

hgame第一周wp

id: Roc826

WEB 部分

1. Who eat my flag

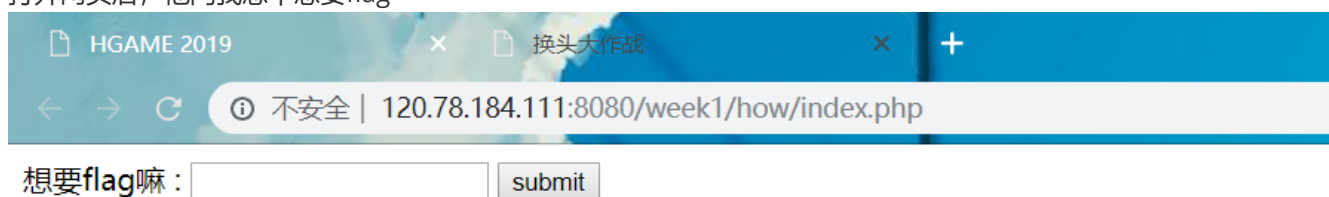
一开始想了好久都没有对上mki的脑电波。。。后来问了一下学长，学长问我有没有用过linux写过东西，然后就想到linux用vim写文件的时候意外退出后会留下一个.swp文件，试着去访问这个文件果然得到了.index.html.swp, 然后把它放到虚拟机里,执行这条命令 `vi -r index.html` 得到

```
File Edit View Search Terminal Help
<!DOCTYPE HTML>
<html>
  <head>
    <title>谁吃了我的flag??</title>
  </head>
  <body>
    <p>damn...hgame2019 is coming soon, but the stupid Mki haven't finished his web-challenge...</p>
    <br>
    <p>fine, nothing serious, just give you flag this time...</p>
    <br>
    <p>the flag is hgame{3eek_diSc10Sure_fRom+wEbsit@}</p>
  </body>
</html>
~
~
~
~
```

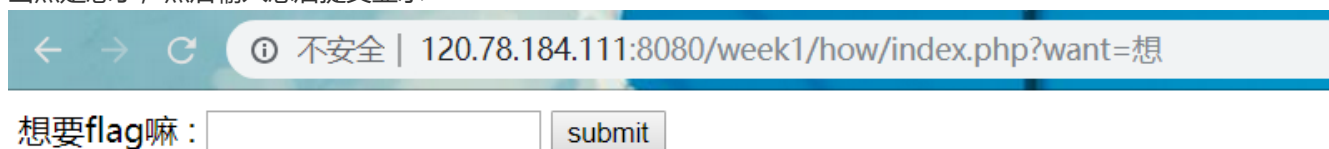
把完整的flag复制出来就可以了

2. 换头大作战

打开网页后，他问我想不想要flag

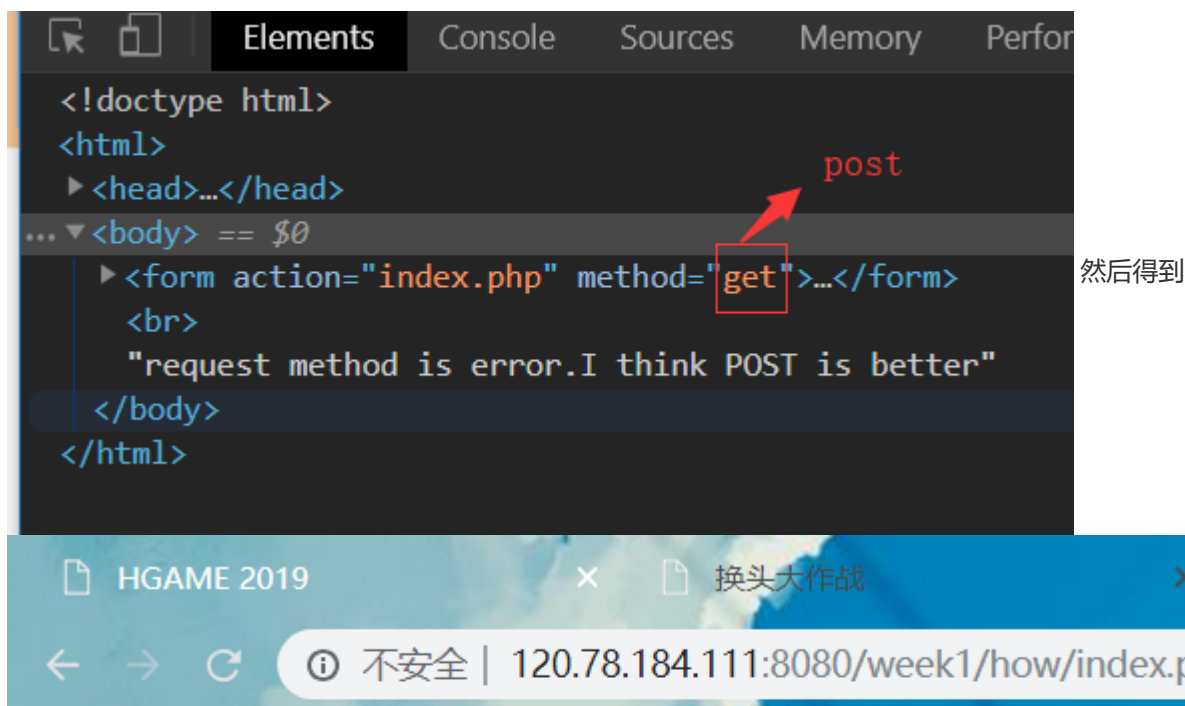


当然是想了，然后输入想后提交显示



request method is error.I think POST is better

于是就把表单发送的方式改成post



想要flag嘛:

