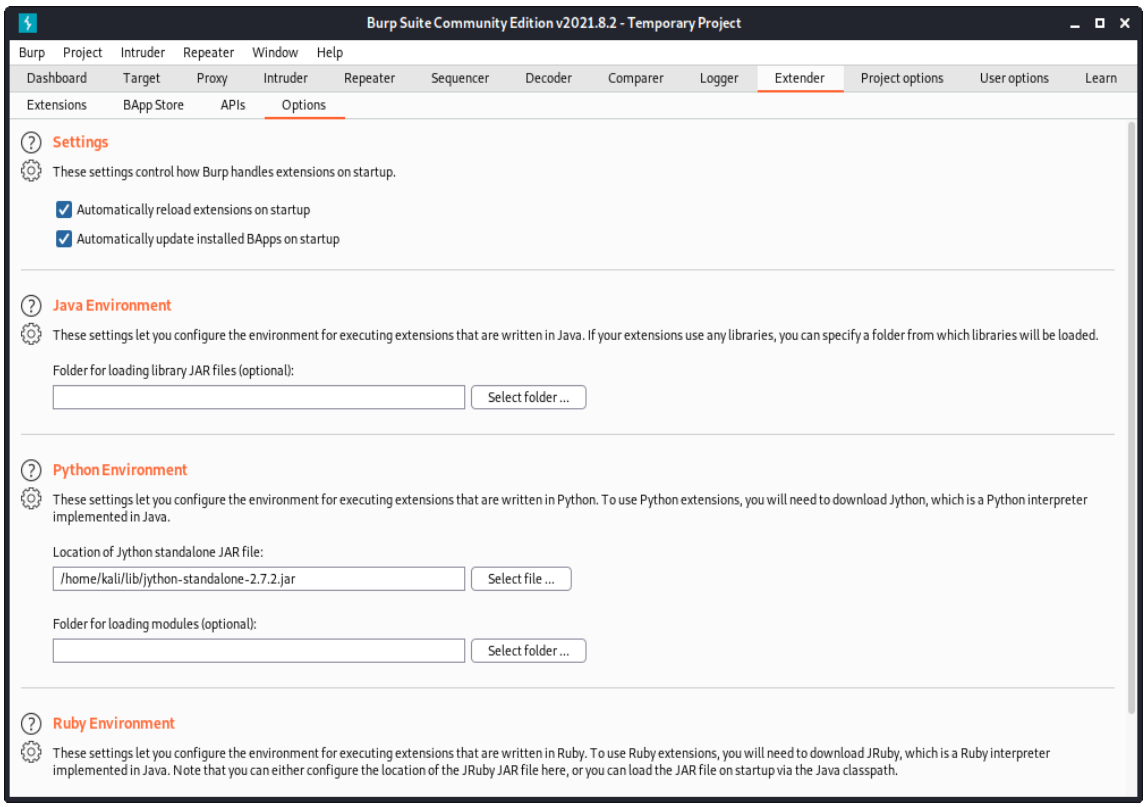
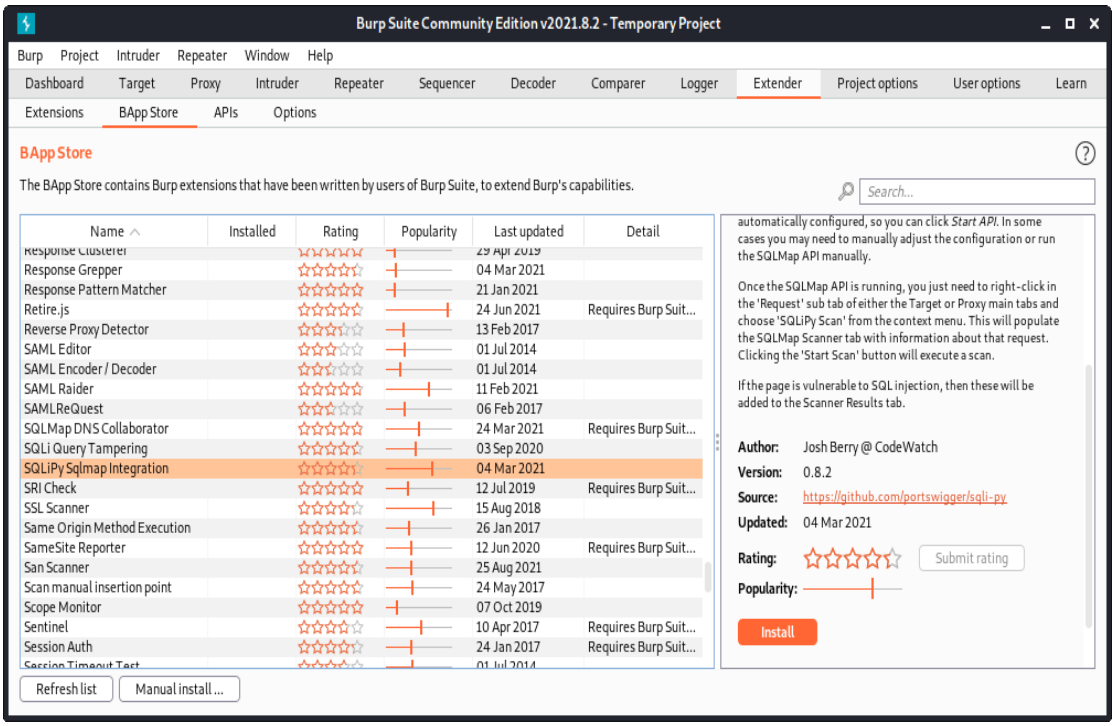
Burp Suite 搭配 SQLiPy 透過 SQLMap 進行 SQL Injection 測試

