

bugku{web writeup笔记}

原创

[L1s4](#) 于 2020-10-19 08:55:58 发布 137 收藏 1

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/baidu_39504221/article/details/104326281

版权



[CTF 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

文章目录

[web2](#)

[计算器](#)

[web基础\\$_GET](#)

[web基础\\$_POST](#)

[矛盾](#)

[web3](#)

[域名解析](#)

[你必须让他停下](#)

[本地包含](#)

[web5](#)

[头等舱](#)

[网站被黑](#)

[管理员系统](#)

[web4](#)

[flag在index里](#)

[输入密码查看flag](#)

[点击一百万次](#)

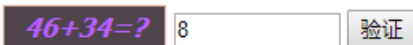
[备份是个好习惯](#)

[web2](#)

F12看一下



计算器



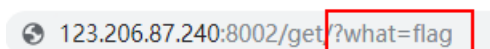
发现这里只能写一位

按F12把下图的maxlength改一下再输入



web基础\$_GET

依照题意提交一个get请求



web基础\$_POST

这里则是提交一个post

可以用火狐的插件hackbar，也可以用在线工具

没有hackbar我就用在线工具了

支持的请求协议有: Post、GetDelete、Put、Trace、Head、Options 请求。本工具源码，本工具更新记录。

Post UTF-8 http://123.206.87.240:8002/post/

备注: 原来需要登陆才能使用, 已经去掉了, 请求内容存储本地。更新时间: 2019年05月05日00:59:41

请使用新版HTTP工具, 不需要登陆。HTTP 模拟请求,

参数名称	参数值
what	flag

添加参数 批量添加 (JSON参数)

https://blog.csdn.net/baidu_39504221

Response Body (返回值是JSON, 会自动格式化)

```
1 $what=$_POST[
2 'what'
3 ];<br>
4 echo$what;<br>
5 if($what=='flag')<br>
6 echo'flag{
7 ****
8 }';<br>
9
10
11 flagflag{
12 bugku_get_ssseint67se
13 }
```

https://blog.csdn.net/baidu_39504221

第二种方法是用BP抓包

POST /post/ HTTP/1.1
Host: 123.206.87.240:8002 这里抓出来是GET, 需要修改一下
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 9
Content-Type: application/x-www-form-urlencoded

what=flag

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 24 Apr 2020 00:44:29 GMT
Content-Type: text/html
Connection: close
Content-Length: 126

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

flagflag{bugku_get_ssseint67se}

https://blog.csdn.net/baidu_39504221

矛盾

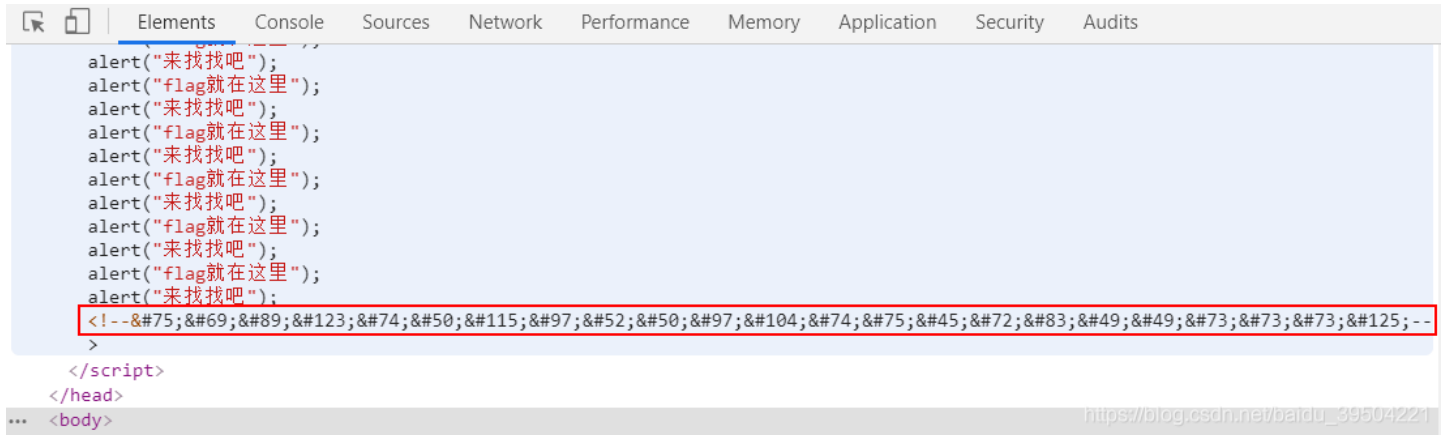
依照题意需要提交一个get参数num，需要num不是数字才能进入第一个if语句，有需要num==1才能输出flag

