CORS(Cross-Origin Resource Sharing)，又稱 跨來源資源共用，是一種使用額外 HTTP 標頭，令目前瀏覽網站的使用者代理取得存取其他來源伺服器特定資源權限的機制。當使用者代理請求一個不是目前文件來源，例如來自於不同網域（domain）、通訊協定或通訊埠的資源時，會建立一個跨來源 HTTP 請求。舉個簡單的例子：http://domain-a.com HTML 頁面裡面一個 <img> 標籤的 src 屬性載入來自 http://domain-b.com/image.jpg 的圖片。現今網路上許多頁面所載入的資源，如 CSS 樣式表、圖片影像、以及指令碼都來自與所在位置分離的網域，如內容傳遞網路。基於安全性考量，程式碼所發出的跨來源 HTTP 請求會受到限制。例如，XMLHttpRequest 及 Fetch 都遵守同源政策，所謂的同源，必須滿足以下三個條件：相同的通訊協定 (protocol)，即 http/https、相同的網域 (domain) 、相同的通訊埠 (port)。這代表網路應用程式所使用的 API 除非使用 CORS 標頭，否則只能請求與應用程式相同網域的 HTTP 資源。另外會使用到 CORS: 使用 XMLHttpRequest 或 Fetch API 進行跨站請求、網頁字體（跨網域 CSS 的 @font-face 的字體用途）、WebGL 紋理、以 drawImage 繪製到 Canvas 畫布上的圖形、CSS 樣式表（讓 CSSOM 存取）、指令碼（for unmuted exceptions）。跨來源資源共用標準的運作方式是藉由加入新的 HTTP 標頭讓伺服器能夠描述來源資訊以提供予瀏覽器讀取。

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。 所謂的「簡單」請求，必須符合下面兩個條件：只能是 HTTP GET, POST or HEAD 方法、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）。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。另外，針對會造成副作用的 HTTP 請求方法，特別是 GET 以外的 HTTP 方法，或搭配某些 MIME types 的 POST 方法，規範要求瀏覽器必須要請求傳送「預檢」請求，以 HTTP 的 OPTIONS 方法之請求從伺服器取得其支援的方法。當伺服器許可後，再傳送 HTTP 請求方法送出實際的請求。伺服器也可以通知客戶端是否要連同安全性資料（包括 Cookies 和 HTTP 認證資料）一併隨請求送出。