網頁程式設計　HW6-COOKIE

資工二甲 B0929056 陳冠宇

在開發網頁時，有一個很重要的觀念，那就是 HTTP 協定是無狀態的。HTTP 的無狀態特性，導致伺服器並不會知道使用者之前做了什麼。Cookie 可以用來解決這個問題，它能夠儲存一些資訊。

Cookie 類型為「小型文字檔案」，指某些網站為了辨別使用者身分而儲存在用戶端（Client Side）上的資料（通常經過加密）。當我們瀏覽網站時，設定於瀏覽器內的 Cookies，會讓瀏覽器記下一些特定的資訊以便未來能夠更加方便被使用。Cookie 最初定義於 RFC 2109，歷經 RFC 2965，至現在的 RFC 6265。目前使用最廣泛的 Cookie 標準卻不是這些 RFC 中定義的任何一個，而是在網景公司（Netscape Communications）制定的標準上進行擴充後的產物。

Cookie 儲存在客戶端中，依照在客戶端中的儲存位置，可分為記憶體 Cookie 和硬碟 Cookie。記憶體 Cookie 由 Browser 維護，儲存在記憶體中，Browser 關閉即消失，存在時間短暫。硬碟 Cookie 儲存在硬碟裡，有過期時間，除非使用者手動清理或到了過期時間，硬碟 Cookie 不會清除，存在時間較長。所以，依照存在時間，可分為非持久 Cookie 和持久 Cookie。

以下是 Cookie 的特性：

1.可以紀錄使用者訊息。

2.儲存在客戶端。

3.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。

4.大小限制 4KB 左右。

5.能夠設置過期時間。

6.專屬於某網域(路徑)，也就是 Google.com 的頁面不能存取 Facebook.com 的 Cookie。

Cookie 依網域所有權分為第一方 Cookie 與第三方 Cookie 兩種類型，第一方 Cookie 是由使用者瀏覽的網站所建立，也就是網址列中所顯示的網站。當使用者瀏覽該網域的網站，Cookie 會記錄使用者的資訊及登錄狀況，讓瀏覽體驗更加方便。第三方 Cookie 是在使用者造訪的第一方網站上的其他網站廣告（快顯視窗、橫幅廣告），這些廣告是由其他網站所建立。當使用者瀏覽網頁時，會看到由其他網站提供的廣告或圖片，這個提供能跨網域存取暫存資料，就是第三方 Cookie。若使用者曾點擊網頁中出現的廣告連結，伺服器就會收到第三方 Cookie。因此對於使用者來說，接受第一方 Cookie，授權給信任網站，不僅能提升瀏覽體驗，對於個資也有所保障，而第三方 Cookie 則會是較難以掌握來源網站的安全性。

至於 Cookie 也存在許多缺陷，如以下幾點：

1. Cookie 會被附加在每個 HTTP 請求中，所以無形中增加了流量。
2. 由於 HTTP 請求中的 Cookie 是明文傳遞的，所以安全性成問題，除非使用超文字傳輸安全協定。
3. Cookie 的大小限制在 4KB 左右，對於複雜的儲存需求來說是不夠用的。

任何一種瀏覽器都提供了 Cookie 的功能，善意的運用，可以在重複瀏覽相同的網站時，省略許多欄位資料的輸入，帶來更好的網站體驗，增加便利性。當然這種方便也存在使用者資訊洩密的問題，尤其在多個使用者共用一部電腦時很容易出現這樣的問題。蒐集紀錄的資訊倘若存放在個人電腦裡，或許無傷大雅。若是使用公共電腦上網就需注意隱私安全的重要性。因此清理 Cookie 不僅僅是刪除了系統重複與多餘的資訊，更可確保使用者的一些私密訊息不被他人窺探。

鑑於 Cookie 的局限和反對者的聲音，有如下一些替代方法：

1. Brownie 方案，是一項開放原始碼工程，由 SourceForge 發起。Brownie 曾被用以共享在不同域中的存取，而 Cookie 則被構想成單一域中的存取。這項方案目前已經停止開發。

2. P3P（Platform for Privacy Preferences Project），用以讓使用者獲得更多控制個人隱私權利的協定。在瀏覽網站時，它類似於 Cookie。這項方案目前也已經停止開發。

3. 在與伺服器傳輸資料時，通過在位址後面添加唯一的查詢串，讓伺服器辨識是否是合法使用者，也可以避免使用 Cookie。