

109AB0716資安報告

壹、WSL

一、安裝WSL

二、檢查目錄

我們先來嘗試找出Ubuntu的檔案根目錄，結果發現裡面檔案都被隱藏起來了
這是為了避免用Window介面意外更動到Linux的檔案，造成錯誤

三、Ubuntu教學

1. 利用 `login` 登入，並且輸入密碼

2. BASH基本指令

3. 這樣我們就進到vim編輯器中

4. 按 `I` 進入編輯模式

5. `#!` 代表通往直譯器的路徑，而我們直譯器 `bash` 預設放在 `/bin` 目錄中

若 `#` 就代表備註，此行並不會被執行

這裡我們用 `read` 指令讀進input，並用 `$name` 抓取變數name，`echo` 印出結果

6. 嘗試利用 `:p` 指令儲存 `hello.sh` 檔案並退出 `vim` 筆記本

7. 但這樣會跳出來退出失敗，這是由於還並沒有儲存

8. 利用 `:wp` 指令儲存 `hello.sh` 檔案並退出 `vim` 編輯器

9. 利用 `cat` 指令查看 `hello.sh` 檔案內容

10. 利用 `bash` 指令執行 `hello.sh` 檔案

貳、WSL的GUI

1. 安裝VcXsrv

2. 透過WSL安裝環境

3. 新增一個Bash Script用來啟動gui

4. 以vim編輯內容

5. 執行

6. 開啟X server

6. 修改用戶名稱

7. 理論上這樣就可以了，但我還是打不開

參、改用套件來安裝GUI

1. 更新apt-get，確保list汰舊換新

2. 安裝 Gedit

3. 安裝 GIMP

4. 安裝 Nautilus

5. 安裝 VLC

6. 安裝 X11 應用程式

7. 安裝 Google Chrome for Linux

切換到暫存目錄：`cd /tmp`

透過 wget 安裝套件：`sudo wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb`

取得穩定的版本：`sudo dpkg -i google-chrome-stable_current_amd64.deb`

修正安裝套件：`sudo apt install --fix-broken -y`

再設定一次套件：`sudo dpkg -i google-chrome-stable_current_amd64.deb`

然後還是失敗了，不過還是有學到很多東西

肆、WebGoat

一、安裝流程:

1. 下載JDK
2. 下載Webgoat
3. 設定環境變數
4. 打開終端機
5. 輸入指令開啟Webgoat
6. 開啟瀏覽器，輸入<http://localhost:8080/WebGoat>

二、使用流程

1. 註冊帳號
2. 登入成功!
3. 打開Lesson 1
4. 第二節內容，輸入名字
5. 當打開F12後發現是一個POST
6. 查驗magic number，先送出之後觀測header

三、模擬Proxy

1. 下載ZAP
2. 設定port為8081
3. 打開工具裡的選項
4. 生成憑證且儲存
5. 打開瀏覽器→設定→安全性→隱私→憑證
6. 選擇受信任的根憑證授權單位
7. 確認無誤點擊完成
8. 設定→查詢→開啟電腦的Proxy設定
9. 設定為一樣的8081

伍、Markdown語法

測試文字

測試文字

測試文字

陸、參考資料

壹、WSL

一、安裝WSL

SETP1 啟用 Windows 子系統 Linux 版

```
dism.exe /online /enable-feature /featurename:Microsoft-Windows-Subsystem-Linux /all /norestart
```

SETP2 啟用虛擬機器功能

```
dism.exe /online /enable-feature /featurename:VirtualMachinePlatform /all /norestart
```

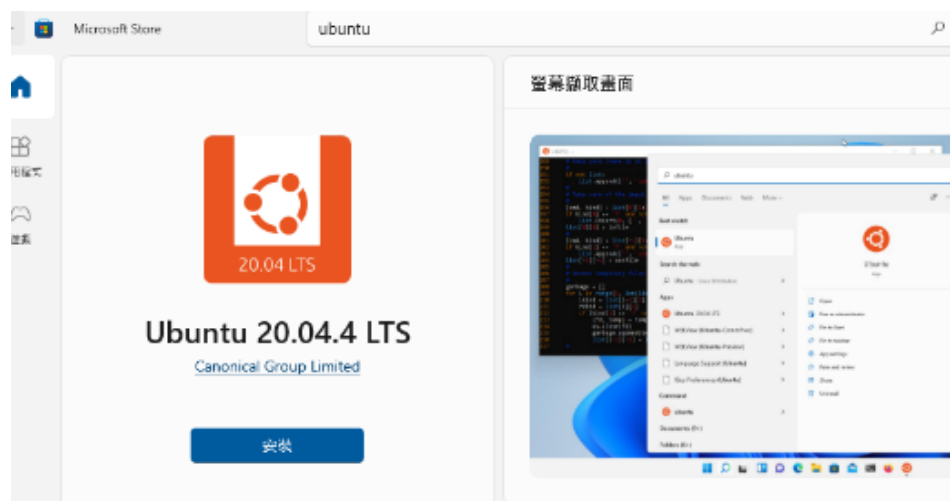
SETP3 從以下連結下載 Linux 核心更新套件

https://wslstorestorage.blob.core.windows.net/wslblob/wsl_update_x64.msi

SETP4 將 WSL 2 設定為預設版本

```
wsl --set-default-version 2
```

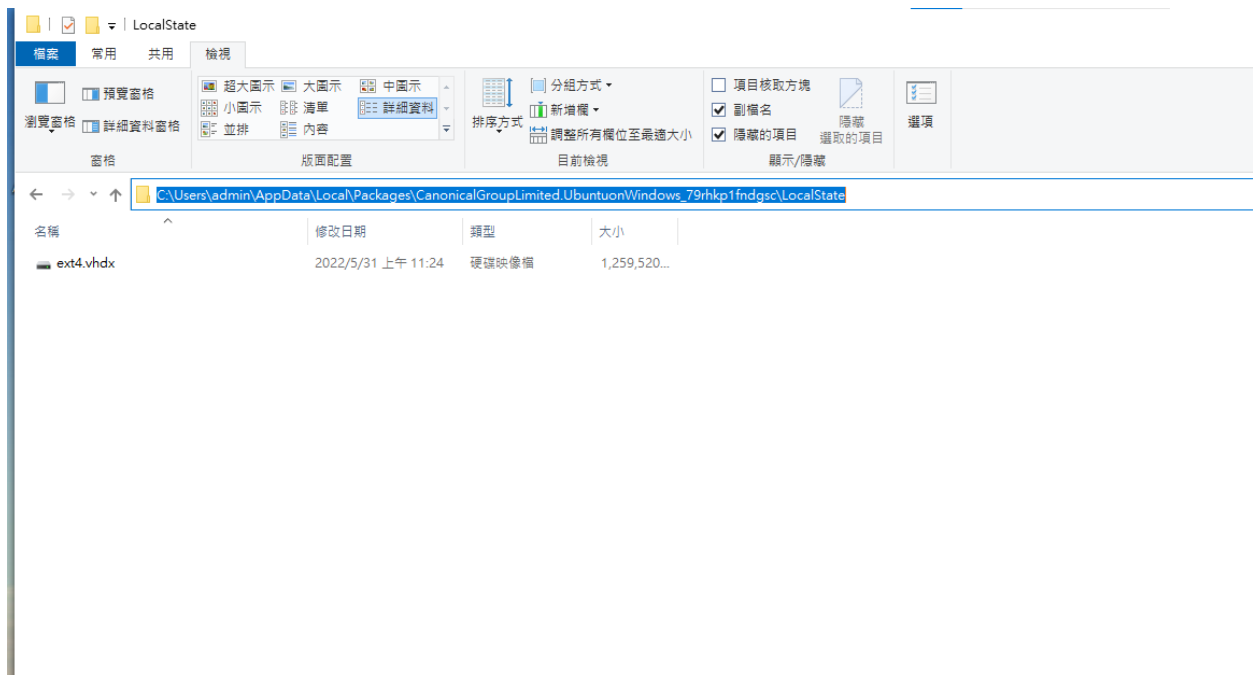
SETP5 到微軟商店安裝Linux，這裡我選用Ubuntu 20.04.4 LTS



二、檢查目錄

我們先來嘗試找出Ubuntu的檔案根目錄，結果發現裡面檔案都被隱藏起來了

這是為了避免用Window介面意外更動到Linux的檔案，造成錯誤



三、Ubuntu教學

1.利用 `login` 登入，並且輸入密碼

```
ez945y@DESKTOP-MBOCTE4:~$ sudo login
[sudo] password for ez945y:
DESKTOP-MBOCTE4 login:
Login timed out after 60 seconds.
ez945y@DESKTOP-MBOCTE4:~$ pwd
/home/ez945y
```

