Hgame - week1

【Hgame - week1】Write up - Moesang

Web

谁吃了我的flag

- 题目地址
- 步骤

  damn...hgame2019 is coming soon, but the stupid Mki haven't finished his web-challenge...

  fine, nothing serious, just give you flag this time...

  the flag is hgame{3eek_diScl0Sure

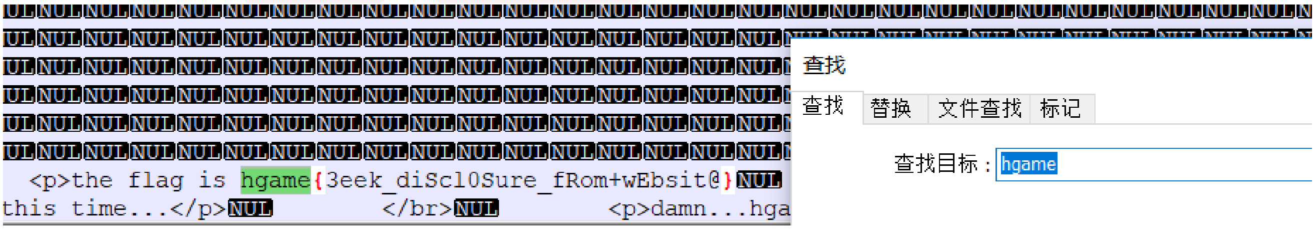
- 看到Mki想要直接给flag，结合题目描述

```
呜呜呜，Mki一起床发现写好的题目变成这样了，是因为昨天`没有好好关机`吗T_T hint: 据当事人回忆，那个夜晚他正在`vim`编写题目页面，似乎没有保存就关机睡觉去了，现在就是后悔，十分的后悔。
```

- 可以得知是vim的临时文件

```
编辑vim时会在同目录下产生`.文件名.swp`的临时文件
```

- 那么爽快地把url里的 `index.html` 改成 `.index.html.swp`



```
ULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULN
ULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULN
ULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULN
ULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULN
ULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULN
ULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULN
  <p>the flag is hgame{3eek_diScl0Sure_fRom+wEbsit@}NUL
this time...</p>NUL        </br>NUL        <p>damn...hga
```

- 下载回来后用文本打开，搜索关键字 `hgame` 可以得到flag
- 以下是没有hint时的考虑：

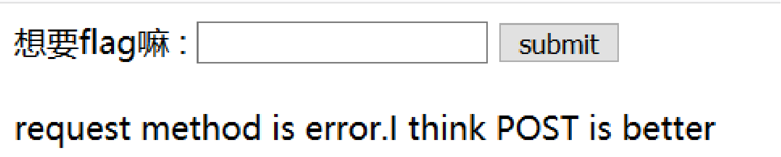
```
不知道是`vim`时，只能猜是临时文件，既然Mki是在写html，那么不可能使用word之类的文稿软件
若是IDE可能有`.idea`之类的`workspace`
但后来发现不对...
```

```
应该是用了普通的编辑器...
那应该不会在win下干这种事...
用ubuntu或者mac os之类的都是`vim`
那试试`vim`的`swp`， 中了!
```

换头大作战

- [题目地址]()

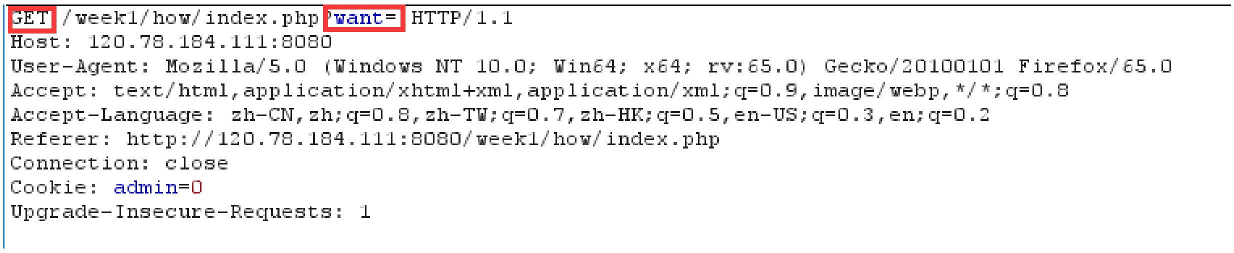
- 步骤



想要flag嘛：

request method is error.I think POST is better

- 一进来，随便`submit`一下，得到提示需要`POST`
- 打开burp，查看刚才的请求

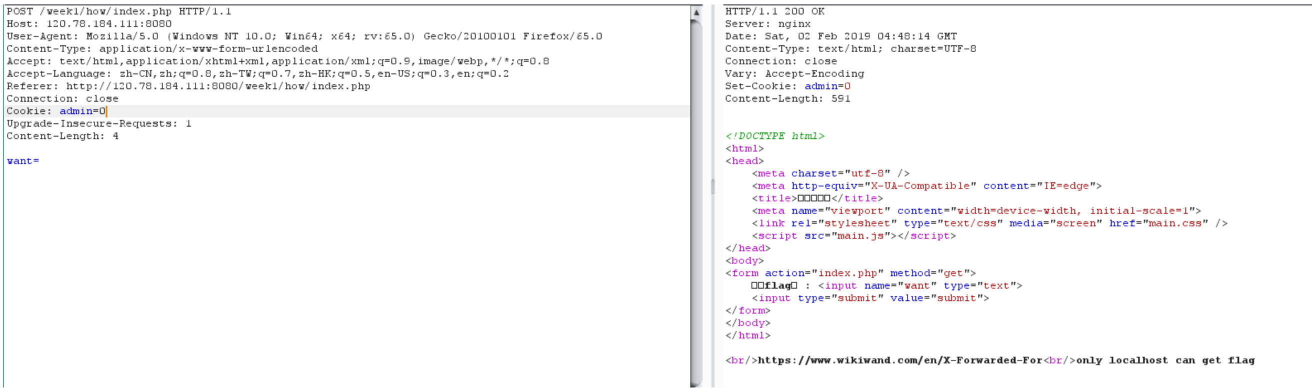


```
GET /week1/how/index.php?want= HTTP/1.1
Host: 120.78.184.111:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://120.78.184.111:8080/week1/how/index.php
Connection: close
Cookie: admin=0
Upgrade-Insecure-Requests: 1
```

- 按Ctrl+R然后进入Repeater
- 把`GET`更改成POST

```
注意:这里需要在header上增加`Content-Type: application/x-www-form-urlencoded`
```

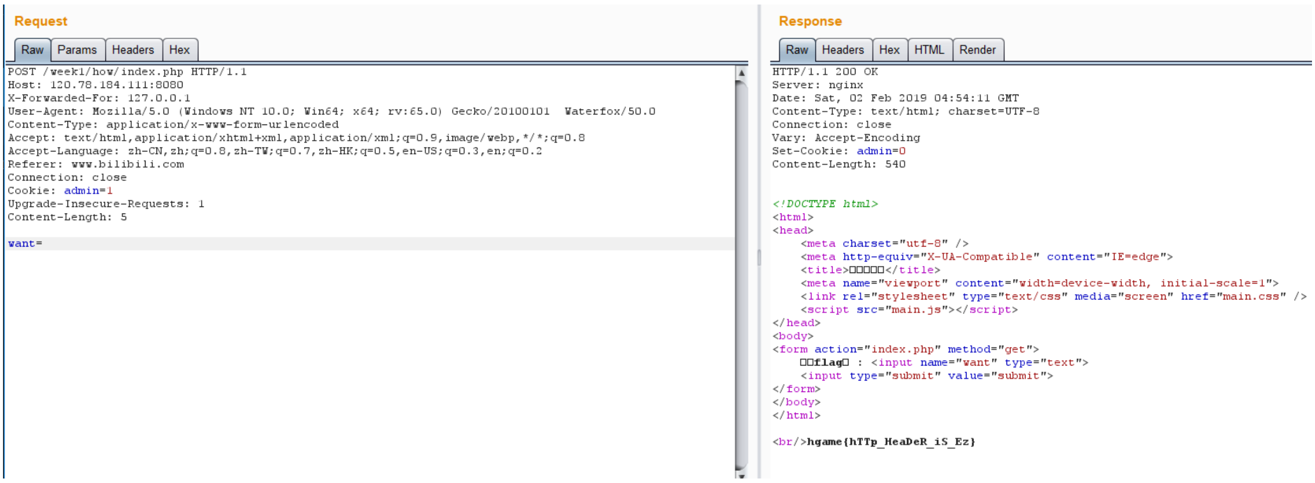
- 然后把`want`参数放进下面的`body`里
- 然后Go



```
POST /week1/how/index.php HTTP/1.1
Host: 120.78.184.111:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://120.78.184.111:8080/week1/how/index.php
Connection: close
Cookie: admin=0
Upgrade-Insecure-Requests: 1
Content-Length: 4

want=
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 02 Feb 2019 04:48:14 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Set-Cookie: admin=0
Content-Length: 591


<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>□□□□□</title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" type="text/css" media="screen" href="main.css" />
    <script src="main.js"></script>
</head>
<body>
<form action="index.php" method="get">
    □□flag□ : <input name="want" type="text">
    <input type="submit" value="submit">
</form>
</body>
</html>

<br/>https://www.wikiwand.com/en/X-Forwarded-For<br/>only localhost can get flag
```

