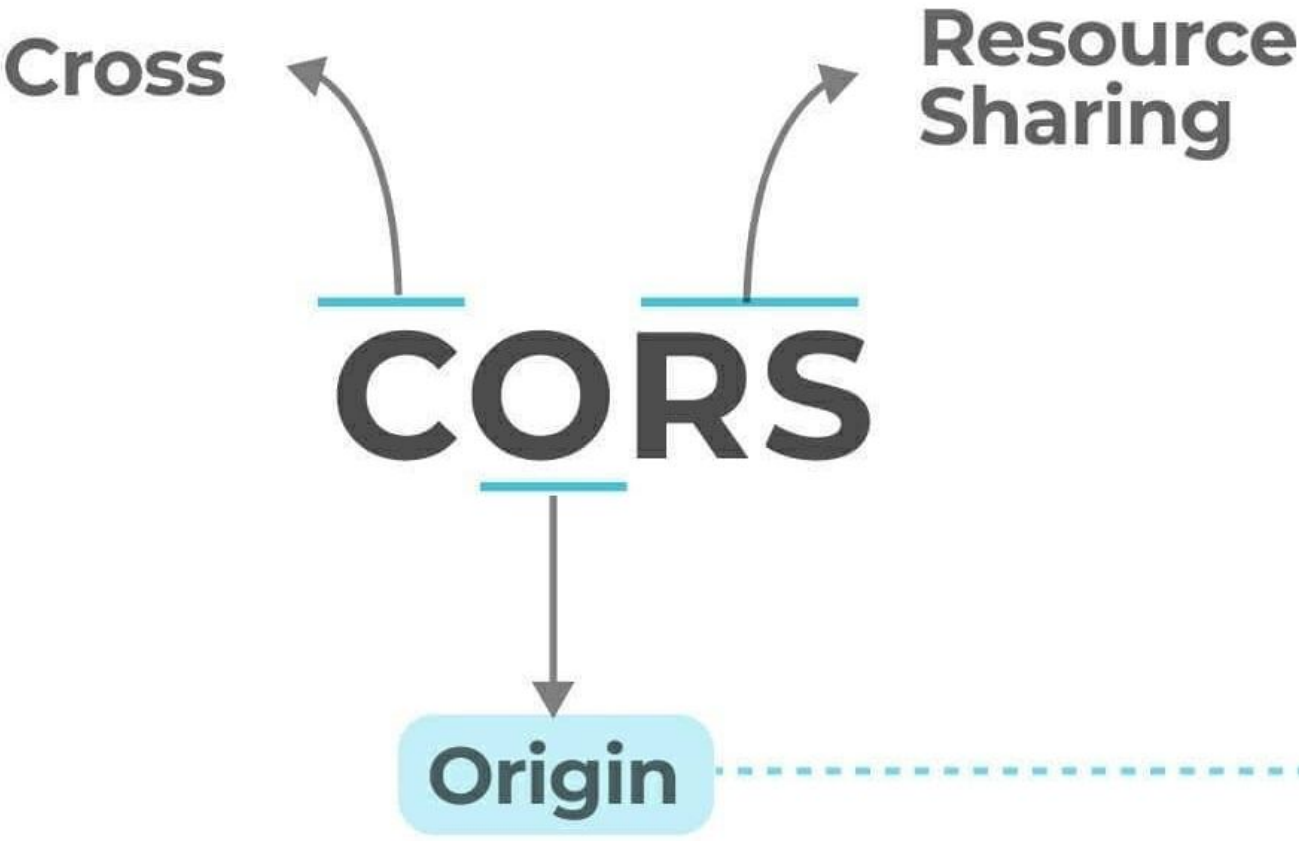
What is CORS?

Oh no!

