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

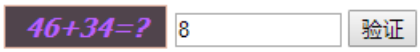
本文链接：https://blog.csdn.net/baidu_39504221/article/details/104326281

文章目录

web2

F12看一下

计算器

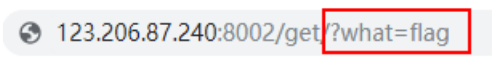


发现这里只能写一位

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

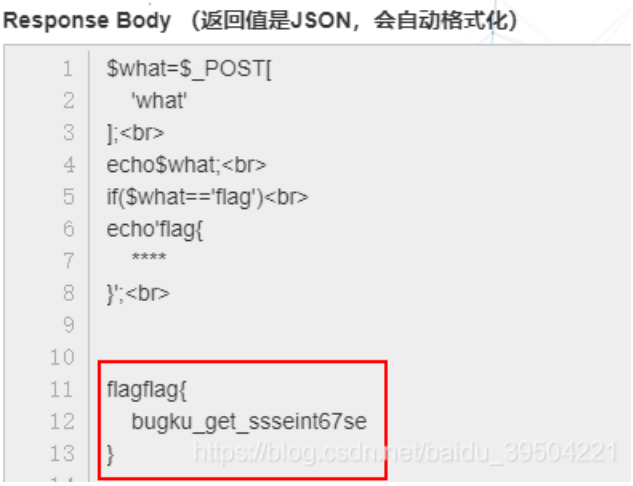


web基础$_POST

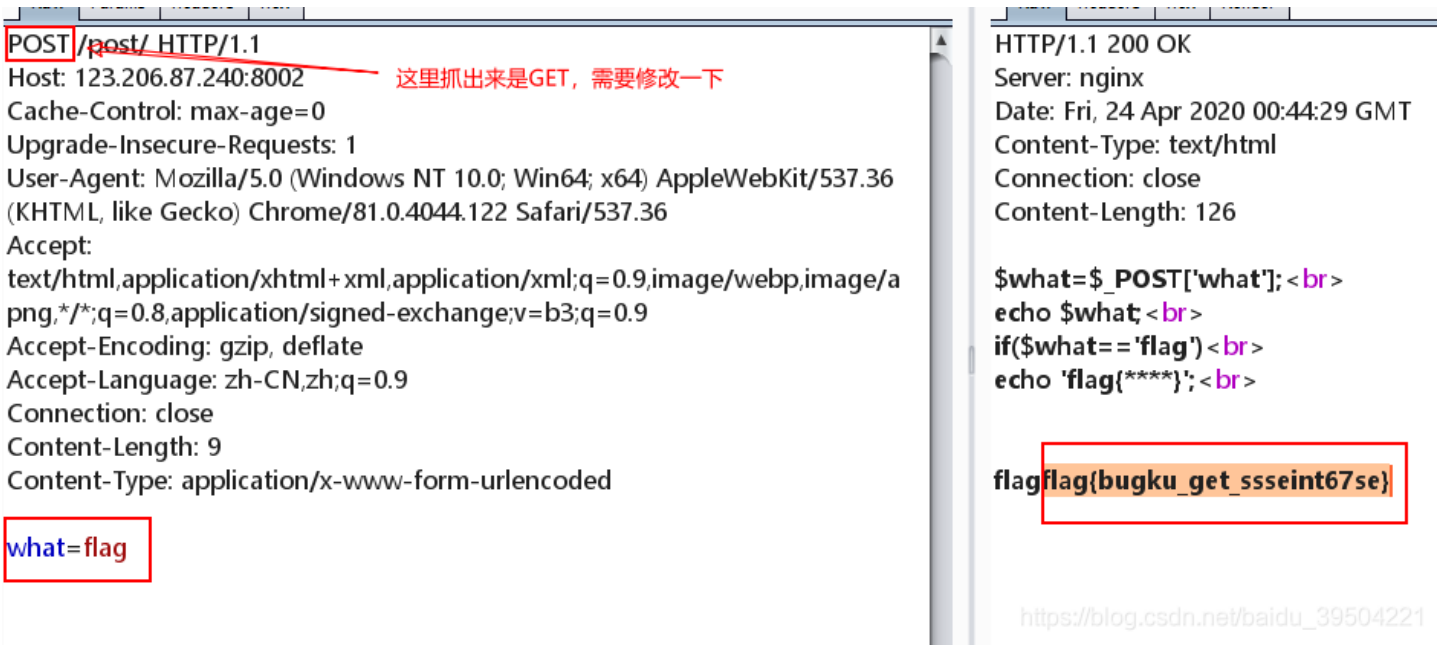
这里则是提交一个post

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

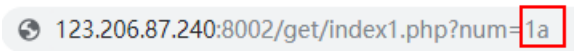


第二种方法是用BP抓包



矛盾

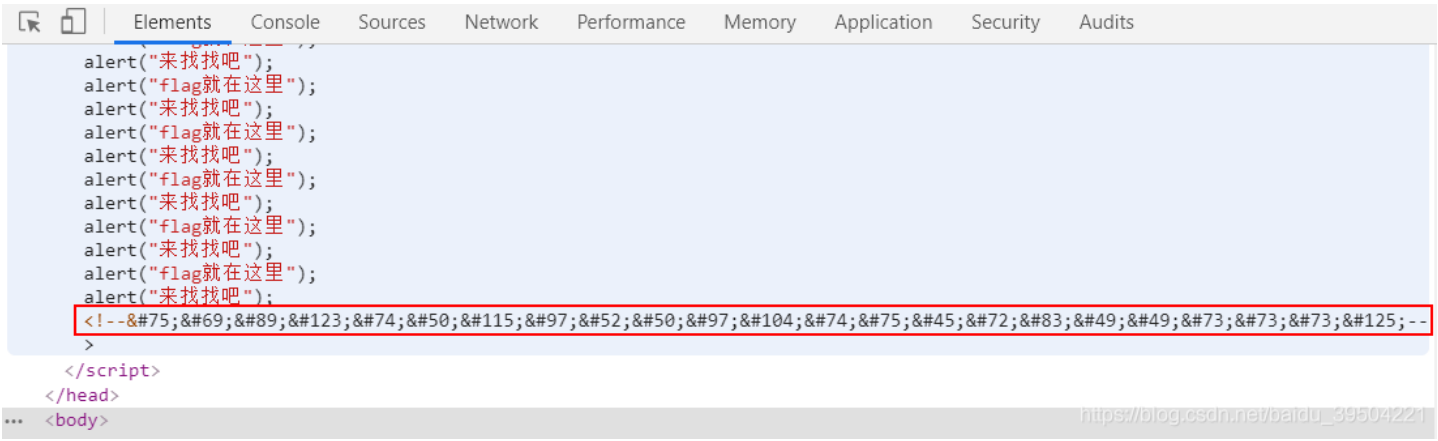
依照题意需要提交一个get参数num，需要num不是数字才能进入第一个if语句，有需要num==1才能输出flag