1. 安裝 SQLiPy Sqlmap Integration 擴充功能



設定 Jython 路徑

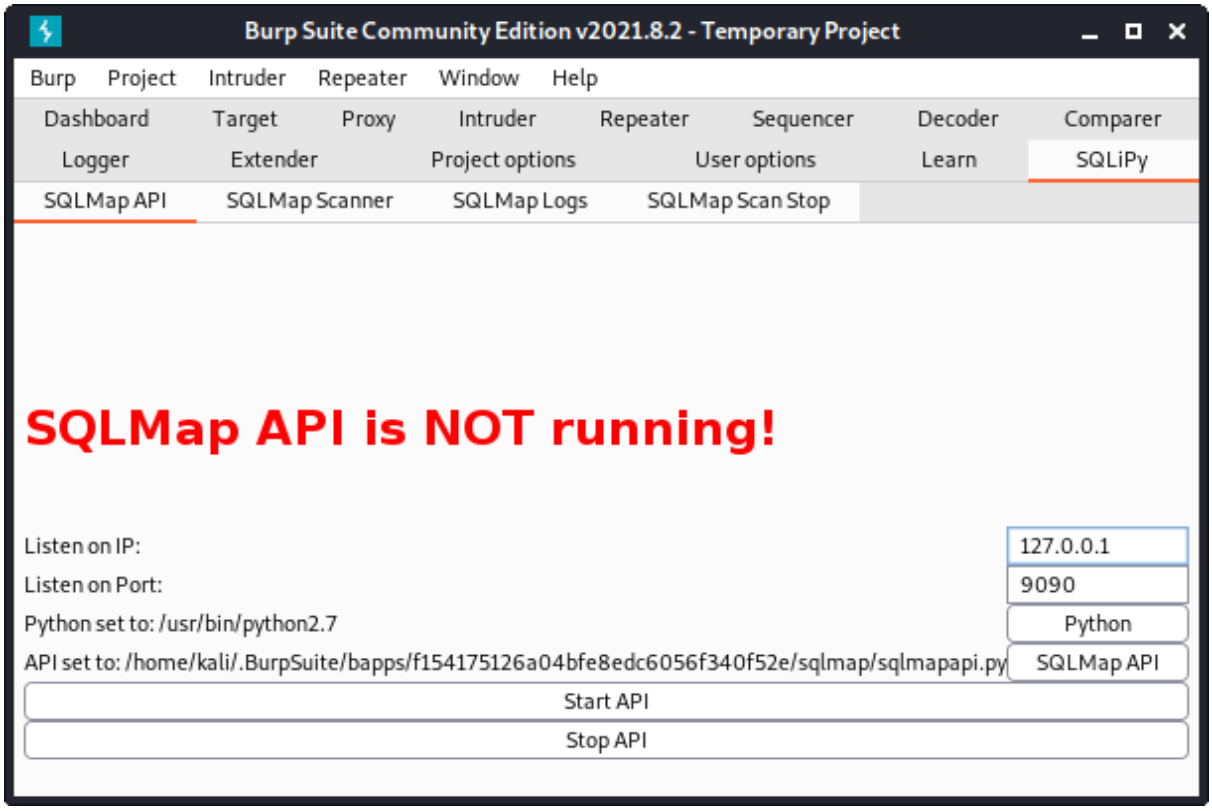
2. 接著在「Extender」中的「BApp Store」，安裝「SQLiPy Sqlmap Integration」擴充功能。



