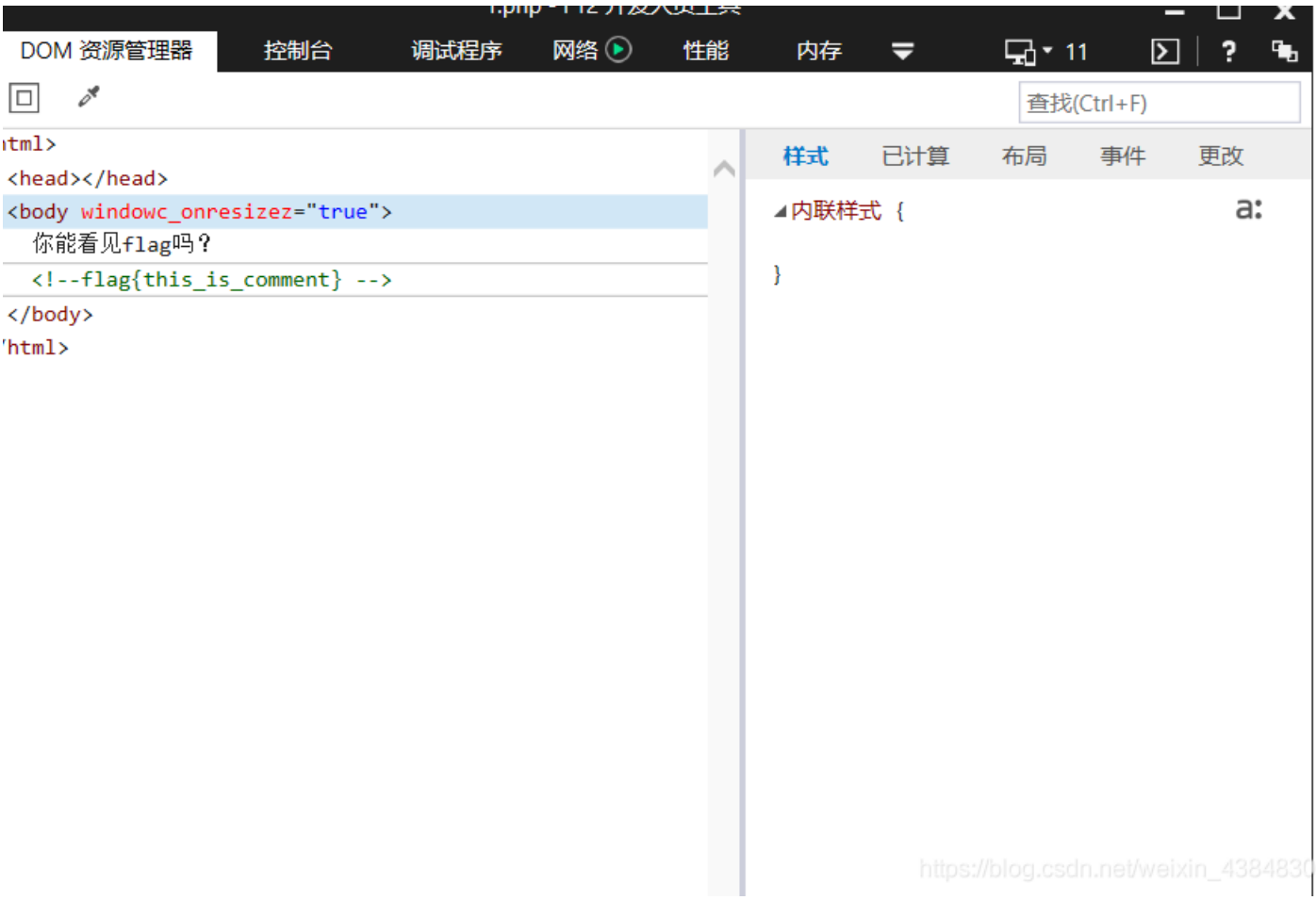
得出flag

```
root@kali:~/Desktop/fujian# python 2.py
flag{3b6d3806-4b2b

-11e7-95a0-

000c29d7e93d}
```