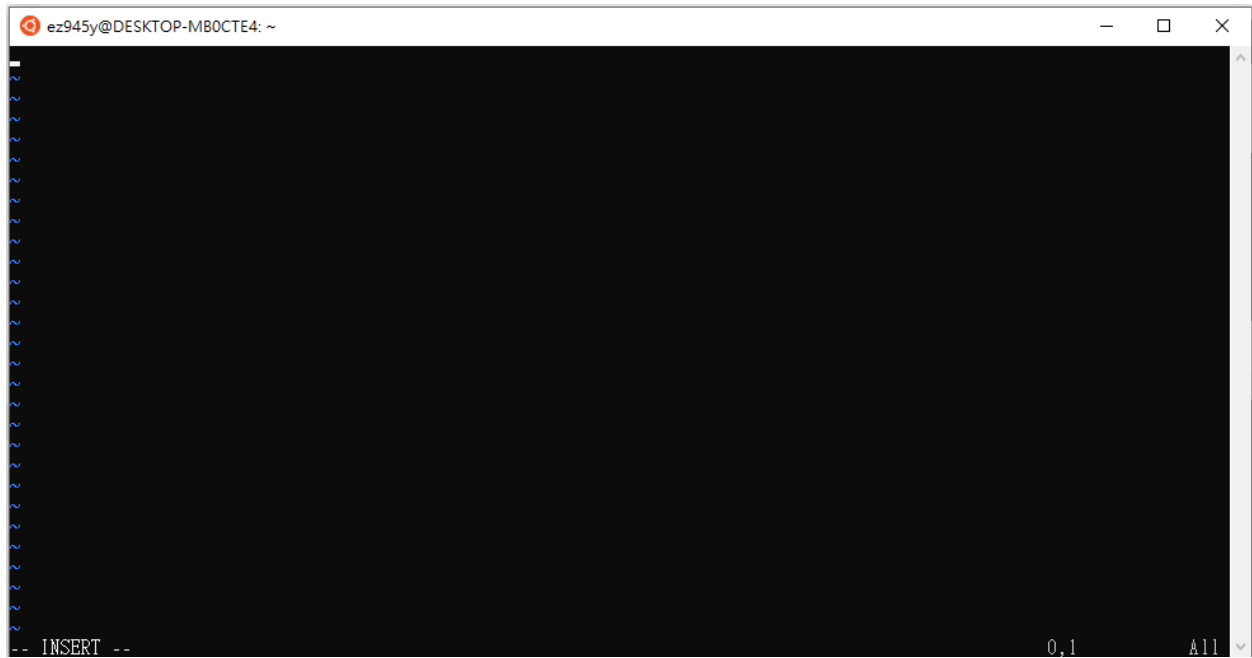
2.BASH基本指令

- `pwd` 顯示目前所在位置(print word)
- `ls` 顯示目前所在位置的檔案(list)
- `cd` 切換當前所在位置的檔案(change word)
- `.` 代表目前所在位置
- `..` 代表目前所在位置的父資料夾

- ```
ez945y@DESKTOP-MBOCTE4: ~
ez945y@DESKTOP-MBOCTE4:~$ pwd
/home/ez945y
ez945y@DESKTOP-MBOCTE4:~$ ls
ez945y@DESKTOP-MBOCTE4:~$ cd ..
ez945y@DESKTOP-MBOCTE4:~/home$ cd ez945y
ez945y@DESKTOP-MBOCTE4:~$ mkdir newbag
ez945y@DESKTOP-MBOCTE4:~$ vim hello.sh
```

ez945y@DESKTOP-MB0CTE4: ~

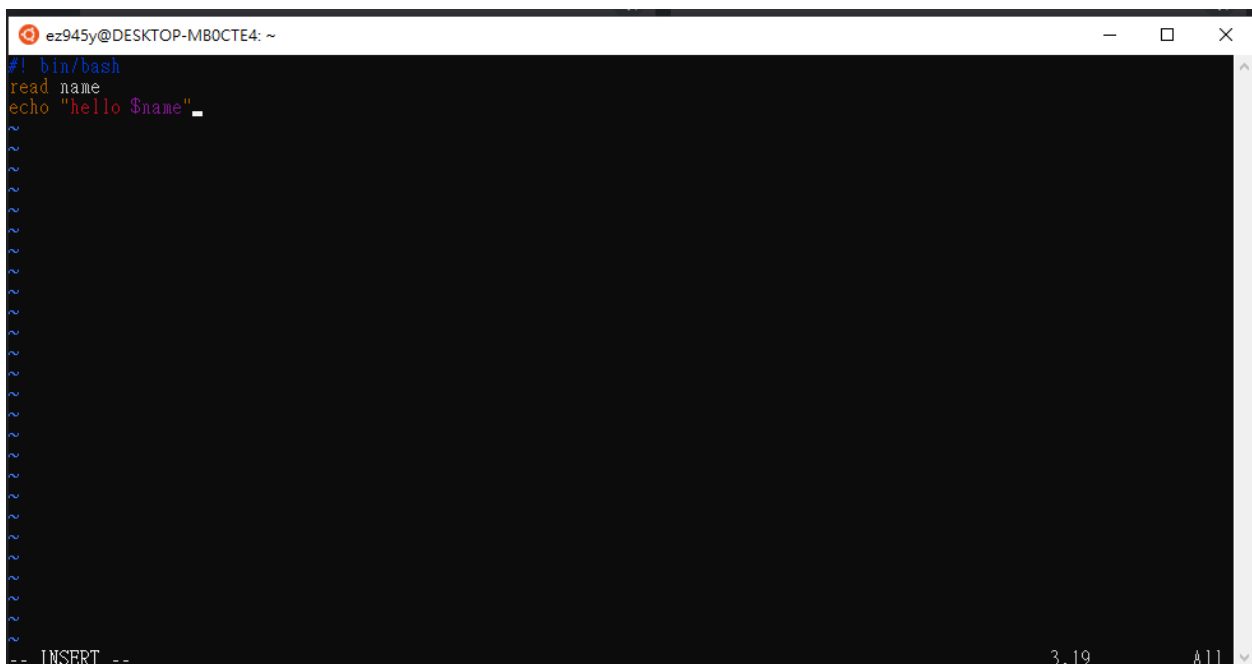
hello.sh [New File] 0,0-1 All



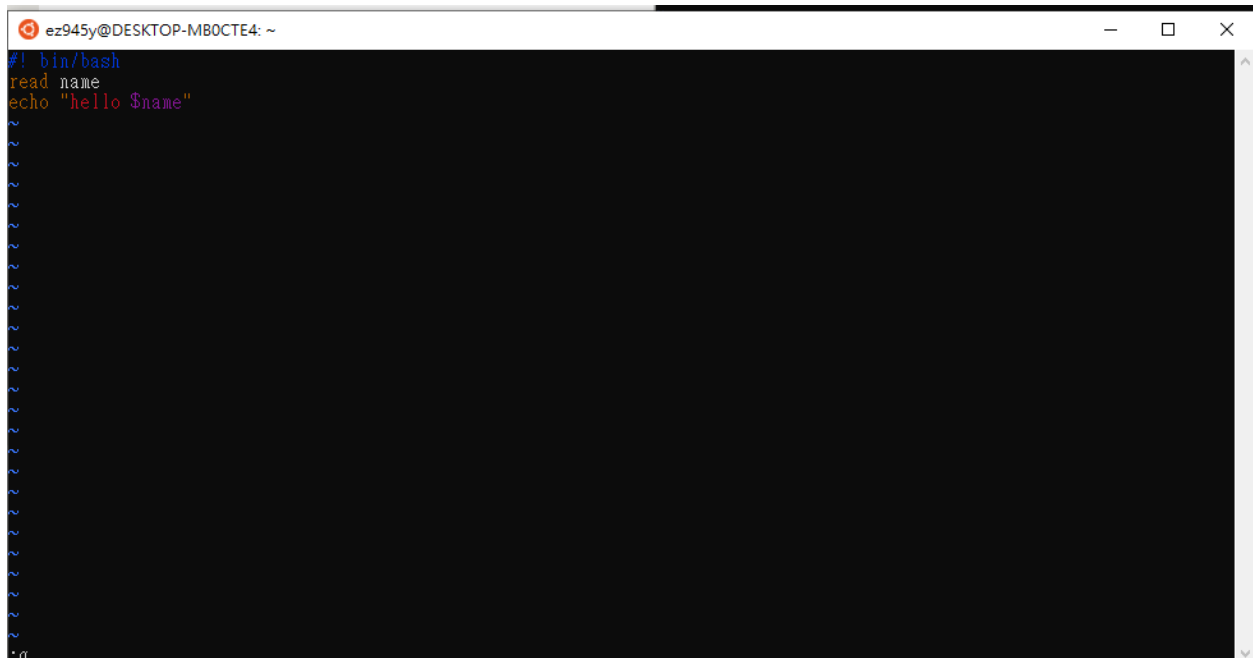
5. `#!` 代表通往直譯器的路徑，而我們直譯器 `bash` 預設放在 `/bin` 目錄中

若 `#` 就代表備註，此行並不會被執行

這裡我們用 `read` 指令讀進input，並用 `$name` 抓取變數name，`echo` 印出結果



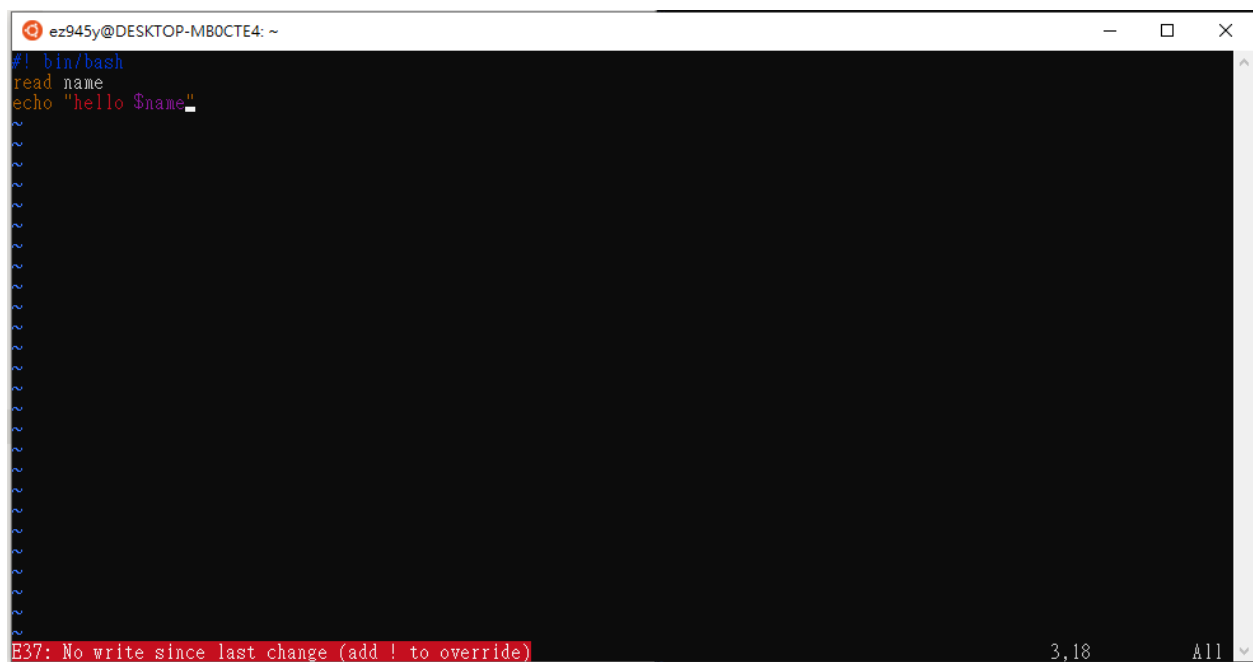
6.嘗試利用 `:p` 指令儲存 `hello.sh` 檔案並退出 `vim` 筆記本

A terminal window titled 'ez945y@DESKTOP-MB0CTE4: ~' with standard window controls. It contains a script: 

```
#!/bin/bash
read name
echo "hello $name"
```

 followed by several tilde (~) characters representing input. The script has been executed, but no output is visible.