- 根据提示在`header`里增加`X-Forwarded-For: 127.0.0.1`，然后Go
  接下来几个提示都差不多，需要依次按照提示
- 在`User-Agent`后增加`Waterfox/50.0`
- 在`header`里增加`Referer: www.bilibili.com`
- 将`admin=0`改成`admin=1`
  最后得到flag

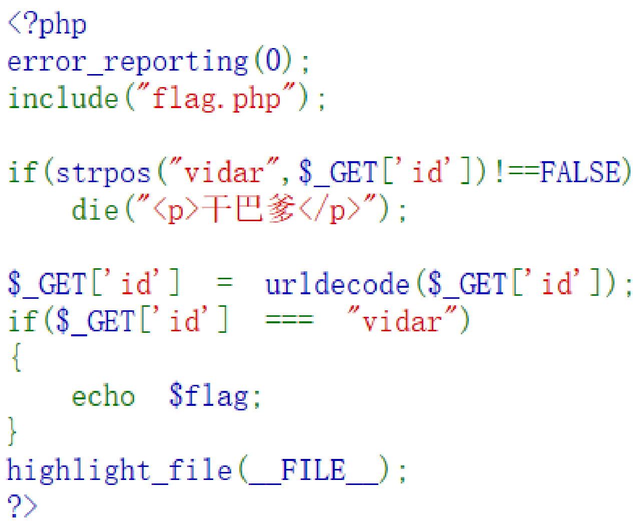


```
POST /week1/how/index.php HTTP/1.1
Host: 120.78.184.111:8080
X-Forwarded-For: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101  Waterfox/50.0
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: www.bilibili.com
Connection: close
Cookie: admin=1
Upgrade-Insecure-Requests: 1
Content-Length: 5

want=
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 02 Feb 2019 04:54:11 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Set-Cookie: admin=0
Content-Length: 540


<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>□□□□□</title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" type="text/css" media="screen" href="main.css" />
    <script src="main.js"></script>
</head>
<body>
<form action="index.php" method="get">
    □□flag□ : <input name="want" type="text">
    <input type="submit" value="submit">
</form>
</body>
</html>

<br/>hgame{hTTp_HeaDeR_iS_Ez}
```

very easy web

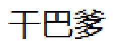
- [题目地址]



```
<?php
error_reporting(0);
include("flag.php");

if(strpos("vidar",$_GET['id'])!==FALSE)
    die("<p>干巴爹</p>");

$_GET['id']  =  urldecode($_GET['id']);
if($_GET['id']  ===  "vidar")
{
    echo  $flag;
}
highlight_file(__FILE__);
?>
```

~~开局一张图，剩下全靠编~~

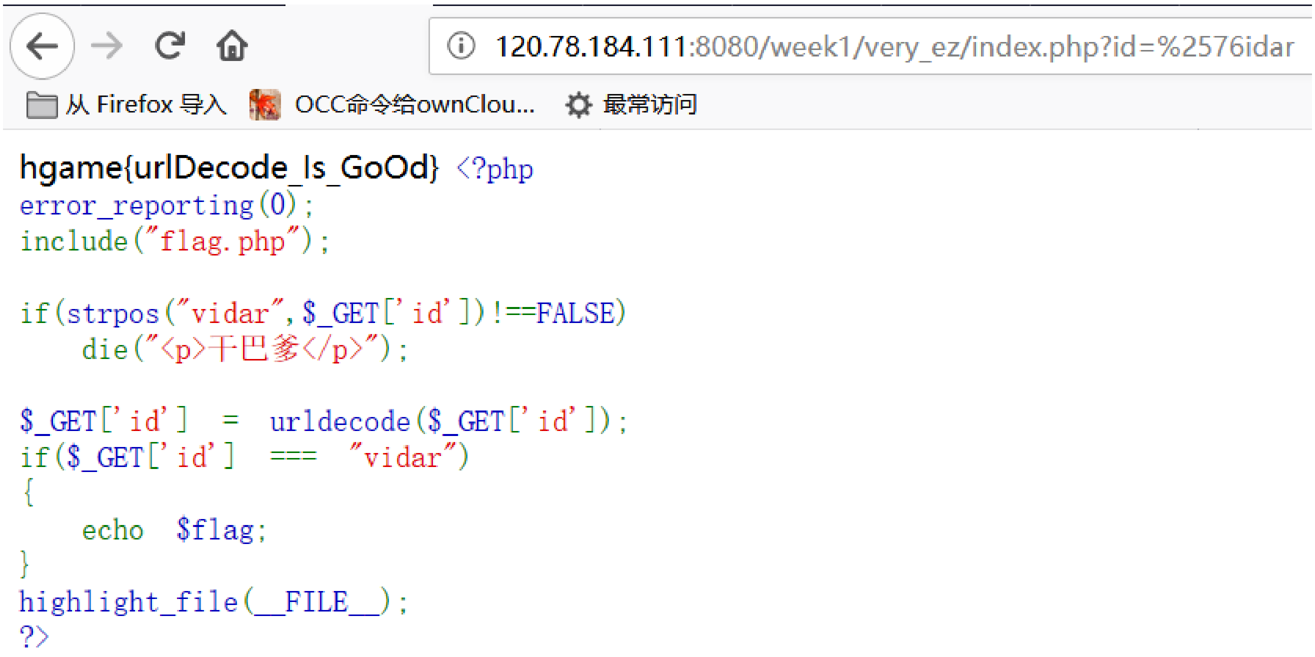
- 这题的重点是在两个 `if` 判断上
- 要跳过第一个 `die()` 得让 `strpos()===FALSE`，也就是不出现字符串 `vidar`
- 但是后面又要求字符串 `vidar`，得利用url编码
- 把 `vidar` 这个字符串丢进在线url编码的地方发现并没有任何变化，于是只能手动查表，得知 `v` 对应的是 `%76`
- 于是传入 `id=%76idar`



干巴爹

我：？？？？？？

- 查了下资料发现需要二次编码，得知 `%` 对应的是 `%25`
- 这时传入 `id=%2576idar`



```
hgame{urlDecode_Is_GoOd} <?php
error_reporting(0);
include("flag.php");

if(strpos("vidar",$_GET['id'])!==FALSE)
    die("<p>干巴爹</p>");

$_GET['id']  =  urldecode($_GET['id']);
if($_GET['id']  ===  "vidar")
{
    echo  $flag;
}
highlight_file(__FILE__);
?>
```

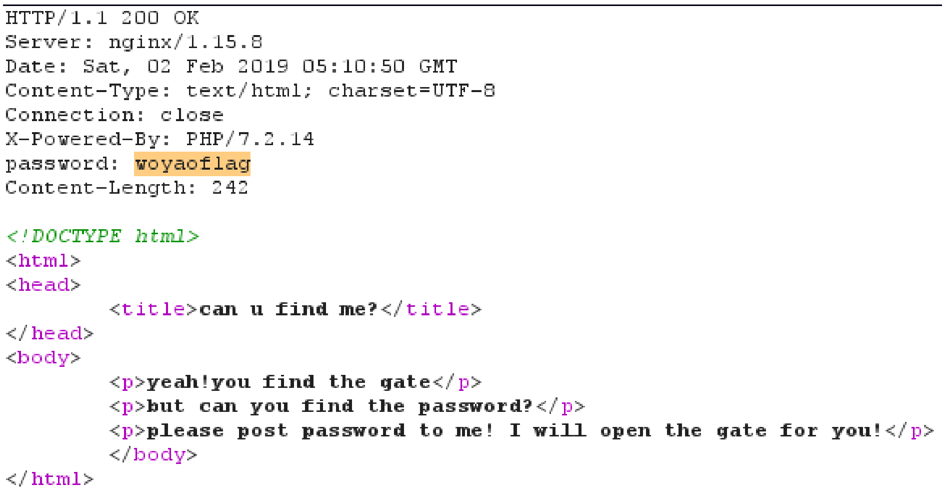
成功得到flag

can u find me?