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

利用了php的一个特性

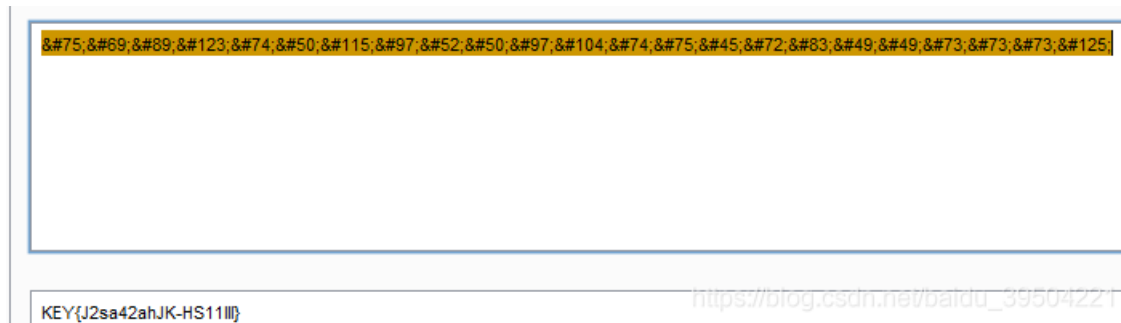
web3

弹窗都过完后 F12 发现一串神秘代码



```
alert("来找我吧");
alert("flag就在这里");
alert("来找我吧");
alert("flag就在这里");
alert("来找我吧");
alert("flag就在这里");
alert("来找我吧");
alert("flag就在这里");
alert("来找我吧");
alert("flag就在这里");
alert("来找我吧");
alert("flag就在这里");
alert("来找我吧");
<!--&#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>
<body>
```

放到burpsuite里用HTML解码就行了



```
&#75;&#69;&#89;&#123;&#74;&#50;&#115;&#97;&#52;&#50;&#97;&#104;&#74;&#75;&#45;&#72;&#83;&#49;&#49;&#73;&#73;&#73;&#125;
```