7.但這樣會跳出來退出失敗，這是由於還並沒有儲存

A terminal window titled 'ez945y@DESKTOP-MB0CTE4: ~' with standard window controls. It contains the same script as the previous image: 

```
#!/bin/bash
read name
echo "hello $name"
```

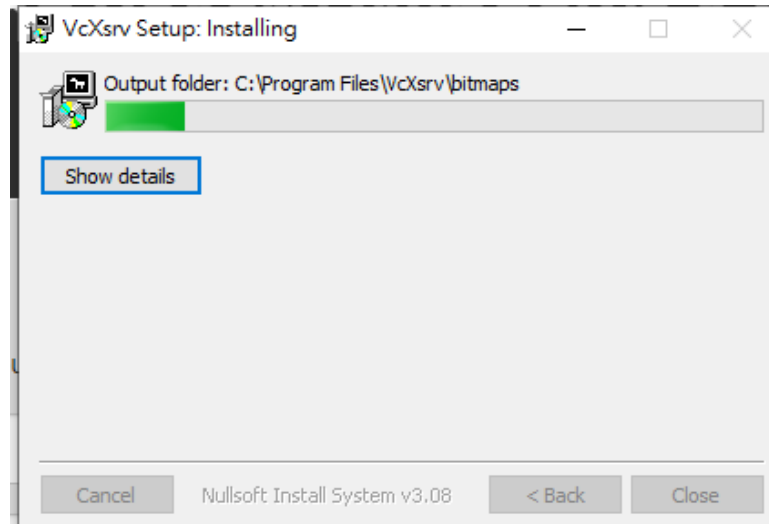
 followed by several tilde (~) characters. At the bottom, a red error message is displayed: `E37: No write since last change (add ! to override)`. To the right of the message, the text '3,18' and 'A11' are visible.

8.利用 `:wp` 指令儲存 `hello.sh` 檔案並退出 `vim` 編輯器





## 貳、WSL的GUI



### 1. 安裝VcXsrv

下載點：<https://sourceforge.net/projects/vcxsrv/files/latest/download>

### 2. 透過WSL安裝環境

```
sudo apt-get install ubuntu-desktop gnome-tweak-tool
```

```
ez945y@DESKTOP-MBOCTE4:/tmp$ xdpinfo
xdpyinfo: unable to open display "".
ez945y@DESKTOP-MBOCTE4:/tmp$ sudo apt-get install ubuntu-desktop gnome-tweak-tool
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package ubuntu-desktop
ez945y@DESKTOP-MBOCTE4:/tmp$ touch gui.sh
ez945y@DESKTOP-MBOCTE4:/tmp$ chmod u+x gui.sh
ez945y@DESKTOP-MBOCTE4:/tmp$ vim gui.sh
```

### 3. 新增一個Bash Script用來啟動gui

```
touch gui.sh
chmod u+x gui.sh
```

```
ez945y@DESKTOP-MB0CTE4: /tmp
~
bin/bash
sudo service dbus restart
/mnt/c/Program\ Files/VcXsrv/vcxsrv.exe :0 -ac &
DISPLAY=0:0 XDG_SESSION_TYPE=x11 gnome-session
/mnt/c/Windows/System32/taskkill.exe /IM vcxsrv.exe /T /F
```

## 4. 以vim編輯內容

```
#!/bin/bash
sudo service dbus restart
/mnt/c/Program\ Files/VcXsrv/vcxsrv.exe :0 -ac &
DISPLAY=0:0 XDG_SESSION_TYPE=x11 gnome-session
/mnt/c/Windows/System32/taskkill.exe /IM vcxsrv.exe /T /F
```

## 5. 執行

```
sudo ./gui.sh
```

```
ez945y@DESKTOP-MB0CTE4:/tmp$ cat gui.sh
#!/bin/bash
sudo service dbus restart
/mnt/c/Program\ Files/VcXsrv/vcxsrv.exe :0 -ac &
DISPLAY=0:0 XDG_SESSION_TYPE=x11 gnome-session
/mnt/c/Windows/System32/taskkill.exe /IM vcxsrv.exe /T /F
ez945y@DESKTOP-MB0CTE4:/tmp$ sudo bash gui.sh
* Stopping system message bus dbus [OK]
* Starting system message bus dbus
dbus[14874]: Unknown username "whoopsie" in message bus configuration file [OK]
Unable to init server: Could not connect: Connection refused

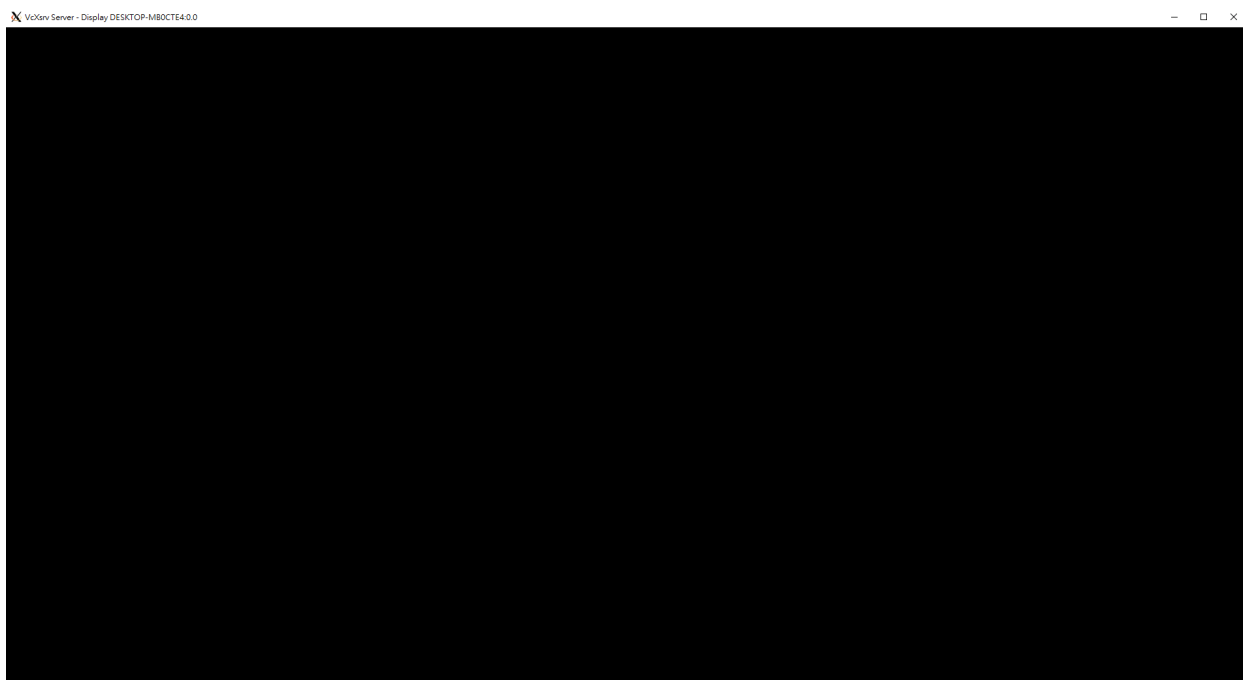
(gnome-session-check-accelerated:14889): Gtk-WARNING **: 13:30:47.535: cannot open display: 0:0
Unable to init server: Could not connect: Connection refused

(gnome-session-check-accelerated:14890): Gtk-WARNING **: 13:30:47.543: cannot open display: 0:0
gnome-session-binary[14879]: WARNING: software acceleration check failed: Child process exited with code 1
gnome-session-binary[14879]: CRITICAL: We failed, but the fail whale is dead. Sorry....
Welcome to the VcXsrv X Server
Vendor: The VcXsrv Project
Release: 1.20.14.0

OS: Windows NT 6.2 build 9200 (64-bit)
Contact: marha@users.sourceforge.net

LoadPreferences: C:\Users\admin\AppData\Roaming\XWinrc not found
LoadPreferences: Loading C:\Program Files\VcXsrv\system.XWinrc
成功: PID 為 7236 (PID 為 16976 的子處理程序) 的處理程序已終止。 [OK]
```