安裝 SQLiPy Sqlmap Integration

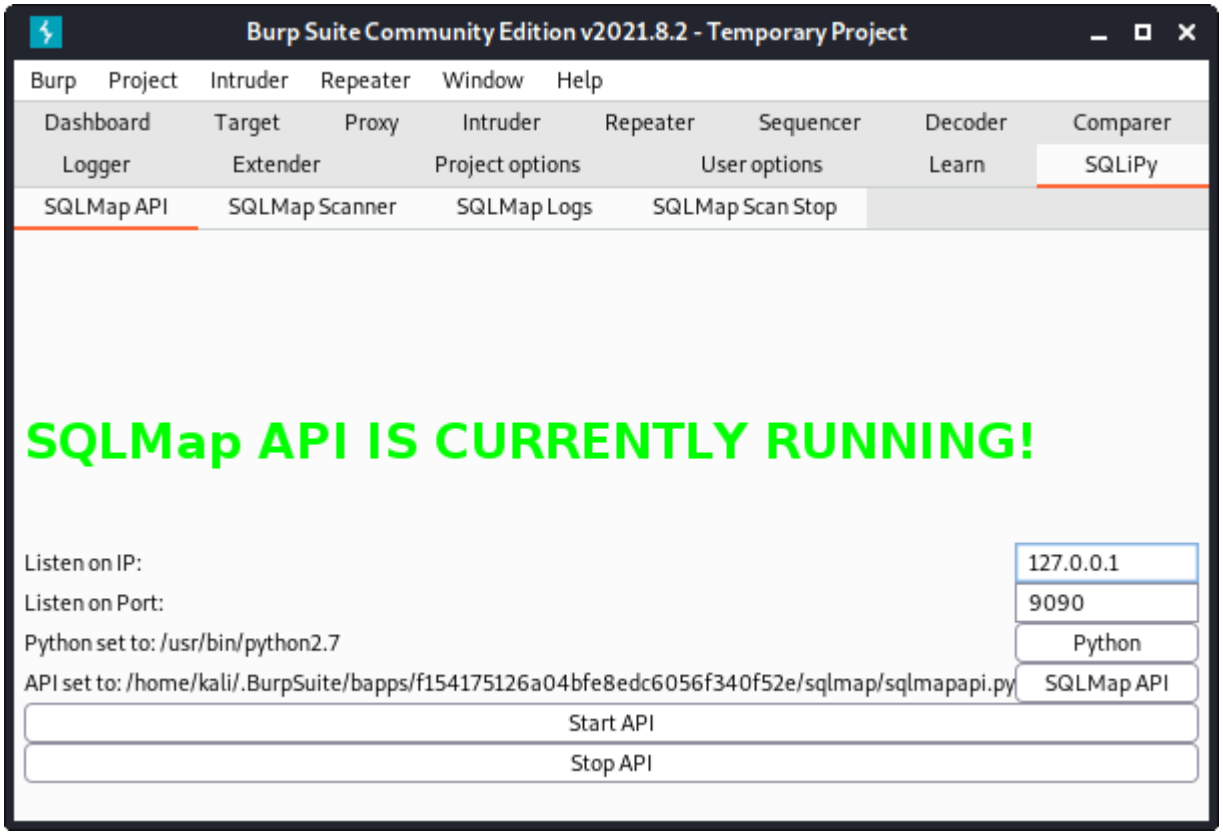
3. 啟動 SQLMap API 伺服器

在開始使用時，要先在「SQLMap API」頁籤中設定好 SQLMap API 伺服器相關的設定（通常使用預設值即可），按下「Start API」啟動 SQLMap API 伺服器。