域名解析

这题我用的是本地解析

📁 > 此电脑 > 本地磁盘 (C:) > Windows > System32 > drivers > etc

这个文件夹里有个host文件，用EditPlus打开，如下编辑

```
1
2 123.206.87.240 flag.baidu.com
```

🏠 > 不安全 | flag.baidu.com

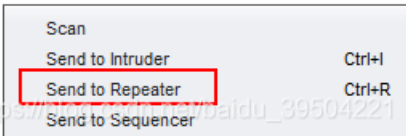
🔍 应用 百度一下，你就知道 📄 sql注入

KEY{DSAHDSJ82HDS2211}

你必须让他停下

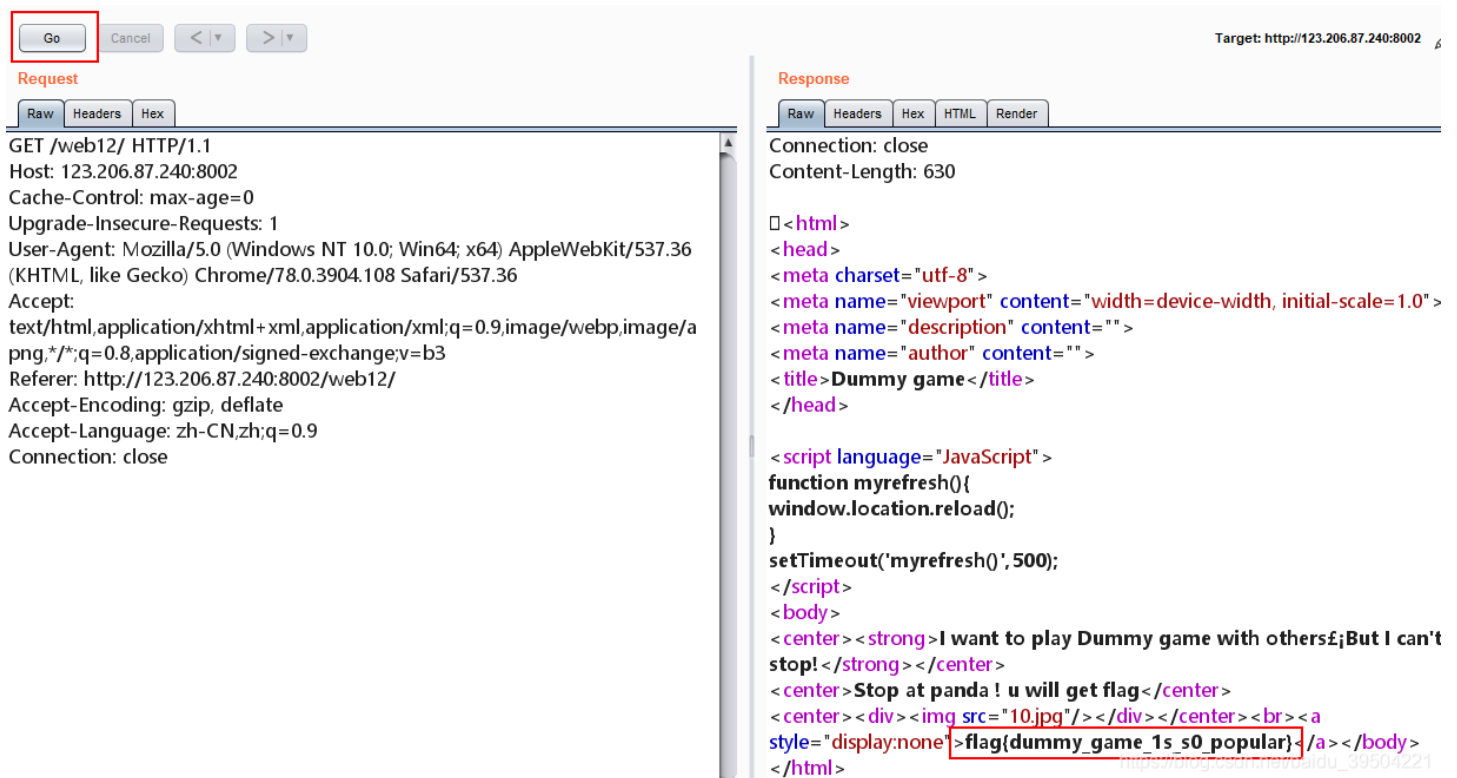
打开后网页一直在跳，我选择用burpsuite抓包试下

```
GET /web12/ HTTP/1.1
Host: 123.206.87.240:8002
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,i
Referer: http://123.206.87.240:8002/web12/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```



Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer

抓到后发到重发器



Go Cancel < >

Request

```
GET /web12/ HTTP/1.1
Host: 123.206.87.240:8002
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://123.206.87.240:8002/web12/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

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(dummy_game_1s_s0_popular)</a></body>
</html>
```

如果没有flag就forward之后重复上述步骤
多抓几次就有了

本地包含



该网页无法正常运行

123.206.87.240 目前无法处理此请求。

HTTP ERROR 500

[重新加载](#) log.csdn.net/baidu_39504221

emmmmm...恶魔妈妈摸猫猫

[web5](#)

查看源代码，题目提示是JSPFUCK，百度了一下