Web

1.你能看见flag吗

那可不肯定能看见啊，不过需要小技巧，这个不就是在眼皮下面吗，首先我们查看下源代码，按下F12，调出开发人员工具，就能看到了



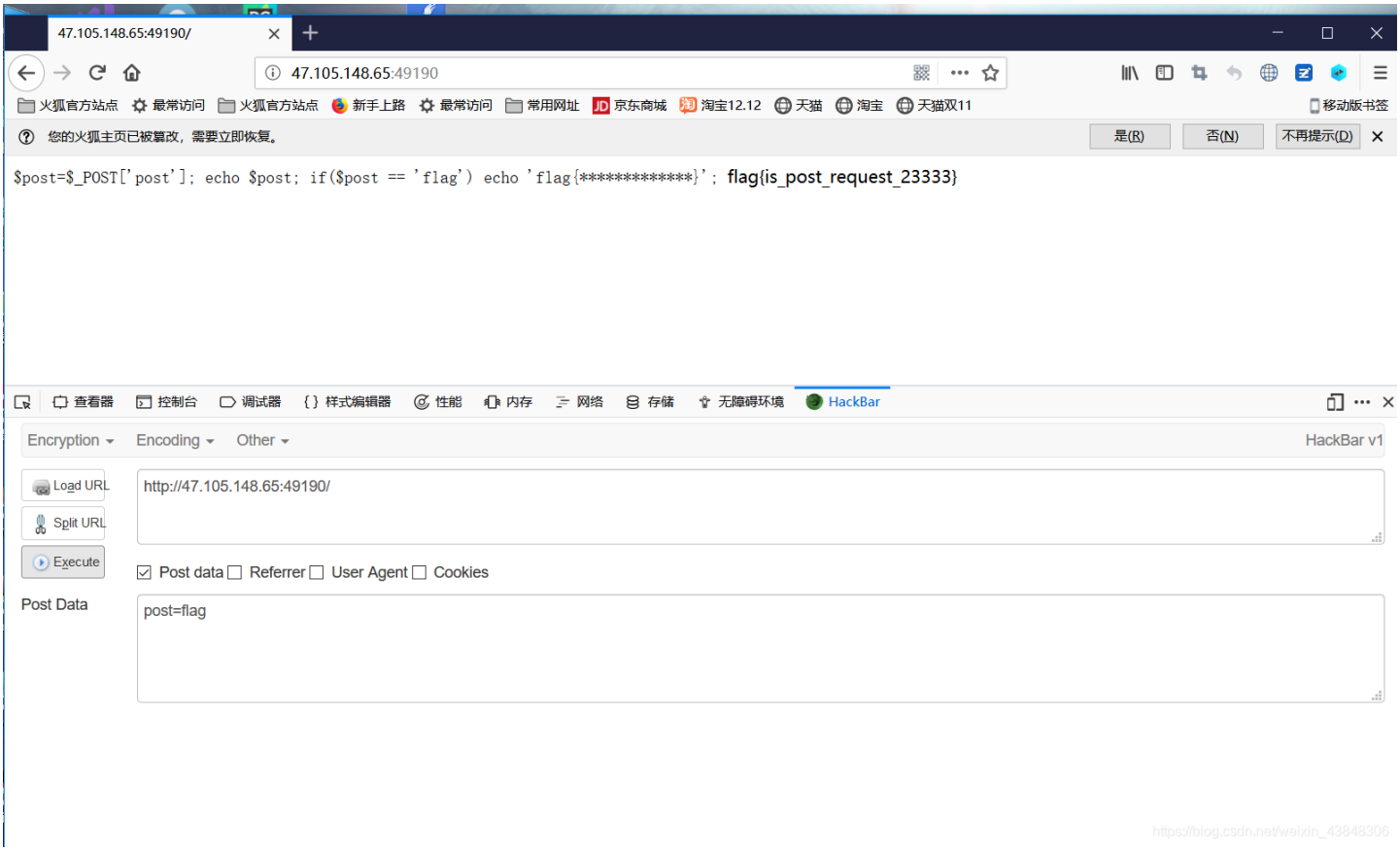
flag{this_is_comment}

2.GET

只需要在地址栏输入？get=flag即可

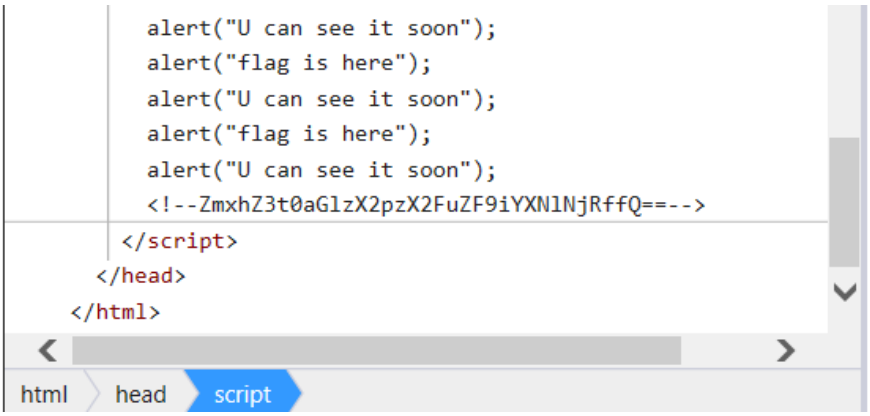
3.POST

这个只是考察对hackbar的使用，在hackbar里输入post=flag就能得到flag了



4.找一找flag

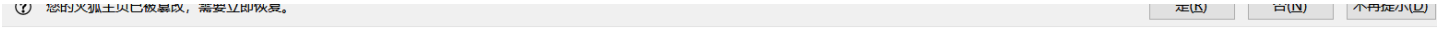
我的做法是直接给他禁止创建更多页面，打开源码就直接找到了类似flag的东西



!–ZmxhZ3t0aGlzX2pzX2FuZF9iYXNlNjRffQ==–这明显是base64啊，就直接解码得到flag

5.where_are_u_from

这个题只是需要更改下地址，从本地访问就行



Please access the server from the local

6.这个题目应该是挺清楚的打开源代码后，发现需要输出a，（可以在控制台直接写a或者在那里执行js代码）就可以得到上交的密码

听说浏览器的控制台可以执行JavaScri

submit

flag{860811cce93639b9701db88dd06183e5}