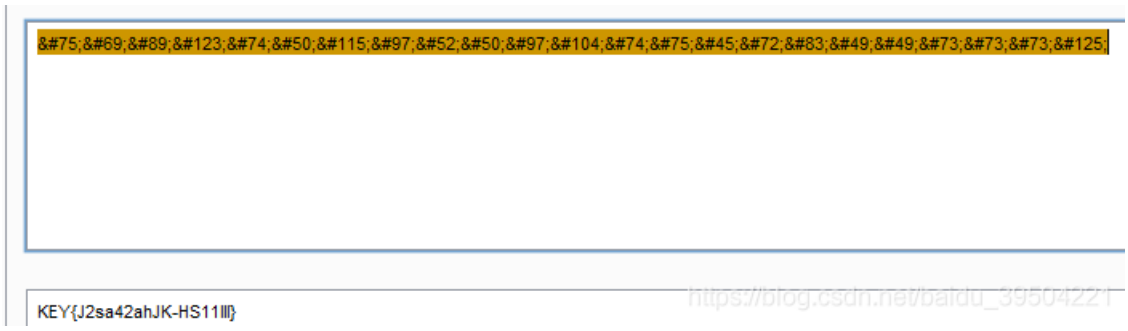
利用了php的一个特性

web3

弹窗都过完后 F12 发现一串神秘代码

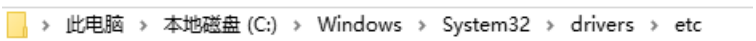


放到burpsuite里用HTML解码就行了

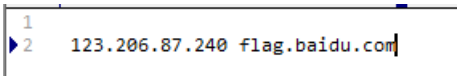


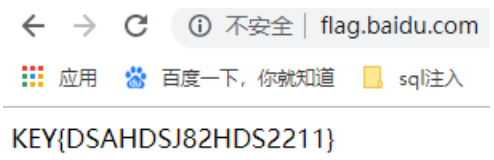
域名解析

这题我用的是本地解析



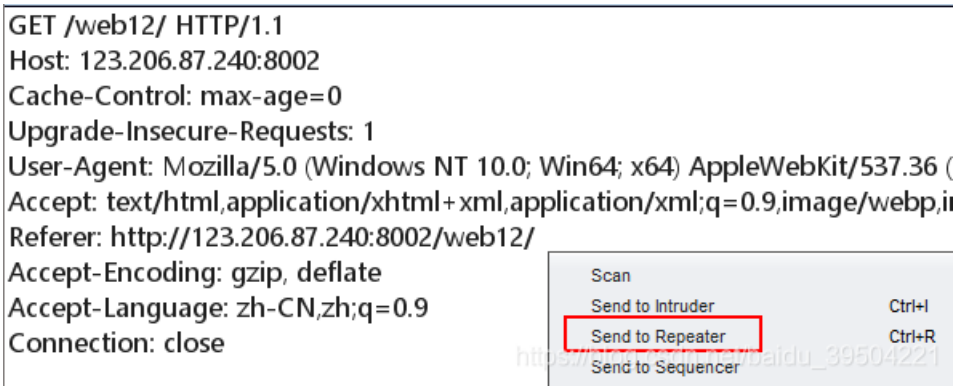
这个文件夹里有个host文件，用EditPlus打开，如下编辑



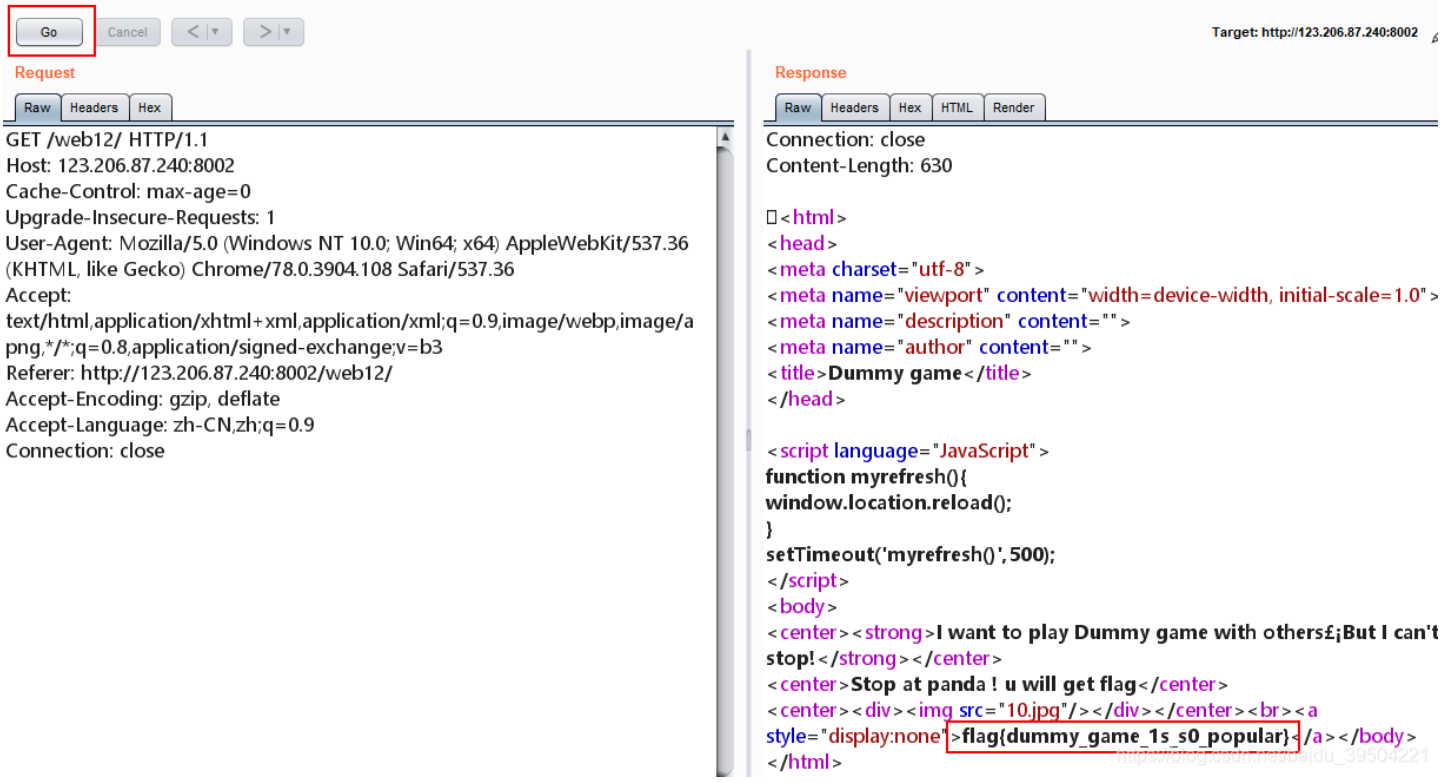


你必须让他停下

打开后网页一直在跳，我选择用burpsuite抓包试下



抓到后发到重发器



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

该网页无法正常运作

123.206.87.240 目前无法处理此请求。