```

Elements Console Sources Network Performance
<html>
  <head></head>
  <body>
    <div style="display:none;">
...
    "( ([ ( (! [ + [ ] ) [ + [ ] ] + [ ( ! [ ] ] + [ [ ] ] ) [ + ! + [ + [ ] ] ] + ( ! [ + [ ] ] [ !
    [ ] ] + [ ] ) [ ! + [ ] ] + [ ] + [ ] ] + ( ! [ + [ ] ] [ + [ ] ] + ( ! [ + [ ] ] [ + [ ] ] + ( + [
    [ ] ] + ( ! [ + [ ] ] [ + [ ] ] + ( ! [ + [ ] ] [ ! + [ ] ] + [ ] + [ ] ] + ( ! [ + [ ] ] [ + [
    [ ] ] + ( ! [ + [ ] ] [ ( ! [ + [ ] ] [ + [ ] ] + ( ! [ ] ] + [ [ ] ] ) [ + ! + [ + [ ] ] ] +
    [ ] ) [ + ! + [ ] ] ] + ! + [ ] + [ ] ] + ( + [ ] + ( [ + [ ] ] ) [ ( ! [ + [ ] ] [ + [ ] ]
    [ + [ ] ] [ ! + [ ] ] + [ ] + [ ] ] + ( ! [ + [ ] ] [ + [ ] ] ] + [ ] ] + [ ] ] + [ ] ] +
    [ ] ] + ! + [ ] ] + ( ! [ + [ ] ] [ + [ ] ] + ( ! [ + [ ] ] [ ! + [ ] ] + [ ] ] + ( ! [ + [ ] ]
    [ + [ ] ] + ( ! [ + [ ] ] [ + [ ] ] + ( ! [ + [ ] ] [ + [ ] ] + ( ! [ + [ ] ] [ + [ ] ] + [ ] ]
    [ + ! + [ ] ] + [ [ ] ] + [ [ ] ] [ ! + [ ] ] + [ ] ] + ( ! [ + [ ] ] [ + [ ] ] + ( ! [ + [ ] ]
    [ + ! + [ ] ] + [ [ ] ] + ( ! [ + [ ] ] [ + [ ] ] + ( ! [ + [ ] ] [ + [ ] ] + ( ! [ + [ ] ] [
  
```

发现这段代码是可以放到控制台执行的

```

]]]]+\:|[|+]]|/+|+]]
]])+(|[|+]]|[|+]]+|+
]]|[|+]]+]]|[|+]]+
< "ctf{whatfk}"
>

```

兴高采烈去提交

JSPFUCK?????答案格式CTF{*****}

唉，已经非常非常接近了。。。

把ctf改成大写再试一下

JSPFUCK?????答案格式CTF{*****}

在好好看看。

全部改成大写再试一下

JSPFUCK?????答案格式CTF{*****}

您的智商已爆表! 恭喜!

flag是CTF{WHATFK}

头等舱

点进去

什么也没有。

看了源码也没什么发现

抓包搞一下

Request

Raw Headers Hex

```
GET /hd.php HTTP/1.1
Host: 123.206.87.240:9009
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Raw Headers HTML Render

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 15 Feb 2020 05:30:42 GMT
Content-Type: text/html
Connection: close
flag{Bugku_k8_23s_istra};
Content-Length: 139