SQLMap API 尚未啟動

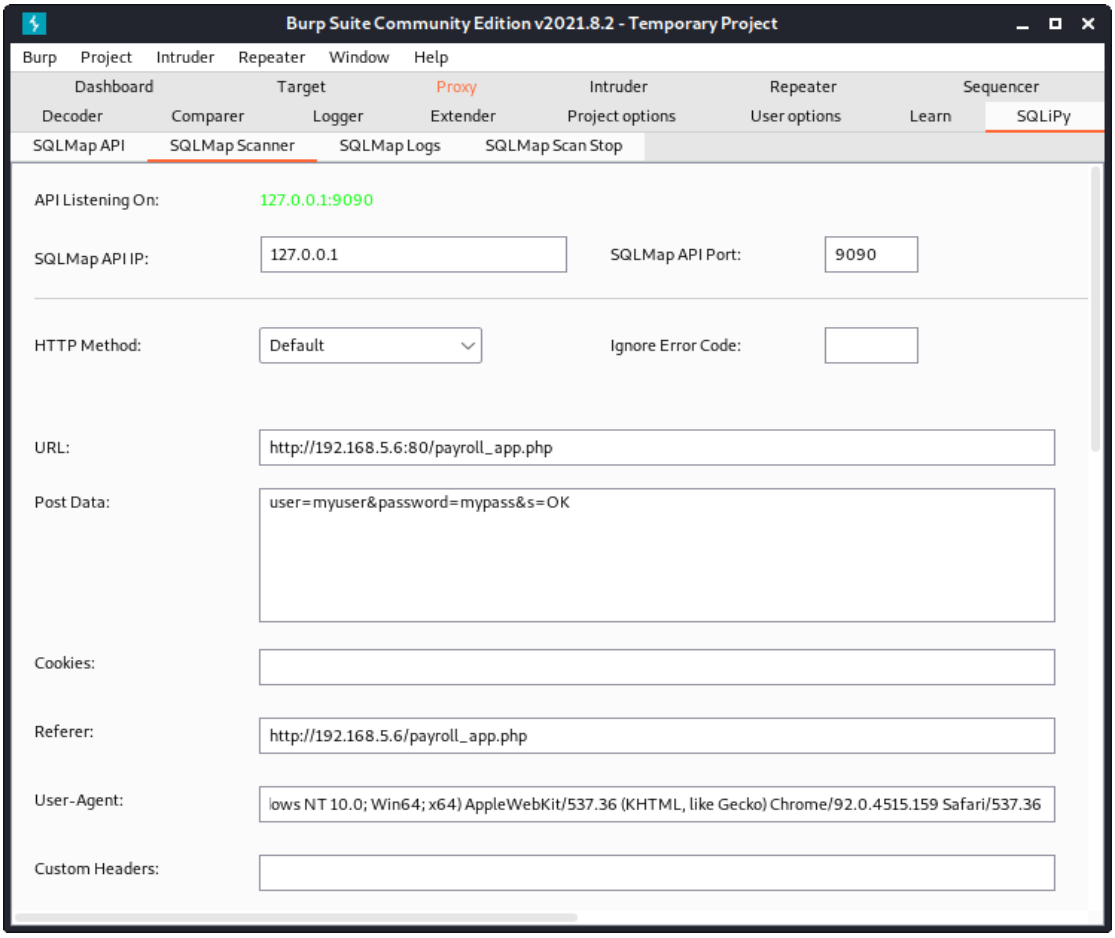
SQLMap API 伺服器啟動之後，會顯示綠色的「SQLMap API IS CURRENTLY RUNNING!」訊息，這時候就可以開始使用 SQLiPy 透過 SQLMap 進行掃描了。



