

WEB

谁吃了我的flag

根据description与网页提示，百度vim泄露

地址栏输入<http://118.25.111.31:10086/index.html.swp>得到文件

对文件进行恢复得到flag

换头大作战

先输个1试试，提示用post,打开f12,method改为post

d>

```
= "index.php" method="post"> ... </fo
```

Wikiwand.com/en/X-Forwarded-For

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

得到提示，使用BP抓包伪造来源

```
Cookie: admin=0
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1
want=1
```

再次得到提示

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

再次伪造

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Waterfox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Accept-Encoding: gzip, deflate
Referer: http://120.78.184.111:8080/week1/how/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 6
Connection: close
```

再次得到提示

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

再伪造

```
Accept-Encoding: gzip, deflate
Referer: www.bilibili.com
Content-Type: application/x-www-form-urlencoded
```

`https://www.wikiwand.com/en/HTTP_cookie`

再提示

you are not admin

再伪造

```
Connection: close
Cookie: admin=1
```

得到flag

想要flag嘛:

hgame{hTTp_HeaDeR_iS_Ez}

very easy web

看得懂php就行了, get发送一个url编码的vidar给网页

创建表单发送id=%76%69%64%61%72

得到flag

can you find me

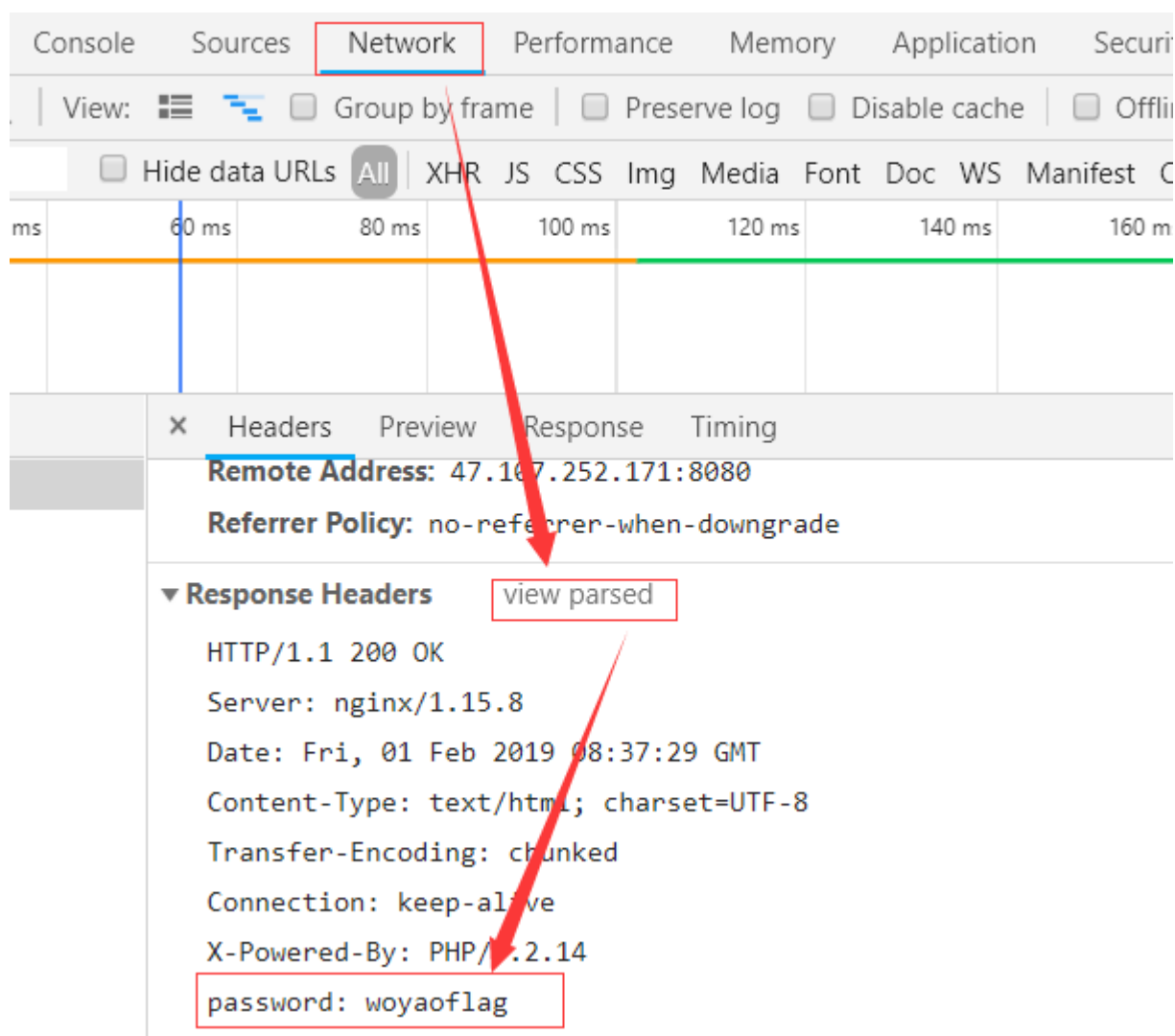
学习资料:

<https://www.cnblogs.com/yaoyaojing/p/9530728.html>

<https://www.cnblogs.com/logsharing/p/8448446.html>

<https://blog.csdn.net/z929118967/article/details/50384529>

f12查看源码找到gate, 再次f12找到对应密码, 并post发送



right!

[click me to get flag](#)

继续点击链接

提示flag被遗漏在某处，在network页面发现iamflag.php文件（页面发生跳转）

Name	Status	Type	Initiator	Size
iamflag.php	302	text/html	Other	
toofast.php	200	document	iamflag.php	

使用BP抓包，得到flag