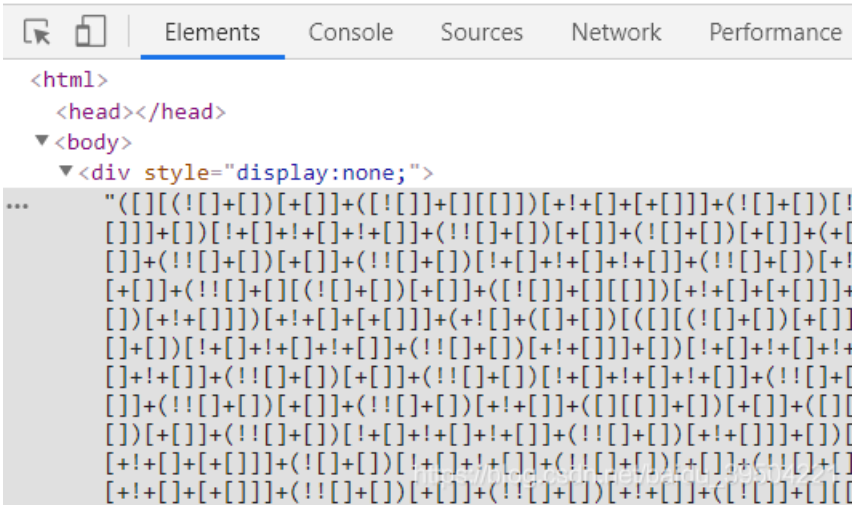
HTTP ERROR 500

重新加载

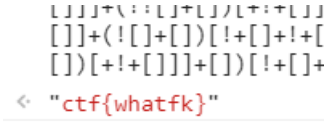
emmmmmm…恶魔妈妈摸猫猫

web5

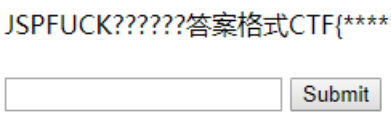
查看源代码，题目提示是JSPFUCK，百度了一下



发现这段代码是可以放到控制台执行的

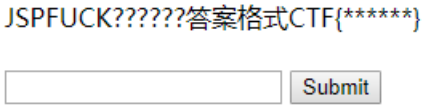


兴高采烈去提交



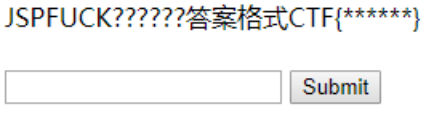
唉吆，已经非常非常接近了。。。

把ctf改成大写再试一下



在好好看看。

全部改成大写再试一下



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/a
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 Hex HTML Render

