Cookie 心得

Cookie 的發明源自於網景公司，發明的原因在於 HTTP 協定是無狀態的因此無法儲存使用者資訊，而 Cookie 儲存在客戶端中，除非使用者手動清理或到了過期時間，硬碟 Cookie 不會清除，Cookie 的缺點在於過多的 Cookie 可能會浪費流量，在 http 的請求 Cookie 是明文的可能產生安全性問題，此外 Cookie 的儲存大小在 4kb，過於複雜的資料會無法儲存，Cookie 會被附加在每個 HTTP 請求中，所以無形中增加了流量，以上是 Cookie 的簡單介紹，以下是我是我整理出的 Cookie 用法

1.用 JS 讀取 Cookie

```
console.log(document.cookie);
```

2.用 JS 寫入 Cookie，可以改特定 cookie 值

```
document.cookie = 'key=value;'
```

再來是 Cookie 的安全設定

1.Domain

```
domain=example.com
```

domin 可以指定特定網域與其子網域來存取 Cookie

2.Path

```
path=/admin
```

path 參數用來指定哪些路徑可以存取這個 Cookie，如果將 Cookie 設為 path=/則所有網站皆可存取，所有 server 皆能存取資料

3.Expires, Max-age

expire

```
cookie=value; expires=Tue, 19 Jan 2038 03:14:07 GMT
```

max-age

```
cookie=value; max-age=3600
```

上面兩個都是關於 Cookie 的期限設定，expire 是設定 UTC 有效期限，max-age 是設定幾秒後的期限

4.Secure

使用 secure 可以只讓 Cookie 用 https 傳遞

Cookie 的種類

1. 1st Party Cookie

   1st Party Cookie 儲存瀏覽歷史、登錄信息、購物車裡的產品信息和個人信息等。

2. 3rd Party Cookie

   3rd Party Cookie 由我們正在訪問的網站域名以外的域名發出的 Cookie。例如投放廣告的廣告商用於儲存用戶信息。該 Cookie 信息因為跨網站被使用，也被稱為跟踪 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 信息。

後面是我在找資料時關於 Cookie 與跨網與請求的關係，當 Cookie 以跨站方式傳送會產生跨站請求偽造問題，使用 samesite 可以防止這個問題 SameSite=strict 可以限制相同網域才能回傳，我認為 Cookie 的設定對資安有重大影響，而現今許多網站都有第三方 Cookie，我們可以選選同意或不同意，許多廣告追蹤都是因為這個可以讀取其他網站，從

而知到我們的喜好，作為一個工程師來說也許是好的，但從使用者被知道自己的網站來看卻不是那麼正面，一個錯誤可能導致資料外洩，此外 google 已宣布在 2023 年前將停止對第三方 Cookie 的支持，Cookie 除了上述問題還有其他問題，像是辨識不精確，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，還有不準確的情況，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，由此可知 Cookie 的使用要十分小心。

參考資料

https://shubo.io/cookies/
https://developer.mozilla.org/en-US/docs/Web/API/Document/
https://www.w3schools.com/js/js_cookies.asp
https://ithelp.ithome.com.tw/articles/10203123
https://sys-blog.net/http-cookie/
https://zh.wikipedia.org/zh-tw/Cookie