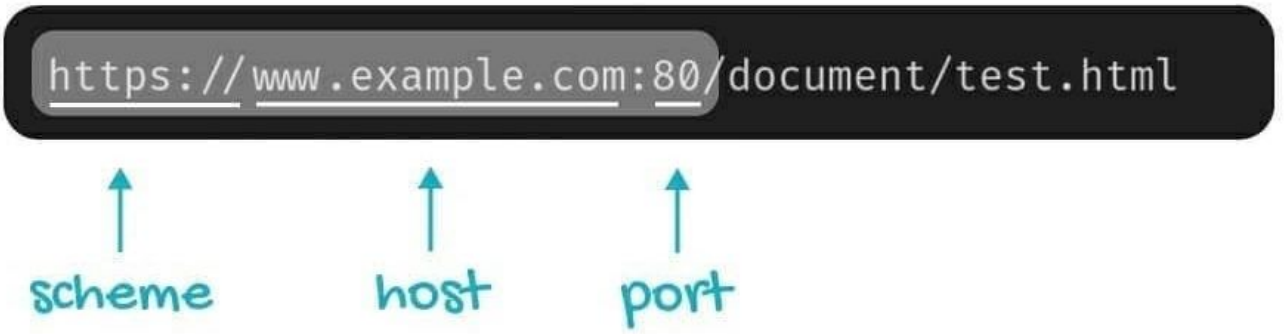
Have you ever run into this type of error before?

This is due to a security mechanism implemented by browsers called **CORS.**


Cross
Resource
Sharing
CORS
Origin

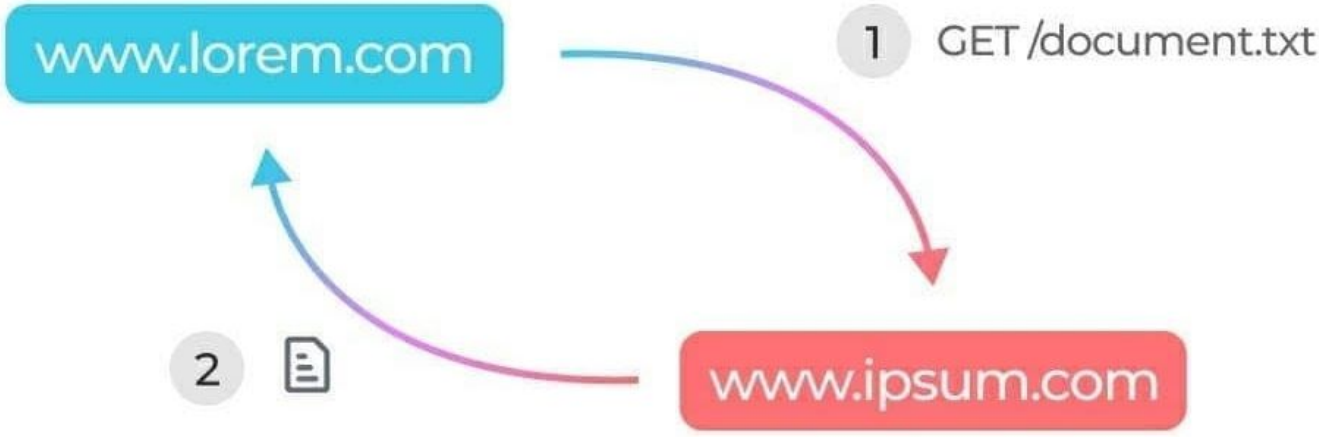
Origin

This part of a URL is called an origin



⚠ (when port is not provided, default is 80 for http and 443 for https)

A **Cross Origin Request** is when a website belonging to one origin requests a resource from another origin



ⓘ This request can be through XHR or Fetch API (also known as AJAX)


www.ipsum.com
CORS allows a **resource owner** to specify some policies as to whether the **requester** can access the **requested resource**
www.lorem.com
document.txt

This is done by using some special HTTP headers called

CORS Headers

The browser will allow lorem.com to access document.txt only if ipsum.com has added either of these two headers in it's response

The first one is to allow only a particular origin. The second is general and allows any origin to access.

Types

There are two types of Cross Origin Requests

- Simple requests
- Pre-flighted requests

Simple Requests

Are those that are considered not to have any side effects in the backend.

