HW6-Cookie 心得文章

Cookie 的定義是：何服器（Server）傳送給瀏覽器（Client）的一小片段資料。Cookie 有分為記憶體 Cookic 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：儲存和追蹤使用者行為，儲存用戶登入、購物車等伺服器所需的資訊，儲存使用者設定和偏好等。舉例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。

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" HTIP 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 cookiie 存放區，並記錄 coookie 的 exoires path •domain 以及 secure。當 Client 瑞再次發出 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"Cookie"Header 中。

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。