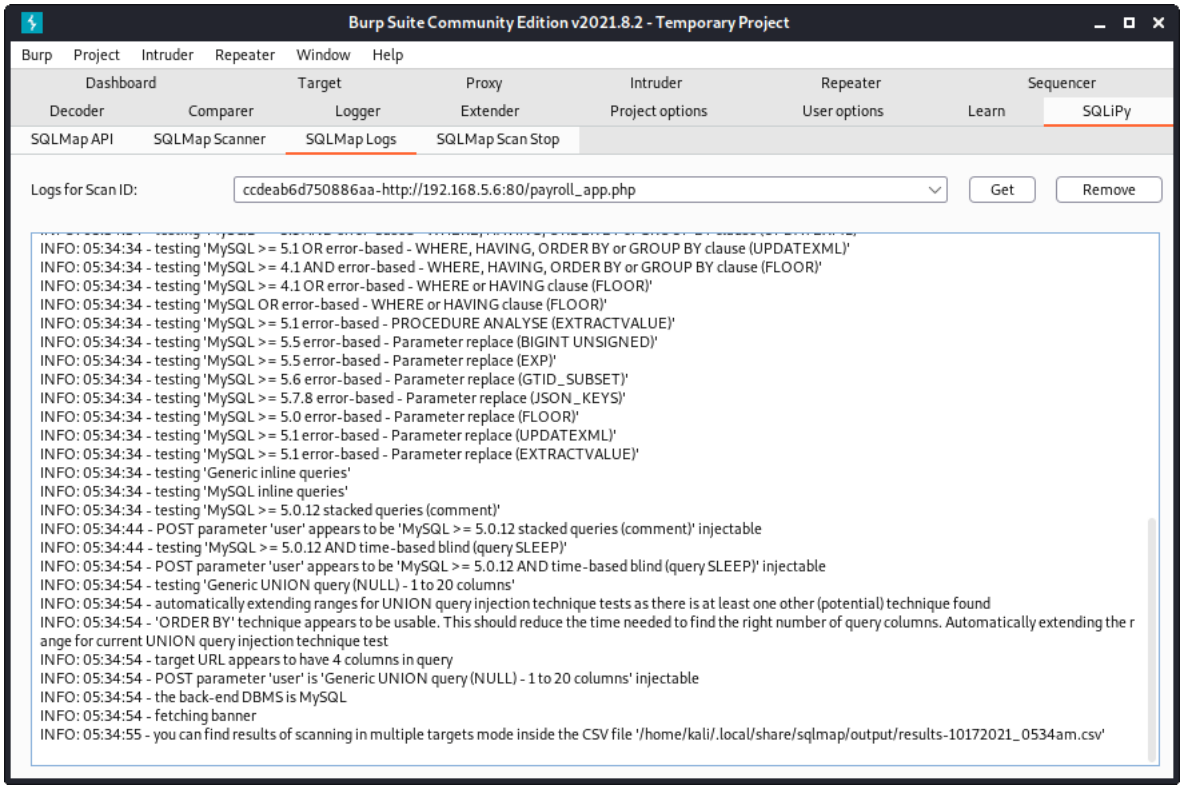
4. 以 SQLiPy 透過 SQLMap 掃描

若要以 SQLiPy 透過 SQLMap 掃描，先使用 Proxy 功能攔截包含表單的 HTTP 請求，在請求內容上按下滑鼠右鍵，選擇「Extensions」、「SQLiPy Sqlmap Integration」、「SQLiPy Scan」，將 HTTP 請求資料傳遞至 SQLMap 掃描功能中。

選擇「SQLiPy」中的「SQLMap Scanner」頁籤，可以看到從 Proxy 轉入的 HTTP 請求資料，此處的掃描選項都對應到 sqlmap 指令的參數，調整必要的設定之後，即可執行掃描。



5.送出掃描請求之後，即可在「SQLMap Logs」中依據掃描的 ID 查詢掃描記錄。



SQLMap Logs

心得:其實自己在實作的時候，都很不順利，只能參考網路上的說明一步步操作，如果有問題只好重新安裝，在從頭來一次，最後終於成功了，非常開心。