## 6. 開啟X server



## 6. 修改用戶名稱

```
sudo chown -R username:username .cache
```

## 7.理論上這樣就可以了，但我還是打不開

# 參、改用套件來安裝GUI

## 1.更新apt-get，確保list汰舊換新

```
ez945y@DESKTOP-MBOCTE4: ~
ez945y@DESKTOP-MBOCTE4:~$ sudo apt-get update
[sudo] password for ez945y:
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [1487 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal/universe amd64 Packages [8628 kB]
Get:7 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [255 kB]
Get:8 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [10.4 kB]
Get:9 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [945 kB]
Get:10 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-en [134 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 c-n-f Metadata [520 B]
Get:12 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [703 kB]
Get:13 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [126 kB]
Get:14 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [14.4 kB]
Get:15 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages [22.2 kB]
Get:16 http://security.ubuntu.com/ubuntu focal-security/multiverse Translation-en [5376 B]
Get:17 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f Metadata [512 B]
Get:18 http://archive.ubuntu.com/ubuntu focal/universe Translation-en [5124 kB]
Get:19 http://archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadata [265 kB]
Get:20 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [144 kB]
Get:21 http://archive.ubuntu.com/ubuntu focal/multiverse Translation-en [104 kB]
Get:22 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 c-n-f Metadata [9136 B]
Get:23 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1830 kB]
Get:24 http://archive.ubuntu.com/ubuntu focal-updates/main Translation-en [336 kB]
Get:25 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [15.4 kB]
Get:26 http://archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [1008 kB]
Get:27 http://archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [143 kB]
Get:28 http://archive.ubuntu.com/ubuntu focal-updates/restricted amd64 c-n-f Metadata [520 B]
Get:29 http://archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [924 kB]
Get:30 http://archive.ubuntu.com/ubuntu focal-updates/universe Translation-en [207 kB]
Get:31 http://archive.ubuntu.com/ubuntu focal-updates/universe amd64 c-n-f Metadata [20.7 kB]
Get:32 http://archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 Packages [24.4 kB]
Get:33 http://archive.ubuntu.com/ubuntu focal-updates/multiverse Translation-en [7336 B]
Get:34 http://archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 c-n-f Metadata [596 B]
Get:35 http://archive.ubuntu.com/ubuntu focal-backports/main amd64 Packages [44.5 kB]
Get:36 http://archive.ubuntu.com/ubuntu focal-backports/main Translation-en [10.9 kB]
Get:37 http://archive.ubuntu.com/ubuntu focal-backports/main amd64 c-n-f Metadata [980 B]
Get:38 http://archive.ubuntu.com/ubuntu focal-backports/restricted amd64 c-n-f Metadata [116 B]
Get:39 http://archive.ubuntu.com/ubuntu focal-backports/universe amd64 Packages [23.6 kB]
Get:40 http://archive.ubuntu.com/ubuntu focal-backports/universe Translation-en [15.9 kB]
Get:41 http://archive.ubuntu.com/ubuntu focal-backports/universe amd64 c-n-f Metadata [860 B]
```

## 2.安裝 Gedit



## 4.安裝 Nautilus

```
ez945y@DESKTOP-MB0CTE4:~$ sudo apt-get install nautilus -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
 gvfs gvfs-backends gvfs-common gvfs-daemons gvfs-libc libcdio-cdda2 libcdio-paranoia2 libcdio18 libcue2 libdee-1.0-4
 libexempi8 libgif7 libgsf-1-114 libgsf-1-common libgxps2 libmtp-common libmtp-runtime libmtp9
 libnautilus-extension1a libnfs13 libtotem-plparser-common libtotem-plparser18 libtracker-control-2.0-0
 libtracker-miner-2.0-0 libtracker-sparql-2.0-0 libunity-protocol-private0 libunity-scopes-json-def-desktop libunity9
 nautilus-data tracker tracker-extract tracker-miner-fs
Suggested packages:
 bluez-obexd samba-common unity-common eog evince l pdf-viewer gnome-sushi nautilus-extension-brasero nautilus-sendto
 totem l mp3-decoder
The following NEW packages will be installed:
 gvfs gvfs-backends gvfs-common gvfs-daemons gvfs-libc libcdio-cdda2 libcdio-paranoia2 libcdio18 libcue2 libdee-1.0-4
 libexempi8 libgif7 libgsf-1-114 libgsf-1-common libgxps2 libmtp-common libmtp-runtime libmtp9
 libnautilus-extension1a libnfs13 libtotem-plparser-common libtotem-plparser18 libtracker-control-2.0-0
 libtracker-miner-2.0-0 libtracker-sparql-2.0-0 libunity-protocol-private0 libunity-scopes-json-def-desktop libunity9
 nautilus nautilus-data tracker tracker-extract tracker-miner-fs
0 upgraded, 33 newly installed, 0 to remove and 163 not upgraded.
Need to get 3890 kB of archives.
After this operation, 16.2 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 gvfs-common all 1.44.1-1ubuntu1.1 [20.0 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 gvfs-libc amd64 1.44.1-1ubuntu1.1 [97.4 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 gvfs-daemons amd64 1.44.1-1ubuntu1.1 [118 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 gvfs amd64 1.44.1-1ubuntu1.1 [115 kB]
Get:5 http://archive.ubuntu.com/ubuntu focal/main amd64 libcdio18 amd64 2.0.0-2 [58.6 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal/main amd64 libcdio-cdda2 amd64 10.2+2.0.0-1 [17.6 kB]
Get:7 http://archive.ubuntu.com/ubuntu focal/main amd64 libcdio-paranoia2 amd64 10.2+2.0.0-1 [16.2 kB]
Get:8 http://archive.ubuntu.com/ubuntu focal/main amd64 libmtp-common all 1.1.17-3 [27.8 kB]
Get:9 http://archive.ubuntu.com/ubuntu focal/main amd64 libmtp9 amd64 1.1.17-3 [163 kB]
Get:10 http://archive.ubuntu.com/ubuntu focal/main amd64 libnfs13 amd64 4.0.0-1 [95.1 kB]
Get:11 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 gvfs-backends amd64 1.44.1-1ubuntu1.1 [344 kB]
Get:12 http://archive.ubuntu.com/ubuntu focal/main amd64 libcue2 amd64 2.2.1-2 [19.8 kB]
Get:13 http://archive.ubuntu.com/ubuntu focal/main amd64 libdee-1.0-4 amd64 1.2.7+17.10.20170616-4ubuntu6 [130 kB]
Get:14 http://archive.ubuntu.com/ubuntu focal/main amd64 libexempi8 amd64 2.5.1-1build1 [528 kB]
Get:15 http://archive.ubuntu.com/ubuntu focal/main amd64 libgif7 amd64 5.1.9-1 [32.2 kB]
Get:16 http://archive.ubuntu.com/ubuntu focal/main amd64 libgsf-1-common all 1.14.46-1 [12.7 kB]
Get:17 http://archive.ubuntu.com/ubuntu focal/main amd64 libgsf-1-114 amd64 1.14.46-1 [98.3 kB]
```

## 5.安裝 VLC

```
ez945y@DESKTOP-MB0CTE4:~$ sudo apt-get install vlc -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
 fonts-freefont-ttf liba52-0.7.4 libaribb24-0 libass9 libbasicusageenvironment1 libcddb2 libdc1394-22 libdca0
 libdouble-conversion3 libdvbpsi10 libdvnav4 libdvread7 libebml4v5 libfaad2 libgroupsock8 libixml10 libkate1
 liblirc-client0 liblivemedia77 liblua5.2-0 libmad0 libmatroska6v5 libmpcdec6 libmpeg2-4 libmysofa1
 libopenmpt-modplug1 libpcre2-16-0 libplacebo7 libpostproc55 libprotobuf-lite17 libproxy-tools libqt5core5a
 libqt5dbus5 libqt5gui5 libqt5network5 libqt5svg5 libqt5widgets5 libqt5xmlextras5 libresid-builder0c2a
 libSDL-image1.2 libSDL1.2debian libsidplay2 libsndio7.0 libspatialaudio0 libsrtp1 libssh2-1 libupnp13
 libusageenvironment3 libva-wayland2 libvlc-bin libvlc5 libvlccore9 libxcb-xinerama0 libxcb-xinput0
 qt5-gtk-platformtheme qttranslations5-l10n vlc-bin vlc-data vlc-l10n vlc-plugin-base vlc-plugin-notify vlc-plugin-qt
 vlc-plugin-samba vlc-plugin-skins2 vlc-plugin-video-output vlc-plugin-video-splitter vlc-plugin-visualization
Suggested packages:
 libdvdcss2 lirc qt5-image-formats-plugins qtwayland5 sndiod
The following NEW packages will be installed:
 fonts-freefont-ttf liba52-0.7.4 libaribb24-0 libass9 libbasicusageenvironment1 libcddb2 libdc1394-22 libdca0
 libdouble-conversion3 libdvbpsi10 libdvnav4 libdvread7 libebml4v5 libfaad2 libgroupsock8 libixml10 libkate1
 liblirc-client0 liblivemedia77 liblua5.2-0 libmad0 libmatroska6v5 libmpcdec6 libmpeg2-4 libmysofa1
 libopenmpt-modplug1 libpcre2-16-0 libplacebo7 libpostproc55 libprotobuf-lite17 libproxy-tools libqt5core5a
 libqt5dbus5 libqt5gui5 libqt5network5 libqt5svg5 libqt5widgets5 libqt5xmlextras5 libresid-builder0c2a
 libSDL-image1.2 libSDL1.2debian libsidplay2 libsndio7.0 libspatialaudio0 libsrtp1 libssh2-1 libupnp13
 libusageenvironment3 libva-wayland2 libvlc-bin libvlc5 libvlccore9 libxcb-xinerama0 libxcb-xinput0
 qt5-gtk-platformtheme qttranslations5-l10n vlc-bin vlc-data vlc-l10n vlc-plugin-base vlc-plugin-notify
 vlc-plugin-qt vlc-plugin-samba vlc-plugin-skins2 vlc-plugin-video-output vlc-plugin-video-splitter
 vlc-plugin-visualization
0 upgraded, 68 newly installed, 0 to remove and 163 not upgraded.
Need to get 27.0 MB of archives.
After this operation, 125 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/universe amd64 libdouble-conversion3 amd64 3.1.5-4ubuntu1 [37.9 kB]
```

## 6.安裝 X11 應用程式

```
ez945y@DESKTOP-MBOCTE4:~$ sudo apt install x11-apps -y
[sudo] password for ez945y:
Reading package lists... Done
Building dependency tree
Reading state information... Done
x11-apps is already the newest version (7.7+8).
0 upgraded, 0 newly installed, 0 to remove and 163 not upgraded.
```

