跨源资源共享

跨源资源共享（CORS，或通俗地译为跨域资源共享）是一种基于 HTTP 头的机制，该机制通过允许服务器标示除了它自己以外的其他源（域、协议或端口），使得浏览器允许这些源访问加载自己的资源。

规范要求，对那些可能对服务器数据产生副作用的 HTTP 请求方法（特别是 GET 以外的 HTTP 请求，或者搭配某些 MIME 类型的 POST 请求），浏览器必须首先使用 `OPTIONS` 方法发起一个预检请求（preflight request），从而获知服务端是否允许该跨源请求。服务器确认允许之后，才发起实际的 HTTP 请求。在预检请求的返回中，服务器端也可以通知客户端，是否需要携带身份凭证（例如 Cookie 和 HTTP 认证相关数据）。

若满足所有下列条件，则该请求视为简单请求：

- 使用下列方法之一：
  - `GET`
  - `HEAD`
  - `POST`
- 除了被用户代理自动设置的标头字段，允许人为设置的字段为 Fetch 规范定义的集合：
  - `Accept`
  - `Accept-Language`
  - `Content-Language`
  - `Content-Type`（需要注意额外的限制）
  - `Range`
- 请求的 MIME 类型（通过 `Content-Type` 消息头指定）只能是：
  - `text/plain`
  - `multipart/form-data`
  - `application/x-www-form-urlencoded`
- 请求中的任意 XMLHttpRequestUpload 对象均没有注册任何事件监听器；XMLHttpRequestUpload 对象可以使用 XMLHttpRequest.upload 属性访问。
- 请求中没有使用 ReadableStream 对象。

1. 预检请求

与简单请求不同，“需预检的请求”要求必须首先使用 `OPTIONS` 方法发起一个预检请求到服务器，以获知服务器是否允许该实际请求。

预检请求时，创建的 `OPTIONS` 请求与简单请求不同。它需要使用以下标头字段：

- `Origin`：请求来自哪个源（协议、域名和端口）
- `Access-Control-Request-Method`：请求所使用的 HTTP 方法
- `Access-Control-Request-Headers`：自定义请求标头字段，如果没有则该字段是可选的。

服务器确认允许之后，才发起实际的 HTTP 请求。

1.1 预检请求的响应

服务器确认允许之后，返回的响应中需要携带以下标头字段：

- `Access-Control-Allow-Origin`：允许访问的源（协议、域名和端口）
- `Access-Control-Allow-Methods`：允许访问的 HTTP 方法
- `Access-Control-Allow-Headers`：允许携带的自定义请求标头字段，如果没有则该字段是可选的。
- `Access-Control-Max-Age`：本次预检请求的有效期，单位为秒。有效期间，不用发出另一条预检请求。

`Access-Control-Allow-Credentials` 头指定了当浏览器的 `credentials` 设置为 `true` 时是否允许浏览器读取 `response` 的内容。