網頁程式設計作業-CORS

學號:B0929016
姓名:蘇稚鈞
系級:資工二甲

在開始 CORS 之前，我們需要先知道瀏覽器的同源政策。瀏覽器基於安全性的考量，規定當你的網站要呼叫 API 時，需要是同一個來源。如果是不同來源，瀏覽器依然會幫你發出 request，但會把收到的 response 阻擋起來不給你的網站。當兩個網址的 schema(protocol) + host + port 皆相同，就是同源(Same-Origin)，只要有一者不同，就是跨來源(Cross-origin)。

因為安全性的考量，瀏覽器預設都會限制網頁做跨網域的連線。但如果要提供資料存取的服務給其它人使用，就必須要開放對應的 API 給其它人連線。而 CORS 就是一個瀏覽器做跨網域連線的時要遵守的規範。

CORS 是一個瀏覽器做跨網域連線的方式。透過 HTTP header 的設定，可以規範瀏覽器在進行跨網域連線時可以存取的資料權限與範圍，包括哪些來源可以存取，或是哪些 HTTP verb, header 的 request 可以存取。當一個支援 CORS 瀏覽器在網頁送出一個 request 時，會做下面的動作：瀏覽器根據送出 request 的 HTTP verb 與 header，判斷這個 request 是一個簡單請求(simple request)或是非簡單請求(判斷的細節可參考 MDN - HTTP access control (CORS) - Simple requests)。如果是一個簡單請求，則直接送出 request。如果是一個非簡單請求的 request，則進行 CORS preflight。先對伺服器送出一個 verb 為 OPTION 的 preflight request，它會帶有特定的 header 告訴伺服器接下來的 request 需要哪些跨網域連線的權限。當伺服器收到 preflight 後，就會回傳帶有特定 header 的 response 給瀏覽器，告訴它有哪些權限是允許的。瀏覽器取得伺服器的 response 後，如果符合連線權限，就會送出真正的 request。如果發現權限不符，就會出現錯誤訊息而中斷送出 request 的步驟。

當然，使用 CORS 往往會遇到很多問題，所以我們也要試著解決這些問題，方法一，就是直接把瀏覽器的安全性設置關掉，但此作法關掉的不只是 CORS，其他安全機制也一起關掉了。方法二、不要用 AJAX 拿資料，既然用 AJAX 會被擋跨來源的請求，那如果可以不用 AJAX 拿資料，不就沒有問題了嗎？因為有一些 tag 是不會受到 same-origin policy 的限制的，例如說 img 或者是 script，script 一般來說都是引入其他人寫好的程式碼，例如說 jQuery 或是其它套件之類的。但在 CORS 規範還不完整的年代，就有一些人想出了用 script 標籤來傳遞資料的妙招。簡單來說是這樣的，因為用 script 可以引入別人的 script，假設我們要引入的 script 長這樣：

```
var data = {
  username: 'huli'
};
```

那我們引入以後，就可以直接存取 data 這個變數，而裡面就是我們想要跨來源拿到的資料了。

參考資料

1. https://sibevin.github.io/posts/2017-06-05-101518-note-cors
2. https://developer.mozilla.org/zh-TW/docs/Web/HTTP/CORS
3. https://ithelp.ithome.com.tw/articles/10267360?sc=iThomeR