http cookie

首先，HTTP cookie 為伺服器傳送給使用者瀏覽器的一小片段資料。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。

看完以上的介紹有大機率還是對於 cookie 處於一個似懂非懂的狀態，因為我也是，以下我們會用其功能來介紹它，相信能更淺顯易懂。

Cookies 主要用於三個目的：

第一，Session 管理。舉例來說，常見的有記住密碼的功能和我們使用網路購物時的購物車。

第二，個人化。各種使用者設定，像是字體大小，或是背景主題……等等。

第三，追蹤。紀錄並分析使用者行為。舉一個簡單的例子，當你在 google 上查詢底片相機，且點進各個和其有關的頁面時，google 便會將這記住，並推薦你相關的廣告。

因為 cookie 常被用於各個網頁中，因此其安全性也是相當重要的，竊取 cookie 可能造成使用者的 authenticated session 被劫持。一班竊取 cookie 的作法

包括社交工程，或是利用應用程式中的 XSS 漏洞，而 cookie 中的 HttpOnly 屬性，能藉由防止透過 JavaScript 取得 cookie 內容，來減少此類型的攻擊。

在維基百科中提到了一個關於 Cross-site request forgery 的例子，能夠讓我們了解安全性的重要。假設某人插入了一個並非真實圖片，而是對你銀行伺服器請求領錢的 image「<img src="http://bank.example.com/withdraw?account=bob&amount=1000000&for=mallory">」，若你載入此圖片的 HTML 時，正好銀行登入的 cookie 仍奏效（及還保持登入狀態），你的錢就會被轉出。

Cookie 有兩種，第一種為第一方 cookie，第二種為第三方，兩者的最大差別在於其網域和你所在的頁面網域是否相同，相同為第一方，不同則為第三方。第一方的 cookie 只會被送到設定他們的伺服器，但是，一個網頁還可能存在其他伺服器，像是插入式的橫幅廣告……等等，這些透過這些第三方組件傳送的 cookies 便是第三方 cookies，通常被被用於廣告和網頁上的追蹤。

在這個重視隱私的時代，若沒有事先告知消費者第三方 cookies 的存在，往往會造成商譽和信譽上的受損，甚至有些國家會明定關於 cookie 的法律條文去做約束，歐盟也在 2001/02/25 定義了與 cookie 有關的約束——在使用 cookie 前，需先經過使用者的同意。當然，以上的規定皆是只防君子不防小人，我們在使用網際網路時仍須多加注意，以免資料被不肖人士使用。