B0929029 黃欣慈

CORS

CORS 叫做跨來源資源共用。主要是用來解決取得不同源的 API 問題。為什麼不同源的資料會無法直接取得?瀏覽器在安全考量下，有設立同源政策。同源政策是指你現在在的網站跟要呼叫 API 的網站不同源的時候，瀏覽器會發送請求，但是響應的結果會被擋下並且發出錯誤資訊。不同源是只要 Domain 不一樣就是不同源。因此大多數情況都會是不同源而不是同源的。如果沒有這個同源政策會發生資料太容易外洩的問題。假設有一公司擁有私人網站並且內部有機密資料。要是沒有任何限制就可以直接獲取資料並且分析利用的話。那間公司的賺錢秘密就被公諸於世。因此避免不當被利用或是安全問題有了同源政策。在大多數需要索取 API 的情況下都是不同源的，因此我們需要方式去解決這個限制。想要解決限制有幾個鑽漏洞的方法。像是直接關掉瀏覽器的安全性設置、更改 fetch mode、不要用 AJAX 拿資料。直接關掉安全性可以成功是因為跨來源請求會被擋是瀏覽器的限制，只要瀏覽器沒有限制就可以直接拿到響應結果。但這些都是錯誤的解法。雖然在更改完 fetch mode 後錯誤訊息會消失，但時仍然無法取得任何 API 內的內容。因為他只是將會錯誤的東西擋住(直接不讓 response 回傳)。正確的解決辦法應該是後端加上 response header。

跨來源請求可以分為兩種，簡單請求跟非簡單請求。若是只是簡單請求的情況下。當遇到 CORS 的問題時，可以先確定後端是否有 access-control-allow-origin 的 header。當沒有的時候絕對無法解決任何問題。而簡單請求只要是 medthod 是 GET、POST 或是 HEAD 且不要帶自訂的 header、Content-Type。在這些情況下可以很快速就解決。但是當是非簡單需求會多送出一個東西，叫做預檢請求。這種時候就需要通過 preflight request。只有通過了 preflight 以後才能成功在前端用 AJAX 的方式送出表單資料。

Preflight 是一個驗證機制，確保後端知道前端要送出的 request 是預期的，瀏覽器才會放行。Preflight 所擋下的是 request 和跨來源請求所被擋住的是不同東西，跨來源請求所擋下的是 response 而不是 request。還有一種情況是對於有 cookie 的情況。在 CORS 回應中設定的 cookies 受限於一般的第三方 cookie 政策，因此如果使用者將瀏覽器設定為禁止使用第三方 cookies，則 cookies 不會被保存。