## 7.安裝 Google Chrome for Linux

```
ez945y@DESKTOP-MBOCTE4:/tmp$ sudo apt-get install --fix-broken -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
Correcting dependencies... Done
The following additional packages will be installed:
 fonts-liberation
The following NEW packages will be installed:
 fonts-liberation
0 upgraded, 1 newly installed, 0 to remove and 163 not upgraded.
1 not fully installed or removed.
Need to get 822 kB of archives.
After this operation, 2139 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 fonts-liberation all 1:1.07.4-11 [822 kB]
Fetched 822 kB in 2s (357 kB/s)
Selecting previously unselected package fonts-liberation.
(Reading database ... 68750 files and directories currently installed.)
Preparing to unpack .../fonts-liberation_1%3a1.07.4-11_all.deb ...
Unpacking fonts-liberation (1:1.07.4-11) ...
Setting up fonts-liberation (1:1.07.4-11) ...
Setting up google-chrome-stable (102.0.5005.61-1) ...
update-alternatives: using /usr/bin/google-chrome-stable to provide /usr/bin/x-www-browser (x-www-browser) in auto mode
update-alternatives: using /usr/bin/google-chrome-stable to provide /usr/bin/gnome-www-browser (gnome-www-browser) in au
to mode
update-alternatives: using /usr/bin/google-chrome-stable to provide /usr/bin/google-chrome (google-chrome) in auto mode
Processing triggers for fontconfig (2.13.1-2ubuntu3) ...
ez945y@DESKTOP-MBOCTE4:/tmp$ sudo dpkg -i google-chrome-stable_current_amd64.deb
(Reading database ... 68773 files and directories currently installed.)
Preparing to unpack google-chrome-stable_current_amd64.deb ...
Unpacking google-chrome-stable (102.0.5005.61-1) over (102.0.5005.61-1) ...
Setting up google-chrome-stable (102.0.5005.61-1) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
```

切換到暫存目錄：`cd /tmp`

透過 wget 安裝套件：`sudo wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb`

取得穩定的版本：`sudo dpkg -i google-chrome-stable_current_amd64.deb`

修正安裝套件：`sudo apt install --fix-broken -y`

再設定一次套件：`sudo dpkg -i google-chrome-stable_current_amd64.deb`

```
ez945y@DESKTOP-MBOCTE4:/tmp$ sudo wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb
--2022-05-31 13:00:09-- https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb
Resolving dl.google.com (dl.google.com)... 172.217.160.110, 2404:6800:4012:4::200e
Connecting to dl.google.com (dl.google.com)|172.217.160.110|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 84701968 (81M) [application/x-debian-package]
Saving to: 'google-chrome-stable_current_amd64.deb' t upgraded.
Need to get 685 kB of archives.
google-chrome-stable_current_ 100%[=====] 80.78M 10.2MB/s in 7.6s
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 x11-apps amd64 7.7+8 [657 kB]
2022-05-31 13:00:17 (10.6 MB/s) - 'google-chrome-stable_current_amd64.deb' saved [84701968/84701968]
Fetched 685 kB in 2s (302 kB/s)
ez945y@DESKTOP-MBOCTE4:/tmp$ sudo dpkg -i google-chrome-stable_current_amd64.deb
Selecting previously unselected package google-chrome-stable.
(Reading database ... 68636 files and directories currently installed.)
Preparing to unpack google-chrome-stable_current_amd64.deb ...
Unpacking google-chrome-stable (102.0.5005.61-1) ...
dpkg: dependency problems prevent configuration of google-chrome-stable:
 google-chrome-stable depends on fonts-liberation; however:
 Package fonts-liberation is not installed.

dpkg: error processing package google-chrome-stable (--install):
 dependency problems - leaving unconfigured
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
Errors were encountered while processing:
 google-chrome-stable
```

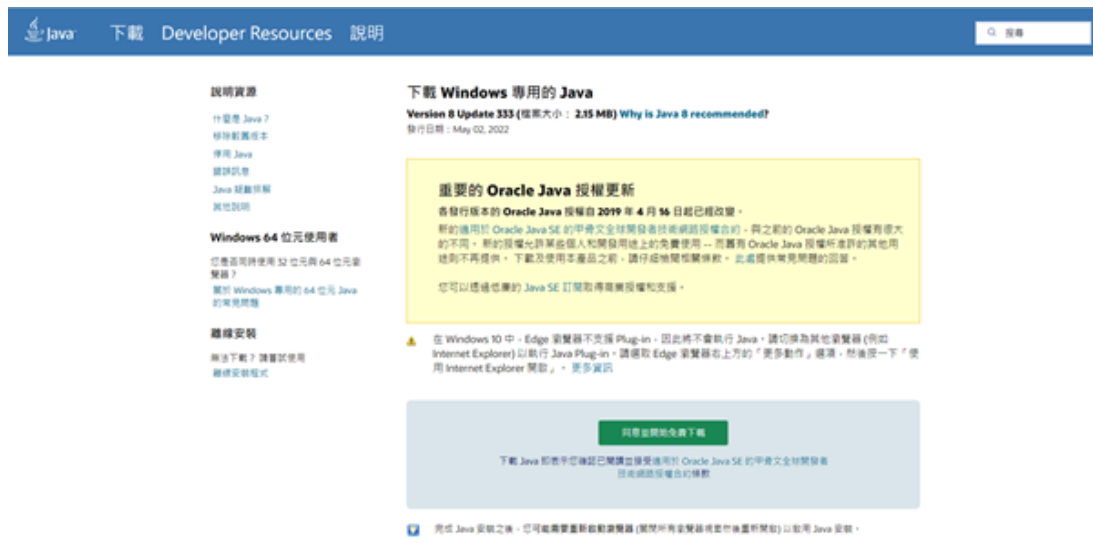
然後還是失敗了，不過還是有學到很多東西



# 肆、WebGoat

## 一、安裝流程:

### 1.下載JDK



說明資源

- 什麼是 Java ?
- 取得新舊版本
- 使用 Java
- 錯誤訊息
- Java 安裝指南
- 其他說明

**Windows 64 位元使用者**

您應如何取得 32 位元與 64 位元 Java 安裝器？

關於 Windows 專用的 64 位元 Java 的常見問題

**繼續安裝**

無法下載？請嘗試使用  
繼續安裝程式

**下載 Windows 專用的 Java**

**Version 8 Update 333 (檔案大小：2.15 MB) Why is Java 8 recommended?**

發行日期：May 02, 2022

**重要的 Oracle Java 授權更新**

各發行版本的 Oracle Java 授權自 2019 年 4 月 16 日起已經改變。

新的適用於 Oracle Java SE 的甲骨文全球開發者技術網路授權合約，與之前的 Oracle Java 授權有重大的不同。新的授權允許某些個人和開發用途上的免費使用 -- 而舊有 Oracle Java 授權所允許的其他用途則不再提供。下載及使用本產品之前，請仔細閱讀相關條款。此處提供常見問題的回應。

您可以透過相應的 Java SE 訂閱取得商業授權和支持。

在 Windows 10 中，Edge 瀏覽器不支援 Plug-in，因此將不會執行 Java。請切換為其他瀏覽器 (例如 Internet Explorer) 以執行 Java Plug-in。請從 Edge 瀏覽器上方的「更多動作」選項，然後按一下「使用 Internet Explorer 開啟」。更多資訊

同意並開始安裝下載

下載 Java 部署平台 (JRE) 已閱讀並接受適用於 Oracle Java SE 的甲骨文全球開發者技術網路授權合約條款

完成 Java 安裝之後，您可能需要重新啟動瀏覽器 (關閉所有瀏覽器視窗然後重新開啟) 以啟用 Java 安裝。

### 2.下載Webgoat



05/2021月 <>

github-actions

8.2.2 版

e75cfbe

比較

**8.2.2 版** (最新)

**版本 8.2.2**

**新功能**

- Docker 映像現在支援 nginx 流覽到 <http://localhost> 顯示登陸頁面。

**錯誤修復**

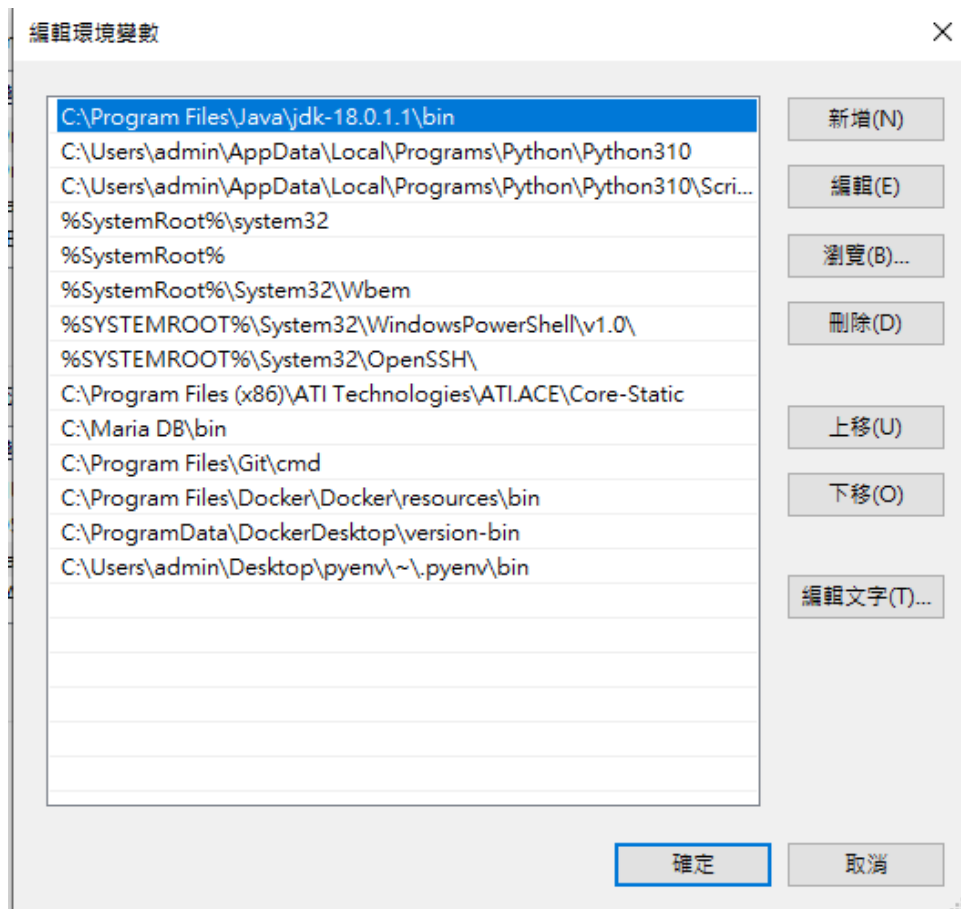
- #1039 jwt-7-代碼審查
- #1031 SQL 注入 (介紹) 5 : 數據控制語言 (DCL) 維基的解決方案不正確
- #1027 Webgoat 8.2.1 Vulnerable\_Components\_12 顯示內部伺服器錯誤

