Set-Cookie

1. Khái niệm cơ bản.

- Set-Cookie là 1 tiêu đề phản hồi bởi máy chủ và được sử dụng để chuyển cookie đến máy khách.

- server chỉ thiết lập trong response nếu muốn thiết lập hoặc cập nhật côkie mới.

2. Cú pháp hợp lệ.

Cú pháp :

Set-Cookie: <name>=<value>; Expires=<date>; Max-Age=<seconds>; Domain=<domain>; Path=<path>; Secure; HttpOnly; SameSite=<value>

Thành phần	Ý nghĩa
name=value	Tên và giá trị của cookie
Expires=<date>	Ngày hết hạn cookie (theo chuẩn HTTP-date)
Max-Age=<seconds>	Cookie sống trong bao nhiêu giây (ưu tiên hơn Expires)
Domain=<domain>	Chỉ gửi cookie đến domain này hoặc subdomain
Path=<path>	Chỉ gửi cookie nếu URL phù hợp path này
Secure	Chỉ gửi cookie qua HTTPS
HttpOnly	Không cho phép JavaScript truy cập cookie (bảo vệ chống XSS)
SameSite=<value>	Lax

3. Hoạt động.

- Bước 1: Server gửi header Set-Cookie trong HTTP Response : Khi một người dùng đăng nhập hoặc truy cập một dịch vụ, server tạo một session hoặc token, rồi gửi nó về cho trình duyệt bằng cách gắn vào header Set-Cookie

- Bước 2: Trình duyệt nhận và lưu cookie: Trình duyệt sẽ lưu cookie này trong bộ nhớ cookie (RAM hoặc local storage tùy loại cookie).

Lưu ý : Nếu cookie không có Expires hoặc Max-Age, thì cookie là session cookie và bị xóa khi đóng trình duyệt.

- Bước 3: Trình duyệt tự động gửi cookie trong các request sau : Khi người dùng truy cập lại cùng domain (và path phù hợp), trình duyệt sẽ gửi lại cookie đó qua header Cookie trong mỗi HTTP request.

- Bước 4: Server nhận cookie và xử lý session

+ Server đọc cookie sessionId=abc123

+ Tra cứu trong database hoặc memory xem session đó có hợp lệ không

+ Nếu hợp lệ → trả về nội dung trang

+ Nếu không hợp lệ (hết hạn, sai giá trị) → trả về lỗi hoặc redirect về trang login

4. Chức năng.

- Session Management(Duy trì phiên làm việc)

- Authentication & Security (Xác thực và bảo mật)

- User Preferences / Personalization (Lưu trữ thông tin người dùng)

- Tracking (Theo dõi hành vi người dùng)

5. Cấu hình.

```
from flask import make_response

@app.route('/login')
def login():
    resp = make_response("Welcome!")
    resp.set_cookie(
        'session_id', 'abc123',
        httponly=True,
        secure=True,
        samesite='Strict',
        max_age=3600
    )
    return resp
```

Tài liệu tham khảo.

- https://medium.com/@ajay.monga73/securing-cookies-why-you-should-always-set-httponly-92489cbf76c1