

SKCTF Writeup

转载

[weixin_30340775](#) 于 2019-04-18 18:42:00 发布 162 收藏

文章标签: [python](#) [php](#) [java](#)

原文链接: <http://www.cnblogs.com/fic7/p/10731542.html>

版权

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，又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

Challenge 48 Solves

HEX

20

听说由十六位组成

666c61677b4865785f69735f656173797d

Flag Submit

https://blog.csdn.net/weixin_43848306

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}

首页 JSON相关 编码/加密 格式化 网络 前端 后端 转换 其他

API 文档 平台工具 赞助商 更多

16进制到文本字符串的转换, 在线实时转换

16进制到文本字符串的转换, 在线实时转换 (支持中文转换)

加密或解密字符串长度不可以超过10M

666c61677b4865785f69735f656173797d

16进制转字符 字符转16进制 清空结果

flag{Hex is easy}

34

https://blog.csdn.net/weixin_43848306

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

题目上写的很明白了，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

Challenge 33 Solves

Ez密码

30

小明喜欢用8位的日期当密码，他用了一个17年以后的日子当做了压缩包的密码，你能破解出来么？

↓ flag.zip

Flag Submit

https://blog.csdn.net/weixin_43848306

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

Ziperello zip password recovery tool

帮助 关于 退出

当前密码长度: 8

当前密码

当前速度

18%

逝去时间: 00:00:03

开

信息

密码: 20170328

确定

步骤 4

准备就绪，请点击 [开始] 按钮

注意：搜索进度条 (%) 及剩余时间字段显示的信息与当前的密码校验长度相关。破解 AES 算法加密的密码可能耗时较长。

16:41:05: 密码: "20170328".时间: 3 s

BACK 步骤 4 / 4: 破解密码.Go NEXT

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

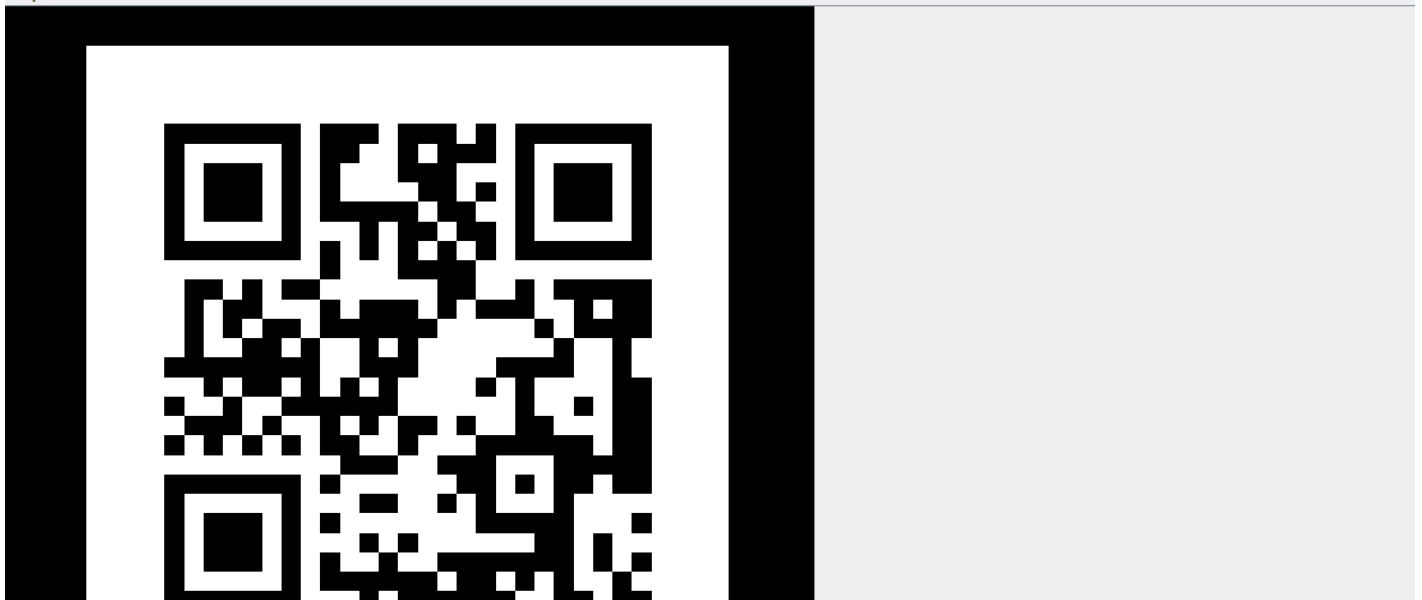


2.小猪佩奇

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

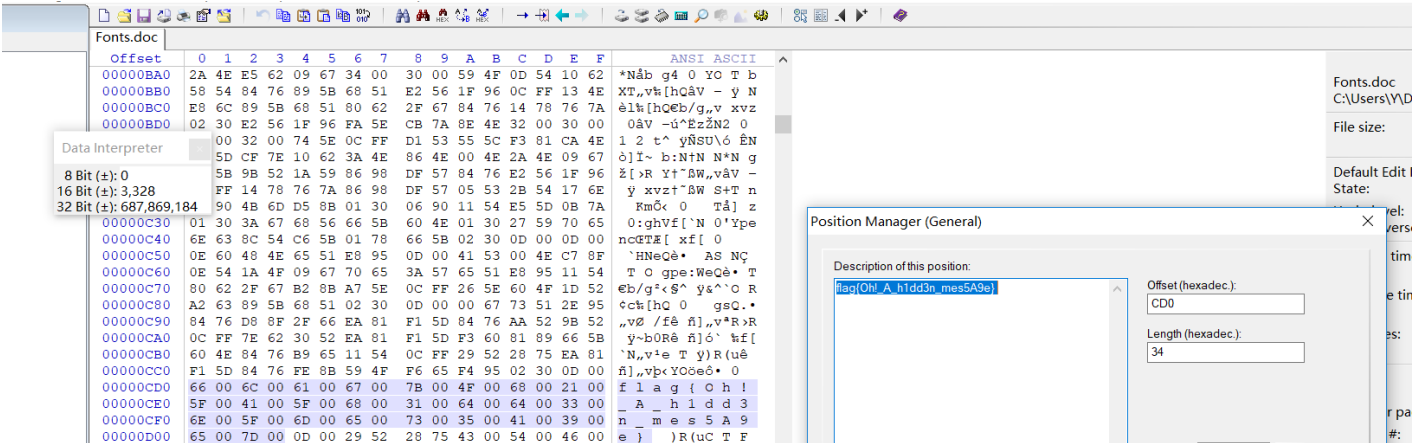
flag{lsb_is_easy}

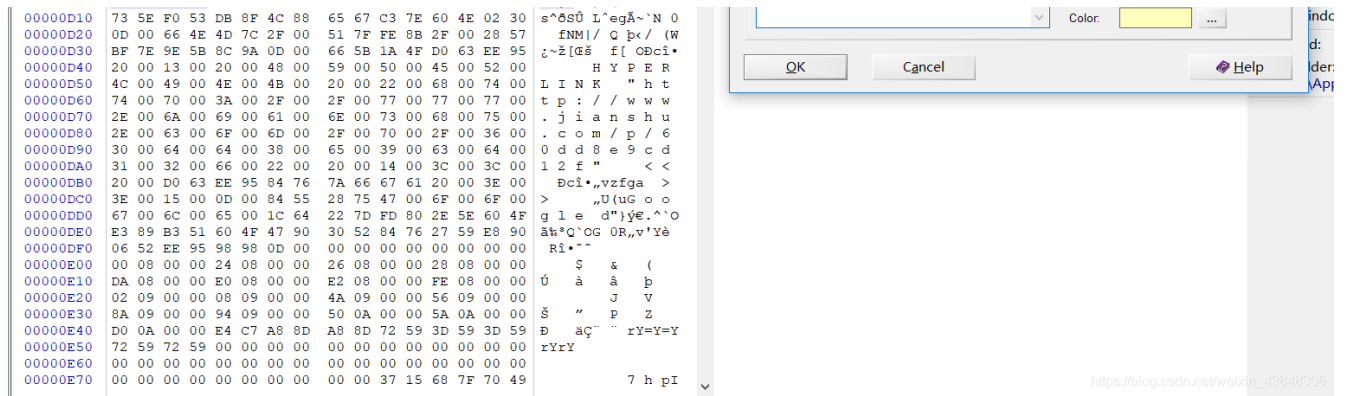
3.Fonts

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:$6$HRMJoyGA$26Flgg6CU0bGUOfqFB0Qo9AE2LRZxG8N3H.3BK8t49wGIYbkFbxVFtGOZqVlq3qQ6k0o
```

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

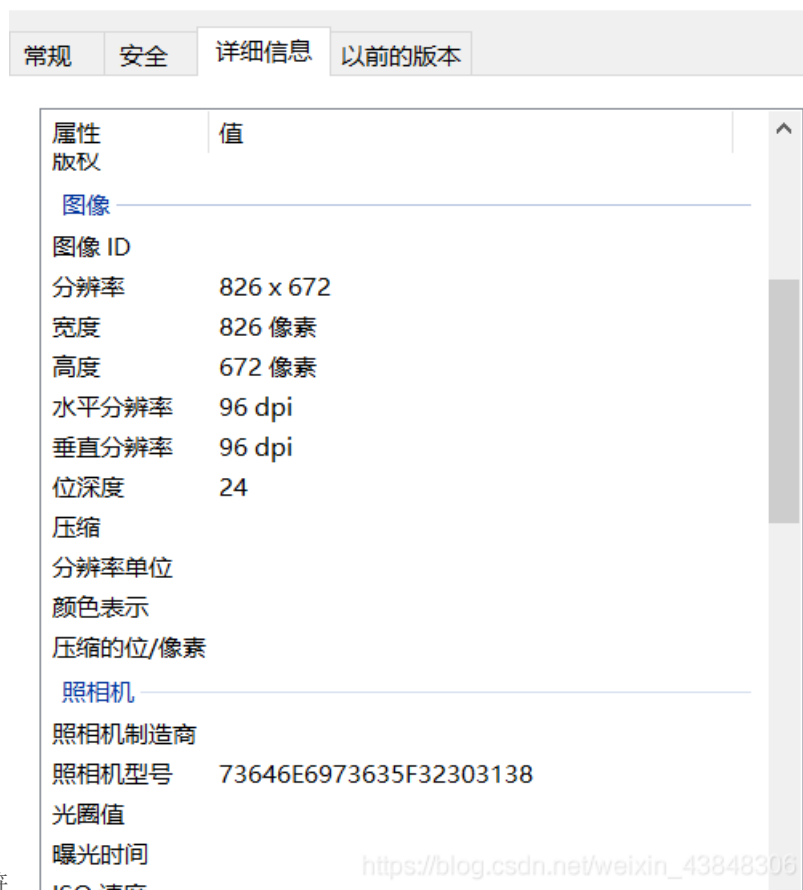
```
root@kali:~/Desktop# john -show shadow
root:hellokitty:17770:0:99999:7:::
1 password hash cracked, 0 left
```

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

ada.jpg 属性



属性	值
图像	
图像 ID	
分辨率	826 x 672
宽度	826 像素
高度	672 像素
水平分辨率	96 dpi
垂直分辨率	96 dpi
位深度	24
压缩	
分辨率单位	
颜色表示	
压缩的位/像素	
照相机	
照相机制造商	
照相机型号	73646E6973635F32303138
光圈值	
曝光时间	
ISO 速度	

秘的字符

这不是base16嘛，解密后发现啊呀，好有规律的数字

```
sdnisc_2018
```

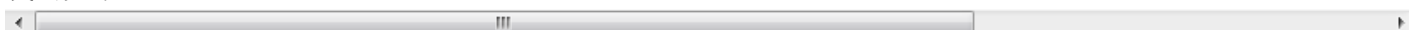
就这样得到了解压密码，打开后发现了**flag flag{3XiF_iNf0rM@ti0n}**

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")
```


fJ9g{RGB_I2_642Y}

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 b
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aabaaaaaabaabbbaaaabaabaaaaaaaabaabbbaabbab

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

直接破解

Baconian Cipher

aabaaaaaabaabbbaaaabaabaaaaaaaabaabbbaabbab

加密

解密

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_tاون}_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>

仿射密码

Affine Cipher

vtusdjdulgyljudgh

11 -7 移除标点 (Remove Punctuation)

加密 解密

mathisintersting

https://blog.csdn.net/weixin_43848306

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

页 共享 查看

↑ << 用户 > Y > 桌面 > 0 > fujian 搜索"fujian" 🔍

名称	修改日期	类型
encrypted.message1	2017/6/7 12:48	MESSAGE1 文件
encrypted.message2	2017/6/7 12:48	MESSAGE2 文件
encrypted.message3	2017/6/7 12:48	MESSAGE3 文件
public.key	2017/6/7 11:08	KEY 文件

es

ve - Perso

盘

象

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-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhANme1SKWptlg38JQSrpUW5RC1gp7npMK
/0Uce0xV1VXrAgMBAAE=
-----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 = 302825536744096741518546212761194311477
q = 325045504186436346209877301320131277983
n = 98432079271513130981267919056149161631892822707167177858831841699521774310891
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