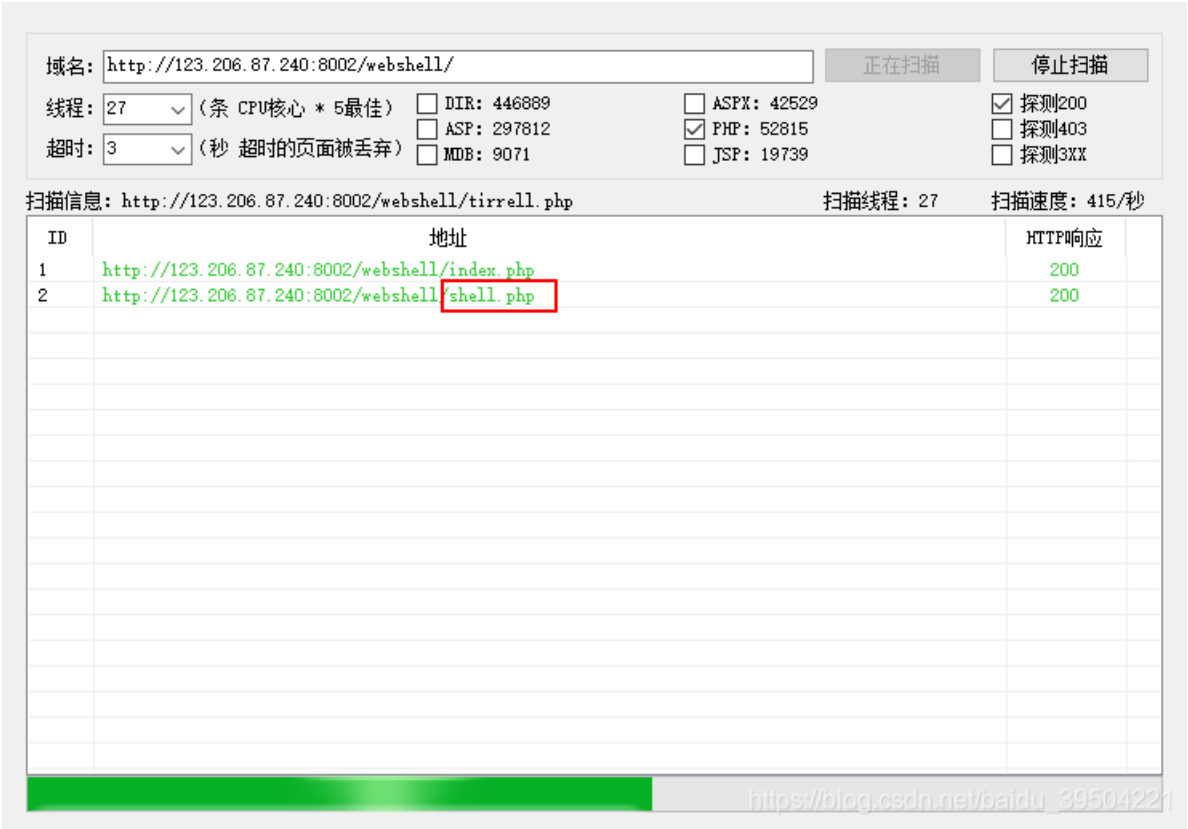
```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 15 Feb 2020 05:30:42 GMT
Content-Type: text/html
Connection: close
flag{Bugku_k8_23s_istra}:
Content-Length: 139


<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

