B0929030 周兆騰

HTTP cookie （ cookie、瀏覽器的一個小請求 cookie）為服務器提供給用戶瀏覽器的一個小請求數據。瀏覽器存儲於下一次瀏覽器至相同的服務器。的進入狀態——如果兩次請求的狀態都來自不同的瀏覽器。舉例來說，它記住了無（stateless）（en-US） HTTP 協議的有狀態信息。Cookies 主要用於三個目的：會話管理:(會員註冊、購物、遊戲分數，或任何其他服務器應該記住的信息)、個人化:(用戶設置、佈景主題，以及其他設置)、追踪:(記錄並分析行為用戶)。Cookies 被一般當做客戶端儲存的方式來使用。方法是把 cookie 儲存出去，然後儲存 API 會在客戶端的唯一時間是有效的，則建議使用現代的。Cookies 被每一個發送的請求，所以可能會對客戶端產生影響（尤其是行動裝置的連線）。 現代的存儲 APIs 為 Web storage API (en-US)（localStorage 和 sessionStorage）以及 IndexedDB。

使用 Cookie 傳送重要資訊的安全性隱憂。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，有趣的是，這些資訊其實用戶是有機會可以在瀏覽器中修改的，因此使用者能透過更改 Cookie 上的內容，讓伺服器收到不正確的訊息 也就是說，以登入的例子來看，使用者可以在串改 isLoggedIn 的值，讓伺服器誤以為使用者已經通過認證：儘量避免將敏感資訊透過 Cookie 存在客戶端。

如果沒有事先告知消費者發現你的 cookie 的存在，當消費者發現你的 cookie 時，對你信任的結果。關於的負面影響。有些人有 cookie 的法律條文。也沒有法律上或技術上可關閉的使用頭，指示應用程序的跟踪、或跨跟踪。

最後舉個小例子，想像你入住了迪士尼飯店，飯店告知有關你的入房、預約餐廳和遊樂設施的資訊都已經存在迪士尼的系統當中了，並附上一只專屬的 MagicBand，手錶晶片中有系統給你的專屬 ID 號碼，因此這幾天在飯店直接感應房門、在餐廳或遊樂設施前感應機器就能透過系統辨識完成開門和報到。
因為你的個人資訊很重要，所以迪士尼將入房、預約資訊以 Session 存放在系統中，這筆資料對應了一個獨特的 Session ID。而 MagicBand 就像是 Cookie，當中帶有這個 Session ID，當你透過 MagicBand 在感應機器時，系統就能快速辨識你的身份，並找到存放你入房和預約資料的 Session 了！
如同上面說的，重要的資訊不建議放在客戶端 — 像是寫在你的 MagicBand 上，你就有機會串改遊樂設施的預約時間、其他人也有機會看到你的隱私等 — 若放在迪士尼的系統中（像是伺服器的概念），就顯得安全許多：你唯一需要的，是那只含有獨特 ID 的 MagicBand 讓系統辨識罷了！