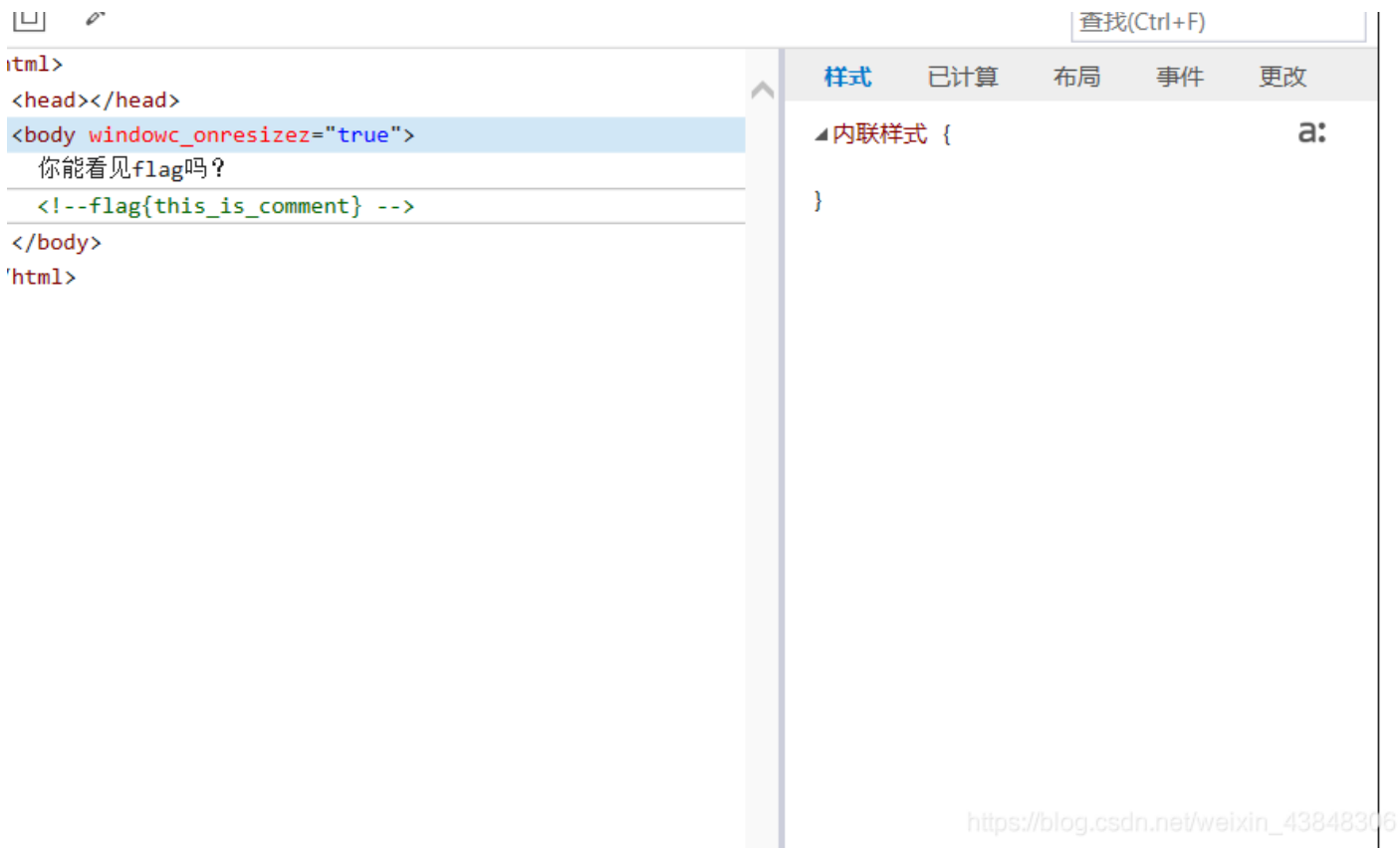
```
root@kali:~/Desktop/fujian# python 2.py
flag{3b6d3806-4b2b-11e7-95a0-000c29d7e93d}
```

