網頁設計HW6-cookie

資工系 B0929026 林哲佑

Cookie 是存儲在您計算機上的小型文本文件中的數據。是網站（網路伺服器）端透過網頁瀏覽器，將使用電腦或智慧手機存取該網站的使用者ID或瀏覽紀錄等資訊加以紀錄與辨識，並進行暫存的機制。等到下一次瀏覽相同發布來源的網站（網路伺服器）時，就會透過網頁瀏覽器遞交給網路伺服器。網站就可因此辨別再次存取網站的使用者身份。

在典型的網路購物場景中，使用者瀏覽了幾個頁面，買了一盒餅乾和兩瓶飲料。最後結帳時，伺服器並不知道使用者到底買了什麼，伺服器可以設定或讀取Cookie中包含的資訊，藉此維護使用者跟伺服器[對談](https://zh.wikipedia.org/wiki/%E4%BC%9A%E8%AF%9D_(%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%A7%91%E5%AD%A6))中的狀態。使用者選購了第一項商品，伺服器在向使用者傳送網頁的同時，還傳送了一段Cookie，記錄著那項商品的資訊。當使用者存取另一個頁面，瀏覽器會把Cookie傳送給伺服器，於是伺服器知道他之前選購了什麼。

Cookie另一個典型的應用是當登入一個網站時，網站往往會請求使用者輸入使用者名稱和密碼，並且使用者可以勾選「下次自動登入」。如果勾選了，那麼下次存取同一網站時，使用者會發現沒輸入使用者名稱和密碼就已經登入了。這正是因為前一次登入時，伺服器傳送了包含登入憑據（使用者名稱加密碼的某種[加密](https://zh.wikipedia.org/wiki/%E5%8A%A0%E5%AF%86)形式）的Cookie到使用者的硬碟上。第二次登入時，如果該Cookie尚未到期，瀏覽器會傳送該Cookie，伺服器驗證憑據，於是不必輸入使用者名稱和密碼就讓使用者登入了。

Cookie在某種程度上說已經嚴重危及使用者的[隱私](https://zh.wikipedia.org/wiki/%E9%9A%90%E7%A7%81)和[安全](https://zh.wikipedia.org/zh-tw/%E5%AE%89%E5%85%A8)。其中的一種方法是：一些公司的高層人員為了某種目的（譬如市場調研）而存取了從未去過的網站（通過搜尋引擎查到的），而這些網站包含了一種叫做[網頁臭蟲](https://zh.wikipedia.org/wiki/%E7%BD%91%E9%A1%B5%E8%87%AD%E8%99%AB)的圖片，該圖片透明，且只有一個像素大小（以便隱藏），它們的作用是將所有存取過此頁面的電腦寫入Cookie。而後，[電子商務](https://zh.wikipedia.org/wiki/%E7%94%B5%E5%AD%90%E5%95%86%E5%8A%A1)網站將讀取這些Cookie資訊，並尋找寫入這些Cookie的網站，隨即傳送包含了針對這個網站的相關產品廣告的[垃圾郵件](https://zh.wikipedia.org/wiki/%E5%9E%83%E5%9C%BE%E9%82%AE%E4%BB%B6)給這些進階人員。雖然Cookie沒有中電腦病毒那麼危險，但它仍包含了一些敏感訊息：使用者名稱、電腦名、使用的瀏覽器和曾經存取的網站。使用者不希望這些內容洩漏出去，尤其是當其中還包含有私人資訊的時候。