- 题目地址
- 根据描述

> 为什么不问问神奇的十二姑娘和她的小伙伴呢

- 使用F12查看源代码，得知入口在`f12.php`
- ~~算了F12这么难用还是用burp吧~~



```
HTTP/1.1 200 OK
Server: nginx/1.15.8
Date: Sat, 02 Feb 2019 05:10:50 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.2.14
password: woyaoflag
Content-Length: 242

<!DOCTYPE html>
<html>
<head>
        <title>can u find me?</title>
</head>
<body>
        <p>yeah!you find the gate</p>
        <p>but can you find the password?</p>
        <p>please post password to me! I will open the gate for you!</p>
        </body>
</html>
```

- 查看请求，发现`password`藏在`header`里
- 按照要求，`POST`发送`password`，得到flag

~~偷懒不截图w~~

RE

brainfxxker

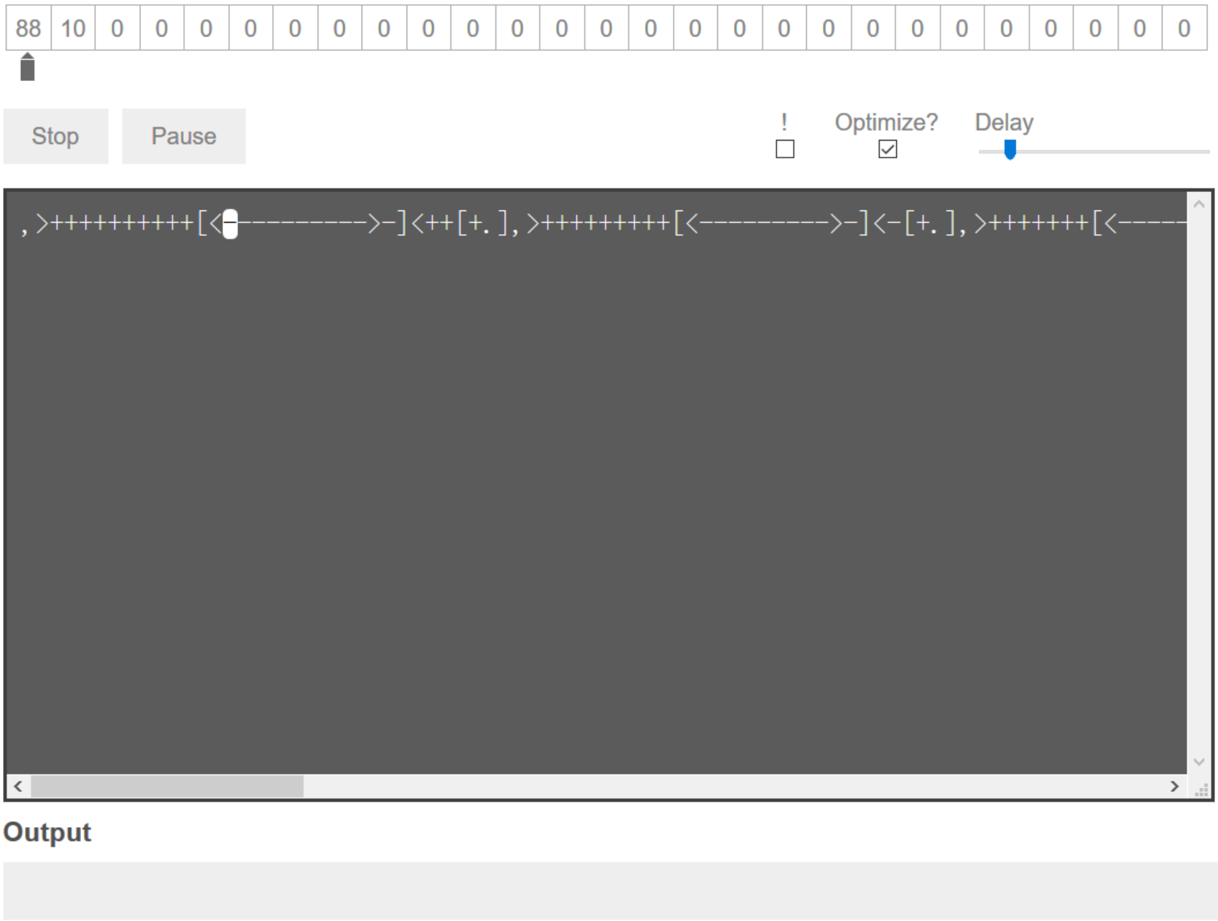
[题目地址]

- 下载文件打开，
- 看到了一段

```
,>++++++++++[<---------->-]<++[+.],>+++++++++[<--------->-]<-[+.],>+++++++[<------->-]<---
[+.],>++++++[<------>-]<+++[+.],>++++++++[<---------->-]<++[+.],>++++++++++[<---------->-]<-
-[+.],>++++++++++[<-------->-]<-----[+.],>++++++++++[<---------->-]<+[+.],>+++++++++[<------
-->-]<---[+.]
```

~~这都是什么啊...~~
查了一下...找到了一个项目

- [brainfuck-visualizer]
- 然后看到有九个`,`，意味着有九个输入
- 猜想，`brainfxxk`也正好是九个字符
- 首先输入了`b`



88	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Optimize? ☑

```
,>++++++++++[<---------->-]<++[+.],>+++++++++[<--------->-]<-[+.],>+++++++[<----
```

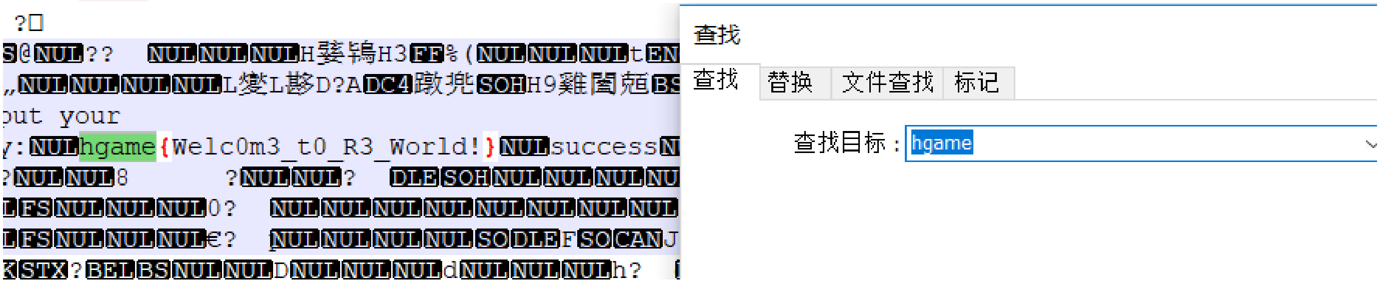
- 经过愉快的运行，没有输出，看起来第一位是正确的
- 然后再尝试
- 最终得到

```
bR4!NfUcK
```

- 看起来加上`hgame{}`就好了

HelloRe

[题目地址]()
* 下回来用文本方式打开
* 搜索`hgame`

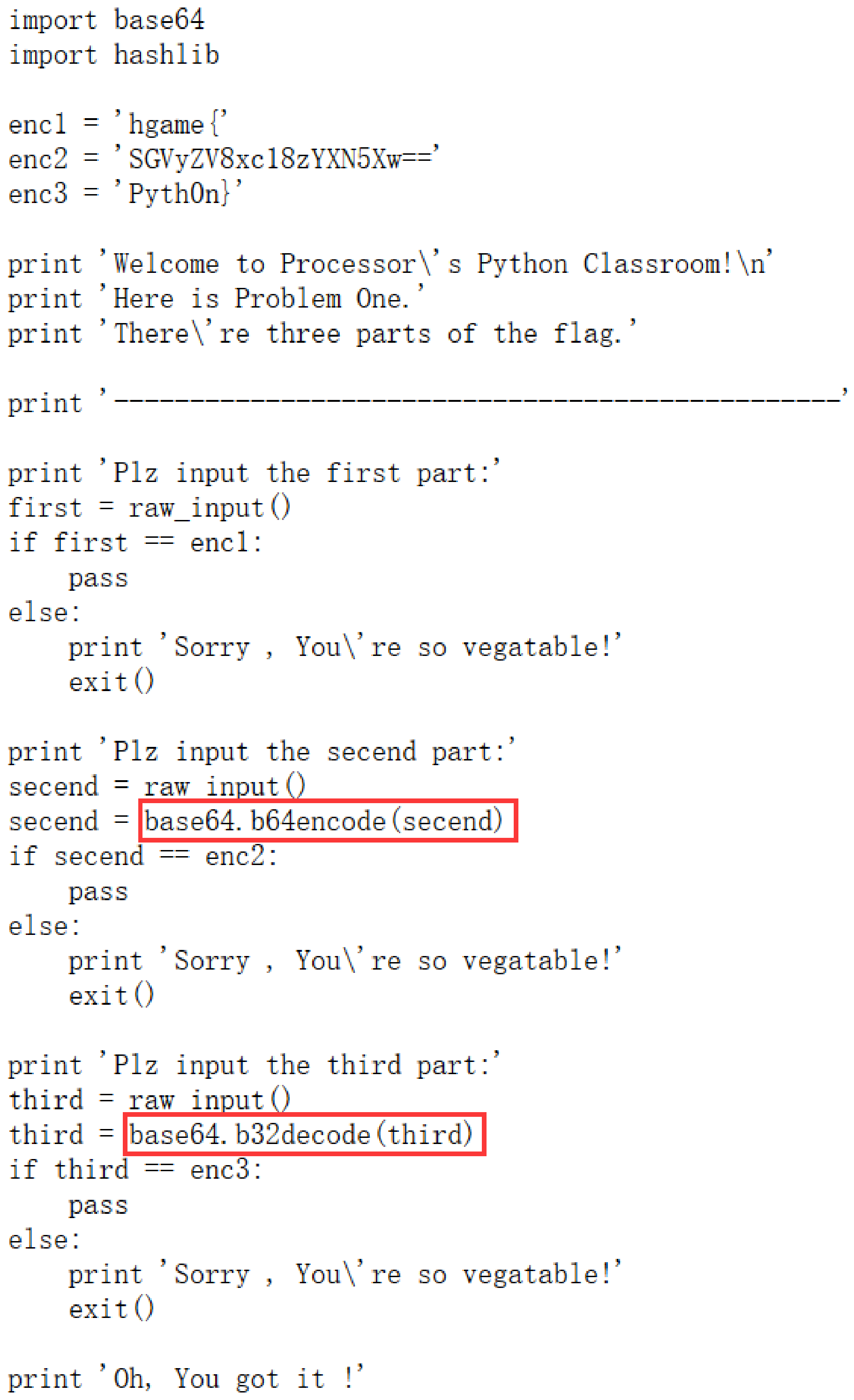


```
 ?□
S@NUL??  NULNULNULH嫠鴇H3FF%(NULNULNULtEN
„NULNULNULNULL夒L髟D?ADC4躑兆SOHH9雞闔菦BS
put your
y:NULhgame{Welc0m3_t0_R3_World!}NULsuccessN
?NULNUL8      ?NULNUL?  DLESOHNULNULNULNU
LFSNULNULNUL0?  NULNULNULNULNULNULNULNUL
LFSNULNULNUL€?  NULNULNULNULSODLEFSOCANJ
KSTX?BELBSNULNULDNULNULNULdNULNULNULh?
```