```
location: /usr/bin/nc
Content-Length: 132

<html>
  <head>
    <title>can you find me?</title>
  </head>
  <body>
    <p>flag:hgame{f12_1s_aMazIng111}</p>
  </body>
</html>
```

RE

brainfxxker

学习资料: <https://zh.wikipedia.org/wiki/Brainfuck>

简单看一下代码，代码说正确输入flag时没异常输出

那么我们简单翻译一下主程序里的符号，可以得知当输入为特定值是可以则不执行 [+.] 这个部分

代码翻译参考以上网址；

flag: hgame{bR4!NfUcK}

HelloRe

文本编辑器打开即可看到flag（续命题啊）

r&xor

把文件拖到IDA里，找到main函数，按下f5，得知异或加密

```
68 | v29 = 30;
69 | puts("Input the flag:");
70 | __isoc99_scanf("%s", s);
71 | if ( strlen(s) == 35 )
72 | {
73 |     for ( i = 0; i < 35; ++i )
74 |     {
75 |         if ( s[i] != (v5[i] ^ *((char *)&v30 + i)) )
76 |         {
77 |             puts("Wrong flag , try again later!");
78 |             return 0;
79 |         }
80 |     }
81 |     puts("You are right! Congratulations!!");
82 |     result = 0;
83 | }
```

发现几个非常大的数字，按R转换成字符（这是假flag）

```
3 v30 = '0Y{emagh';
3 v31 = '_3byam_u';
L v32 = '1ht_deen';
2 v33 = '!!!en0_s';
3 v34 = '}!!!';
```

memset(v5, 0, 144uLL); // 数组置0, 38size

```
rep stosq
mov     [rbp+var_118], 1
mov     [rbp+var_110], 7
mov     [rbp+var_108], 5Ch
mov     [rbp+var_104], 12h
mov     [rbp+var_100], 26h
mov     [rbp+var_FC], 08h
mov     [rbp+var_F8], 5Dh
mov     [rbp+var_F4], 28h
mov     [rbp+var_F0], 08h
mov     [rbp+var_EC], 17h
mov     [rbp+var_E4], 17h
mov     [rbp+var_E0], 28h
mov     [rbp+var_DC], 45h
mov     [rbp+var_D8], 6
mov     [rbp+var_D4], 56h
mov     [rbp+var_D0], 2Ch
mov     [rbp+var_CC], 36h
mov     [rbp+var_C8], 43h
mov     [rbp+var_C0], 42h
mov     [rbp+var_BC], 55h
mov     [rbp+var_B8], 7Eh
mov     [rbp+var_B4], 48h
mov     [rbp+var_B0], 55h
mov     [rbp+var_AC], 1Eh
mov     edi, offset s_0 ; "Touut"
```

根据汇编以及置0（hgame与0异或）

得到异或数组

