HW6-CORS 心得文章

跨源資源共享（Cs-Origin Resource Sharing CORS）是一種使用額外的 HTTP 頭令當前瀏覽網站的用戶代理（en-US）標明訪問其他（網域）服務器資源權限的機制當一個用戶不是當前文件來源（例如來自於（域名）、跨不同時網端口（跨端口協議）請求）的來源——例如建立一個來源（域名）或通訊的 HTTP（跨端口）的資源請求）。

當使用者代理請求一個不是目前文件來源——例如來自 於不同網域、通訊協定或通訊埠的資源時，會建立一個跨來源 HTTP 請求 （cross-origin HTTP request）。透過 JavaScript 存取非同源資源時，server 必須 明確告知瀏覽器允許何種請求，只有 server 允許的請求能夠被瀏覽器實際發 送，否則會失敗。

基於代表性安全考量，程序所發出的跨源 HTTP 碼請求會受到限制。例如，XMLHttpRequest 及 Fetch 都遵循這同源政策（同源策略）。 網路應用程序所使用的 API 使用 CORS 標頭，否則請求與應用程序相同的網域只是 HTTP 資源。

來源資源使用標準的准許方式是通過新增的 HTTP 標頭讓服務器以提供能力瀏覽器來訪問的 GET。或用於某些 MI 類型的 POST 方法），規範要求瀏覽器必須請求“預檢”（preflight）請求，以之 HTTP 的 OPTIONS (en-US)方法從服務器獲得其支持的方法。當設備許可後，再發送 HTTP 請求方法送出具體的請求。服務器也可以通知客戶端是否需要安全性資料（包括 Cookies 和 HTTP 認證（Authentication））一併隨送出。

在 CORS 的規範裡面，跨來源請求有分兩種：「簡單」的請求和非「簡單」的請求。所謂的「簡單」請求，必須符合以下兩個條件： 1.只能是 HTTP GET, POST or HEAD 方法 2.自訂的 request header 只能是 Accept、Accept Language、Content-Language 或 Content-Type（值只能是 application/x-www form-urlencoded、multipart/form-data 或 text/plain）。只要不符合以上任一條 件的請求就是非簡單請求。

一般的 http request 會帶有該網域底下的 cookie；然而，跨來源請求預設是不 能帶 cookie 的。因為帶有 cookie 的請求非常強大，如果請求攜帶的 cookie 是 session token，那這個請求可以以你的身份做很多的事情，像是存取你的隱 私資料、從你的銀行帳戶轉帳等。所以瀏覽器端針對跨來源請求的 cookie 也 做了規範。請求必須要明確地標示「我要存取跨域 cookie」。使用 fetch API 和 XMLHttpRequest 透過 fetch API 發送跨來源請求，需要定 credentials: 'include'：透過 XMLHttpRequest 發送跨來源請求，需要定 withCredentials = true; 如此一來跨來源請求就會攜帶 cookie 了。