查找目标：hgame

Pro的Python教室(一)

[题目地址]()



```
import base64
import hashlib

enc1 = 'hgame{'
enc2 = 'SGVyZV8xc18zYXN5Xw=='
enc3 = 'Pyth0n}'

print 'Welcome to Processor\'s Python Classroom!\n'
print 'Here is Problem One.'
print 'There\'re three parts of the flag.'

print '------------------------------------------------'

print 'Plz input the first part:'
first = raw_input()
if first == enc1:
    pass
else:
    print 'Sorry , You\'re so vegatable!'
    exit()

print 'Plz input the secend part:'
secend = raw_input()
secend = base64.b64encode(secend)
if secend == enc2:
    pass
else:
    print 'Sorry , You\'re so vegatable!'
    exit()

print 'Plz input the third part:'
third = raw_input()
third = base64.b32decode(third)
if third == enc3:
    pass
else:
    print 'Sorry , You\'re so vegatable!'
    exit()

print 'Oh, You got it !'
```

* 看起来标红两处是重点
* 然鹅实际上只要把 `enc2` 进行一次 `base64` 解码就ok了

```
Here_1s_3asy_
```

- 然后拼接三段就好了，得到flag

```
hgame{Here_1s_3asy_Pyth0n}
```

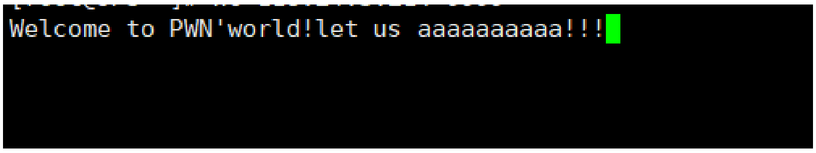
PWN

---

aaaaaaaaaa

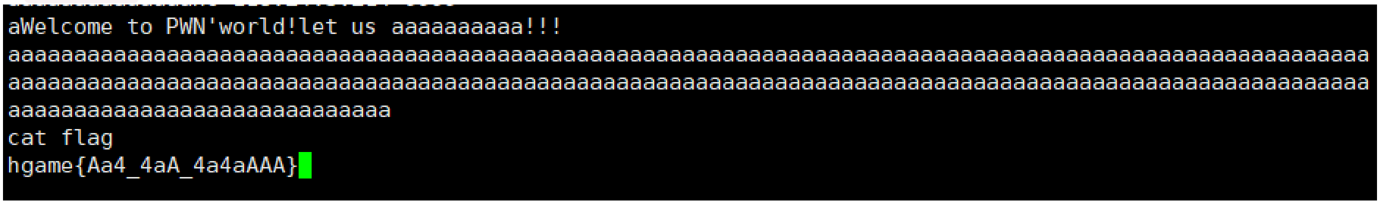
```
pwn很简单的，a上去就完事了 nc 118.24.3.214 9999
```

[题目地址]()
* 用题目描述里的nc去连接



```
Welcome to PWN'world!let us aaaaaaaaaa!!!
```

* 然后疯狂`a`，就会弹shell
* `cat flag`



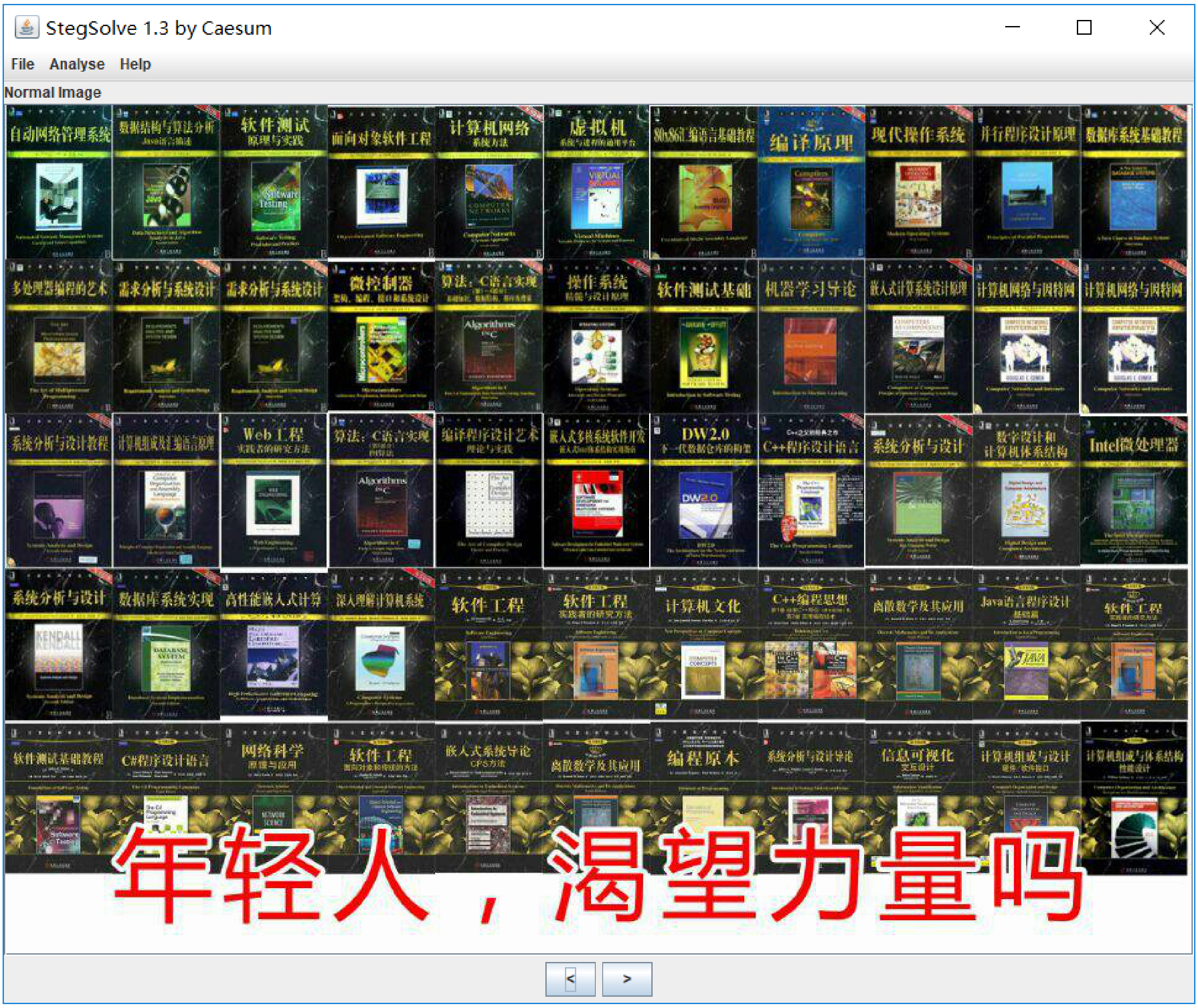
```
aWelcome to PWN'world!let us aaaaaaaaaa!!!
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaa
cat flag
hgame{Aa4_4aA_4a4aAAA}
```

