Hw6-cookie

系級:資工二甲　姓名:謝牧辰 學號:B0929055

相信大家對 Cookie 這個詞並不陌生，甚至沒有程式背景的人也都知道這個詞，在刪除瀏覽器紀錄時，會出現是否要刪除 Cookie 的選項，要是刪除的話，之後在進入 FB 或 Youtube 之類需要登入的頁面時，就會發現帳密需要重登了。而 Cookie 到底是什麼呢?Session 的物件存在於伺服器(程式)裡面為了避免伺服器的負擔太重，所以我們將使用者的資料儲存在使用者的電腦裡面，而該資料檔案就是 Cookie。Cookie 存放的位置會隨著瀏覽器的不同而有所不同，只要程式對使用者的電腦寫入 Cookie，之後使用者每次登入網站時就可以直接去使用者的電腦找 Cookie，使用之前的資料了。Cookie 的存取寫得好，可以省去很多設定與查詢的時間。在開發網頁時，要有一個很重要的觀念，那就是 **HTTP 協定是無狀態的**。「簡單來說就是伺服器處理完你的 request 之後就與你無關了，而且它也不會記得你和它之間的故事，你們的關係形同陌生人，下班好累，開個 IG 看廢文，咦!怎麼要我打帳密登入，我不是昨天才登入過，我的密碼抄在小紙上面，那張紙不知道跑去哪裡了，而且不對吧，這個使用者體驗是怎麼回事，每天打帳密就飽了!」，這個就是 HTTP 無狀態 特性，伺服器並不會知道你之前做了什麼，常見的例子還有**購物車**，買了好幾個商品要結帳，結果伺服器不知道我到底買了什麼。cookie 可以用來解決這個問題，它能夠儲存一些資訊，像是我拿著會員卡，就能夠直接進入商店，因為上面的卡號說明了我是這家店已經付費過的客人，也就是他們的會員，所以我不用再付費就能夠入場。cookie 說穿了就是 key=value 的形式而已，但是透過 document.cookie 查看時，發現它們全部被組成字串，如果我只是要單純存取某個屬性的值而已，不就還要自己切割字串嗎?沒錯! 還真的要自己切割字串， JS 本身沒有提供這些方法，所幸 W3C 有附上常用操作的函數。路徑限制並不能阻止從其他路徑訪問 cookie，使用簡單的 DOM 即可輕易地繞過限制(比如創建一個指向限制路徑的，隱藏的 iframe，然後訪問其 contentDocument.cookie 屬性)，保護 cookie 不被非法訪問的唯一方法是將它放在另一個域名/子域名之下，利用同源策略保護其不被讀取。Web 應用程序通常使用 cookies 來標識用戶身份及他們的登錄會話，因此通過竊聽這些 cookie，就可以劫持已登錄用戶的會話，竊聽的 cookie 的常見方法包括社會工程和 XSS 攻擊。HttpOnly 屬性可以阻止通過 javascript 訪問 cookie，從而一定程度上遏制這類攻擊。