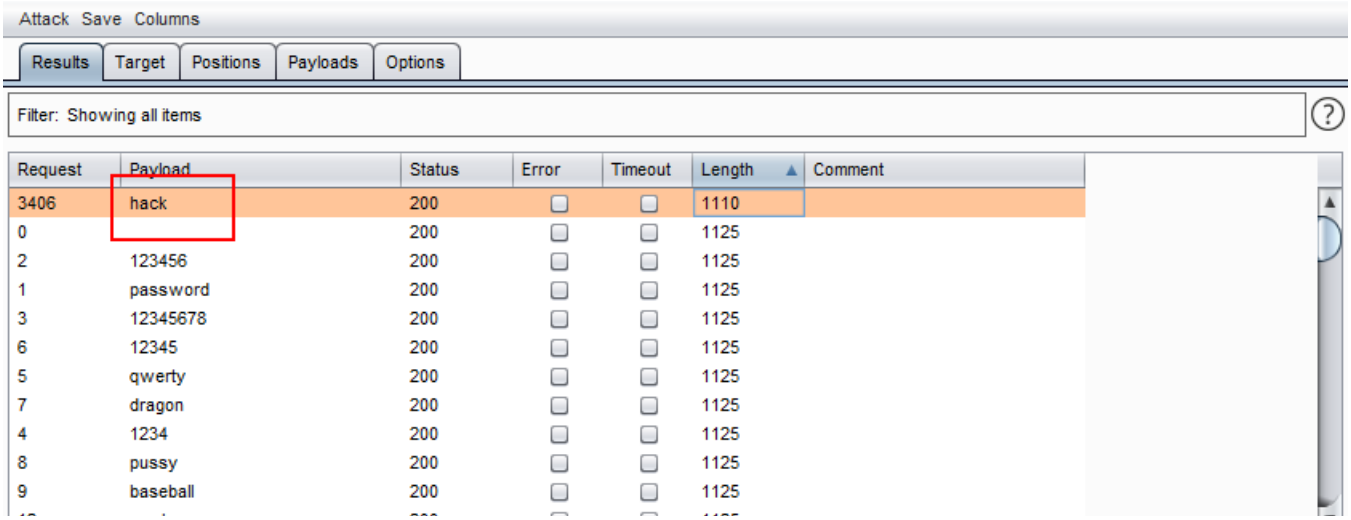
右键菜单被禁了，但F12还有用，但是没什么提示
因为是网站被黑且URL提示webshell

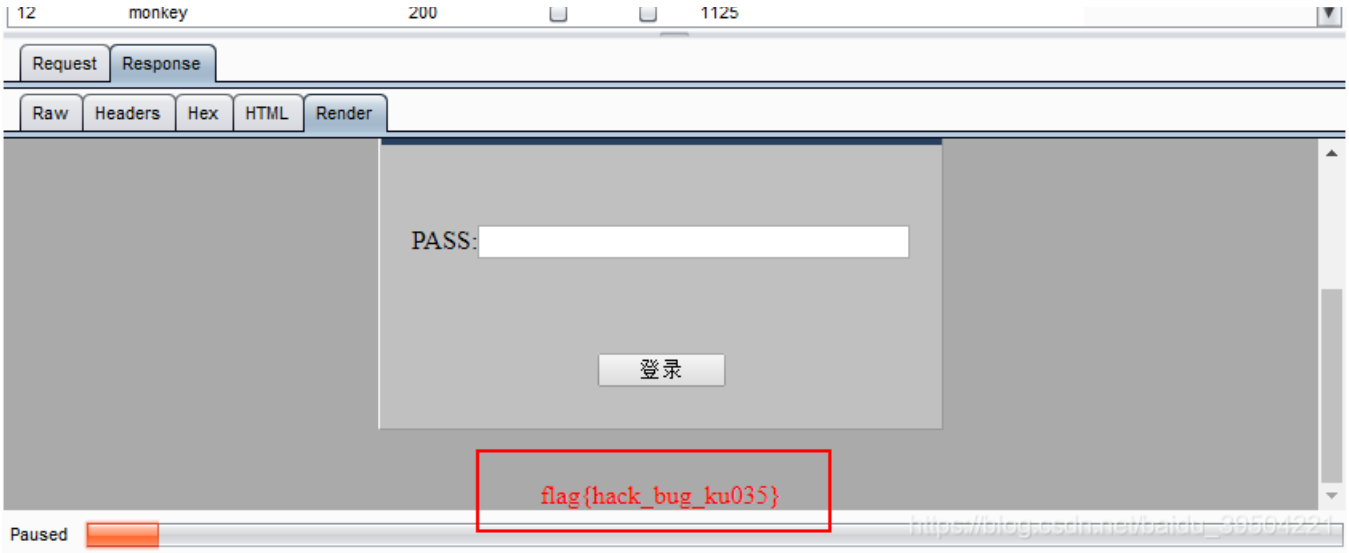
所以我用御剑扫了一下



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 <!-- dGVzdDEyMw== -->
```

