HTTP cookies，通常又稱作“cookies”，已經存在了很長時間，但是仍舊沒有被予以充分的理解。 首要的問題是存在了諸多誤區，認為 cookies 是後門程式或病毒，或壓根不知道它是如何工作的。 第二個問題是對於 cookies 缺少一個一致性的介面。 儘管存在著這些問題，cookies 仍舊在 web 開發中起著如此重要的作用，以至於如果 cookie 在沒有可替代品出現的情況下消失，我們許多喜歡的 Web 應用將變得毫無用處。

坦白的說，一個 cookie 就是存儲在使用者主機瀏覽器中的一小段文本檔。 Cookies 是純文本形式，它們不包含任何可執行代碼。 一個 Web 頁面或伺服器告之瀏覽器來將這些資訊存儲並且基於一系列規則在之後的每個請求中都將該資訊返回至伺服器。 Web 伺服器之後可以利用這些資訊來標識使用者。 多數需要登錄的網站通常會在你的認證資訊通過後來設置一個 cookie，之後只要這個 cookie 存在並且合法，你就可以自由的瀏覽這個網站的所有部分。 再次，cookie 只是包含了數據，就其本身而言並不有害。 HTTP 是無狀態（stateless）的協定，使用 Cookie 來管理會話（session）狀態及跟蹤用戶行為等。 Cookie 是把 Web 伺服器（或者網站）發送過來的信息臨時保存到瀏覽器的機制。

Cookie 有 2 種，“1st Party Cookie”和“3rd Party Cookie”。

“1st Party Cookie”是由 Web 伺服器（既網站域名）發出的 Cookie，而“3rd Party Cookie”是由 Web 伺服器以外的域名發出的 Cookie。

1st Party Cookie 我們正在訪問的網站發出的 Cookie。 1st Party Cookie 存儲瀏覽歷史、登錄資訊、購物車裡的產品資訊和個人資訊等。 1st Party Cookie 的資訊，基於用於同一個功能變數名稱（既正在訪問的網站功能變數名稱）的原則。

3rd Party Cookie 而 3rd Party Cookie 由我們正在訪問的網站功能變數名稱以外的功能變數名稱發出的 Cookie。 例如投放廣告的廣告商用於存儲用戶資訊。 該 Cookie 信息因為跨網站被使用，也被稱為跟蹤 Cookie。 以廣告為例，在 A 網站顯示的商品或者服務，當訪問 B 網站時也顯示同樣的商品或服務也是使用了 3rd Party Cookie 資訊。 對於廣告商來說，3rd Party Cookie 非常有效，然而從使用者安全和隱私保護的觀點來看，是一個不受歡迎的機制。