Http Cookie 及其用法

Cookie 技術是網路時代的快速變遷下所誕生的產物，為了讓用戶在訪問網站時可以提高訪問速度、減少現有的人工填寫，而發明了現在被大家廣為人知的 Cookie。早期 Cookie 是由 Web server 端產生的，發送給瀏覽器端，而當瀏覽器接收到 Cookie 後，會將其中的 key，保存到某個路徑內的文本文件之中，下次造訪同一網站時，就可以將 Cookie 自動發送給 Web Server 端。所以我們知道 Cookie 是屬於一種小型的文字檔案，透過加密的方式儲存在用戶端上的資料，一般來說 cookie 會紀錄用戶的資訊，使 Web service 可以用來辨別用戶身分，來取得相關的資訊 。

Cookie 通常可以儲存在記憶體或硬體內，記憶體是由瀏覽器來維護的，通常會在瀏覽器關閉後清除，而各個瀏覽器之間的 Cookie 是無法相互使用；而硬體的 Cookie 則會有一個保存期限，除非過期或是手動刪除，不然他的儲存時間會較瀏覽器來的長。

以登入的應用為例，使用者登入一個網站時，伺服器端往往會請求用戶輸入使用者帳號及密碼，並且用戶可以勾選「下次自動登入」，如果勾選了，在使用者前一次登入時，伺服器就會傳送了包含登入憑據的 Cookie 到使用者的硬碟或記憶體上，在之後登入時，瀏覽器會傳送該 Cookie 給伺服器作驗證憑據，來減少重複登入的輸入行為。

而 Cookie 屬性除了 name（名）和 value（值）之外，還有以下四種可選擇的屬性 expires：表示 Cookie 的保存期限，在默認情況下為暫時性的 cookie，只要關閉瀏覽器就會消失；path：指定與 cookie 關連在一起的網頁，默認狀況下為和當前網頁同一目錄的網頁中有效。Domain：設定 cookie 有效的網域名稱，可以和 path 一同設定，讓類似的 domain 可以享有同樣的 cookie。Secure：算是 cookie 的安全值，在默認的情況 cookie 的傳輸上是不安全的，

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。

瀏覽記錄也可以算是 cookie 的一種，許多人員在使用 cookie 的狀況下，常會造訪一些安全性不夠或是不合法的網站，而這些不僅會有資安上的風險，更是讓隱私曝光，還有些廣告公司更是會把資訊寫入 cookie 來達到發送垃圾訊息的目的。若你的電腦裡有多個瀏覽器，個別在不同空間存放 cookie，或是使用單一瀏覽器卻在不同的電腦上作操作，也會得到不同的 cookie 訊息。