MISC

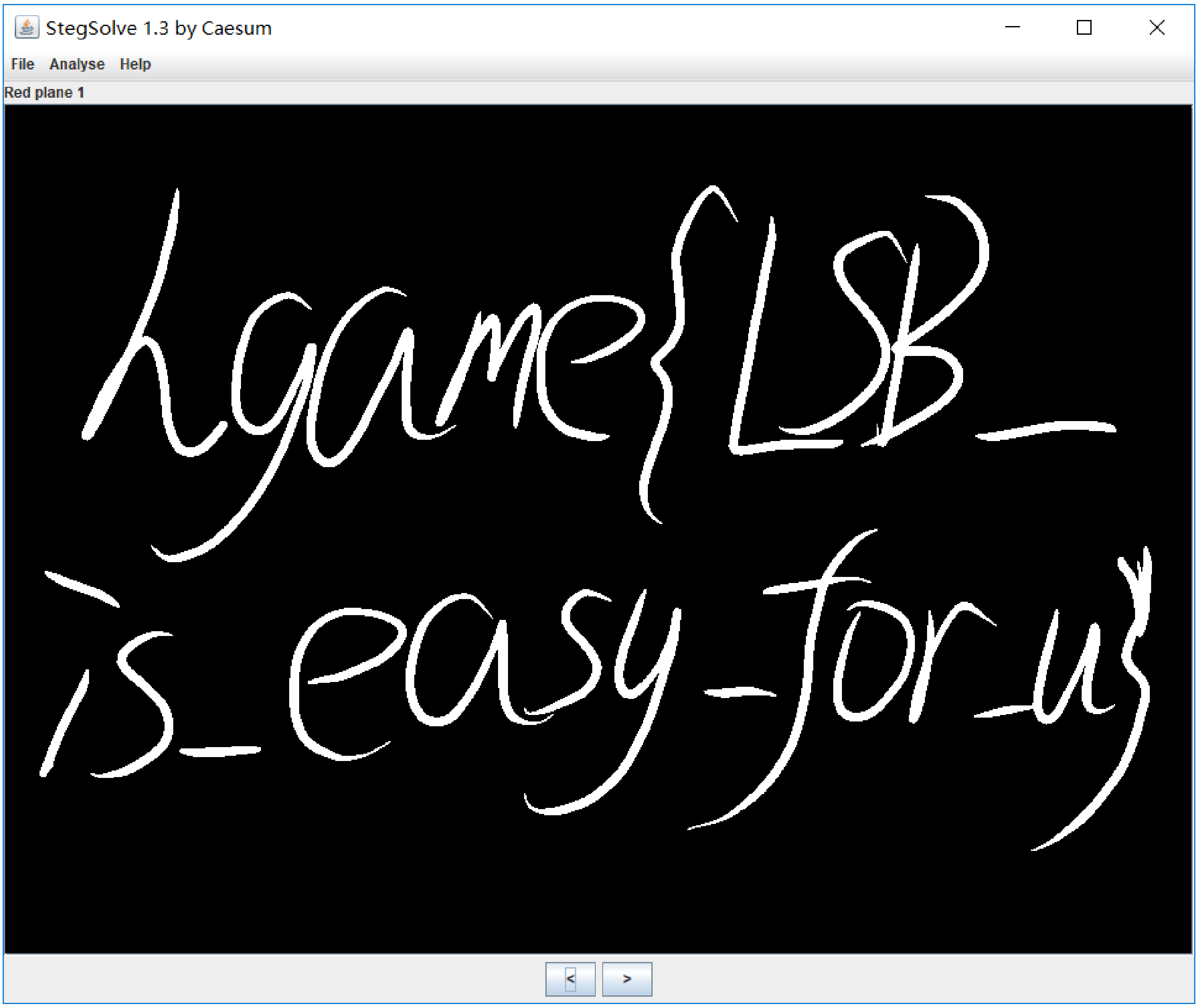
Hidden Image in LSB

```
Here are some magic codes which can hide information in an ordinary picture, can you extract
the hidden image in the provided picture?
其实本来想让大家写写代码，后来干脆就送分了
有个神器叫 stegsolve，利用它可以直接提取本题 flag
```

[题目地址]()
* 按照hint，用StegSolve打开图片



* 点击下方的箭头直至红色低通部分

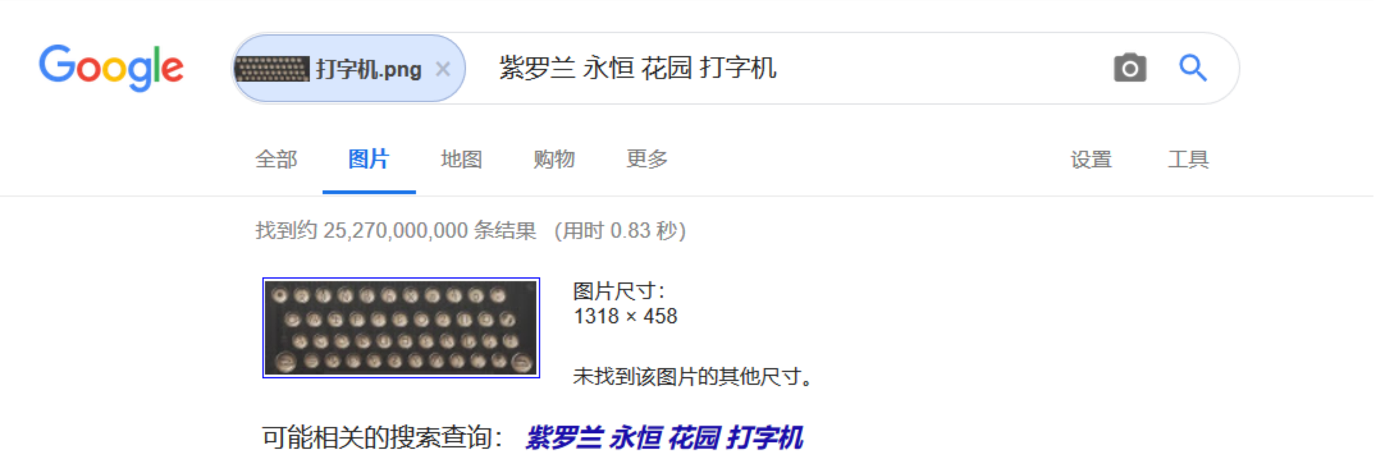


flag到手...

打字机

```
Aris(划掉)牌打字机，时尚时尚最时尚~
hint:谷歌有个以图搜图功能很不错，百度识图好垃圾的。。。
```

题目地址
* 下载得到图片，按照hint去识图



找到约 25,270,000,000 条结果 （用时 0.83 秒）

图片尺寸：
1318 × 458

未找到该图片的其他尺寸。

可能相关的搜索查询：**紫罗兰 永恒 花园 打字机**

* 找着找着就能找到相关资料了

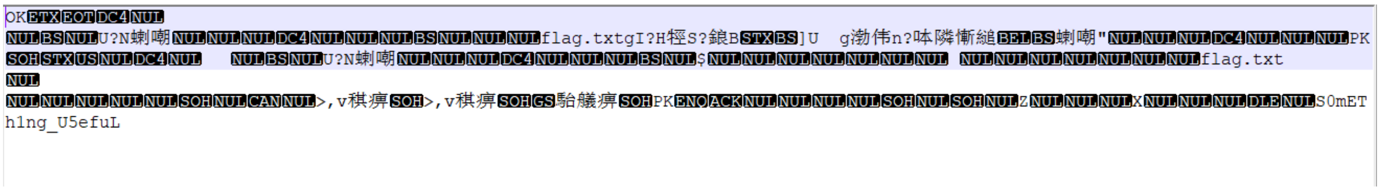
```
https://www.bilibili.com/read/cv142910?from=articleDetail
```