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

X-Forward-For表示请求端的真实ip，经过代理服务器的时候会把代理服务器的ip地址增加上去，一般来说第一个就是客户端的ip地址，所以我只需要在请求头中添加X-Forward-For:127.0.0.1即可，所以在这里我用burp截取发送的请求添加这一条

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Suite Community Edition v1.7.36 - Temporary Project

Intercept HTTP history WebSockets history Options

Request to http://120.78.184.111:8080

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST /week1/how/index.php HTTP/1.1
Host: 120.78.184.111:8080
Content-Length: 14
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Origin: http://120.78.184.111:8080
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://120.78.184.111:8080/week1/how/index.php?want=%E6%83%B3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7
Cookie: admin=0
Connection: close
X-Forwarded-For: 127.0.0.1

want=%E6%83%B3

注意：这里也需要将表单发送的方式改为post 得到



想要flag嘛： submit

https://www.wikiwand.com/en/User_agent
please use Waterfox/50.0

这里告诉我们要用Waterfox/50.0这个版本的浏览器，我一开始还真去下了waterfox。。。后来发现好像应该不是这样做的，应该把请求头上的浏览器版本改成Waterfox/50.0 所以

Intercept HTTP history WebSockets history Options

Request to http://120.78.184.111:8080

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST /week1/how/index.php HTTP/1.1
Host: 120.78.184.111:8080
Content-Length: 14
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Waterfox/50.0
Origin: http://120.78.184.111:8080
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://120.78.184.111:8080/week1/how/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7
Cookie: admin=0
Connection: close
X-Forward-For: 127.0.0.1

want=%E6%83%B3

然后得到



想要flag嘛: submit

再在

https://www.wikiwand.com/en/HTTP_referer
the requests should referer from www.bilibili.com

请求头添加Referer:www.bilibili.com

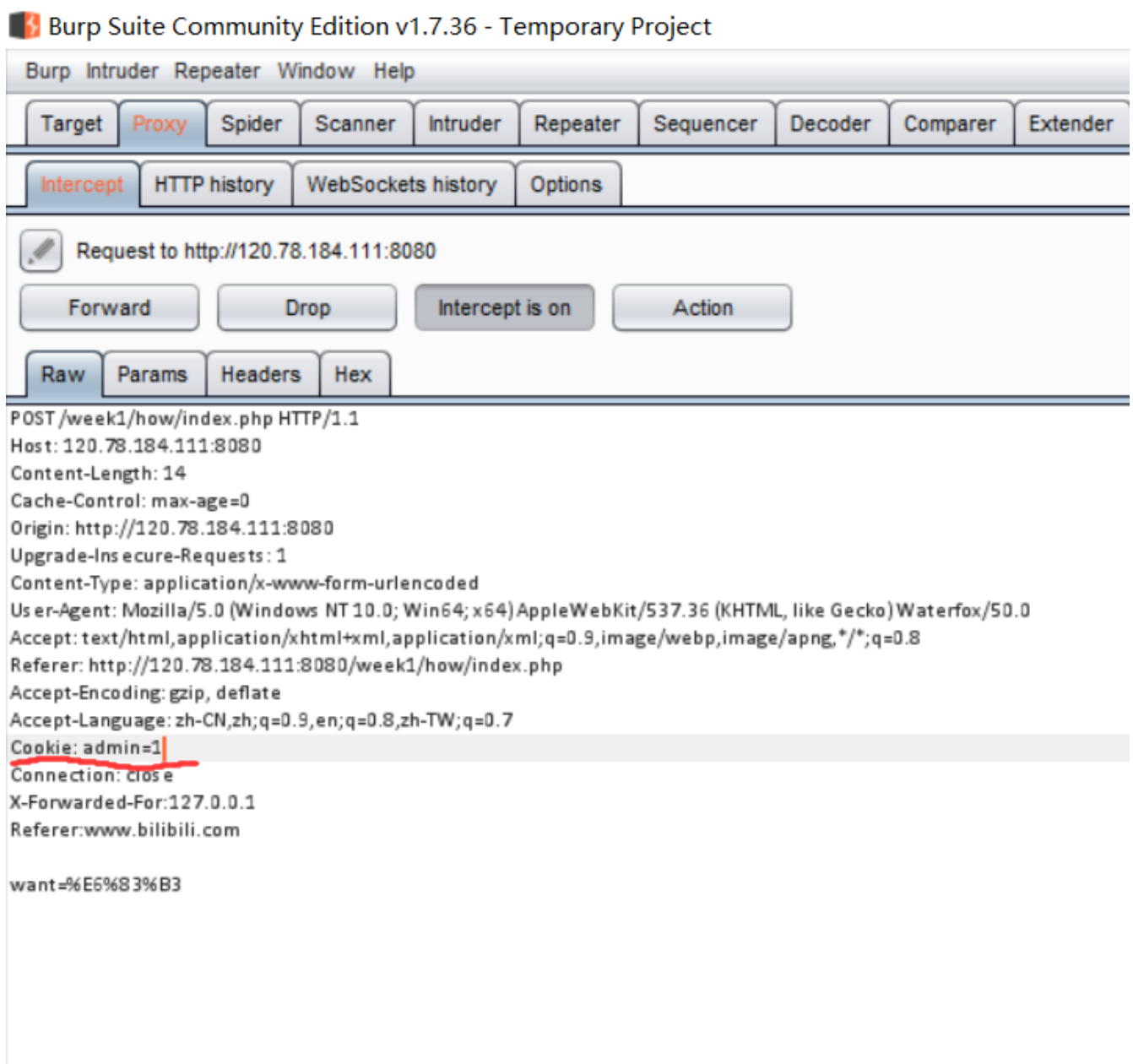


想要flag嘛: submit

检查发现cookie的

https://www.wikiwand.com/en/HTTP_cookie
you are not admin

admin字段的值为0, 我们把它改成1

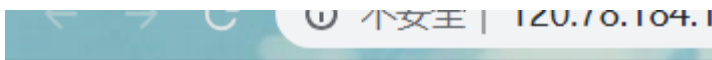




提交后得到flag 想要flag嘛: submit

hgame{hTTP_HeaDeR_iS_Ez}

3.very easy web



```
<?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__);
?>
```

