07

Para saber mais: Segurança com CORS e mais

Além dos cabeçalhos que usamos para habilitar o CORS na nossa API, existem outros que você pode conhecer melhor na documentação MDN (https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Controle_Acesso_CORS). Através do CORS conseguimos configurar camadas de segurança para a nossa API, seguindo as boas práticas da web, evitando que pessoas indesejadas usem o navegador para acessar nossa API e nossos dados. Vale ressaltar que conhecemos o cabeçalho Access-Control-Allow-Origin, resposável por indicar ao navegador quem pode ou não acessar a nossa API, onde devemos colocar o domínio (sem barra no final!) do nosso site, mas também aprendemos que é possível passar um asterisco (*) indicando que qualquer pessoa pode acessar a API - apesar de ser possível, não é uma boa prática, já que permitimos que qualquer pessoa acesse a API pelo navegador, o que na maioria das vezes não é o caso, então o ideal é sempre evitar usar o asterisco, e sempre colocar o domínio correto de quem pode acessar nossa API.

Se quiser ler mais sobre o método de requisição OPTIONS, que nos permite conhecer o que é possível fazer com uma determinada rota, trabalhando assim como uma auto documentação da nossa API, há também uma página (https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Methods/OPTIONS) completa com todas as informações sobre.

Para versionar a nossa API, seguimos o padrão de versionamento semântico (https://semver.org/lang/pt-BR/), que nos permite gerenciar e organizar números de versões de uma forma mais simples e intuitiva.