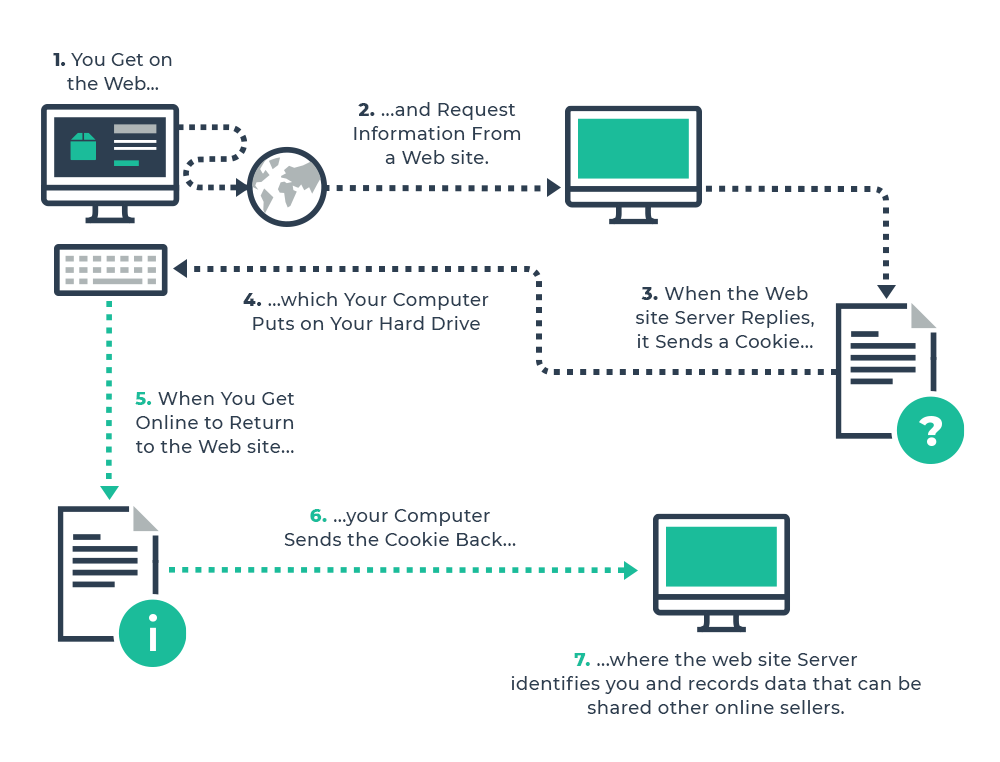
HW6網頁設計作業2



HTTP cookie（web cookie、browser cookie）為伺服器傳送予使用者瀏覽器的一個小片段資料。瀏覽器可能儲存並於下一次請求回傳 cookie 至相同的伺服器。Cookie 通常被用來保持使用者的登入狀態——如果兩次請求都來自相同的瀏覽器。

Cookies 主要用於三個目的：

1. Session管理:帳號登入、購物車、遊戲分數，或任何其他伺服器應該記住的資訊
2. 個人化:使用者設定、佈景主題，以及其他設定
3. 追蹤:記錄並分析使用者行為

Cookies曾被當作一般的客戶端儲存方式來使用。這在當時 cookie仍是將資料儲存在客戶端的唯一方法，現在則建議使用現代的 storage APIs。Cookies會被每一個請求發送出去，所以可能會影響效能，尤其是行動裝置的資料連線。

Cookie是網站端透過網頁瀏覽器，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。

例如:購物網站會員網頁的使用情境，在重新造訪購物網站，而前一次放入購物車中的商品仍然保留，或是推薦商品依舊顯示在螢幕上，這些都是因為Cookie起了作用，網站端參考了Cookie，對於相應的使用者顯示接續前次造訪時瀏覽的網路內容。

透過 Cookie，我們的確達成目標，讓伺服器可以在往後透過客戶端發出的請求，辨識使用者及其登入狀態，非常方便。然而，這些資訊其實用戶是有機會可以在瀏覽器中修改的，因此使用者能透過串改 Cookie 上的內容，讓伺服器收到不正確的訊息。因此這會造成使用者在資安上的漏洞與威脅，是每個人都需要注意的。

常見的攻擊手法叫做Session hijacking，就是透過 JavaScript將Cookie 偷偷傳遞出來，然後冒用別人的Cookie來登入，因此帳號和密碼不能儲存於Cookies中，Cookie 及 Session是網頁應用不可或缺的機制之一，特別是在前端越來越複雜的現代網站上，如何在無狀態的HTTP上得知使用者的身分，並接續使用者狀態，是非常重要的一環。但儲存身分的同時，也就代表著身分被冒用的風險，在應用上就需要特別注意。因此我們在學習的過程中要非常注意類似的技術，因為這在當我們越熟悉網頁開發的技巧後，資訊安全的部分會越來越重要。