- 按照题主的解释对应得到flag

```
hgame{My_vi0let_tyPewRiter}
```

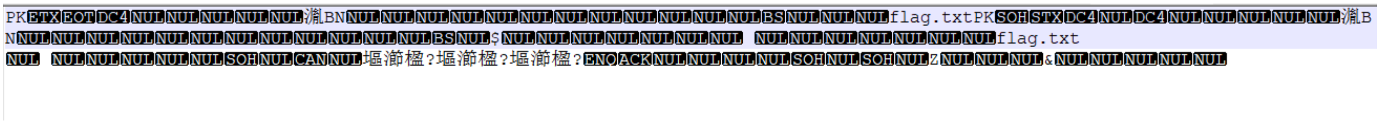
Broken Chest

[题目地址]
* 把压缩包下回来，发现已经损坏了。
* 用文本方式打开压缩包



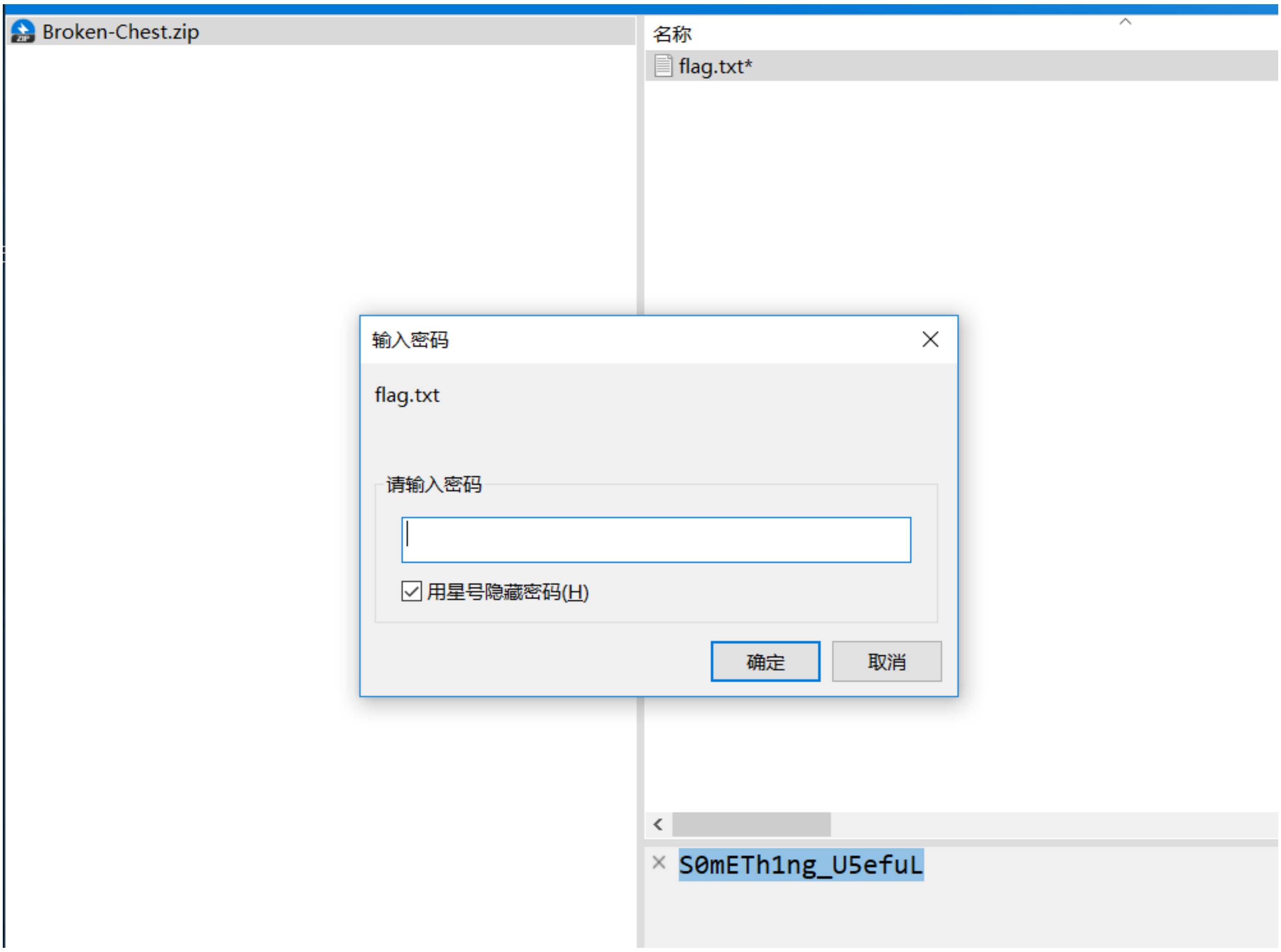
```
OKETXEOTDC4NUL
NULBSNULU?N蝲嘲NULNULNULDC4NULNULNULBSNULNULNULflag.txtgI?H桎S?鍡BSTXBS]U  g渤伟n?味隣慚縋BELBS蝲嘲"NULNULNULDC4NULNULNULPK
SOHSTXUSNULDC4NUL    NULBSNULU?N蝲嘲NULNULNULDC4NULNULNULBSNUL$NULNULNULNULNULNULNUL  NULNULNULNULNULNULNULflag.txt
NUL
NULNULNULNULNULSOHNULCANNUL>,v祺痹SOH>,v祺痹SOHGS駘艤痹SOHPKENQACKNULNULNULNULSOHNULSOHNULZNULNULNULXNULNULNULDLENULS0mET
h1ng_U5efuL
```

* 发现尾部似乎有一段`S0mETh1ng_U5efuL`可能有用，加hgame{}后提交发现不是flag
* 自己新建一个`flag.txt`并且压缩成`zip`
* 用文本方式打开



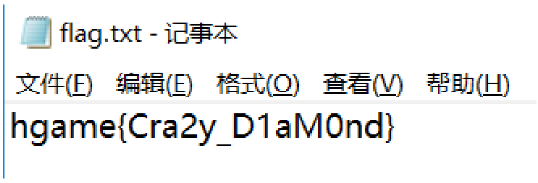
```
PKETXEOTDC4NULNULNULNULNUL淵BNNULNULNULNULNULNULNULNULNULNULNULNULBSNULNULNULflag.txtPKSOHSTXDC4NULDC4NULNULNULNULNUL淵B
NNULNULNULNULNULNULNULNULNULNULNULNULBSNUL$NULNULNULNULNULNULNUL  NULNULNULNULNULNULNULflag.txt
NUL  NULNULNULNULNULSOHNULCANNUL堰澌楹?堰澌楹?堰澌楹?ENQACKNULNULNULNULSOHNULSOHNULZNULNULNUL&NULNULNULNULNUL
```

* 发现就最开头的`PK`被更改成`OK`
* 尝试更改回`PK`，重新打开，成了！



S0mETh1ng_U5efuL

* 发现需要密码，而注释里又正好有之前看到的那段，拿来试一下，成功得到flag

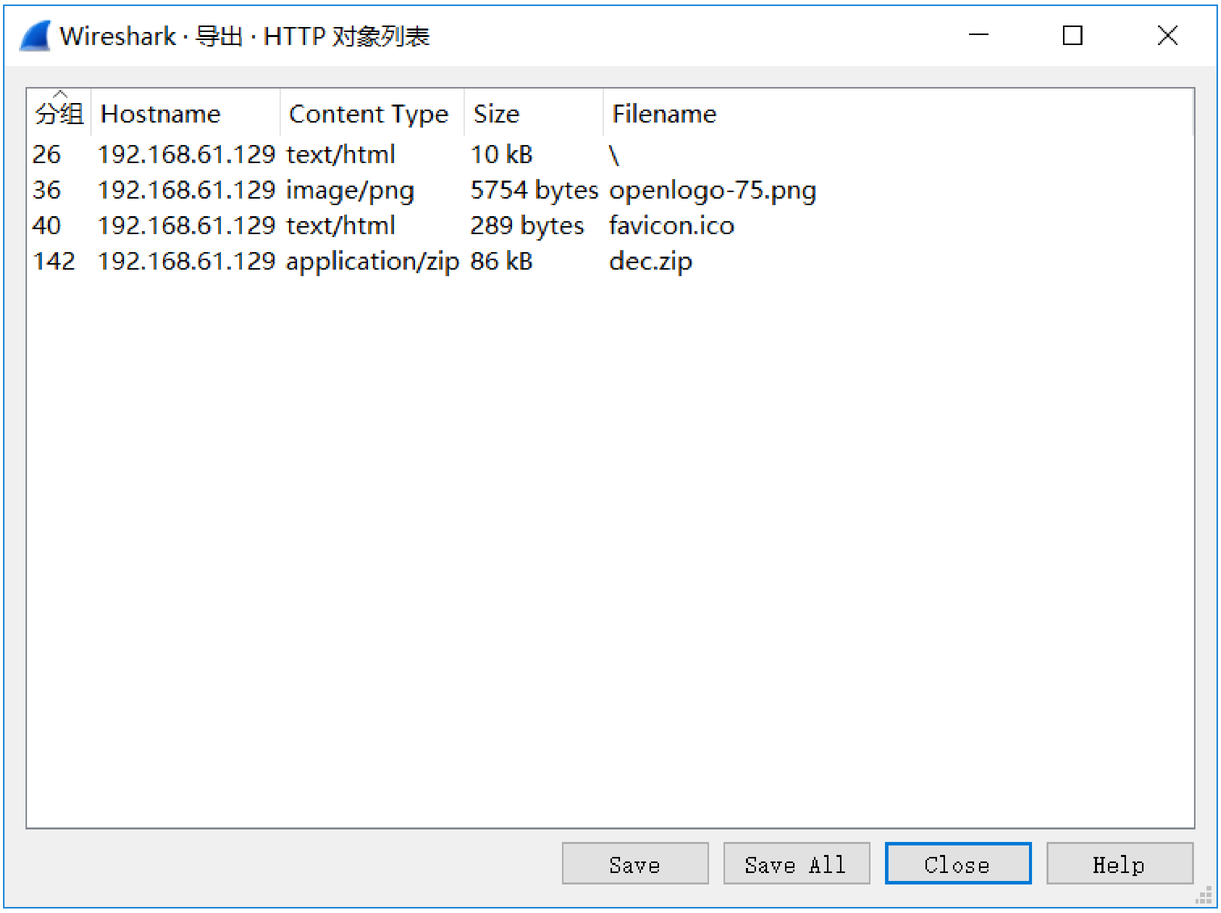


hgame{Cra2y_D1aM0nd}

Try

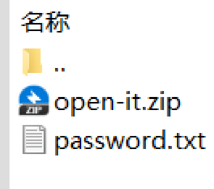
题目地址

* 下载后得到一个wireshark的抓包文件
* 用wireshark打开



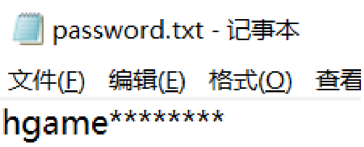
分组	Hostname	Content Type	Size	Filename
26	192.168.61.129	text/html	10 kB	\
36	192.168.61.129	image/png	5754 bytes	openlogo-75.png
40	192.168.61.129	text/html	289 bytes	favicon.ico
142	192.168.61.129	application/zip	86 kB	dec.zip

