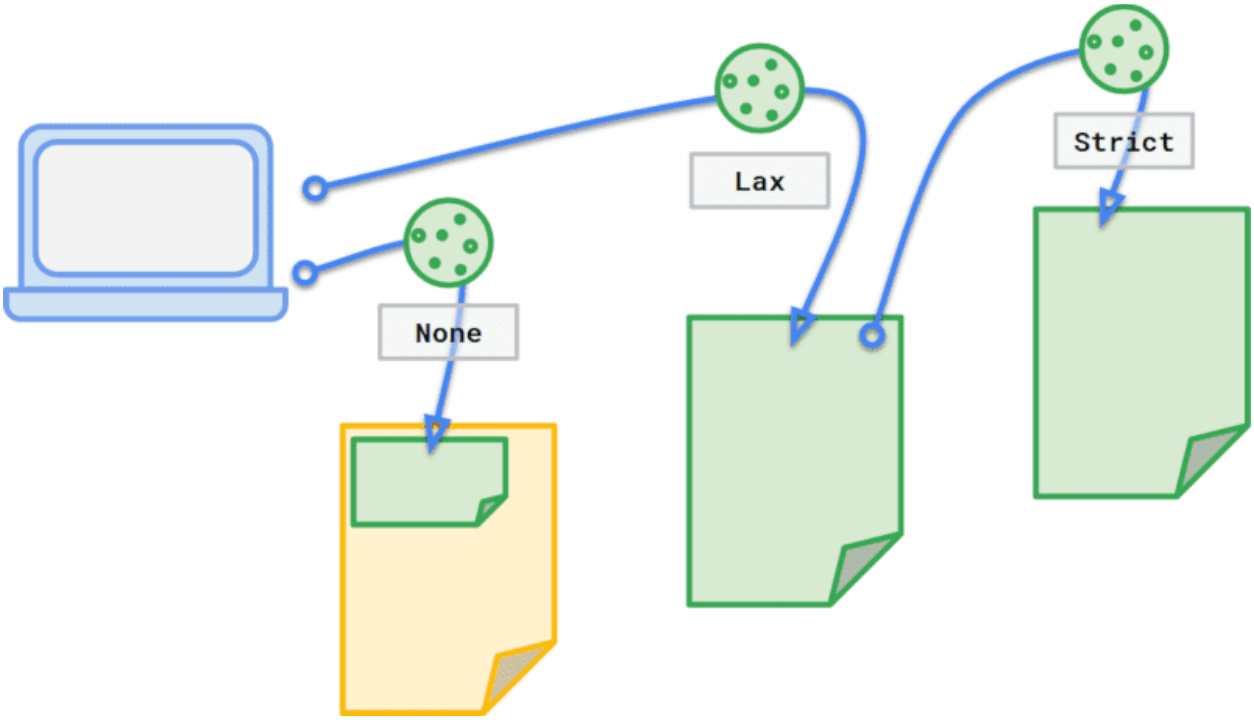
Samesite



1. Khái niệm.

- SamSite : là thuộc tính cookie được trình đuyệt hỗ trợ để giới hận việc gửi cookie trong các request.

2. cú pháp:

Cookie: SameSite=<GIÁ TRỊ>

Giá trị	Hành vi
Strict	Cookie chỉ gửi khi request cùng site.
Lax	Cookie gửi GET request cross-site, không gửi với POST
None	Cookie gửi với mọi request, cả cross-site.

3. hoạt động.

- SameSite=Strict

+ Trình duyệt chỉ gửi cookie nếu trang được truy cập từ chính domain đó.

+ Bất kỳ request nào từ domain khác (kể cả khi người dùng click vào link từ site A để đến site B) → Cookie không được gửi.

- SameSite=Lax

+ Cookie vẫn được gửi trong một số tình huống:

- Người dùng click link từ site khác
- Điều hướng bằng GET request

+ Không gửi cookie với các request tự động (như POST, iframe, fetch từ site khác)

- SameSite=None

+ Hoàn toàn không hạn chế (gửi mọi lúc)

- Cookie được gửi với mọi request, bất kể từ site nào
- Phải đi kèm Secure (tức là chỉ gửi qua HTTPS)

4. cài đặt.

```
setcookie("sessionid", "abc123", [
    "samesite" => "Lax",
    "secure" => true,
    "httponly" => true
]);
```