<html>
<meta http-equiv="Content-Type" content="text/ht
<pre><br><br><br><br>什么也没有。<br><br>
</html>
```

诶，藏在响应头里

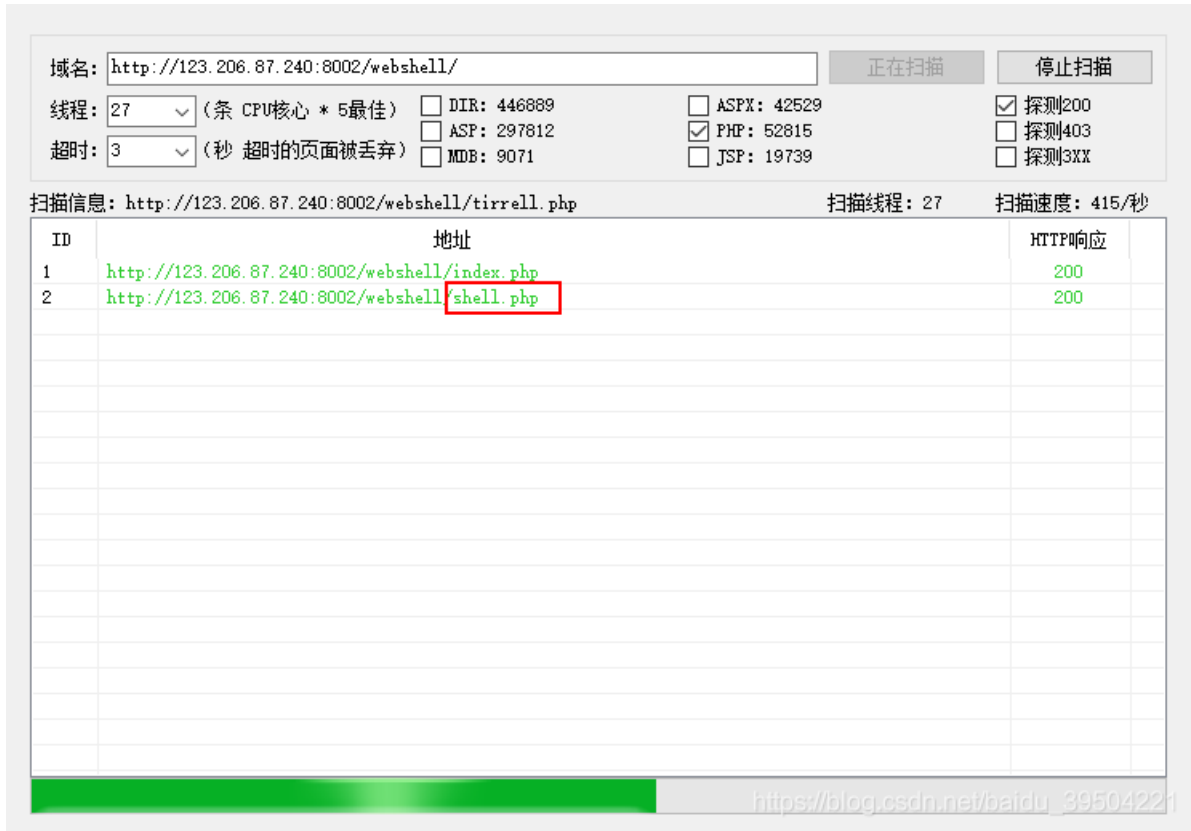
网站被黑



右键菜单被禁了，但F12还有用，但是没什么提示

因为是网站被黑日URI 提示webshell

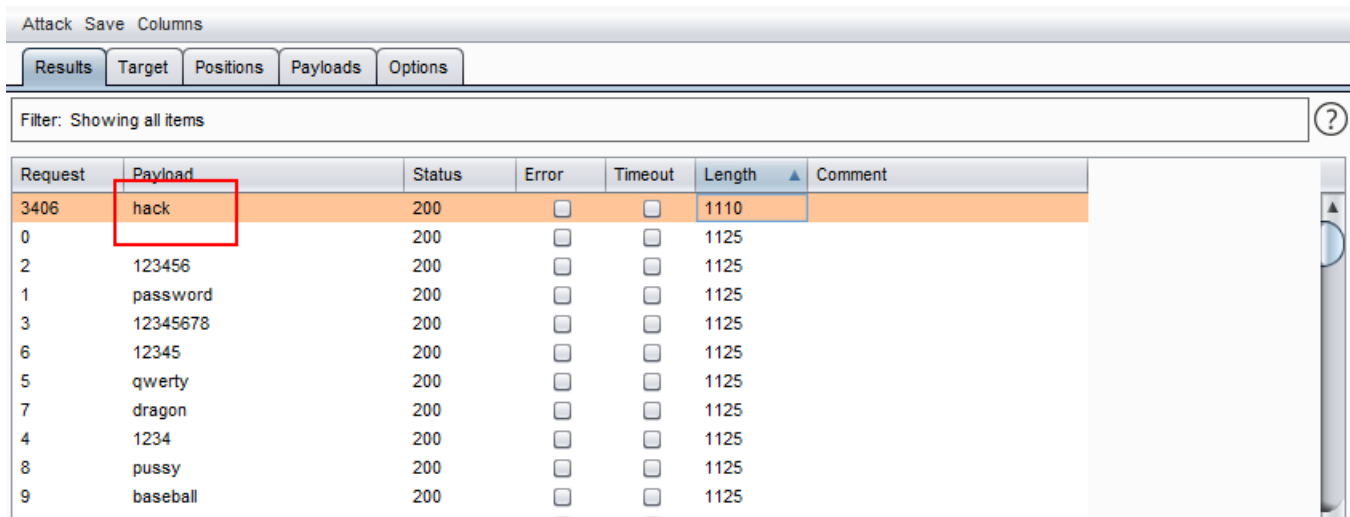