**資產** (4)

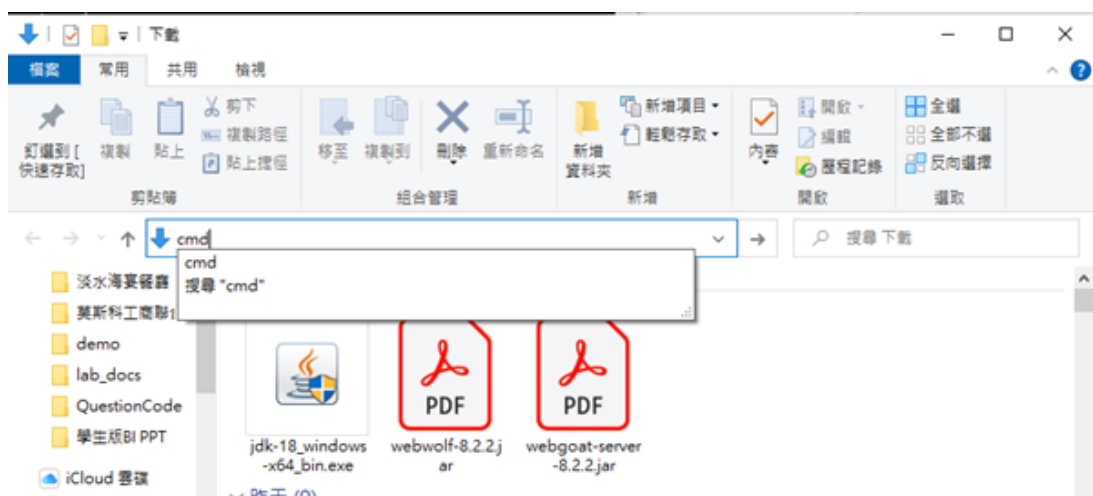
| 資產                       | 大小        |
|--------------------------|-----------|
| webgoat-server-8.2.2.jar | 91.9 兆位元組 |
| 網路器-8.2.2.jar            | 51.3 兆位元組 |
| 原始碼 (腳本)                 |           |
| 原始碼 (tar.gz)             |           |

19 3 4 2 25 人回應了

### 3.設定環境變數



#### 4. 打開終端機



#### 5. 輸入指令開啟Webgoat

```

C:\Users\admin\Downloads>java -jar webgoat-server-8.2.2.jar [--server.port=8080] [--server.address=localhost]
12:21:10.096 [main] INFO org.owasp.webgoat.StartWebGoat - Starting WebGoat with args: [--server.port=8080],[--server.address=localhost]

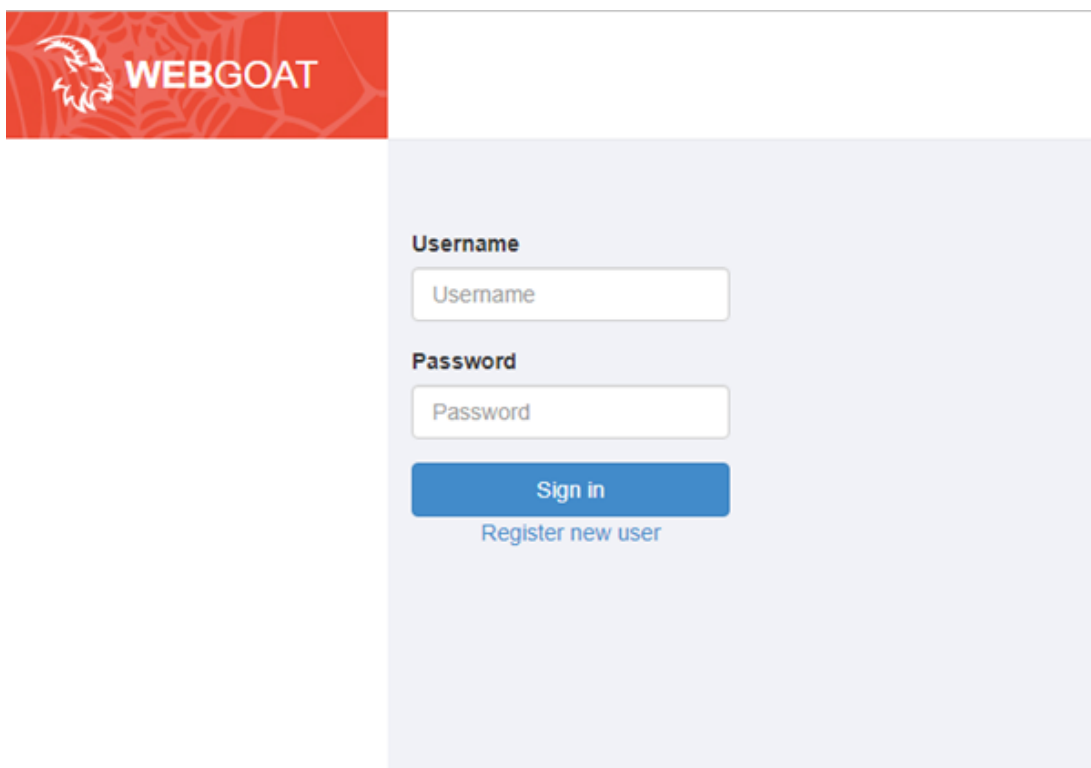
 /_/\
 (oo)_____)
 (____) (
 ||----w)
 || ||

:: Spring Boot :: (v2.4.3)

2022-05-14 12:21:11.372 INFO 6120 --- [main] org.owasp.webgoat.StartWebGoat : Starting StartWebGoat
t v8.2.2 using Java 18.0.1.1 on DESKTOP-MBOCTE4 with PID 6120 (C:\Users\admin\Downloads\webgoat-server-8.2.2.jar started
by admin in C:\Users\admin\Downloads)
2022-05-14 12:21:11.374 DEBUG 6120 --- [main] org.owasp.webgoat.StartWebGoat : Running with Spring
Boot v2.4.3, Spring v5.3.4
2022-05-14 12:21:11.375 INFO 6120 --- [main] org.owasp.webgoat.StartWebGoat : No active profile se
t, falling back to default profiles: default
2022-05-14 12:21:14.322 INFO 6120 --- [main] .s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring
Data JPA repositories in DEFAULT mode.
2022-05-14 12:21:14.524 INFO 6120 --- [main] .s.d.r.c.RepositoryConfigurationDelegate : Finished Spring Data
repository scanning in 189 ms. Found 2 JPA repository interfaces.
2022-05-14 12:21:15.463 WARN 6120 --- [main] io.undertow.websockets.jsr : UT026010: Buffer pool
l was not set on WebSocketDeploymentInfo, the default pool will be used
2022-05-14 12:21:15.487 INFO 6120 --- [main] io.undertow.servlet : Initializing Spring
EmbeddedWebApplicationContext

```

## 6. 開啟瀏覽器，輸入<http://localhost:8080/WebGoat>




The image shows the WebGoat login page. On the left, there is a red banner with a white goat head icon and the text "WEBGOAT". On the right, there is a light blue login form with the following elements:

- Username**: A text input field with the placeholder text "Username".
- Password**: A text input field with the placeholder text "Password".
- Sign in**: A blue button with white text.
- Register new user**: A blue link with white text.

## 二、使用流程

### 1. 註冊帳號



## Register

Username

Password

Confirm password

Terms of use

While running this program your machine will be extremely vulnerable to attack. You should disconnect from the Internet while using this program. WebGoat's default configuration binds to localhost to minimize the exposure.

This program is for educational purposes only. If you attempt these techniques without authorization, you are very likely to get caught. If you are caught engaging in unauthorized hacking, most companies will fire you. Claiming that you were doing security research will not work as that is the first thing that all hackers claim.

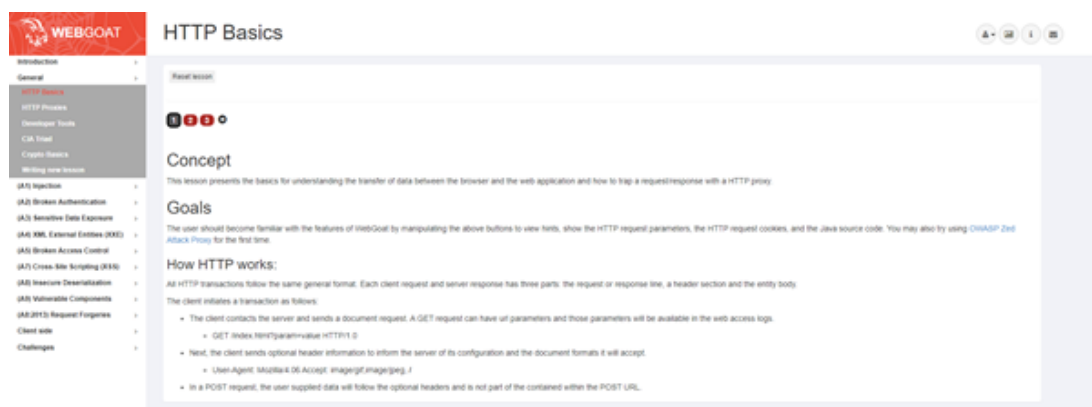
☐ Agree with the terms and conditions

Sign up

## 2.登入成功!



## 3.打開Lesson 1



## 4.第二節內容，輸入名字

Show hints

Reset lesson

←

1

2

3

→

Enter your name in the input field below and press "Go!" to su

## Try It!

Enter your name in the input field below and press "Go!" to su

Enter Your Name:

mike

Go!

