CORS

What is CORS?

CORS, which stands for Cross-Origin Resource Sharing, is a security feature implemented by web browsers to control how web applications can request resources from different origins (domains). The primary purpose of CORS is to prevent malicious websites from making unauthorized requests to another site on behalf of the user.

How does it work?

When a web application makes a request to a resource on a different origin (domain, protocol, or port), the browser checks if the target server allows the request. This is done by the server sending specific HTTP headers in its response. These headers dictate what types of requests are allowed from different origins.

Example :

Imagine you have a web application hosted on `delta.com`, and it needs to make a request to an API hosted on `zoom.delta.com`. By default, the browser will block this request due to the Same-Origin Policy. However, if the API server includes the appropriate CORS headers in its response, such as `Access-Control-Allow-Origin: delta.com`, the browser will allow the request to proceed.

Important CORS Headers

1. **Access-Control-Allow-Origin**: Specifies which origins are allowed to access the resource. It can be a specific origin or a wildcard (`*`), which allows any origin.
2. **Access-Control-Allow-Methods**: Lists the HTTP methods (e.g., GET, POST, PUT, DELETE) that are permitted for cross-origin requests.
3. **Access-Control-Allow-Headers**: Specifies which HTTP headers can be used in the actual request.
4. **Access-Control-Allow-Credentials**: Indicates whether the request can include user credentials (cookies, HTTP authentication, etc.).
5. **Access-Control-Expose-Headers**: Indicates which headers can be exposed to the browser.