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

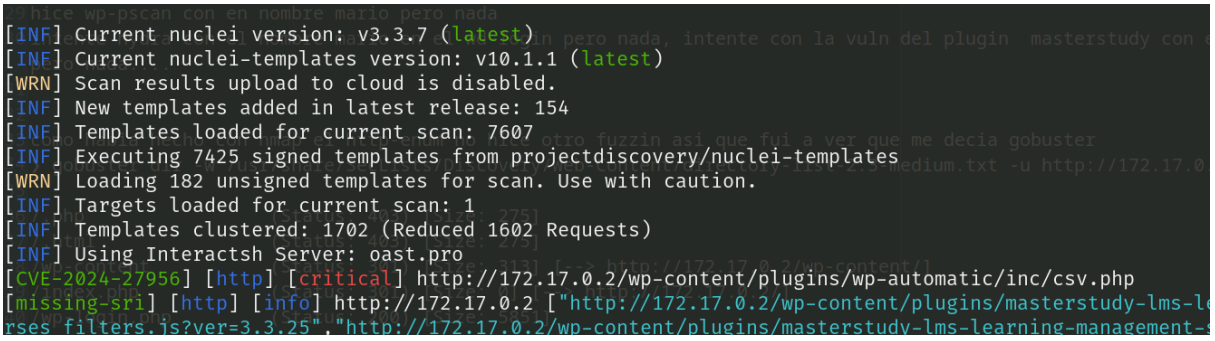
plugin masterstudy con el CVE 2023 4278 q loguea un usuario como admin pero nada....

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]

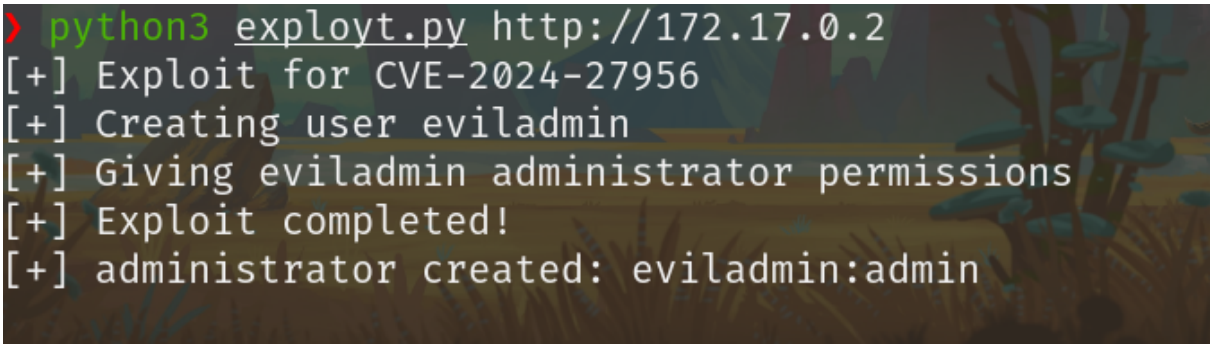
chequeamos con nuclei, herramienta que estoy usando por primera vez

`nuclei -u http://172.17.0.2`

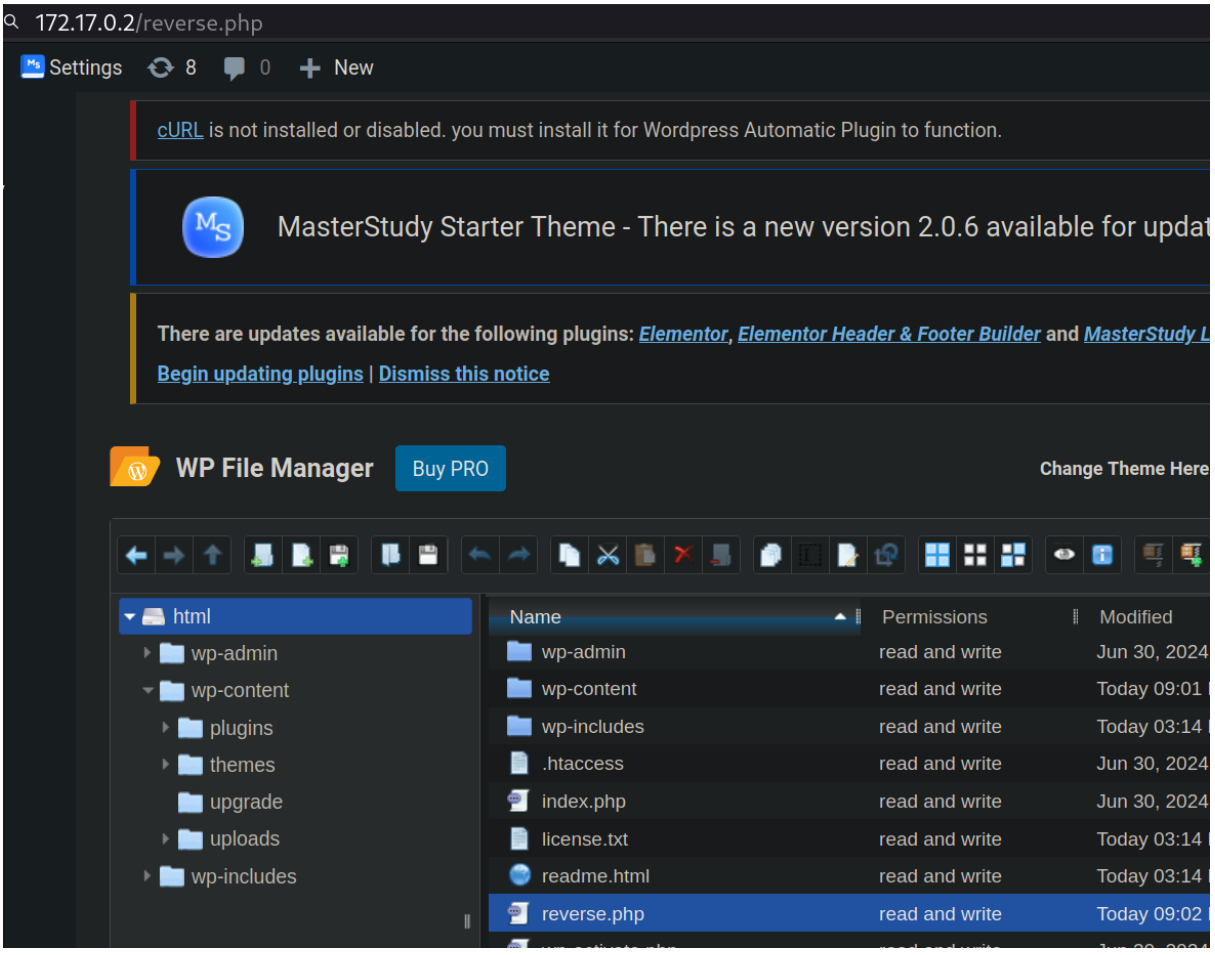


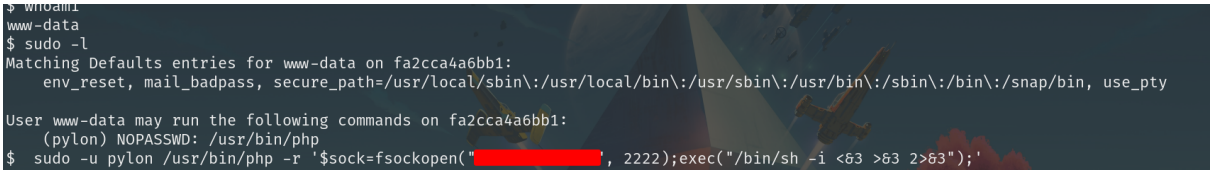
nos encuentra un plugin wp-automatic despues de provar unos cuantos q no funcionaron por diversos motivos, intente por vurpsuit pero no lo consegui, asi que encontre esta q lo hizo rapidisimo

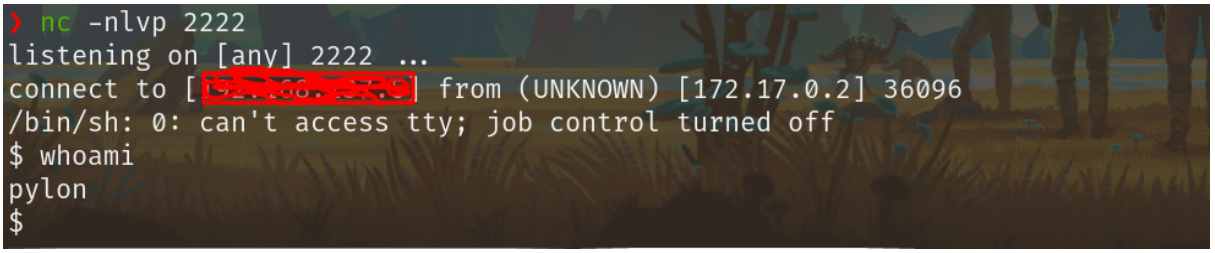
https://raw.githubusercontent.com/diego-tella/CVE-2024-27956-RCE/refs/heads/main/exploit.py



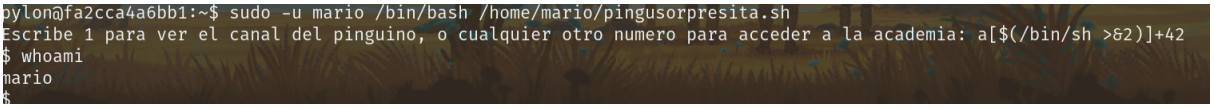
yo hice esto de costumvre







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



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