### What is CORS?

CORS stands for Cross-Origin Resource Sharing. It allows us to relax the security applied to an API. This is done by bypassing the Access-Control-Allow-Origin headers, which specify which origins can access the API.

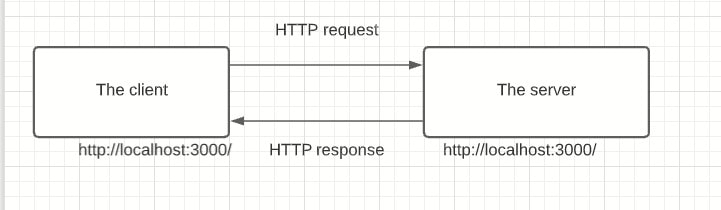
In other words, CORS is a browser security feature that restricts cross-origin HTTP requests with other servers and specifies which domains access your resources.

Check this guide to learn more about the [CORS policy](https://www.section.io/engineering-education/what-is-cors-policy/).

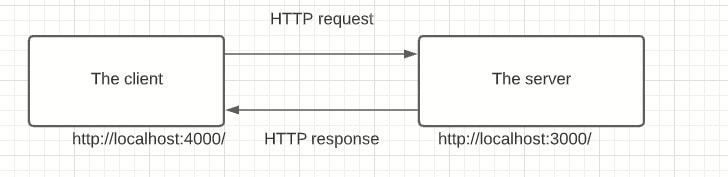
### How CORS works

An API is a set procedure for two programs to communicate. This means that API resources are consumed by other clients and servers.

Here are two scenarios:



The client and the server have the same origin. In this example, accessing resources will be successful. You’re trying to access resources on your server, and the same server handles the request.



The client and server have a different origin from each other, i.e., accessing resources from a different server. In this case, trying to make a request to a resource on the other server will fail.

This is a security concern for the browser. CORS comes into play to disable this mechanism and allow access to these resources. CORS will add a response header access-control-allow-origins and specify which origins are permitted. CORS ensures that we are sending the right headers.

Therefore, a public server handling a public API will add a CORS related header to the response. The browser on the client machine will look at this header and decide whether it is safe to deliver that response to the client or not.