

B0929057_游少嫻_cookie

HTTP cookie（又稱 web cookie、browser cookie）是一個為伺服器傳送給使用者的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。舉例來說，它記住了無狀態（stateless）HTTP 協議的有狀態資訊。因為 HTTP 協定是無狀態的，即伺服器不知道使用者上一次做了什麼，這嚴重阻礙了互動式 Web 應用程式的實現。而 Cookie 就是一種用來繞開 HTTP 的無狀態性的「額外手段」之一。就如同購物車可以藉由 cookie 的小型文字網站中獲取使用者先前的購買清單。

其用於三個目的 Session 管理（包含購物車、帳號登入或是其他伺服器資訊）、個人化使用（包含使用者的設定、佈景主題...）、追蹤（紀錄與分析使用者行為，包含自動登入）。而種類分為記憶體 cookie（瀏覽器關閉即消失）和硬碟 cookie（只有手動清除或是到其過期時間才會消失）。

其使用方式（在此以 Javascript 為例）包含了

創建：`document.cookie = "username=John Doe";`

添加日期：`document.cookie = "username=John Doe; expires=Thu, 18 Dec 2013 12:00:00 UTC";`

添加路徑參數：`document.cookie = "username=John Doe; expires=Thu, 18 Dec 2013 12:00:00 UTC; path=/"`;

讀取：`let x = document.cookie;`

更改：`document.cookie = "username=John Smith; expires=Thu, 18 Dec 2013 12:00:00 UTC; path=/"`;

刪除：`document.cookie = "username=; expires=Thu, 01 Jan 1970 00:00:00 UTC; path=/"`;

而一個設置完整的 cookie 函式便會如下：

```
function setCookie(cname, cvalue, exdays) {  
  const d = new Date();  
  d.setTime(d.getTime() + (exdays * 24 * 60 * 60 * 1000));  
  let expires = "expires="+d.toUTCString();  
  document.cookie = cname + "=" + cvalue + ";" + expires  
+ ";path=/"  
}
```

```
function getCookie(cname) {  
  let name = cname + "=";  
  let ca = document.cookie.split(';');  
  for(let i = 0; i < ca.length; i++) {
```

```

    let c = ca[i];
    while (c.charAt(0) == ' ') {
        c = c.substring(1);
    }
    if (c.indexOf(name) == 0) {
        return c.substring(name.length, c.length);
    }
}
return "";
}

function checkCookie() {
    let user = getCookie("username");
    if (user != "") {
        alert("Welcome again " + user);
    } else {
        user = prompt("Please enter your name:", "");
        if (user != "" && user != null) {
            setCookie("username", user, 365);
        }
    }
}

```

但 **cookie** 仍有許多缺點如因為附加在 **http** 裡而增加的流量、因為明文傳遞而增加的資訊安全風險和其限制 **4KB** 大小無法處理複雜處存資料。而也有許多人反對 **cookie**，原因包含其辨識不準確，如果在同一台機器上使用多個瀏覽器，每個瀏覽器在不同的儲存位置儲存 **Cookie**，因此，**Cookie** 並不能定位到一個具體的人，而是使用者、電腦和瀏覽器的組合、狀態不準確，如果使用者在取得了一個 **Cookie** 之後，點擊了瀏覽器的「回退」按鍵，則瀏覽器的狀態和取得 **Cookie** 的狀態就出現了不一致。例如，如果網站基於 **Cookie** 技術實現了購物車的應用，當使用者添加了物品後點擊了「回退」按鍵，購物車的物品狀態可能並沒有發生變化、與隱私安全的廣告的問題。