網頁設計 HW6-CORS

資工系 B0929043 莊泓德

跨來源資源共用（Cross-Origin Resource Sharing (CORS)）是一種使用額外 HTTP 標頭令目前瀏覽網站的使用者代理 (en-US)取得存取其他來源（網域）伺服器特定資源權限的機制。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（domain）、通訊協定（protocol）或通訊埠（port）的資源時，會建立一個跨來源 HTTP 請求（cross-origin HTTP request）。簡單地說，CORS (Cross-Origin Resource Sharing) 是針對不同源的請求而定的規範，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。

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，必須符合下面兩個條件：

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）。

不符合以上任一條件的請求就是非簡單請求。

非「簡單」的跨來源請求，例如：HTTP PUT/DELETE 方法，或是 Content-Type: application/json 等，瀏覽器在發送請求之前會先發送一個 「preflight request（預檢請求）」，其作用在於先問伺服器：你是否允許這樣的請求？真的允許的話，我才會把請求完整地送過去。

Preflight request (預檢請求)是一個 http OPTIONS 方法，會帶有兩個 request header：Access-Control-Request-Method 和 Access-Control-Request-Headers。

Access-Control-Request-Method： 非「簡單」跨來源請求的 HTTP 方法。

Access-Control-Request-Headers 非「簡單」跨來源請求帶有的非「簡單」header。

跨來源資源共用標準的運作方式是藉由加入新的 HTTP 標頭讓伺服器能夠描述來源資訊以提供予瀏覽器讀取。另外，針對會造成副作用的 HTTP 請求方法（特別是 GET 以外的 HTTP 方法，或搭配某些 MIME types 的 POST 方法），規範要求瀏覽器必須要請求傳送「預檢（preflight）」請求，以 HTTP 的 OPTIONS (en-US) 方法之請求從伺服器取得其支援的方法。當伺服器許可後，再傳送 HTTP 請求方法送出實際的請求。伺服器也可以通知客戶端是否要連同安全性資料（包括 Cookies 和 HTTP 認證（Authentication）資料）一併隨請求送出。

遇到 CORS 的問題，可以歸納出這樣的 SOP：

1.先認清楚是否為「簡單」的跨來源請求，如果是，在後端 GET/POST/HEAD 方法本身加上 Access-Control-Allow-Origin header。

2.如果非「簡單」跨來源請求，在後端 OPTIONS 加上 Access-Control-Allow-

Methods 及 Access-Control-Allow-Headers header。另外，在後端方法本身加上 Access-Control-Allow-Origin header。

3.(Optional) 需要使用 cookie 的情況下，前端要加上 credentials: 'include' 或是 withCredentials 參數，後端要加上 Access-Control-Allow-Credentials header，而且 Access-Control-Allow-Origin header 不能用 *。