观察代码我们可以发现我们需要传入的id值

为'vidar'urlencode一次后的值，但由于浏览器自动会给url进行urldecode一次，所以我们在这里要将'vidar'urlencode两次后传入 第一次得到%76%69%64%61%72 再将这个值进行url编码得到%25%37%36%25%36%39%25%36%34%25%36%31%25%37%32 将这个值传入，得到flag

```
<?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__);
?>
```

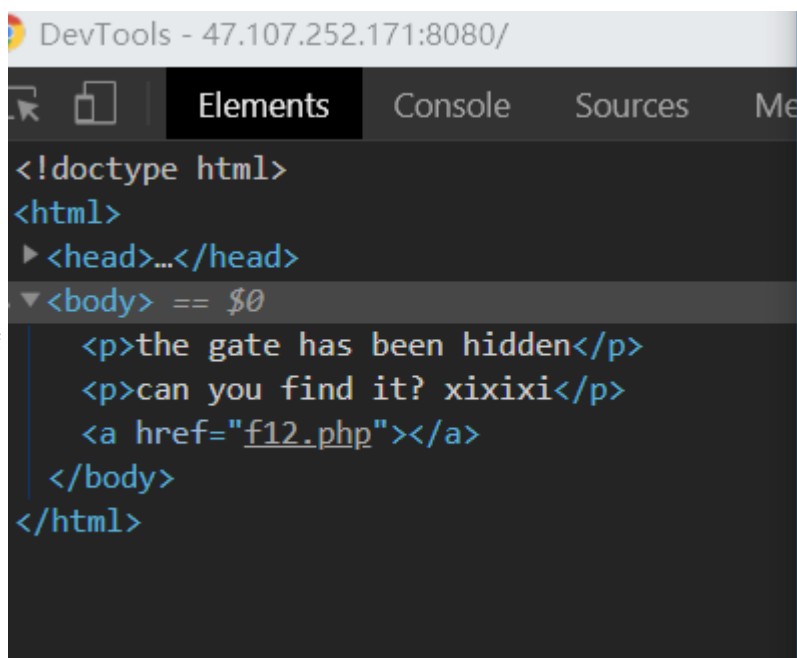
或者我们可以自己写一个表单

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Document</title>
</head>
<body>
    <form action="http://120.78.184.111:8080/week1/very_ez/index.php" method="get">
        <input type='text' name=id>
        <button type="submit"></button>
    </form>
</body>
</html>
```

这样我们只需要urlencode一次后提交即可

4.can u find me

第一个页面按f12可以看到网页上有个链接

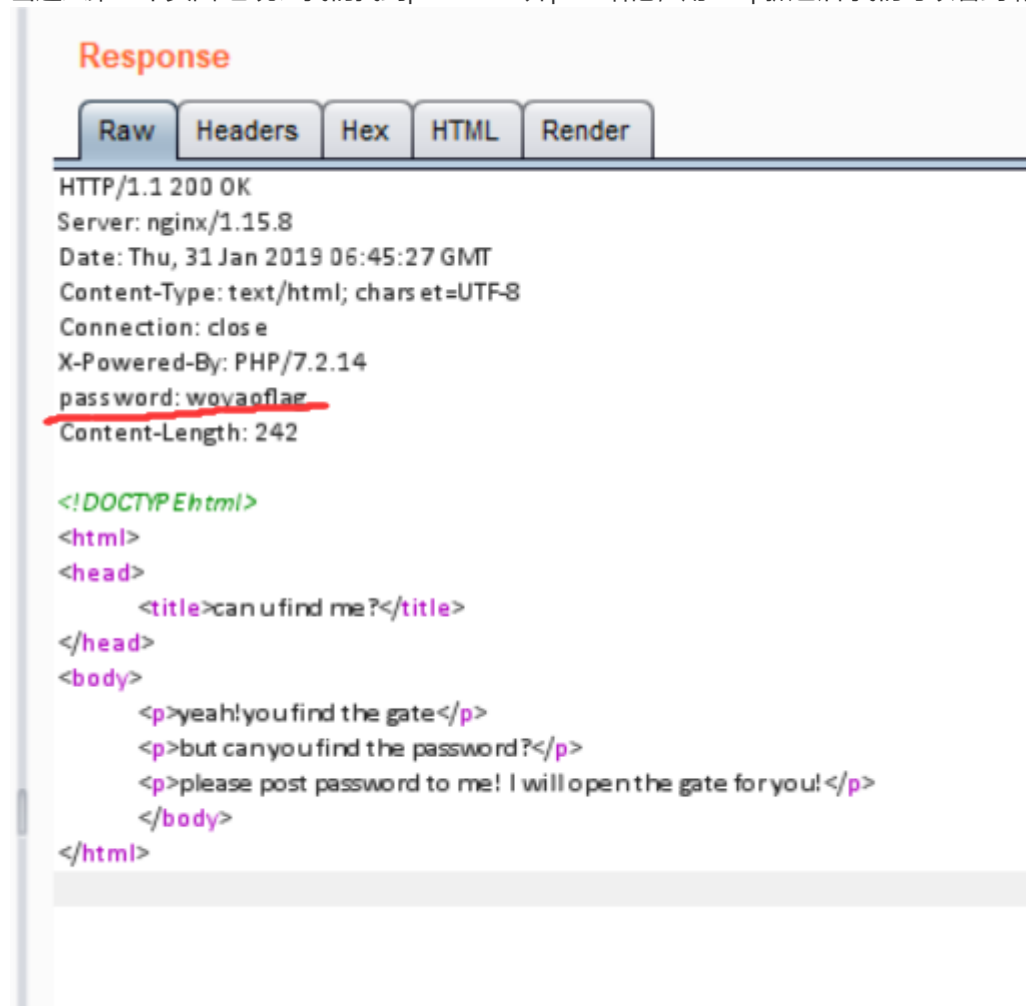


The screenshot shows the Chrome DevTools 'Elements' panel for a web page at 47.107.252.171:8080/. The HTML structure is as follows:

