HTTP cookie

B0929060 張孟佳

Cookie 的定義是：伺服器（Server）傳送給瀏覽器（Client）的一小片段資料。Cookie 有分為記憶體 Cookie 以及硬碟 Cookie 兩種，前者又稱為非持久 cookie（Session Cookie），儲存在記憶體，資料由瀏覽器來維護，瀏覽器關閉就會立即消失；後者又稱為持久 cookie（Persistent Cookie），儲存在硬碟裡，除非手動清理或是到了過期時間，cookie 不會清除。

Cookie 常見的使用目的有三：

1. 儲存和追蹤使用者行為。
2. 儲存用戶登入、購物車等伺服器所需的資訊。
3. 儲存使用者設定和偏好等。

為什麼需要 cookie？基於 HTTP 的無狀態性，每次從客戶端（Client）對伺服器（Server）發出的請求都是獨立的，意思是每次的請求都無法得知上一次請求的內容與資訊。因此我們使用 cookie 讓伺服器可以設定或讀取 cookie 中所包含的資訊，藉此使用者在使用服務時可以持續跟伺服器發送請求以及維持對談中的狀態。

Cookie 是如何運作的？首先 Server 端會回應給 Client 端(瀏覽器)一個或多個 "Set-Cookie" HTTP Header。Client 端接收到此指令時，會將 cookie 的名稱和值儲存在瀏覽器的 cookie 存放區，並記錄 cookie 的 expires、path、domain 以及 secure。當 Client 端再次發出 HTTP Request 指令給 Server 端時，就比對瀏覽器中的 cookie 存放區有沒有符合該網域、該目錄，且沒有過期並為安全連線的 cookie。如果有就會包含在指令中的“Cookie”Header 中。

Cookie 的四種特性：

1. Expires: 表示 cookie 的有效期限，為非持久性 cookie，只要關閉瀏覽器就會消失。
2. Path: 指定與 cookie 關聯在一起的網頁，默認的狀況下為和當前網頁同一

目錄的網頁中有效。

3. Domain: 設定 cookie 有效的網域名稱，可以和 path 一同設定，讓類似獲相同的 domain 可以享有同樣的 cookie。
4. Secure: Cookie 的安全值，在默認的情況下 cookie 是不安全的，可以通過一個不安全且一般的 http，若設置為安全的狀況下，可以讓 cookie 只在安全的 http 上進行傳輸。

Cookie 的缺陷：由於 cookie 會附加在每次 HTTP 的請求中，造成額外增加流量。因 cookie 為一小片段資料，大小限制約在 4KB，無法儲存過於複雜的資料，如果設定的大小超出限制，瀏覽器就會丟棄整個 cookie。而 HTTP 請求中的 cookie 是明文傳遞的，所以有安全性上的疑慮，除非是使用超文字傳輸安全協定（HTTPS)。但還是盡量避免將個人隱私如使用者名稱、使用的瀏覽器或曾經存取的網站等敏感資訊透過 cookie 存放在 Client 端。