HTTP cookie（web cookie、browser cookie）為伺服器傳送予使用者瀏覽器的一個小片段資料。瀏覽器可能儲存並於下一次請求回傳 cookie 至相同的伺服器。Cookie 通常被用來保持使用者的登入狀態—如果兩次請求都來自相同的瀏覽器。舉例來說，它記住了無狀態（stateless） (en-US)HTTP 協議的有狀態資訊。Cookies 主要用於三個目的：Session 管理(如:帳號登入、購物車、遊戲分數，或任何其他伺服器應該記住的資訊)、個人化(使用者設定、佈景主題，以及其他設定)、追蹤(記錄並分析使用者行為)。而 cookie 的特性有以下幾點:可以紀錄使用者訊息、儲存在客戶端、連線時會自動帶上(但過多的 cookie 可能會浪費流量、或是帶上無用之 cookie)、大小限制 4kb 左右、能夠設置過期時間、專屬於某網域(路徑)。

Cookies 曾被當作一般的客戶端儲存方式來使用。這在當時 cookie 仍是將資料儲存在客戶端的唯一方法時是合法的，而且 Cookies 會被每一個請求發送出去，所以可能會影響效能（尤其是行動裝置的資料連線），所以現在則建議使用現代的 storage APIs。

HTTP 本身 無狀態 (Stateless) 的特性，要在網路上識別瀏覽者的身份，必須透過一些機制來保存狀態，而 Cookie 就是其中一種保存狀態的機制，也是我們開發 Web 應用程式經常要面對的事，而 cookie 的運作如下:收到一個 HTTP 請求時，伺服器可以傳送一個 Set-Cookie (en-US) 的標頭和回應。Cookie 通常存於瀏覽器中，並隨著請求被放在 Cookie HTTP 標頭內，傳給同個伺服器。可以註明 Cookie 的有效或終止時間，超過後 Cookie 將不再發送。此外，也可以限制 Cookie 不傳送到特定的網域或路徑。

假設 Browser 在取得一張網頁時如果裡面包含 20 張圖、3 個 CSS、2 個 JavaScript 檔的話，同樣一份 Cookie 就會送出 25 次到 Server 端，如果你 Cookie 的大小有 4K 的話，光是看一張網頁你可能就要從你的電腦發送出 100KB 的頻寬，且可能只有一張網頁用的到這個 Cookie 而已。

所以使用 Cookie 並非「多多益善」，而是要「小心使用」，否則光是 Cookie 就會讓你的網頁顯示的時間變慢。

由於 Cookie 是儲存在 Client 端，所以一些比較機密的資料不建議存放在 Cookie 中，有些軟體就可以輕易的將一台電腦中的所有 Cookie 取出，如果你的 Cookie 中有帳號、密碼、身份證字號等資料，那就真的全都暴露了，如果真的要放也要加密過後再放比較安全。

參考資料:

https://blog.miniasp.com/post/2008/02/22/Explain-HTTP-Cookie-in-Detail
https://developer.mozilla.org/zh-TW/docs/Web/HTTP/Cookies
https://ithelp.ithome.com.tw/articles/10203123