```
= {0, 0, 0, 0, 0,
    0, 1, 0, 7, 0,
    92, 18, 38, 11, 93,
    43, 11, 23, 0, 23,
    43, 69, 6, 86, 44,
    54, 67, 0, 66, 85,
    126, 72, 85, 30, 0};
```

与假flag异或一下得到真flag

game{X0r_1s_interest1ng_isn't_it?}

Pro的Python教室（一）

简单读一下，就是base64加密的问题

在线解个密拼起来就是flag了

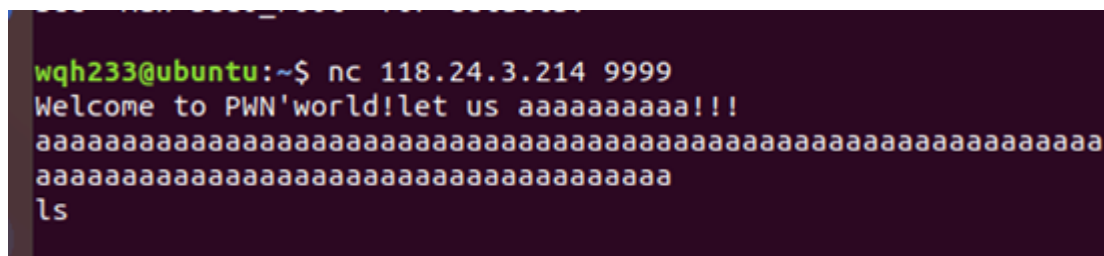
PWN

aaaaaa

把文件拖IDA里看一下，

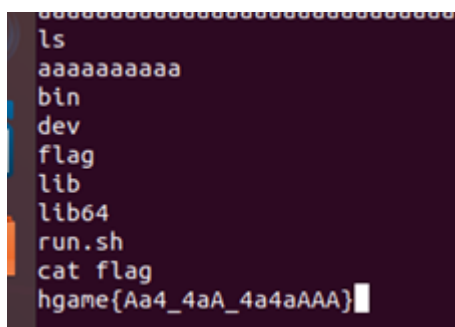
```
9 puts("Welcome to PWN'world!le
10 v5 = 0;
11 while ( 1 )
12 {
13     v3 = v5++;
14     if ( v3 > 99 )
15         break;
16     if ( getchar() != 97 )
17         exit(0);
18 }
19 system("/bin/sh");
20 return 0;
```

发现只要a个99次就行了，



```
wqh233@ubuntu:~$ nc 118.24.3.214 9999
Welcome to PWN'world!let us aaaaaaaaaa!!!
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
ls
```

ls查看当前目录的文件（需要在10s内完成操作）