Web

1.你能看见flag吗

那可不一定能看见啊，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





https://blog.csdn.net/weixin_43848306

flag{this_is_comment}

2.GET

只需要在地址栏输入? get=flag即可

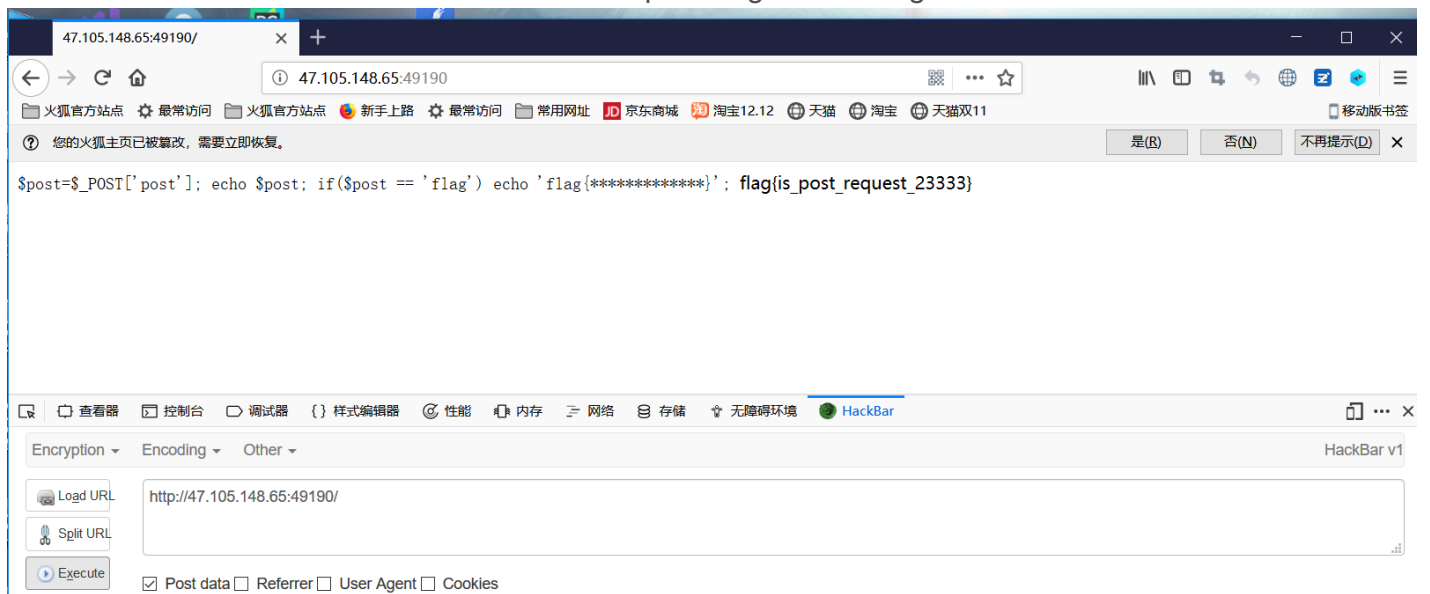
http://47.105.148.65:49189/?get=flag



https://blog.csdn.net/weixin_43848306

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



Post Data

post=flag

https://blog.csdn.net/weixin_43848306

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



https://blog.csdn.net/weixin_43848306

!--ZmxhZ3t0aGlzX2pzX2FuZF9iYXN1NjRffQ==--这明显是base64啊，就直接解码得到flag



5.where_u_from

这个题只是需要更改下地址，从本地访问就行

您的浏览器地址已被修改，需要立即恢复。

Where are you from

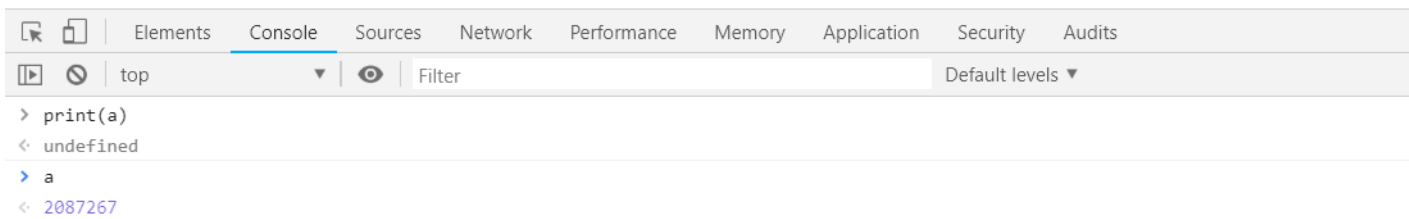
Please access the server from the local



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JavaScript

`flag{860811cce93639b9701db88dd06183e5}`



https://blog.csdn.net/weixin_43848306

转载于:<https://www.cnblogs.com/ftc7/p/10731542.html>