### 5.當打開F12後發現是一個POST

Show hints

Reset lesson

←

1

2

3

→

Enter your name in the input field below and press "Go!" to submit. The ser

## Try It!

Enter your name in the input field below and press "Go!" to submit. The ser

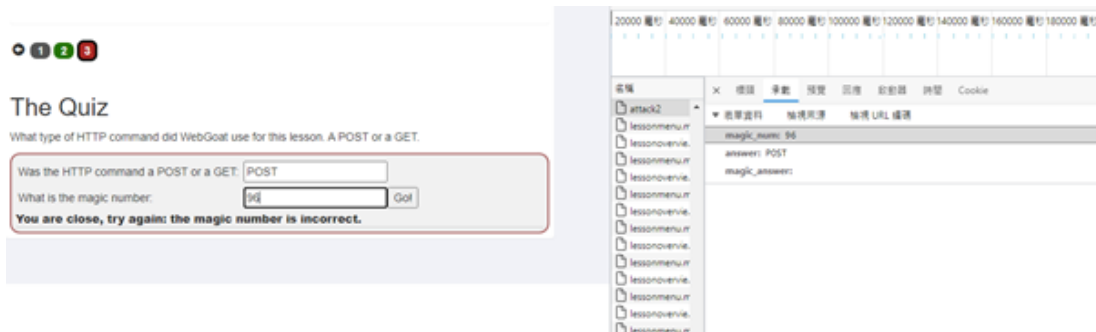
✓

Enter Your Name:

Go!

**The server has reversed your name: ekim**

### 6.查驗magic number，先送出之後觀測header



## 三、模擬Proxy

### 1.下載ZAP


幹掉

[家](#)
[博客](#)
[視頻](#)
[文件](#)
[社區](#)
[Q](#)

[下載](#)

[G](#)
[T](#)

## 下載 ZAP

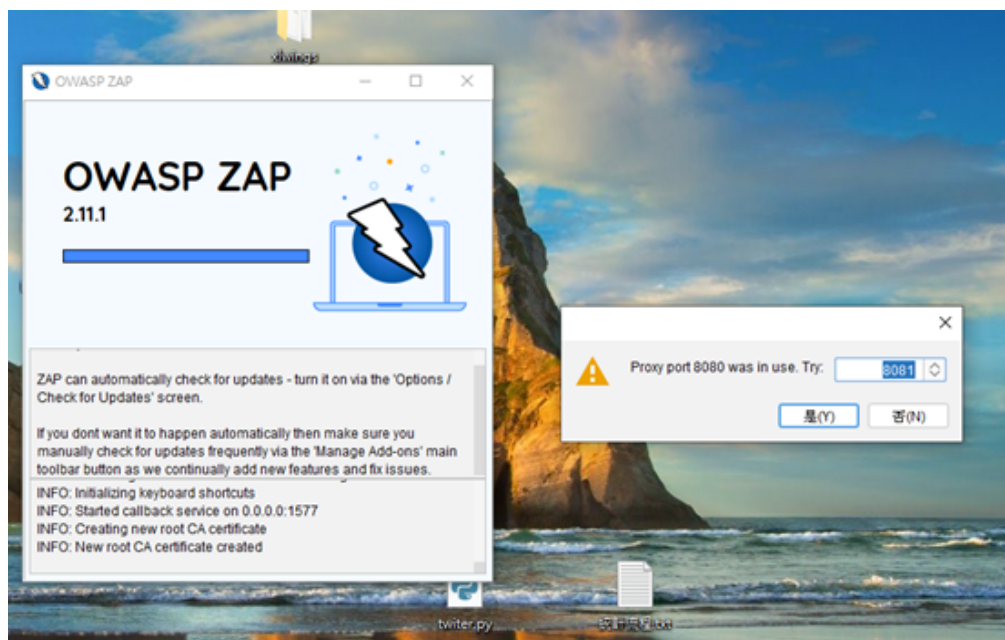
所有 ZAP 下載的校驗和都保留在 [2.11.1 發行頁面](#) 和 [相關版本](#) 中。

與所有軟體一樣，我們強烈建議僅在完全修補和積極維護的作業系統和 JRE 上安裝和使用 ZAP。

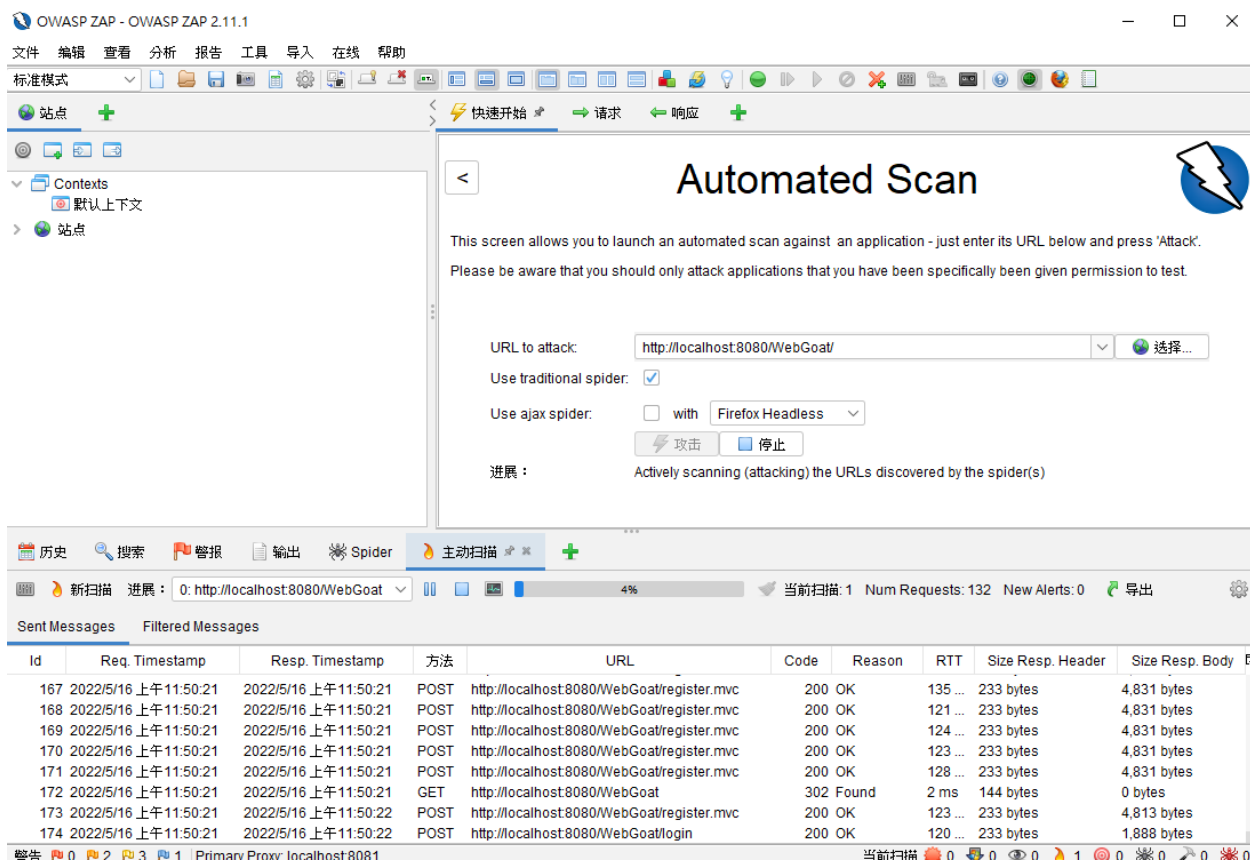
### ZAP 2.11.1

|                 |        |                    |
|-----------------|--------|--------------------|
| 視窗（64）安裝程式      | 183 MB | <a href="#">下載</a> |
| 視窗（32）安裝程式      | 183 MB | <a href="#">下載</a> |
| Linux Installer | 188 MB | <a href="#">下載</a> |
| Linux Package   | 186 MB | <a href="#">下載</a> |
| MacOS Installer | 213 MB | <a href="#">下載</a> |
| 跨平臺包            | 204 MB | <a href="#">下載</a> |
| 核心跨平台套件         | 55 MB  | <a href="#">下載</a> |