- 👉 Modifying any state in the back end is a side effect - such as adding a row in a DB, removing a record, etc

- 👉 Reading for eg, does not cause side effects

Simple requests meet some conditions such as:

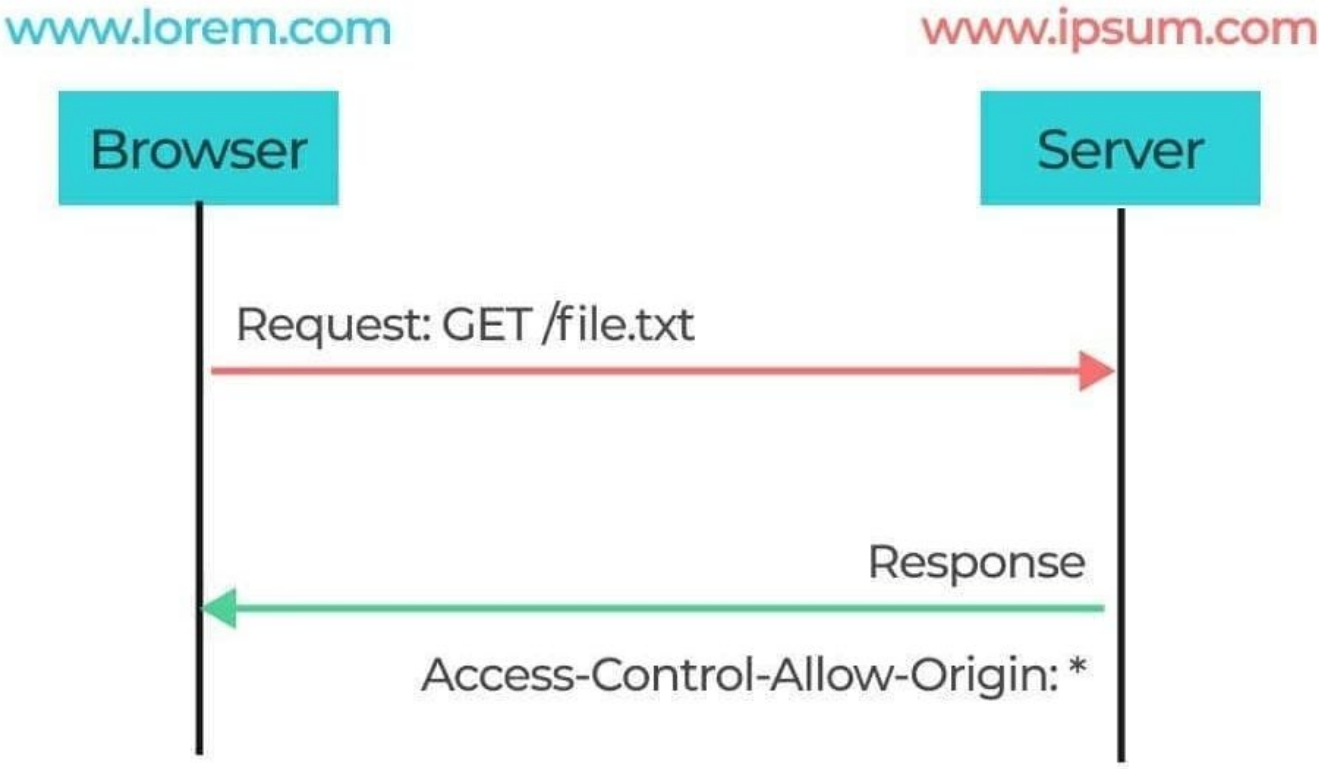
👉 Should be **GET**, **HEAD** or **POST** request

👉 Can use only a selected set of headers

👉 And a bunch more finer requirements

(you can refer to the full set of conditions in the official MDN docs on CORS)

For simple requests, the browser checks whether the CORS Headers are present in the response, to allow access to the requested resource