```
<!doctype html>
<html>
  <head>...</head>
  <body> == $0
    <p>the gate has been hidden</p>
    <p>can you find it? xixixi</p>
    <a href="f12.php"></a>
  </body>
</html>
```

点

点击进入第二个页面 它说让我们找到password并post给他，用burp抓包后 我们可以看到响应头里有个password



The screenshot shows the 'Response' tab in Burp Suite. The HTTP status is 200 OK. The headers include 'Server: nginx/1.15.8', 'Date: Thu, 31 Jan 2019 06:45:27 GMT', 'Content-Type: text/html; charset=UTF-8', 'Connection: close', 'X-Powered-By: PHP/7.2.14', and a custom header 'password: wovaoflag' which is underlined in red. The 'Content-Length' is 242. The HTML body contains the following text:

```
<!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>
```

这就是我们要找的密码 然

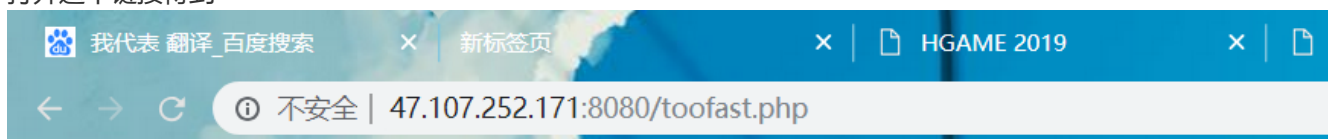
后用postman发送password得到


```

1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>can u find me?</title>
5   </head>
6   <body>
7     <p>yeah!you find the gate</p>
8     <p>but can you find the password?</p>
9     <p>please post password to me! I will open the gate for you!</p>
10    <p>right!</p>
11    <a href='iamflag.php'> click me to get flag</a>
12  </body>
13 </html>

```

打开这个链接得到



aoh,your speed is sososo fast,the flag must have been left in somewhere

说我速度太快了,应该是那个页面有个重定向, 那我用burp去抓取他的f返回内容,得到flag

Raw	Headers	Hex	HTML	Render
HTTP/1.1 302 Found Server: nginx/1.15.8 Date: Thu, 31 Jan 2019 06:57:26 GMT Content-Type: text/html; charset=UTF-8 Connection: close X-Powered-By: PHP/7.2.14 location: toofast.php Content-Length: 132				
<pre> <html> <head> <title>canyoufind me?</title> </head> <body> <p>flag:hgame{f12_1s_aMazIng111}</p> </body> </html> </pre>				

RE部分

其实不会re, 但发现re一些简单的不用汇编的也能做, 就蹭了点分走

1.HelloRe

在linux打开后

```
root@ubuntu:/home/blithe/Documents# ./HelloRe
Please input your key:
```

然后。。。

什么都不知道的我把它丢到winhex里，找到了flag。。。

C 48 83 C3	L變L夥D?A .踰兜0
1 5C 41 5D	.H9雞闖頑.[]A\A]0
0 00 00 00	A^A_?f...?.....].
3 00 00 00	竺..H發.H頑.?..t0
E 70 75 74Please input
7 61 6D 65	your key:..hgame0
2 33 5F 57	{Welc0m3_t0 R3_W
3 73 00 66	orld!}.success.f0
4 00 00 00	ailed.....;4...
8 FD FF FF? €'...犁
8 FF FF FF	P...~? ?..8
0 00 00 00	?..?
1 78 10 01zR...y...0

2.Pro的Python教室(一)

