B0929036 林湘庭

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。

Cookies 功用：

- 可以紀錄使用者訊息。
- 儲存在客戶端。
- 連線時會自動帶上，但過多的 cookie 可能會浪費流量、或是帶上無用之 cookie。
- 大小限制 4kb 左右。
- 能夠設置過期時間。
- 專屬於某網域(路徑)，也就是 google.com 的頁面不能存取 facebook.com 的 cookie。

建立 cookie:

收到一個 HTTP 請求時，伺服器可以傳送一個 Set-Cookie (en-US) 的標頭和回應。Cookie 通常存於瀏覽器中，並隨著請求被放在 Cookie HTTP 標頭內，傳給同個伺服器。

也可以註明 Cookie 的有效或終止時間，超過時間後 cookie 就不會再發送。

此外，也可以限制 Cookie 不傳送到特定的網域或路徑。

Set-Cookie 及 Cookie 標頭，一個簡單的 cookie 可以如下例設定：

Set-Cookie: <cookie-name>=<cookie-value>

這個來自伺服器的標頭就會告訴客戶端要儲存一個 cookie。

分類：

- session cookie：當客戶端關閉時即被刪除，因為它並沒有註明過期 Expires 或可維持的最大時間 Max-Age。
- 常駐 cookies：不會在客戶關閉後到期，而是在一個特定的日期 (Expires) 或一個標明的時間長度後 (Max-Age)。
- Secure 以及 HttpOnly cookies:

  Secure cookie 只有在以加密的請求透過 HTTPS 協議時，傳送給伺服器。但即便是 Secure ，敏感的資訊絕對不該存在 cookies 內，因為他們本質上是不安全的。現在不安全的網站 (http:) 就不能以 Secure 的指示設定 cookies。

  不需要讓 JavaScript 可以取用仍在伺服器 sessions 中的 cookies 時，就應該立 HttpOnly 的旗幟(如下):

  Set-Cookie: id=a3fWa; Expires=Wed, 21 Oct 2015 07:28:00 GMT; Secure; HttpOnly

Cookies 的作用範圍:

Domain 及 Path 的指示定義了 cookie 的作用範圍： cookies 應該被送到哪些 URLs 。

Domain: 受允許的 hosts 能接收 cookie。若無註明，則預設給當前文件位置的 host (en-US)。
Path: 一個必定存在於請求 URL 中的 URL 路徑，使 Cookie 標頭能被傳出。

- SameSite cookies Experimental: 讓伺服器要求 cookie 不應以跨站請求的方式寄送，某種程度上避免了跨站請求偽造的攻擊 (CSRF)。(補充:SameSite cookies 目前仍在實驗階段)。

JavaScript 使用 Document.cookie 存取(如下):

```
document.cookie = "yummy_cookie=choco";
document.cookie = "tasty_cookie=strawberry";
console.log(document.cookie);
// logs "yummy_cookie=choco; tasty_cookie=strawberry"
```

安全性:
Session hijacking 以及 XSS:
一般偷取 cookies 的作法包括社交工程 (Social Engineering)，或利用應用程式中的 XSS (en-US) 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。
Cross-site request forgery (CSRF):
舉例: 假設在一個未經過濾的對話或論壇中，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。此時如果你的銀行帳戶仍在登入狀態中，你的 cookies 仍然有效，並且沒有其他的驗證方式，當你載入包含此圖片的 HTML 同時，你的錢即會被轉出。預防方法如下:

- Input filtering 和 XSS (en-US) 一樣是重要的。
- 做任何敏感的動作前，都應該要求使用者確認。
- 用於敏感動作的 Cookies 都只應該有短時間的生命週期。
- 更多防範的技巧，參見 OWASP CSRF prevention cheat sheet。

追蹤及隱私:
大部分的瀏覽器預設允許第三方 cookies，但也有些可以阻擋他們的 add-on (例如 EFF 的 Privacy Badger)。
Cookie 會公開表明 cookie ，以減少不信任等負面影響。

- Do-Not-Track:
  可利用 DNT 標頭，指示網頁應用程式關閉頁面的追蹤、或跨站的使用者追蹤。
- Zombie cookies and Evercookies:
  是一個更激進的手段，刻意讓 cookies 在被刪除後重新創造，使其很難被永遠的刪除。

參考資料:

https://developer.mozilla.org/zh-TW/docs/Web/HTTP/Cookies

https://ithelp.ithome.com.tw/articles/10203123