跨來源資源共用（CORS）

什麼是(CORS)

跨來源的英文是 cross origin，顧名思義，當你想要從來源 A 去拿來源 B 的東西，就是跨來源。

那為什麼不能拿跨來源資料，如果今天我恰好知道你們公司有一個「內部」的公開網站，網址，這是外部連不進去的，只有公司員工的電腦可以連的到，然後我在我的網頁寫一段 AJAX 去拿它的資料，是不是就可以拿得到網站內容？那我拿到以後是不是就可以傳回我的 server？這樣就有了安全性的問題，因為攻擊者可以拿到一些機密資料。

CORS 限制的是「拿不到 response」，而不是「發不出 request」。所以 request 其實已經發出去了，瀏覽器也拿到 response 了，只是它因為安全性考量不給你。

技術層面的時做

對於可以修改數據的 Ajax 和 HTTP 請求方法（通常是 GET 以外的 HTTP 方法，或用於某些 MIME 類型的 POST），規範要求瀏覽器“預檢”請求，通過 HTTP OPTIONS 請求從服務器請求支持的方法方法，然後，在服務器“批准”後，使用實際的 HTTP 請求方法發送實際請求。服務器還可以通知客戶端是否應隨請求發送“憑據”（包括 Cookie 和 HTTP 身份驗證數據）

怎麼解決？

1.這個 header 的名稱叫做 Access-Control-Allow-Origin，內容就是想要放行的 origin，例如說：Access-Control-Allow-Origin: http://localhost:8081，這樣就是允許 http://localhost:8081 的跨來源請求。

那如果想要允許多個來源呢？那是不行的，沒辦法在 header 內放入多個 origin，只能放一個，或是可以選擇放 *，就代表允許任何 origin 的意思

2.第二種方式 proxy server

Proxy server 是代理伺服器，原理是如果你想拿 A 網站的資料，但是它沒有提供 Access-Control-Allow-Origin 這個 header，你就自己寫個 server，從後端去拿 A 網站的資料，再把資料丟回給自己的前端就行了。因為自己的後端可以自己控制，所以你想加什麼 header 就加什麼 header，想拿什麼資料就拿什麼。

*而最常用的應該要是「請後端加上 CORS header」這一種，因為這通常是最正確的解法。但如果對後端沒有掌控權，例如說你就是想要抓其他不認識的來源的資料，那大概會自己架一個 proxy server 或者是找現成的，讓 proxy 幫你加上 CORS header。

總結：

跨域資源共享(CORS) 是一種機制，允許從提供第一個資源的域之外的另一個域請求網頁上的受限資源

網頁可以自由嵌入跨域圖像、視頻..。同源安全策略默認禁止某些“跨域”請求，尤其是 Ajax 請求。CORS 定義了一種瀏覽器和服務器可以交互以確定允許

跨域請求是否安全的方式。它允許比純粹的同源請求更多的自由和功能，但比簡單地允許所有跨域請求更安全。