```

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 !'

```

审查代码后得知，我们只需要把第二部分进行base64解密后与第一第三部分相连接就是flag 将SGVyZV8xc18zYXN5Xw==解密得 Here_1s_3asy_ 将三个部分连在一起得到flag hgame{Here_1s_3asy_Pyth0n}

MISC部分

1. Hidden Image in LSB

用stegsolve打开文件里的图片 在Blue plane 0这个视图看到flag

hgame{LSB_
is_easy_for_us}

2. 打字机

用google以图搜图得到 这个打字机是京紫打字机 然后百度搜到京紫打字机得字体

! 2 9 N B h X 8 9 0
Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk Ll Mm
Nn Oo Pp Qq Rr Ss Tt Uu Vv Ww Xx Yy Zz
@ # \$ % & * () - _ ; : ' " , . / 1/2 1/4 3/4
与

Pyana{Mr_vz0Lai_irDaWpziar}

——对应得到flag

3.Broken Chest

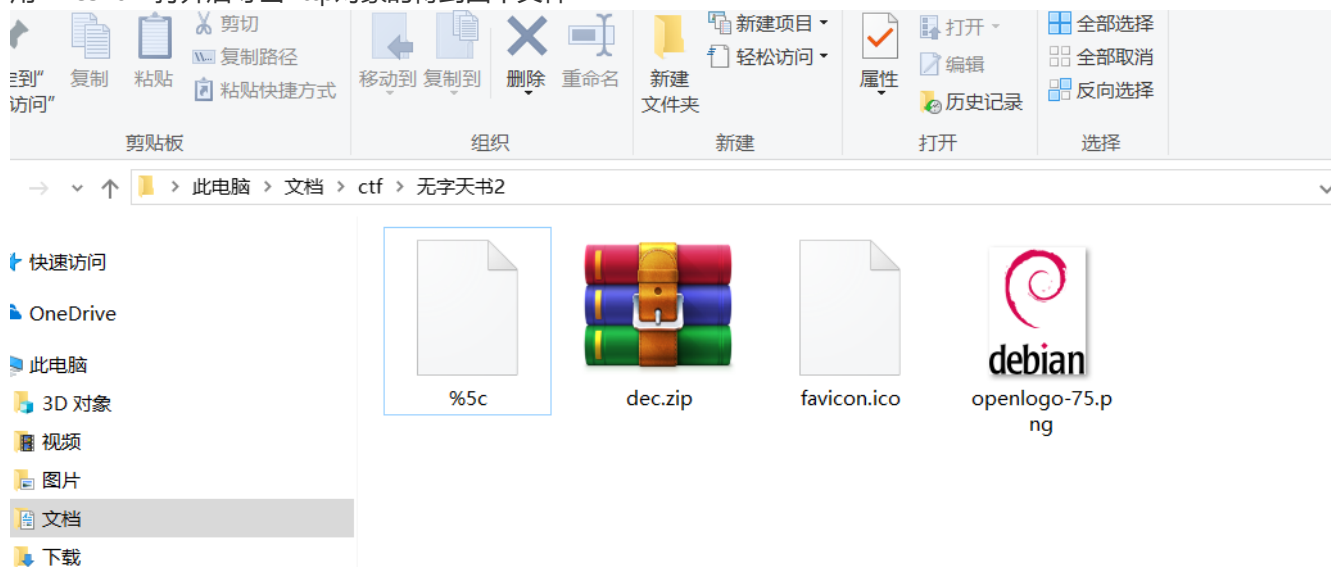
下载下来发现压缩包里有flag.txt,但是文件打不开说压缩文件损坏,放到winhex里看一下

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
000000	4F	4B	03	04	14	00	09	00	08	00	55	BB	35	4E	CE	7C	OK.....U?N刺
000010	B3	B0	22	00	00	00	14	00	00	00	08	00	00	00	66	6C	嘲".....f1