```
ls
aaaaaaaaaaaa
bin
dev
flag
lib
lib64
run.sh
cat flag
hgame{Aa4_4aA_4a4aAAA}
```

cat查看flag文件

MISC

Hidden Image in LSB

emmm 原谅我太菜.....使用stegosovle一顿乱操作，然后拿到flag



打字机

以图搜图（得到关键字：紫罗兰打字机）

对照图案分析（相似小写，一样是大写（我猜的））



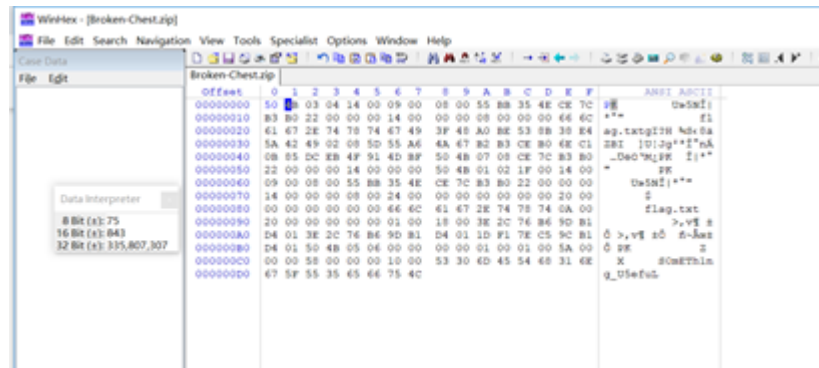
对照flag翻译，根据提示

hgame{My_violet_tyPewRiter} // 我的紫罗兰打字机

brkoen-chest

参考资料 <https://ctf-wiki.github.io/ctf-wiki/misc/archive/zip/>

收到破损的zip文件，使用winhex查看压缩包，发现头被更改，将文件头改回来



更改头后发现需要解压密码，在注释里看到密码，解压得到flag



Try-it

学习资料：（出现看不懂的看学习资料就对了）

<https://veritas501.space/2017/06/23/%E7%BB%99%E4%BD%A0%E5%8E%8B%E7%BC%A9%E5%8C%85%E5%8D%B4%E4%B8%8D%E7%BB%99%E4%BD%A0%E5%AF%86%E7%A0%81%E7%9A%84%E4%BA%BA%E5%88%B0%E5%BA%95%E5%9C%A8%E6%83%B3%E4%BB%80%E4%B9%88/>

<https://www.cnblogs.com/WangAoBo/p/6944477.html>

<https://blog.csdn.net/kajweb/article/details/76474476>

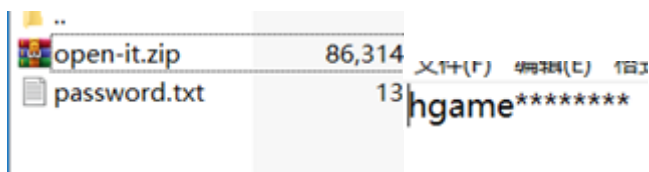
<https://www.jianshu.com/p/02fdd5edd9fc>

https://blog.csdn.net/syh_486_007/article/details/55537439

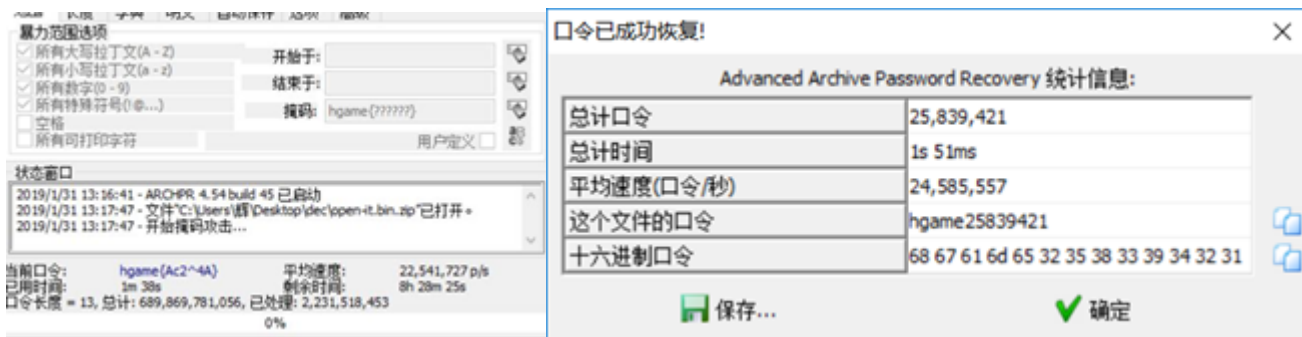
.pcapng后缀用wireshark打开

找到HTTP协议，发现zip包，导出更改后缀，打开发现需要密码

No.	Time	Source	Destination	Protocol	Length	Info
28	29.095170	192.168.61.1	192.168.61.129	HTTP	414	GET /icons/openlogo-75.png HTTP/1.1
36	29.149810	192.168.61.129	192.168.61.1	HTTP	254	HTTP/1.1 200 OK (PNG)
38	29.240427	192.168.61.1	192.168.61.129	HTTP	404	GET /favicon.ico HTTP/1.1
40	29.241340	192.168.61.129	192.168.61.1	HTTP	559	HTTP/1.1 404 Not Found (text/html)
52	40.679234	192.168.61.1	192.168.61.129	HTTP	443	GET /dec.zip HTTP/1.1
142	40.685708	192.168.61.129	192.168.61.1	HTTP	964	HTTP/1.1 200 OK (application/zip)
5	14.438864	192.168.61.1	192.168.61.129	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=64 (



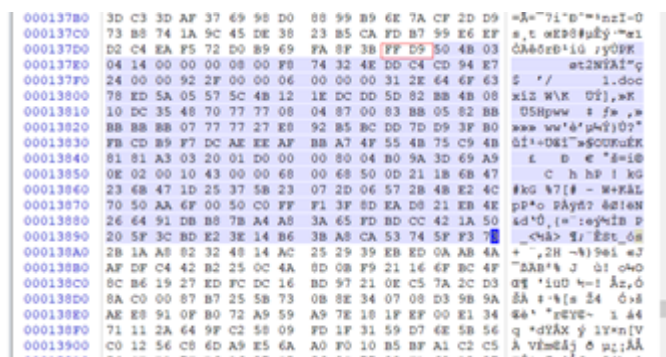
看到密码提示，用掩码攻击（工具：ARCHPR），只勾选数字。



解压看到图片 (emmm 是拿来欣赏的吗?)



用winhex打开, 发现不是jpg结尾字符, 搜索FF D9

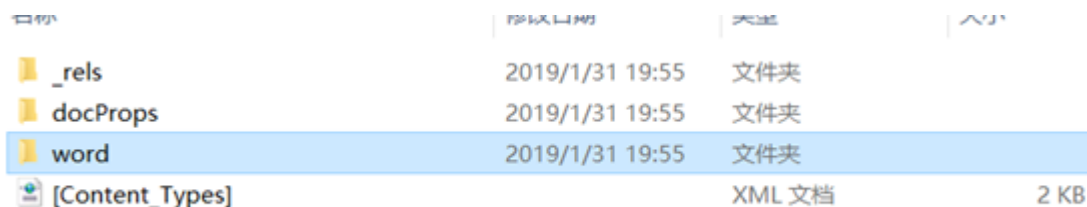


导出FFD9之后字符, 以zip格式开头, 更改后缀名为zip,发现需要密码

再次用winhex打开, 发现, 加密标记为0000, 推断为伪加密, 搜索09 00, 更改为00 00后保存

打开文档发现为无字天书 (新手表示果然是压轴题, 累死了)

百度一下, 发现这不是文档是个zip压缩包, 用winrar打开, 解压得到文件夹, 在一个文件中发现flag



