**2. WebAPI HandsOn**

Question 1. Explain CORS enablement for Web API access for local application.

Cross-Origin Resource Sharing (CORS) is a security feature implemented by browsers to restrict web pages from making requests to a different domain than the one that served the web page.

For example:

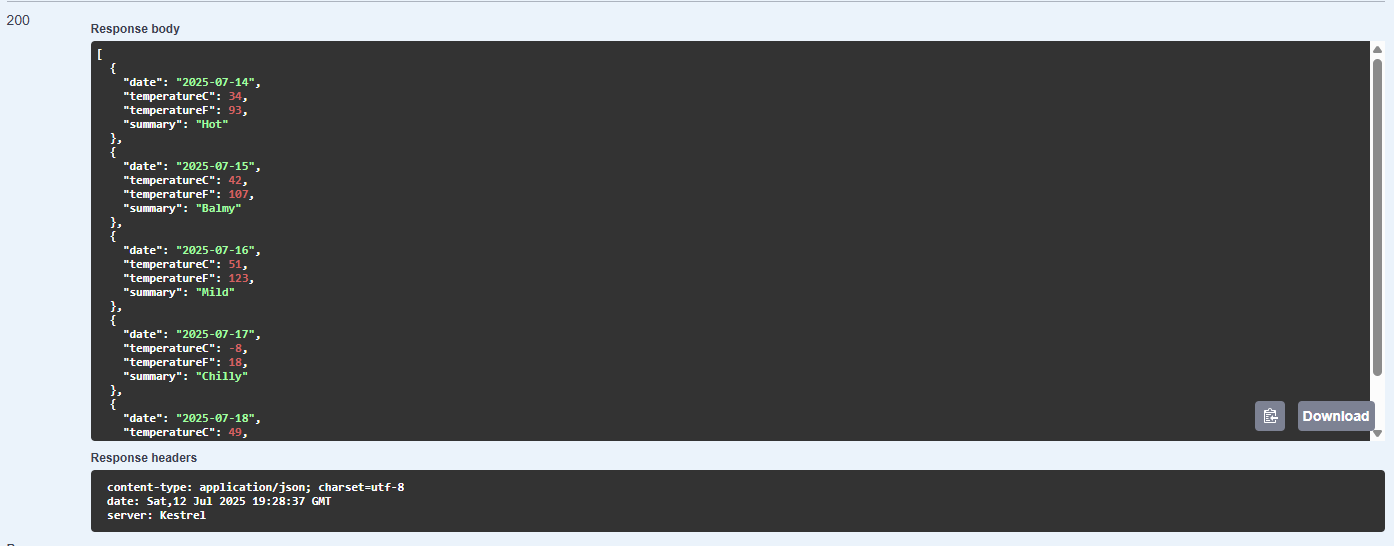
* Frontend (React/Angular) runs at: http://localhost:3000
* Backend API runs at: http://localhost:5000  
  Browser blocks calls from localhost:3000 → localhost:5000 unless CORS is explicitly enabled on the server.

DEMONSTRATION OF ACCESS CONTROL :

## Role-based Access Control

### 🔹 Test with Different Roles:

* Token with role = "Admin" → Allowed
* Token with role = "User" or wrong role → Blocked
* Authorize(Roles = "Admin,POC") means token must include either Admin or POC in claims.

GET Request:

POST Request:

