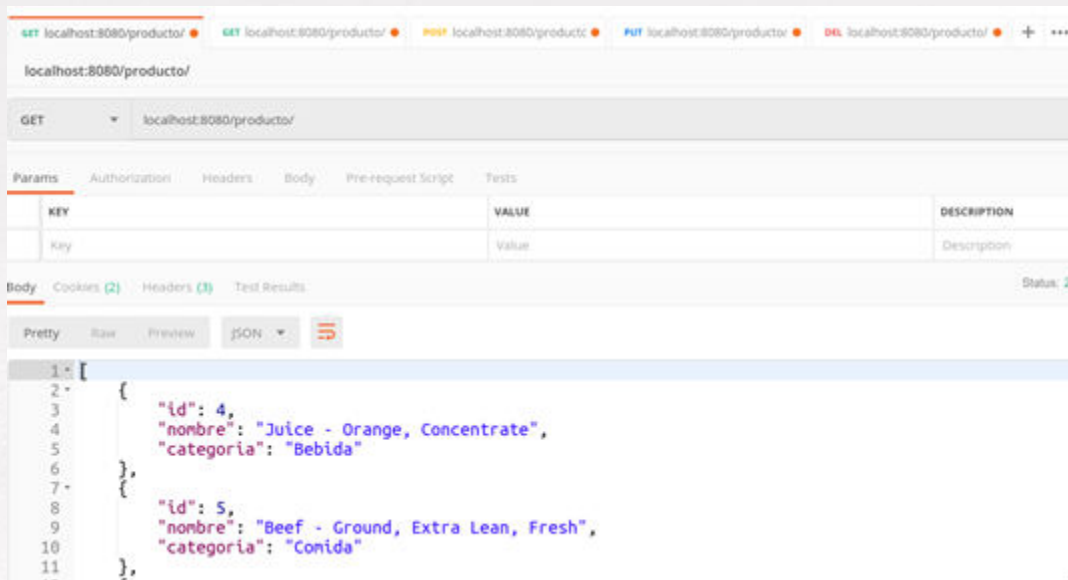


¿Qué es CORS y por qué me va a dar problemas?

Desarrollo de un API REST con Spring Boot

Hasta ahora

- Hemos probado nuestra API con Postman o curl y no hemos tenido ningún problema en consumir/producir datos.



Sin embargo...

- Si queremos consumir de nuestra API desde una aplicación angular, vue, jQuery o un objeto XHR... la respuesta que da el navegador es:

Listado de productos

Id	Nombre	Categoria
----	--------	-----------

Access to XMLHttpRequest at 'http://localhost:8080/producto/' from origin 'null' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.

¿Qué hemos hecho mal?



Por seguridad...

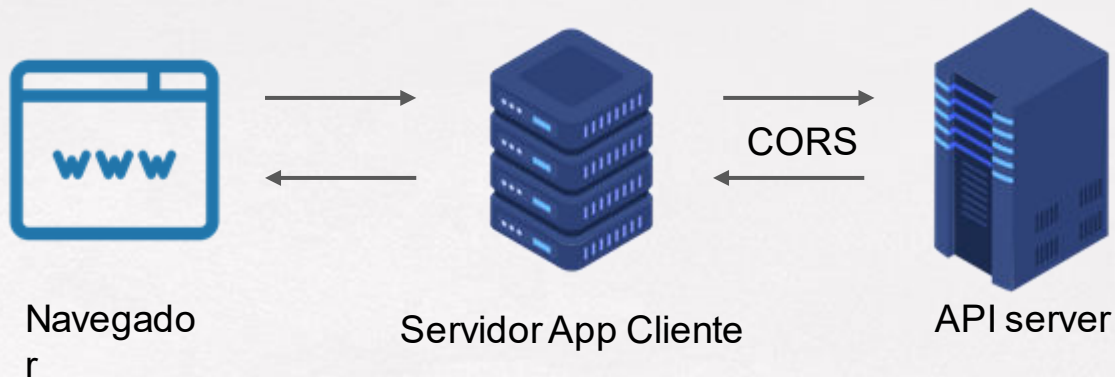
- Por razones de seguridad, los navegadores prohíben las llamadas AJAX a recursos que residen fuera del origen actual.
- Por ejemplo, mientras revisas tu cuenta bancaria en una pestaña, podrías tener el sitio web *evil.com* en otra pestaña. Los scripts de *evil.com* no deberían poder realizar solicitudes AJAX a la API de tu banco (¡retirar dinero de tu cuenta!) utilizando sus credenciales.
- CORS es una especificación del W3C implementada por casi todos los navegadores que permite especificar qué dominios estarán autorizados para qué.

¿Qué es CORS?

- Es una política de seguridad.
- ¿Y qué es una política de seguridad?
 - Es lo que significa *ser seguro* para una entidad.
 - Puede implicar una serie de reglas de control de acceso, autenticación, ...

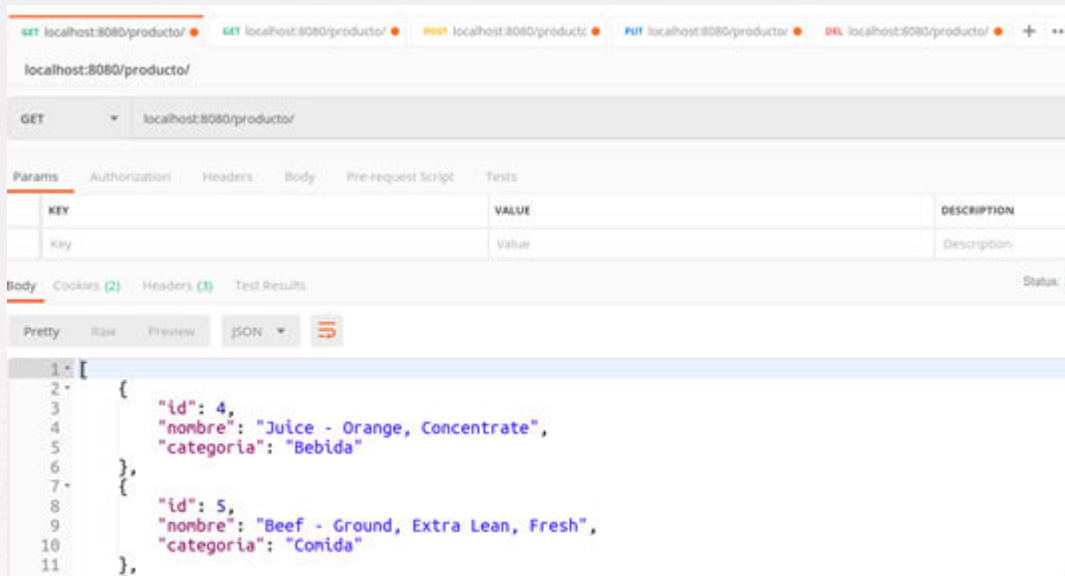
Entonces... ¿qué es CORS?

- Cross-Origin Resource Sharing (CORS)
- Mecanismo que utiliza cabeceras HTTP adicionales para permitir a un cliente (*User-Agent*) acceder a recursos desde un (servidor) origen diferente al sitio (servidor) actual.



¿Cómo es que funciona en POSTMAN?

- Es una herramienta de desarrollo, y no un navegador al uso.



Ventajas del uso de CORS

- Permite indicar quién puede acceder a nuestros recursos
- También permite indicar cómo se puede acceder (métodos HTTP)
 - Puedes habilitar GET...
 - Y deshabilitar PUT, DELETE, ...

¿Qué se puede hacer?

- Cabecera *Access-Control-Allow-Origin*

- Puede indicar un dominio

`Access-Control-Allow-Origin: http://www.example.com`

- O un carácter comodín

`Access-Control-Allow-Origin: *`

- ¡OJO! Usar comodines en casos específicos (por ejemplo, un CDN de jQuery o Bootstrap).

¿Y con Spring?

- Lo aprenderemos en las próximas lecciones