* 查看http对象里发现了有一个`dec.zip`似乎很可疑，导出预备



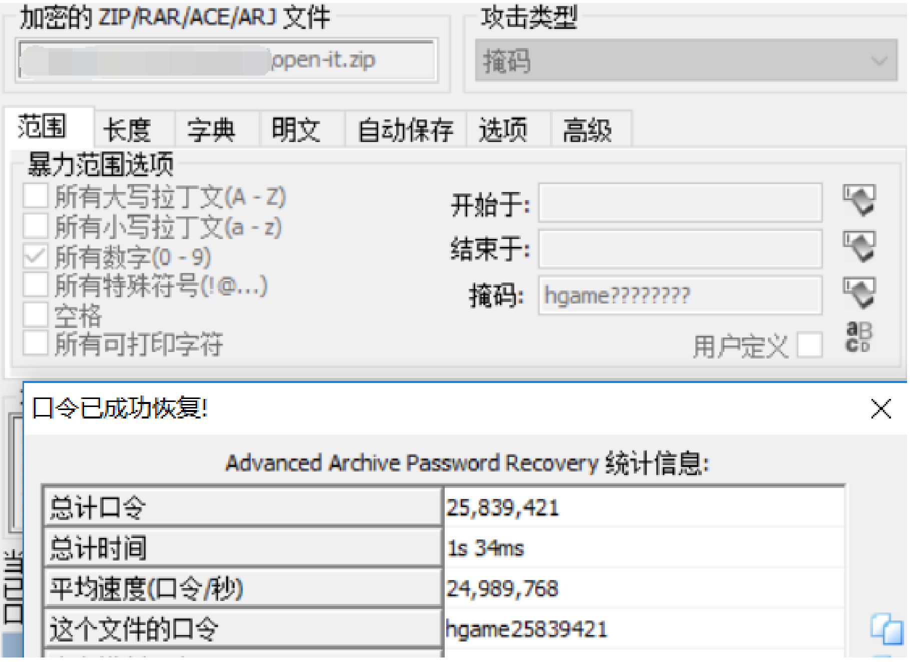
名称
..
open-it.zip
password.txt

* 发现里面有这些文件，其中`password.txt`提醒了`hgame********`



hgame********

* 尝试打开`open-it.zip`
* 里面是一个加密的图片，这时候需要工具(`Advanced Archive Password Recovery`)来跑压缩包的密码



加密的 ZIP/RAR/ACE/ARJ 文件 open-it.zip

攻击类型 掩码

范围 | 长度 | 字典 | 明文 | 自动保存 | 选项 | 高级

暴力范围选项

□ 所有大写拉丁文(A - Z)
□ 所有小写拉丁文(a - z)
☑ 所有数字(0 - 9)
□ 所有特殊符号(!@...)
□ 空格
□ 所有可打印字符

开始于:

结束于:

掩码: hgame????????

用户定义 □

口令已成功恢复!

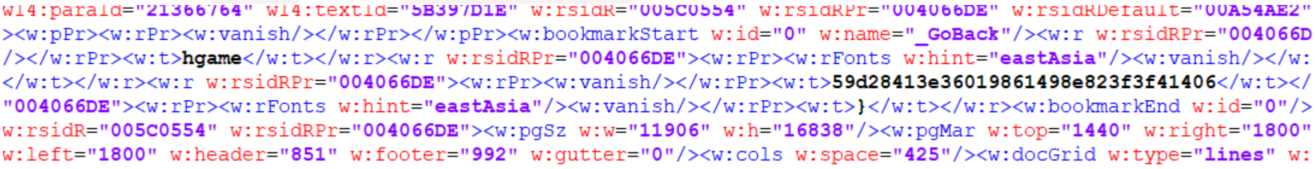
Advanced Archive Password Recovery 统计信息:

总计口令	25,839,421
总计时间	1s 34ms
平均速度(口令/秒)	24,989,768
这个文件的口令	hgame25839421

* 因为有前面的提示，这里使用掩码爆破密码，很快就得到了密码，解压后得到一张`1.jpg`
* 然后用`binwalk`可以发现里面有一个`137DD.zip`同时带着`1.docx`

```
binwalk -e 1.jpg
```

- 分离得到1.docx，打开发现里面一片空白什么也没有
- 用压缩包方式打开`1.docx`，然后在`word/document.xml`里有了收获



```
w14:paraId="21366764" w14:textId="5B397D1E" w:rsidR="005C0554" w:rsidRPr="004066DE" w:rsidRDefault="00A54AE2"
><w:pPr><w:rPr><w:vanish/></w:rPr></w:pPr><w:bookmarkStart w:id="0" w:name="_GoBack"/><w:r w:rsidRPr="004066D
/></w:rPr><w:t>hgame</w:t></w:r><w:r w:rsidRPr="004066DE"><w:rPr><w:rFonts w:hint="eastAsia"/><w:vanish/></w:
</w:t></w:r><w:r w:rsidRPr="004066DE"><w:rPr><w:vanish/></w:rPr><w:t>59d28413e36019861498e823f3f41406</w:t></
"004066DE"><w:rPr><w:rFonts w:hint="eastAsia"/><w:vanish/></w:rPr><w:t>}</w:t></w:r><w:bookmarkEnd w:id="0"/>
w:rsidR="005C0554" w:rsidRPr="004066DE"><w:pgSz w:w="11906" w:h="16838"/><w:pgMar w:top="1440" w:right="1800"
w:left="1800" w:header="851" w:footer="992" w:gutter="0"/><w:cols w:space="425"/><w:docGrid w:type="lines" w:
```

- flag到手

```
hgame{59d28413e36019861498e823f3f41406}
```

CRYPTO

MIX

```
--.../....-/....-/-.../--.../...--/...../..-./-..../-../-..../..-./--.../----./....-/....-/-
-.../.----/-..../-.../--.../-.../-..../..---/...../.----/-..../-..../...--/....-/...--/----
-/-..../...../--.../-..
```

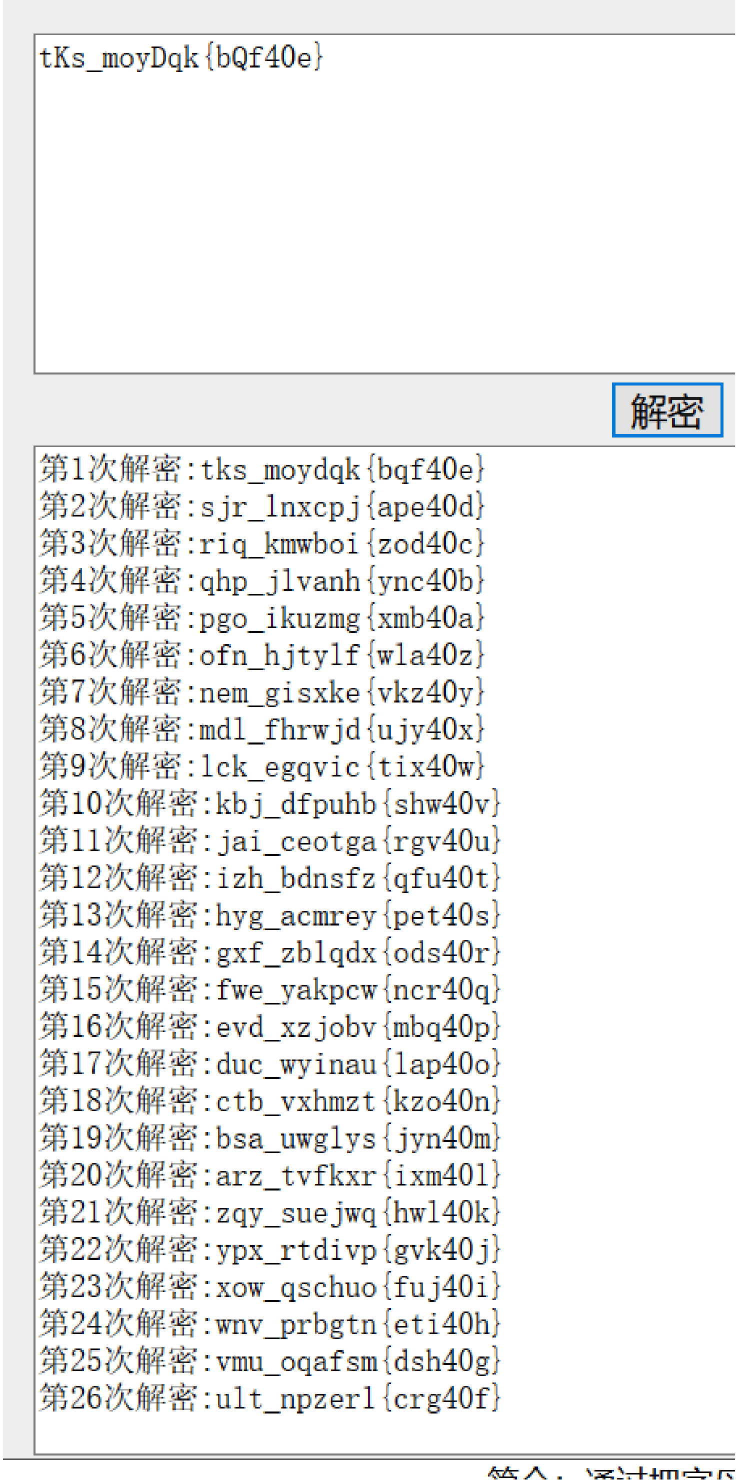
- 目测有摩斯电码加密，尝试解密一次，得到一串十六进制
  在线解密

```
744B735F6D6F7944716B7B6251663430657D
```