000020	61	67	2E	74	78	74	67	49	3F	48	A0	BE	53	8B	38	E4	ag.txtgI?H怪S??
000030	5A	42	49	02	08	5D	55	A6	4A	67	B2	B3	CE	B0	6E	C1	ZBI..]U g勃伟n?
000040	0B	85	DC	EB	4F	91	4D	BF	50	4B	07	08	CE	7C	B3	B0	.味隣斬縋K..刺嘲
000050	22	00	00	00	14	00	00	00	50	4B	01	02	1F	00	14	00	".....PK.....
000060	09	00	08	00	55	BB	35	4E	CE	7C	B3	B0	22	00	00	00U?N刺嘲"...
000070	14	00	00	00	08	00	24	00	00	00	00	00	00	00	20	00\$......
000080	00	00	00	00	00	00	66	6C	61	67	2E	74	78	74	0A	00flag.txt..
000090	20	00	00	00	00	00	01	00	18	00	3E	2C	76	B6	9D	B1>,v??
0000A0	D4	01	3E	2C	76	B6	9D	B1	D4	01	1D	F1	7E	C5	9C	B1	?>,v?痹..駘驤?
0000B0	D4	01	50	4B	05	06	00	00	00	00	01	00	01	00	5A	00	?PK.....Z.
0000C0	00	00	58	00	00	00	10	00	53	30	6D	45	54	68	31	6E	..X.....S0mETh1n
0000D0	67	5F	55	35	65	66	75	4C									g_U5efuL

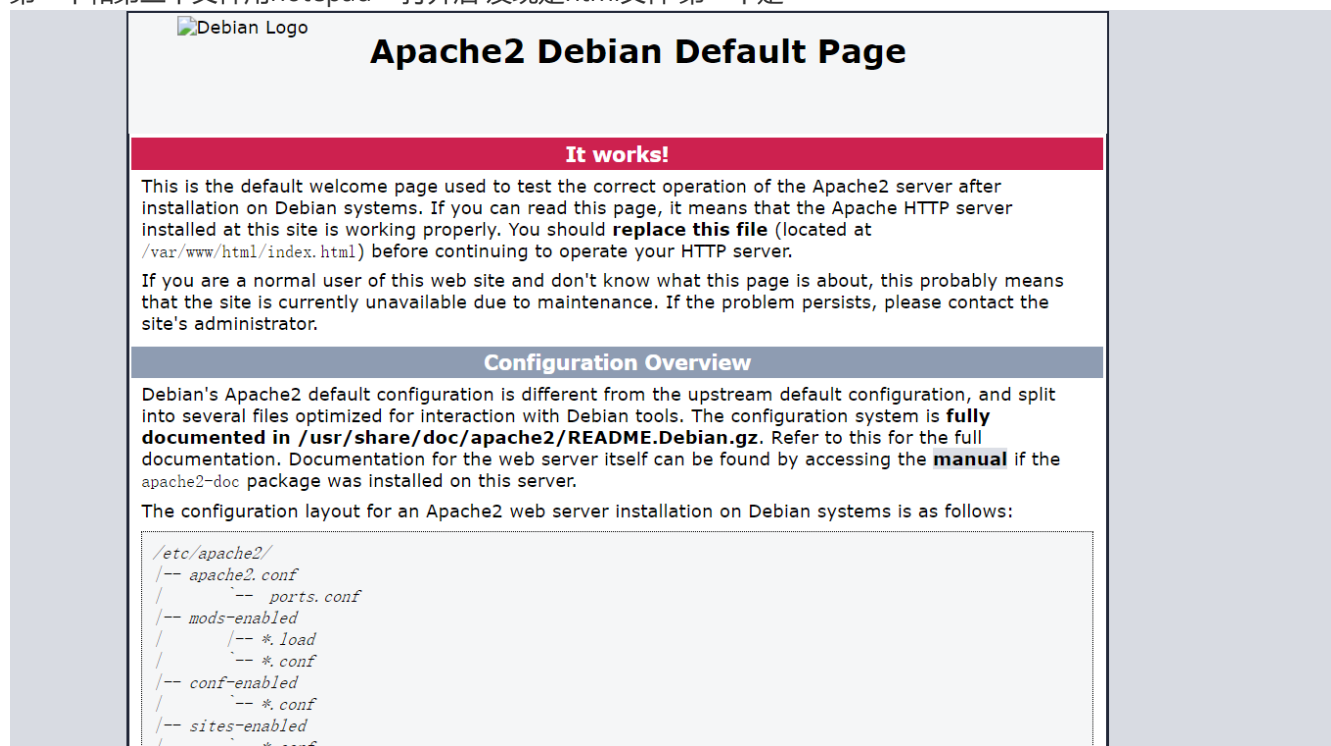
