hw6-cors

B0929008 劉振宇

簡介:

跨來源資源共用（CORS）是一種使用額外 HTTP 標頭令目前瀏覽網站的使用者代理 (en-US)取得存取其他來源（網域）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檔來源——例如來自於不同網域（domain)、通訊協定（protocol）或通訊埠（port）的資源時，會建立一個跨來源 HTTP 請求（cross-origin HTTP request)。

一個網頁可以自由地嵌入跨源圖像、樣式表、腳本、iframe 和影片。某些 "跨域 "請求，特別是 Ajax 請求，被同源安全性原則默認為禁止的。CORS 定義了一種方式，流覽器和伺服器可以通過互動來決定是否允許跨源請求。與純粹的同源請求相比，它允許更多的自由和功能，但比簡單地允許所有跨源請求更安全。

CORS 的規範包括在 WHATWG 的 Fetch Living Standard 中。這個規範描述了 CORS 目前在流覽器中的實現方式。

技術概述:

對於可以修改資料的 Ajax 和 HTTP 請求方法（通常是 GET 以外的 HTTP 方法，或者是某些 MIME 類型的 POST 用法)，該規範規定流覽器要對請求進行 preflight，用 HTTP OPTIONS 請求方法向伺服器徵求支援的方法，然後在伺服器的 "批准 "下，用實際的 HTTP 請求方法發送實際請求。伺服器還可以通知客戶是否應將 "憑證"(credentials)，包括 Cookies 和 HTTP 認證資料與請求一起發送。

舉例說明:

假設一個用戶存取了 http://www.example.com，並且該頁面試圖進行 CORS 請求，從 http://service.example.com 獲取使用者的資料。相容 CORS 的流覽器將嘗試向 service.example.com 發出跨源請求，具體如下。

1. 流覽器向 service.example.com 發送帶有額外 Origin HTTP 頭的 GET 請求，其中包含提供父頁面的功能變數名稱。

   Origin: http://www.example.com

2. service.example.com 的伺服器可能會回應

   a. 所請求的資料連同其回應中的 Access-Control-Allow-Origin（ACAO）頭，表明來自原點的請求是允許的。

      Access-Control-Allow-Origin: http://www.example.com

   b. 所請求的資料與（ACAO）標頭(header)一起，表明允許來自所有域的請求。

      Access-Control-Allow-Origin: *

   c. 如果伺服器不允許跨源請求，則出現錯誤頁面

Preflight 範例:

當執行某些類型的跨域 Ajax 請求時，支持 CORS 的現代流覽器將啟動一個額外的 "預檢 "請求，以確定他們是否有許可權執行該動作。跨源請求以這種方式被預檢，因為它們可能對使用者資料有影響。

OPTIONS /

Host: service.example.com

Origin: http://www.example.com

Access-Control-Request-Method: PUT

如果 service.example.com 願意接受該行動，它可能會用以下頭資訊進行回應。

然後，流覽器將進行實際的請求。如果 service.example.com 不接受來自這個來源的跨站請求，那麼它將對 OPTIONS 請求做出錯誤回應，而流覽器將不進行實際請求。