CORS

Computing

Why the browser blocks a request, and what actually fixes it.

A cross-origin request is one to a different scheme, host or port.

1. **The browser checks the origin**
   Different origin means the response must opt in.

2. **Simple requests go straight out**
   GET or POST with basic headers. The response is checked afterwards.

3. **Others get a preflight**
   An OPTIONS request asks whether the real one is allowed.

4. **The server answers with headers**
   Access-Control-Allow-Origin, -Methods, -Headers.

5. **The browser allows or blocks**
   The request may have reached the server either way.

COMMON CAUSES

Missing Access-Control-Allow-Origin
Credentials with a wildcard origin — not allowed
A custom header not listed in Allow-Headers

A blocked response often still executed on the server. CORS protects the reader, not the server.