```

<?xml version="1.0" encoding="UTF-8" standalone="yes" type="application/xml" >
<w:document xmlns:w="http://schemas.microsoft.com/office/word/2010/wordprocessingGroup" xmlns:wpi="http://schemas.microsoft.com/office/word/2006/wordml" xmlns:wps="http://schemas.microsoft.com/office/word/2006/wordml" w:rsidR="005C0554" w:rsidRPr="004066DE" w:rsidRDefault="00A5456DE">
<w:rPr><w:vanish/></w:rPr><w:t>hgame</w:t></w:r><w:r w:rsidRPr="004066DE">
<w:rPr><w:sectPr w:rsidR="005C0554" w:rsidRPr="004066DE">
<w:pgSz w:w="0"/>
<w:cols w:space="425"/>
<w:docGrid w:type="lines" w:linePitch="12" />
</w:rPr>
</w:r>
</w:document>

```

CRYPT

MIX

显而易见，摩斯密码，翻译一下：**744B735F6D6F7944716B7B6251663430657D**

看成16进制转换成ASCII码：tKs_moyDqk{bQf40e}

由于_括号外面，所以是栅栏密码，又因为没有h g a m e

通过凯撒密码，一个个试：（ROT14 得到）

hYg_acmRey{pEt40s}

通过栅栏密码得到：hgame{E4sY_cRypt0}

base全家

查百度得知有base64,base58,base32,base16

解密过程均使用python库函数完成

出现数字9，还有字母推断为base64加密，先解密看看

解密之后还有小写字母继续base64解密，这次只有数字（推断base16加密）

用python的base64.b16decode处理一下，啊呀，还是数字，再处理一下

出现了字母，继续base16，出现了三个等号，开始base32，解码之后出现数字9,大写字母，base16,出现四个“===”，base32,出现小写字母，base64（以下简写），base16，

base64,base16,base16,base16,base16,base32,base64,base64,base64, base32之后出现: base58 :

2BAja2VqXoHi9Lo5kfQZBPjq1EmZHGEudM5JyDPREPM53CxrPB8BnC

用base58解密（网上下载个库就行了）

得到flag:hgame{40ca78cde14458da697066eb4cc7daf6}