所以我用御剑扫了一下

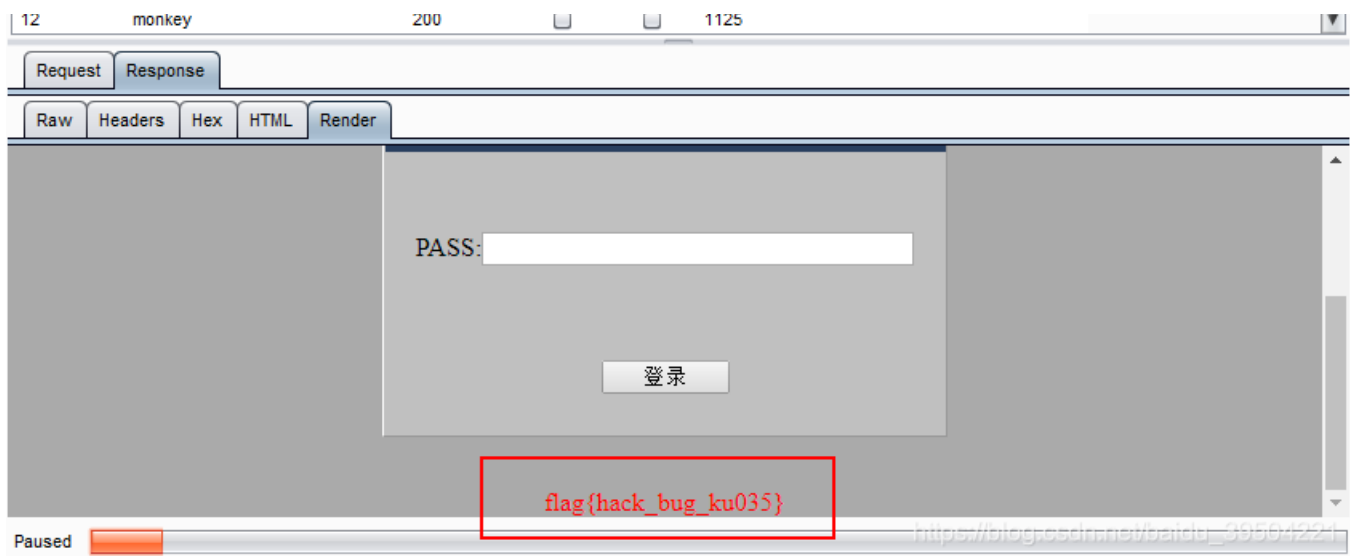


噢，白给的shell



需要密码，用burpsuite抓包爆破一下





给几个网上搜集的字典

链接: <https://pan.baidu.com/s/1M1YFwLKtURFpw84NeT08sQ>

提取码: 7xft

[管理员系统](#)

进去是一个登陆表单，遇事不决看看源码
拉到最下面发现有一行注释

