hw6-cors

CORS 跨來源資源共用

我們經常會需要跨來源請求資料，就像我們之前寫的作業，要去抓桃園捷運的時間和價格，那時候我們就是需要利用瀏覽器傳送 http request 串接其他網頁的 API 來取得資料，那時候因為有符合 CORS 機制，所以沒有遇到 CORS 問題。那麼什麼是 CORS 呢？CORS 是一種我們在要取得跨來源資源的時候，需要遵守的規範。因為安全的考量，所以程序發出的跨源 HTTP 碼請求都會遵循同源策略(Same-origin policy)，因為同源策略，所以使用者代理只能請求來自相同網域(domain)、通訊協定(protocol)或通訊埠(port)的資源，但只要滿足 CORS 規範，使用額外的 HTTP 標頭令目前瀏覽網站的使用者代理取得存取其他來源(網域)伺服器特定資源權限的機制，就能夠突破同源政策限制取得其他 Origin 的資源。

那麼要怎麼請求 CORS 呢？有兩種方式：簡單請求（Simple requests）和預檢請求（Preflighted requests）。

簡單請求就是瀏覽器會直接發出跨域請求，並加上標頭增加 Origin 字段表示請求的來源，讓伺服端用以判斷是否允許請求。而請求方法只能用 HEAD、GET、POST，而可以使用的標頭，只有是 Accept、Accept-Language (en-US)、Content-Language (en-US)、Last-Event-ID、DPR、Save-Data、Viewport-Width、Width，而 Content-Type 也只允許三個值 application/x-www-form-urlencoded、multipart/form-data、text/plain，其他的都是預檢請求。

預檢請求就是瀏覽器會先使用 OPTIONS 來詢問伺服器，並附上 Origin 及 Access-Control-Request-Method、Access-Control-Request-Headers 標頭，以確認後續實際請求是否可安全送出。當伺服器同意當前網頁所在的網域，並規範好可以使用哪些 HTTP 動詞和頭信息字段後，瀏覽器才會發出正式的 XMLHttpRequest 請求，否則就會報錯。在伺服器通過了"預檢"請求後，之後每次瀏覽器的 CORS

請求，就會跟簡單請求一樣，會有一個 Origin 標頭字段。那麼為什麼要先以 HTTP 的 OPTIONS 方法送出請求到另一個網域呢？因為跨域請求可能會攜帶一些使用者的資料，為了安全考量，所以要先進行預檢請求。