发现它的文件头的第一个字节错了 zip是以50 4B 03 04开头 所以我把第一个字节4F改成50 文件可以打开后发现被加密了 在注释发现S0mETh1ng_U5efuL, 把它作为密码, 成功打开文件 得到flag: hgame{Cra2y_D1aM0nd}

4.Try

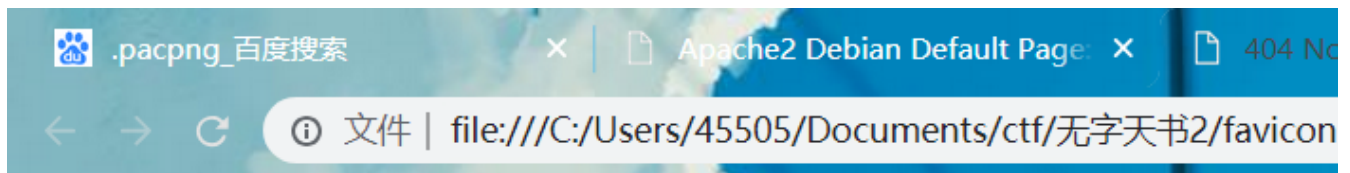
用wireshark打开后导出http对象的得到四个文件



第一个和第三个文件用notepad++打开后 发现是html文件 第一个是



第二个是





Not Found

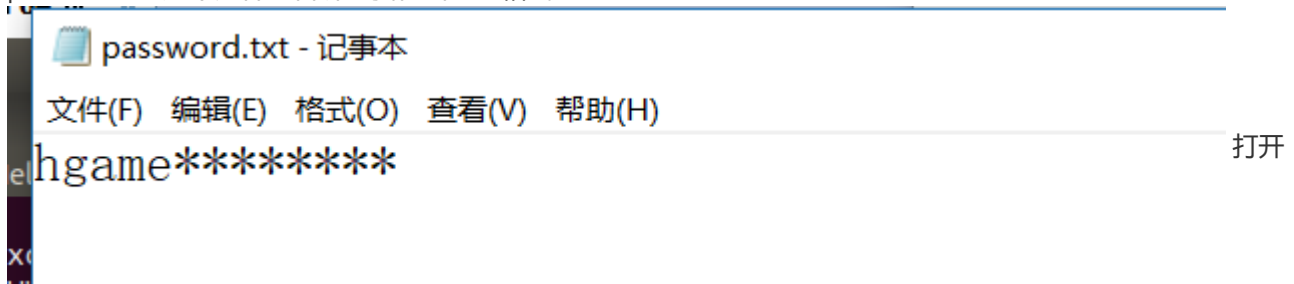
The requested URL /favicon.ico was not found on this server.

Apache/2.4.37 (Debian) Server at 192.168.61.129 Port 80

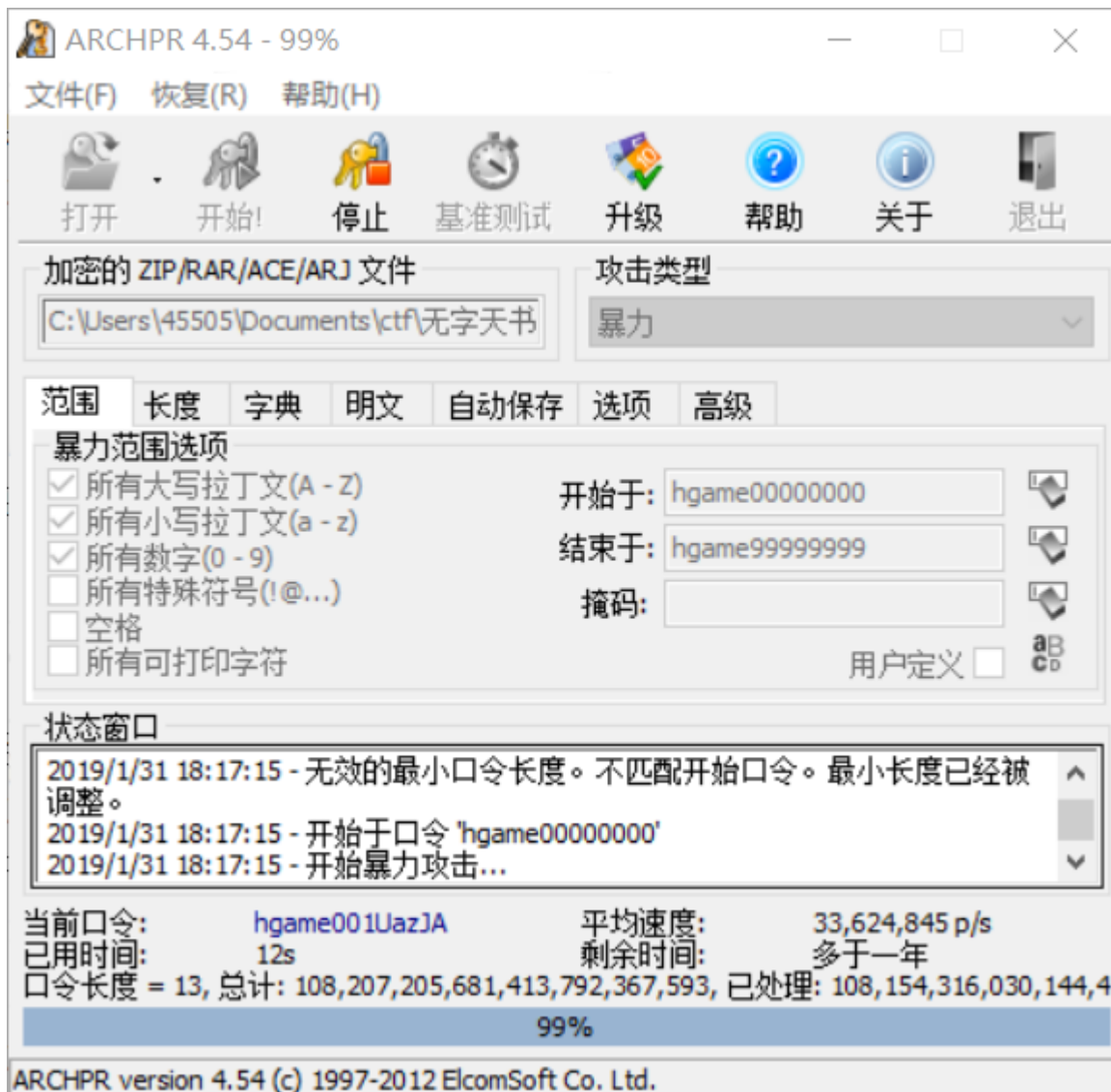
看起来和题目没什么关系，所以我将注意力放到了那个压缩包上 解压开这个压缩包里面有两个文件

 open-it.zip	2019/1/24 12:31	WinRAR ZIP 压缩...	85 KB
 password.txt	2019/1/24 12:32	文本文档	1 KB

password.txt这个文件里告诉了我们密码的格式



open-it.zip,果然被加密了 本来想拿archpr暴力破解一下

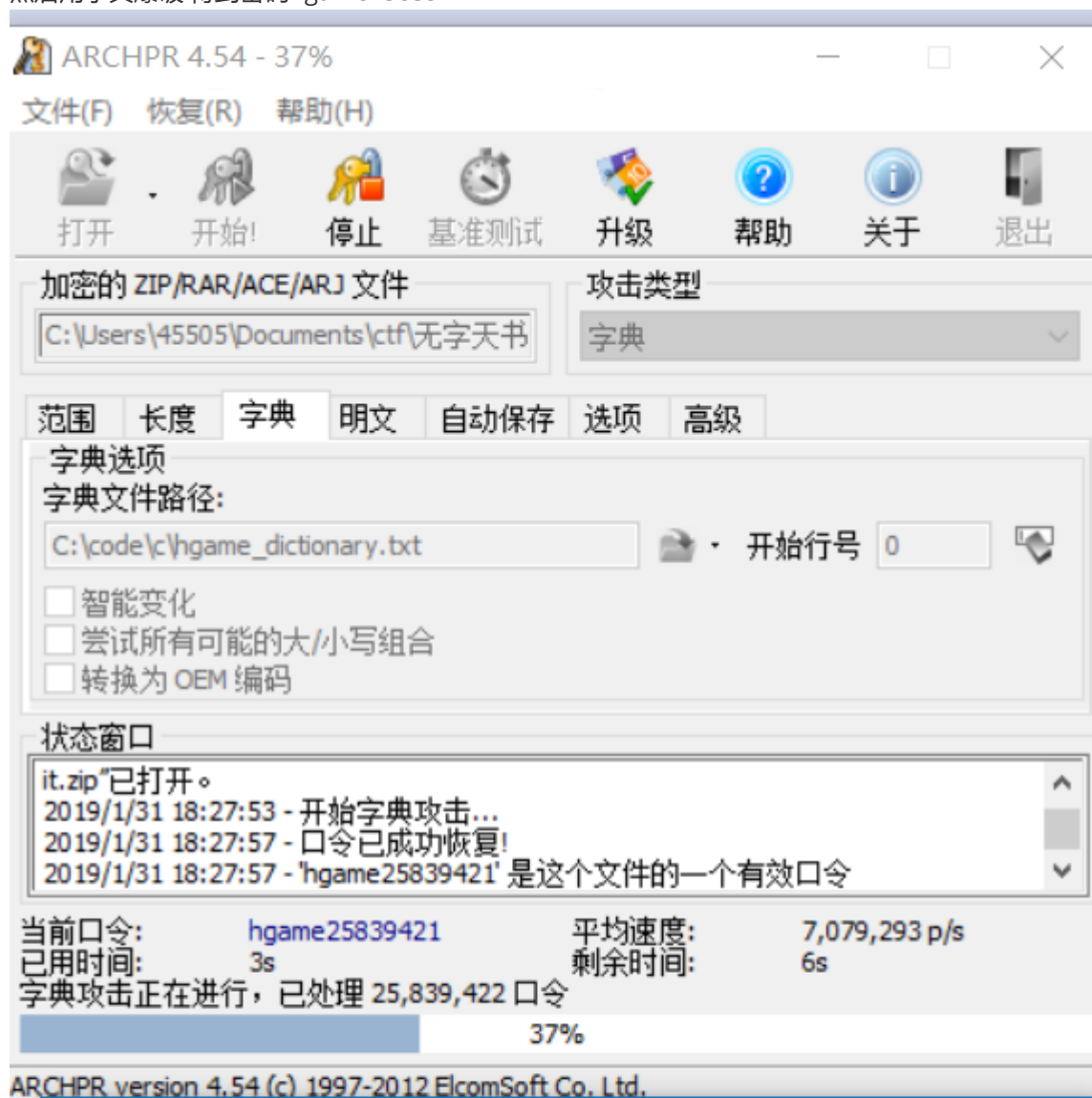


结果时间多于

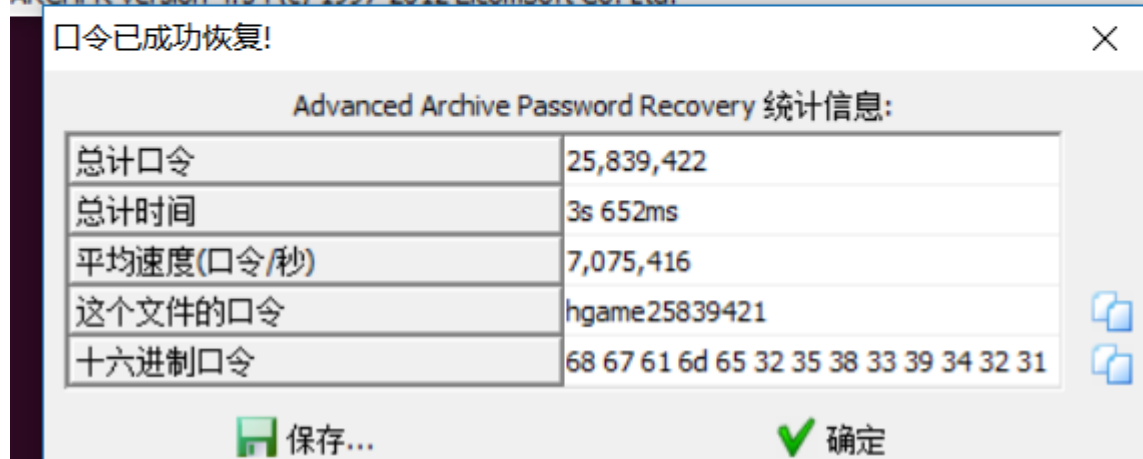
一年???。莫非是要下届hgame再交flag? 想想后面八位应该不可能包含字符了, 不然跑不完啊, 那就用纯数字试一下 然后写了一小段程序导出字典, 程序代码如下

