HW6-Cookie 心得文章

Cookie 是網路伺服器透過網頁瀏覽器，將使用電腦或智慧型手機存取該網站的使用者 ID 或瀏覽紀錄等資訊加以記錄與辨識，並進行暫存的機制，等到下次瀏覽相同發布來源的網站時，就會透過網頁瀏覽器遞交給網路伺服器，網站就因此辨別再次存取網站的使用者身分。

Cookie 的用途很廣，最常見的用途像是網路購物中的購物車，點選了第一項商品後還想再買第二項商品，這時瀏覽器就會傳送一段 Cookie 給伺服器，讓伺服器知道你之前買了第一項商品，並在購買第二項商品後在原本的 Cookie 追加新的商品資訊，最後結帳時，伺服器讀取 Cookie 就能知道你全部要買的商品了；另一個很實用的用途是自動登入，很多網站或 app 會在帳號密碼下面有一個自動登入的選項，點選後之後再開就可以不輸入帳號密碼直接登入了，這是因為第一次登入時伺服器傳送了 Cookie 到您的硬碟上，下次登入時， Cookie 便會記住您網站的偏好設定，免去經常輸入會員帳密的麻煩，甚至是所填的姓名、電話、地址、信用卡號之類的都會記錄下來，讓操作更加便利，更容易搜尋到所需要的資訊；還有一個用途是投放廣告，廣告商（第三方網站）會在很多大型網站入口刊登廣告(EX: Yahoo 、 Hinet 、 MSN 、 PChome)，而在這些網站上，你連上的每一頁網址都會被 Cookie 記錄下來(此為第三方 Cookie)，用來追蹤與統計使用者到訪網站的偏好與習慣。比如什麼時間造訪、造訪了哪些頁面、在每個網頁的停留時間等等。利用各大網站蒐集到的資訊，提供投放適合您個人的廣告內容，但這個功能喜不喜歡見仁見智，有些人就會很不喜歡自己的瀏覽紀錄這樣被偷窺。

Cookie 是存在用戶端的，所以需要一個叫做 session 的東西，讓 Cookie 建立一個 session 的 ID ，才能在後端確認這個 Cookie 是對的；也有可以不用 session ID 的方法，只是就要設置一個寫著加密字串的 Cookie，之後進入網站時，後端再解密這個字串來辨別用戶身分。

那 Cookie 會造成危害嗎? 隨著行銷技術日益複雜， Cookie 也更常被用來搜集用戶的上網行為。駭客通常使用跨網站指令碼攻擊（XSS）盜取用戶的 Cookie，並從 Cookie 內容中取得相關資訊，然後入侵用戶設備或竊取資料。如果不喜歡上網行為被追蹤的話，可以禁用 Cookie 或直接打開「無痕模式」瀏覽網頁，無痕模式會在瀏覽器視窗關閉後，將無痕模式下創建的 Cookie 全部刪除。