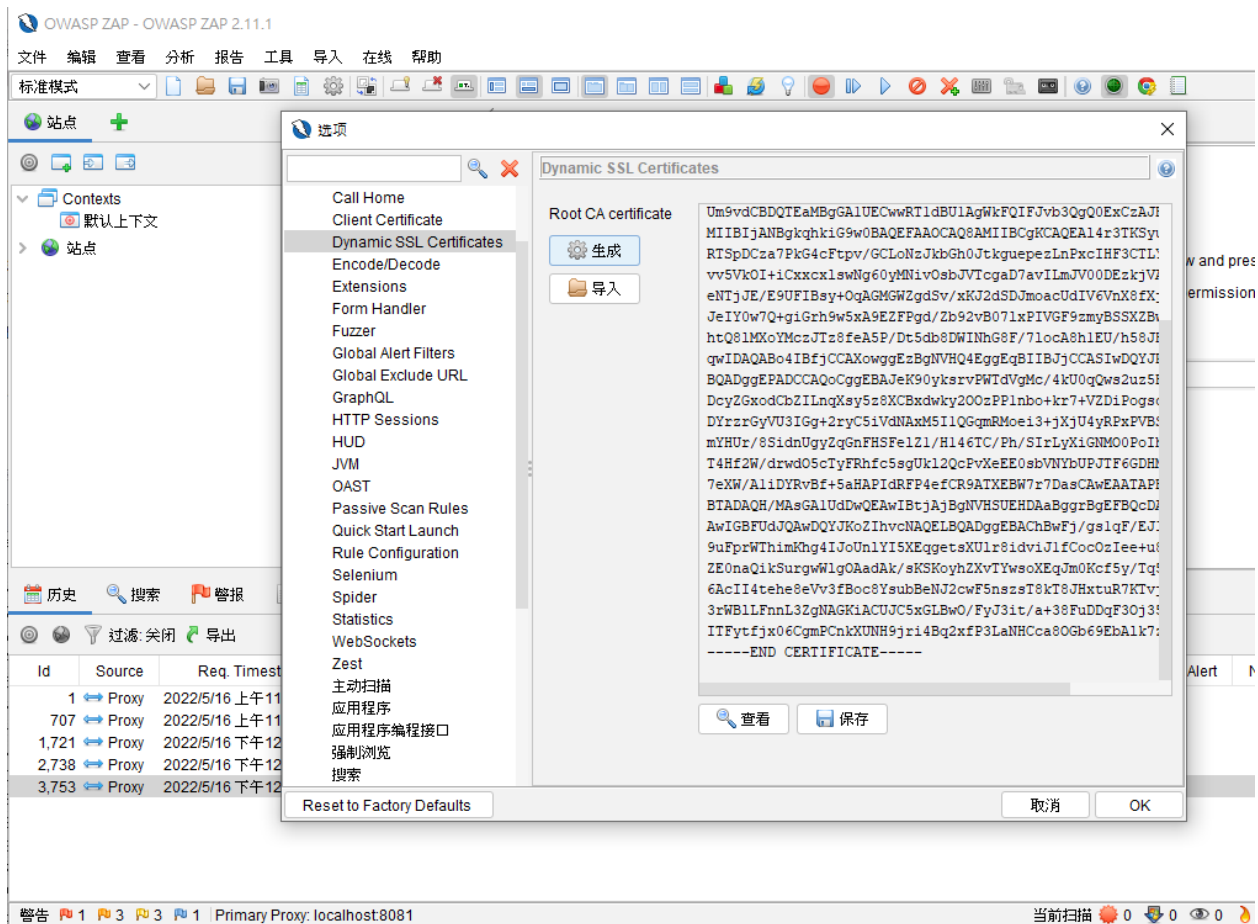
### 2.設定port為8081



### 3.打開工具裡的選項

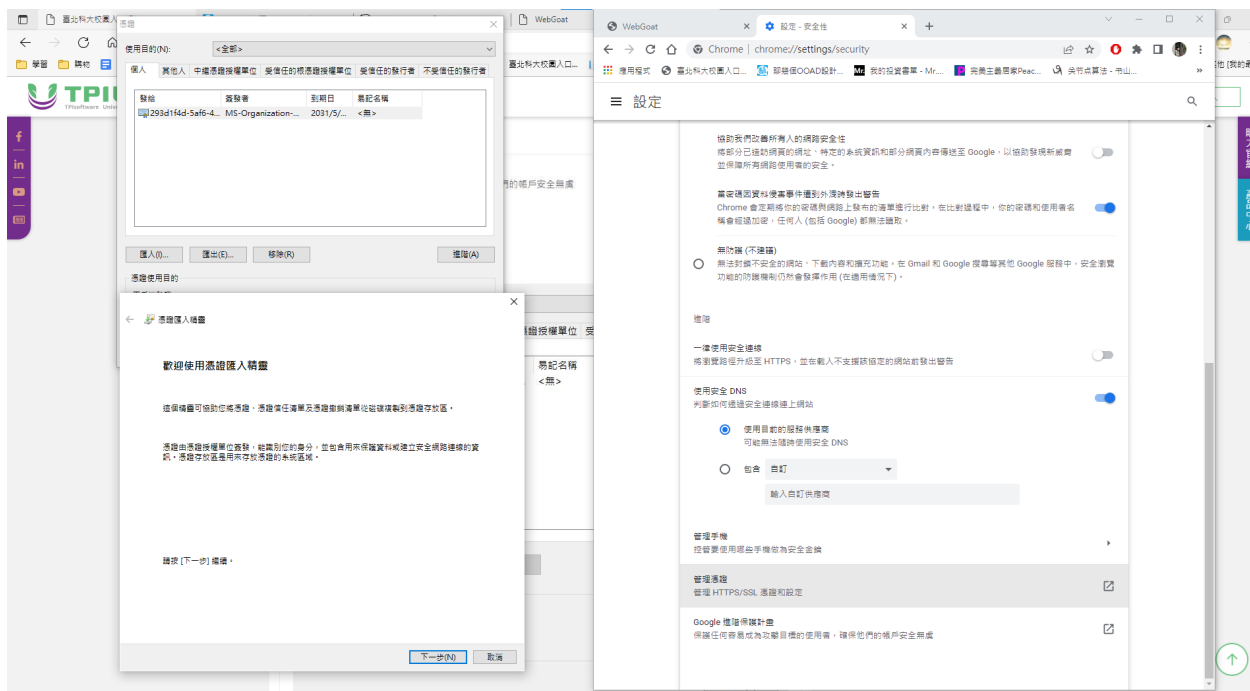


### 4.生成憑證且儲存



## 5. 打開瀏覽器 → 設定 → 安全性 → 隱私 → 憑證





## 6.選擇受信任的根憑證授權單位



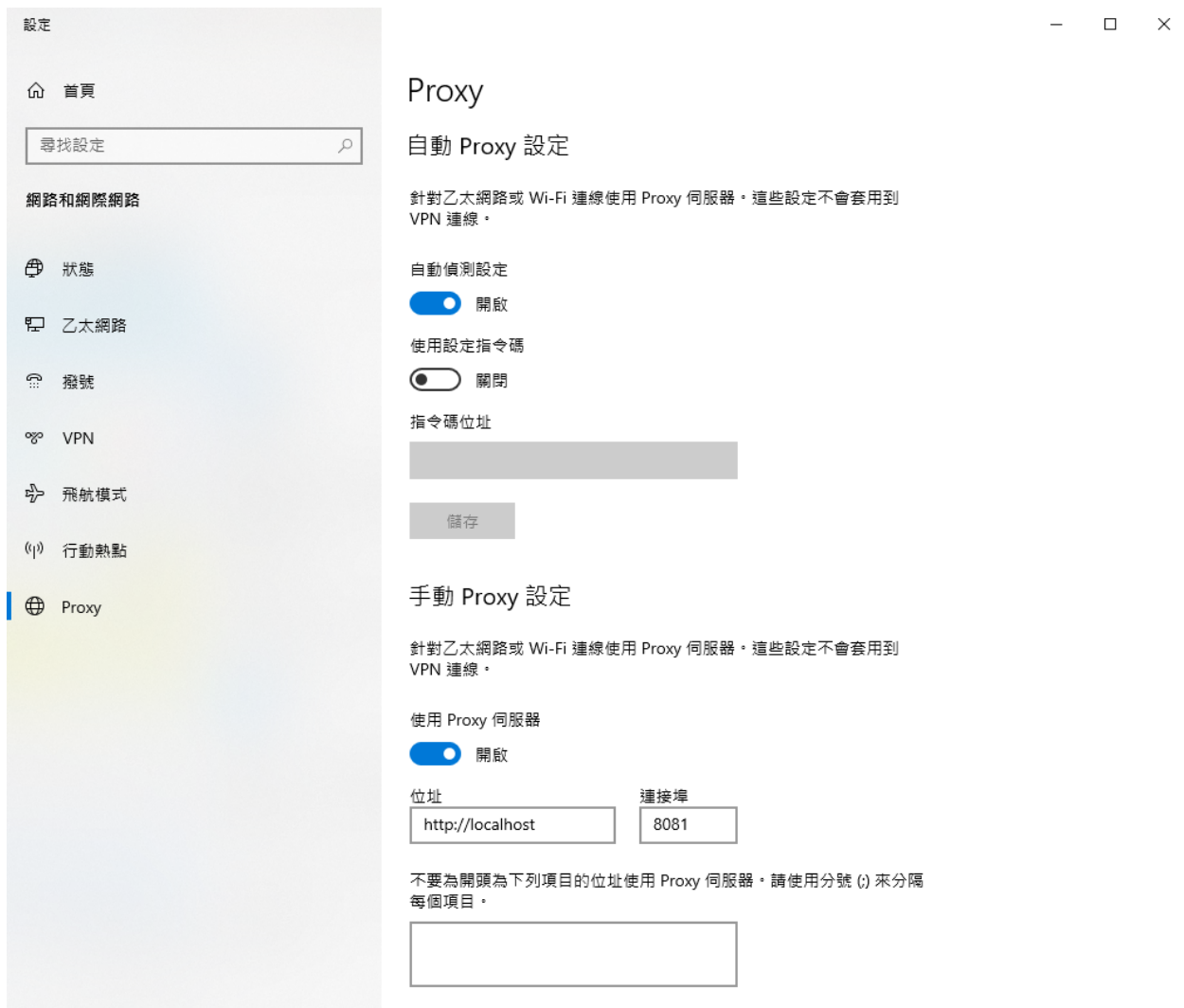
## 7. 確認無誤點擊完成



## 8.設定 → 查詢 → 開啟電腦的Proxy設定



## 9.設定為一樣的8081



# 伍、Markdown語法

H1

# 測試文字

## 測試文字

H3

## 測試文字

## 測試文字

H6

### 測試文字

## 測試文字

斜體

\*測試文字\*

*測試文字*

粗體

**\*\*測試文字\*\***

**測試文字**

刪除線

~測試文字~

測試文字

小區間

`測試文字`

測試文

大區間

/Callout

程式碼

/code

```
print("Hello World")
```

代辦

[]

□

引用

>

▼

清單

- 測試文字

+ 測試文字

\* 測試文字

- 測試文字

數字清單

1.

1.

照片

/image

字體顏色

/color

超連結

/web

目錄

/toc

![GITHUB](https "雙氣")

## 陸、參考資料

Windows PowerShell基本語法及常用命令

Windows 10 WSL GUI介面 - HackMD

[Ubuntu][教學] Linux基本指令#04. 產生空白資料夾、檔案與命名注意事項 - YouTube

鳥哥私房菜 - 第十二章、學習 Shell Scripts (vbird.org)

Bash Shell Script教學與心得 (google.com)

Shell echo命令 | 菜鸟教程 (runoob.com)

使用 WSL 執行 Linux GUI 應用程式 | Microsoft Docs

[Day 13] 來玩WebGoat！之1：安裝 - iT 邦幫忙::一起幫忙解決難題，拯救 IT 人的一天 (ithome.com.tw)

Markdown - 易編易讀，優雅的寫文吧！

筆記&寫作神器 Markdown 真希望我學生時期就懂

Draw Diagrams With Markdown

Math and Academic Functions

為什麼許多人都改用 Notion 做為主力筆記軟體？看完這個你就明白了