```
#include<stdio.h>
int main(void){
    long num=0;
    char header[] ="hgame";
    FILE *fp;
    fp=fopen("hgame_dictionary.txt","w+");
    while(num<=99999999){
        fprintf(fp,"%s%08d\n",header,num);
        num++;
    }
    fclose(fp);
    return 0;
}
```


然后用字典爆破 得到密码hgame25839421



得到一张图



片, 觉得这图片应该有文件隐藏再里面 放到linux binwalk一下

```
root@ubuntu:/home/blithe/Documents# binwalk 1.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
566	0x236	LZMA compressed data, properties: 0xD0, dictionary size: 10747904 bytes, uncompressed size: 274877906944 bytes
79837	0x137DD	Zip archive data, at least v2.0 to extract, compre

```

ssed size: 9447, uncompressed size: 12178, name: 1.docx
89408          0x15D40          End of Zip archive, footer length: 22

root@ubuntu:/home/blithe/Documents#

```

果然有压缩包隐藏在里面 执行这条命令将压缩包分离出来 `dd if=./1.jpg of=myzip skip=79837 bs=1` 发现又需要密码。。。可这次什么提示都没有，觉得应该是个伪加密 把它放到winhex看一下

000024E0	7F E7 8C F8 23 9C 08 FF CA FE E5 9A F8 45 FF FD	.鏢?? 漱鍤勳 ?
000024F0	B9 F0 17 A8 49 FE E5 94 F8 37 32 04 E4 CF 2C B8	桂. 施72. 酒, ?
00002500	D7 5F C7 6B 6F 9B E8 7E A6 FE 02 50 4B 01 02 3F	警洗o?鐵 .PK..?
00002510	00 14 00 09 00 08 00 F8 74 32 4E DD C4 CD 94 E7	... 鴻2N菽蛤?
00002520	24 00 00 92 2F 00 00 06 00 24 00 00 00 00 00	\$.?....\$......
00002530	00 20 00 00 00 00 00 00 00 31 2E 64 6F 63 78 0A 1.docx.
00002540	00 20 00 00 00 00 00 01 00 18 00 C6 82 9F 9A F8 菽黏?
00002550	AE D4 01 B7 3B 22 83 9C B3 D4 01 4A 37 DD 06 F8	☐.?"價吃.J7??
00002560	AE D4 01 50 4B 05 06 00 00 00 00 01 00 01 00 58	☐.PK.....X
00002570	00 00 00 0B 25 00 00 00 00 00 00 00 00 00 00%.

把这里的09 00改成00 00 成功打开压缩包得到里面的flag