- 对照ASCII码表进行翻译，得到

```
tKs_moyDqk{bQf40e}
```

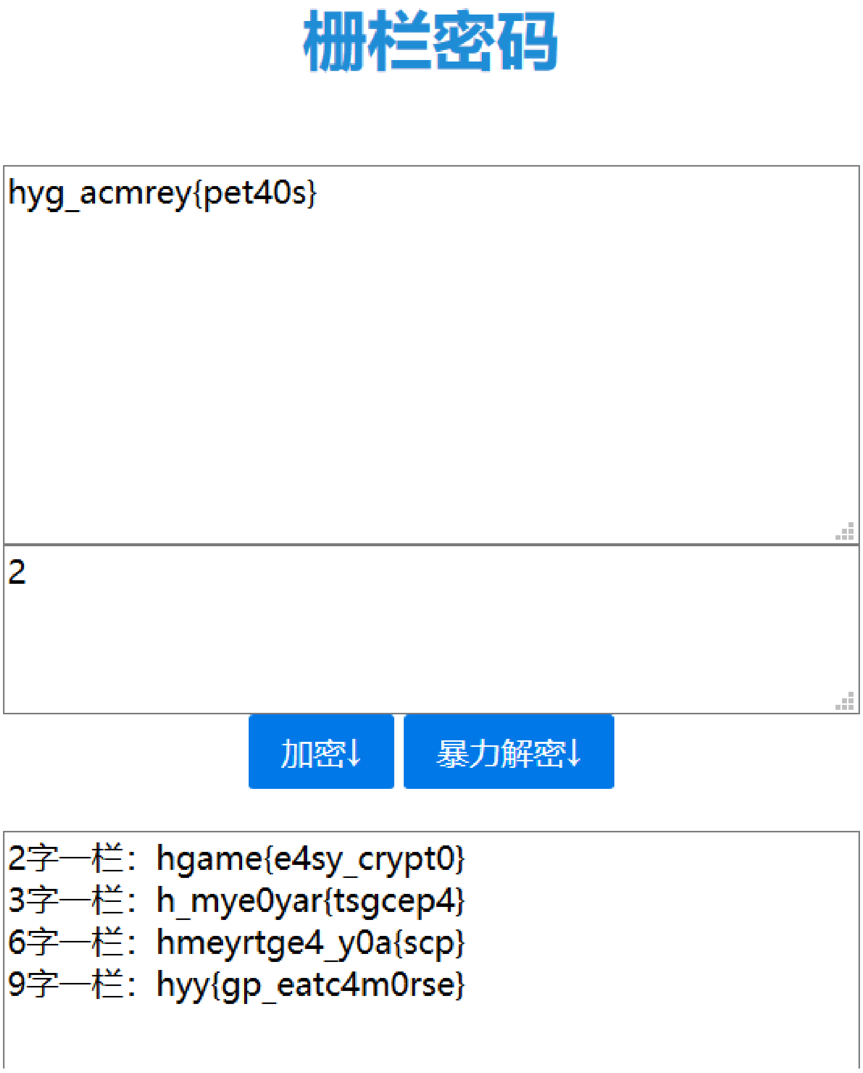
- 已经出现了`` {``} ``等，可以猜测是凯撒密码，尝试解密



```
tKs_moyDqk{bQf40e}
```

```
第1次解密:tks_moydqk{bqf40e}
第2次解密:sjr_lnxcpj{ape40d}
第3次解密:riq_kmwboi{zod40c}
第4次解密:qhp_jlvanh{ync40b}
第5次解密:pgo_ikuzmg{xmb40a}
第6次解密:ofn_hjtylf{wla40z}
第7次解密:nem_gisxke{vkz40y}
第8次解密:mdl_fhrwjd{ujy40x}
第9次解密:lck_egqvic{tix40w}
第10次解密:kbj_dfpuhb{shw40v}
第11次解密:jai_ceotga{rgv40u}
第12次解密:izh_bdnsfz{qfu40t}
第13次解密:hyg_acmrey{pet40s}
第14次解密:gxf_zblqdx{ods40r}
第15次解密:fwe_yakpcw{ncr40q}
第16次解密:evd_xzjobv{mbq40p}
第17次解密:duc_wyinau{lap40o}
第18次解密:ctb_vxhmzt{kzo40n}
第19次解密:bsa_uwglys{jyn40m}
第20次解密:arz_tvfkxr{ixm40l}
第21次解密:zqy_suejwq{hwl40k}
第22次解密:ypx_rtdivp{gvk40j}
第23次解密:xow_qschuo{fuj40i}
第24次解密:wnv_prbgtn{eti40h}
第25次解密:vmu_oqafsm{dsh40g}
第26次解密:ult_npzerl{crg40f}
```

- 取第13个密码，`hyg_acmrey{pet40s}`，进行栅栏解密，栅格数2



hyg_acmrey{pet40s}

2

2字一栏：hgame{e4sy_crypt0}
3字一栏：h_mye0yar{tsgcep4}
6字一栏：hmeyrtge4_y0a{scp}
9字一栏：hyy{gp_eatc4m0rse}

- 得到flag

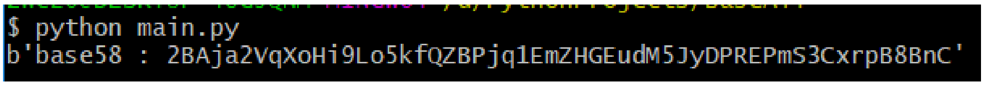
```
hgame{e4sy_crypt0}
```

上述在线解密网址

Base全家

题目地址
* 根据python的base解码失败后会报错，进行尝试，最终得到如下python代码

```
import base64
enc = ...#那段太长了，贴上来就死了..
print(base64.b32decode(base64.b64decode(base64.b64decode(base64.b64decode(base64.b32decode(base64.b16decode(base64.b16decode(base64.b16decode(base64.b16decode(base64.b64decode(base64.b16decode(base64.b64decode(base64.b32decode(base64.b16decode(base64.b32decode(base64.b16decode(base64.b16decode(base64.b16decode(base64.b64decode(base64.b64decode(enc))))))))))))))))))))
```

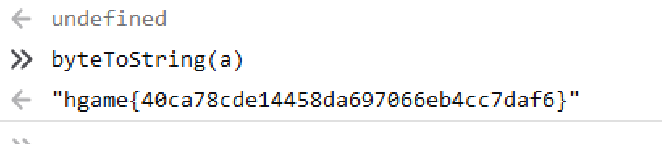


```
$ python main.py
b'base58 : 2BAja2VqXoHi9Lo5kfQZBPjq1EmZHGEudM5JyDPREPmS3CxrpB8BnC'
```

* 得到一段似乎是base58的字符串

```
2BAja2VqXoHi9Lo5kfQZBPjq1EmZHGEudM5JyDPREPmS3CxrpB8BnC
```

- 找到一篇文章用js进行解密
  传送门

  ```
  ← undefined
  » byteToString(a)
  ← "hgame{40ca78cde14458da697066eb4cc7daf6}"
  ```

- 最终解密得到flag

```
hgame{40ca78cde14458da697066eb4cc7daf6}
```