Security Tips

HttpOnly: Prevents JavaScript access → protects against XSS

Secure: Sent only over HTTPS → prevents MITM attacks

SameSite=Lax/Strict: Reduces CSRF attacks

Access Token should be short-lived, Refresh Token long-lived and rotated

Do not put sensitive information in the JWT payload

2. **Error Handling**

Expired Access Token: 401 response → use Refresh Token

Expired or invalid Refresh Token: 401 response → user must log in again

Tampered token: 401 response with a general message "Invalid token"

Revoked token or reuse attack: immediate user logout