```
5023 <!-- dGVzdDEyMTIz -->
```

base64解码后是test123

以admin为用户名，test123为密码登陆

管理员系统

Username:

Password:

IP禁止访问，请联系本地管理员登陆，IP已被记录。

这个本地让我想到了XFF头，试一波

```
POST / HTTP/1.1
Host: 123.206.31.85:1003
Content-Length: 23
Cache-Control: max-age=0
Origin: http://123.206.31.85:1003
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/78.0.3904.108
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://123.206.31.85:1003/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
X-Forwarded-For: 127.0.0.1
```

```
user=admin&pass=test123
```

```
<html>
<head>
<title>
管理员系统
</title>
</head>
<body>
<h1>管理员系统</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>
```

https://blog.csdn.net/baidu_39504221

单车变摩托

web4

让我们看源码，看呗

JavaScript代码有东西

有两个参数需要解密，解密网站

```
eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));
```

这行代码告诉我中间还要加上一串%35%34%61%61%32

也就是解下面这串

%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

解密出来其中有一行代码是这样的

```
if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)
```

将 67d709b2b54aa2aa648cf6e87a7114f1 直接提交就行了

看看源代码?

KEY{J22JK-HS11}

flag在index里

点开链接

[click me? no](#)

再点进去



test5

发现这里有文件包含的嫌疑

根据题目 flag在index里 把show改成index试了一下

一点hint都没用 百度看了看大佬的文章

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

发现是用了 php://filter/ 协议，受教了

[输入密码查看flag](#)

输入查看密码

请输入5位数密码查看，获取密码可联系我。

很自然想到爆破

写了个c把五位数都读出来

```
#include<stdio.h>
int main()
{
    int a;
    for( a = 10000 ; a < 100000 ;a++)
    {
        printf("%d\n",a);
    }
    return 0;
}
```

然后任意输入任意数字用burpsuite抓包

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
Upgrade-Insecure-Requests
Content-Type: application/x-
User-Agent: Mozilla/5.0 (Win
Accept: text/html,application/
Referer: http://123.206.87.24
Accept-Encoding: gzip, defla
Accept-Language: zh-CN,zh;
Connection: close

pwd=12345

- Scan
- Send to Intruder
- Send to Repeater
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser
- Engagement tools
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file

https://blog.csdn.net/qq_39504221

加载字典，start attack

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
3580	13579	200	<input type="checkbox"/>	<input type="checkbox"/>	246	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
1	10000	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
2	10001	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
6	10005	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
3	10002	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	
4	10003	200	<input type="checkbox"/>	<input type="checkbox"/>	1327	

5	10004	200	<input type="checkbox"/>	<input type="checkbox"/>	1327
7	10006	200	<input type="checkbox"/>	<input type="checkbox"/>	1327
8	10007	200	<input type="checkbox"/>	<input type="checkbox"/>	1327

Request Response

Raw Headers Hex Render

Content-Type: text/html
Connection: close
Set-Cookie: **isview=13579**; expires=Sat, 29-Feb-2020 06:12:11 GMT
Content-Length: 46

flag{bugku-baopo-hah}

</body>
</html>

? < + > Type a search term 0 matches

Paused https://blog.csdn.net/baidu_39564224

点击一百万次

404了额、

备份是个好习惯

给了一串密文

d41d8cd98f00b204e9800998ecf8427ed41d8cd98f00b204e9800998ecf8427e

以为是md5，抓去解密

查询结果：

[空密码]/[Empty String]

后来观察了一下发现

d41d8cd98f00b204e9800998ecf8427e d41d8cd98f00b204e9800998ecf8427e

是由两串一样的密文组成（后来发现这两串密文没一点用）

根据题目，我们是要找备份文件做突破口，百度了一下

bak

编辑

讨论

bak是备份文件，为文件格式扩展名。

外文名 bak

释义 备份文件

https://blog.csdn.net/baidu_39504221

也就是要找某个bak文件

试了一下在URL后加个 flag.php.bak 404了（我之前用御剑扫出flag.php）

那加个 index.php.bak 下载了一个文件噢 放到vscode

```
$str = str_replace('key', '', $str);
```

代码提示要提交key1和key2，以上替换规则可以重写绕过

也就是写成kkeyey1和kkeyey2

```
if(md5($key1) == md5($key2) && $key1 !== $key2){  
    echo $flag."取得flag";  
}
```

这一段绕过要用md5碰撞

123.206.87.240:8002/web16/?kkeyey1=s878926199a&kkeyey2=s155964671a

论坛社区

靶场

在线工具

288558410200e342768416822451524974117254469Bugku{OH_YOU_FIND_MY_MOMY} 蓋



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)