B0929019 陳昀聖

什麼是 CORS (Cross-Origin Resource Sharing)?

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。

「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。

Origin (來源)

首先，瀏覽器發送跨來源請求時，會帶一個 Origin header，表示這個請求的來源。

Origin 包含通訊協定、網域和通訊埠三個部分。

Access-Control-Allow-Origin

當 server 端收到這個跨來源請求時，它可以依據「請求的來源」，亦即 Origin 的值，決定是否要允許這個跨來源請求。如果 server 允許這個跨來源請求，它可以「授權」給這個來源的 JavaScript 存取這個資源。

授權的方法是在 response 裡加上 Access-Control-Allow-Origin header

Access-Control-Expose-Headers

JavaScript 預設可以存取的「簡單」response header 有以下這些：

- Cache-Control
- Content-Language
- Content-Type
- Expires
- Last-Modified
- Pragma

如果要讓 JavaScript 存取其他 header，server 端可以用 Access-Control-Expose-Headers header 設定。

「非簡單」的請求(一般跨來源請求)：

非「簡單」的跨來源請求，例如：HTTP PUT/DELETE 方法，或 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)

什麼是 preflight request 呢？

Preflight request 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。

Preflight Response

那收到 preflight request 時，Server 該做什麼呢？

Server 必須告訴瀏覽器：我允許的方法和 header 有哪些。因此 Server 的回應必須帶有以下兩個 header:

Access-Control-Allow-Methods: 允許的 HTTP 方法。

Access-Control-Allow-Headers: 允許的非「簡單」header。

當瀏覽器看到跨來源請求的方法和 header 都有被列在允許的方法和 header 中，就表示可以實際發送請求了！

跨來源請求的 Cookie

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機敏的事情，像是存取你的隱私資料、從你的銀行帳戶轉帳等。