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:

Submit Reset

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>
```


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?

Submit

KEY{J22JK-HS11}

flag在index里

点开链接

click me? no

再点进去

test5

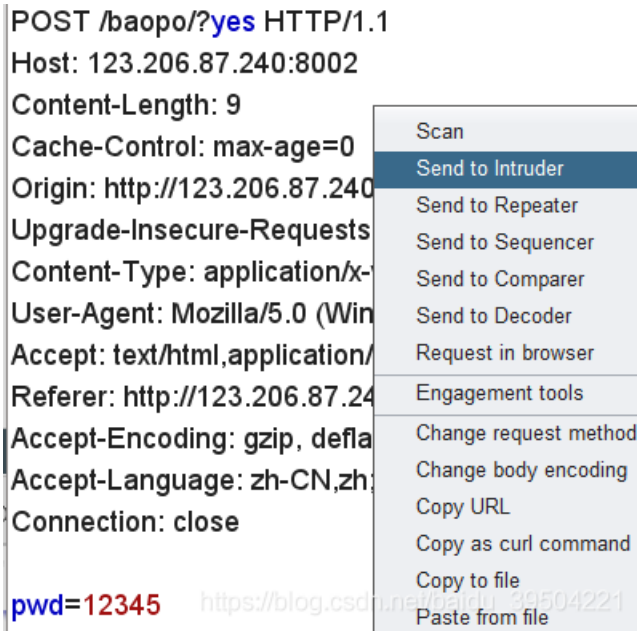
发现这里有文件包含的嫌疑
根据题目 flag在index里 把show改成index试了一下
一点hint都没用 百度看了看大佬的文章
https://blog.csdn.net/zpy1998zpy/article/details/80585443
发现是用了 php://filter/ 协议，受教了

输入密码查看flag

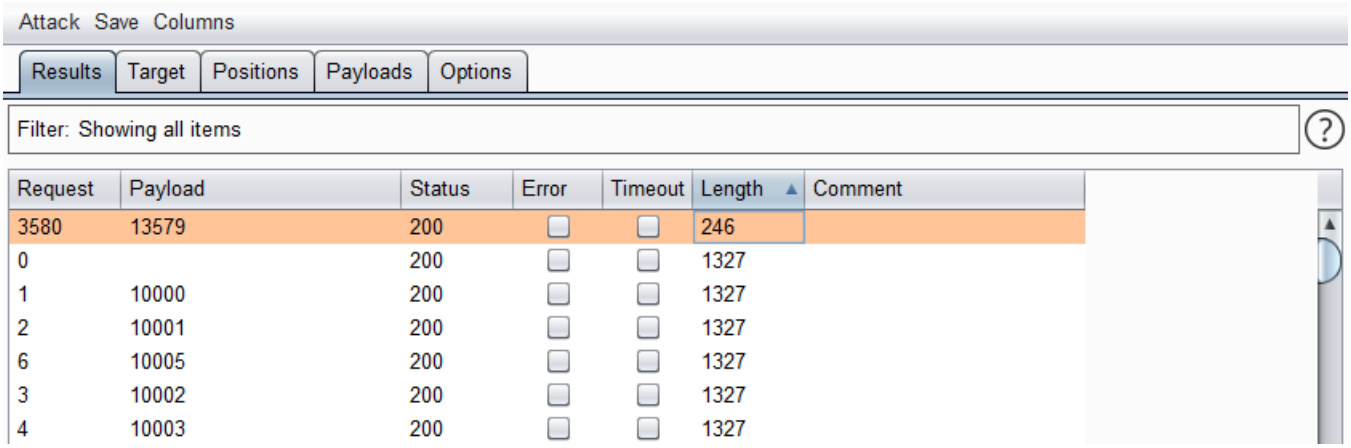
很自然想到爆破
写了个c把五位数都读出来

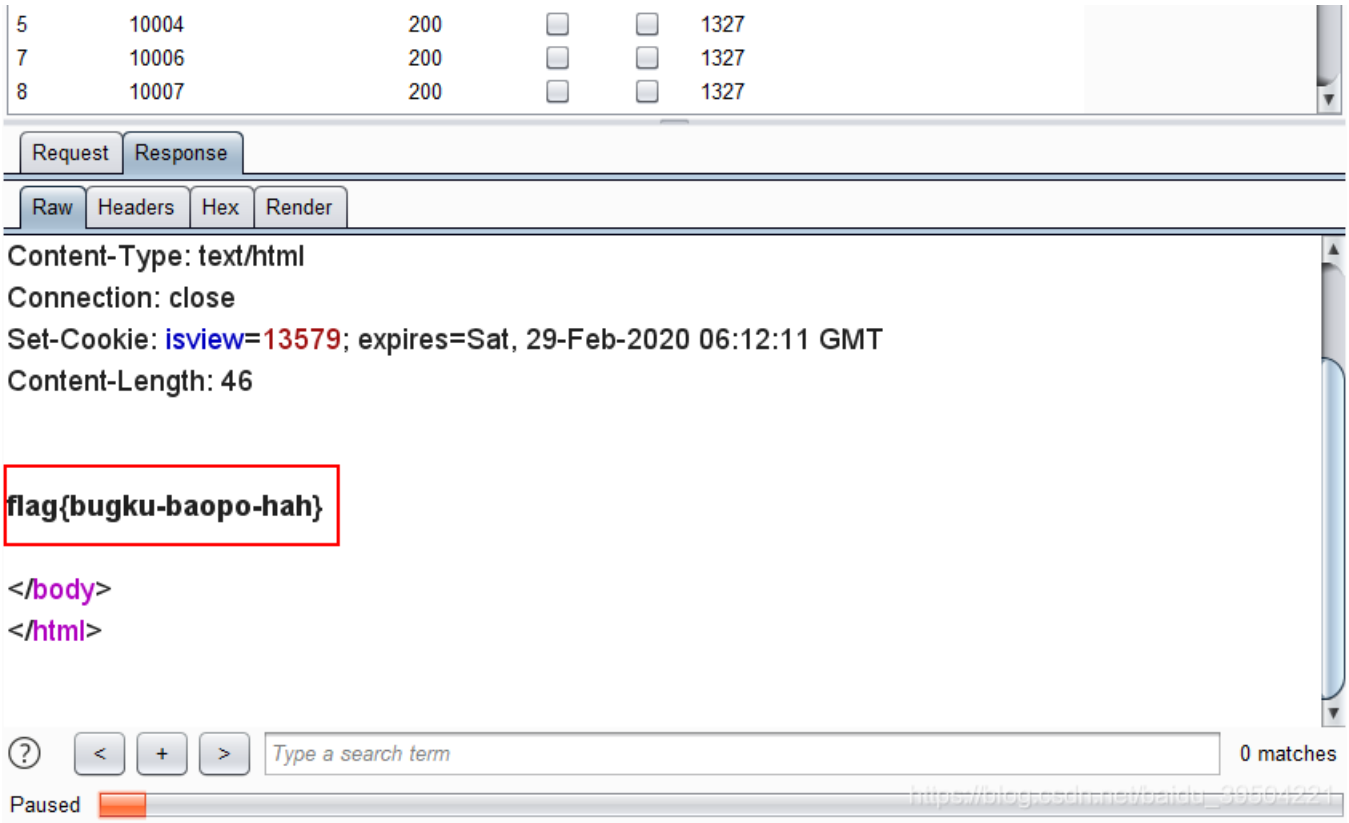
```c
#include<stdio.h>
int  main()
{
    int a;
    for( a = 10000 ; a < 100000 ;a++)
    {
        printf("%d\n",a);
    }
    return 0;
}
```

然后任意输入任意数字用burpsuite抓包



加载字典，start attack





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

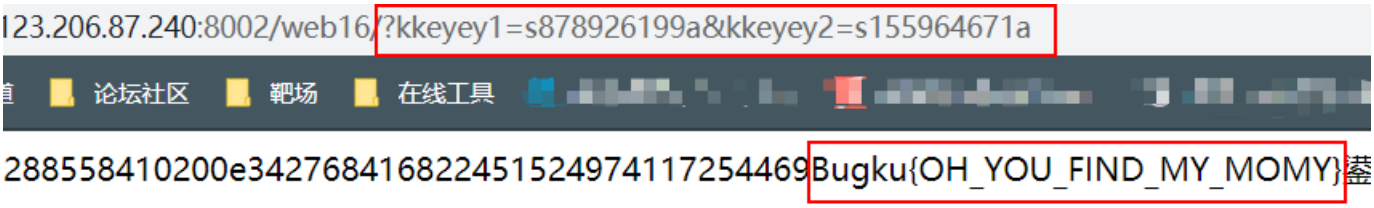
也就是要找某个bak文件
试了一下在URL后加个 flag.php.bak 404了（我之前用御剑扫出flag.php）
那加个 index.php.bak 下载了一个文件噢 放到vscode

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



创作打卡挑战赛