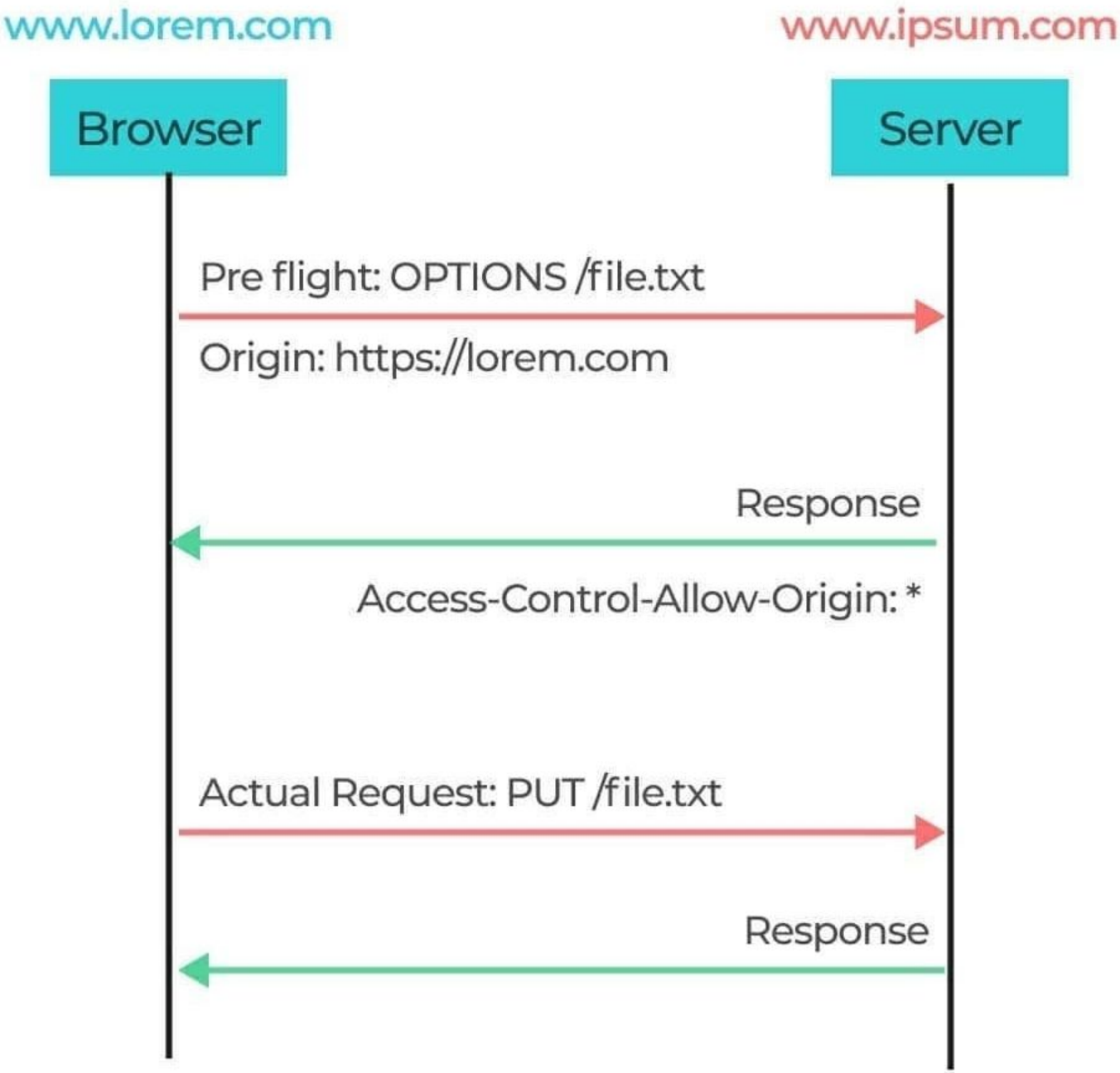


Pre-flighted Requests

For other types of requests that may have side effects, the browser sends two requests

👉 A request with OPTIONS method to check whether the resource can be accessed (called a pre-flight request)

👉 If the servers says that it is ok, the browser will send the actual request


www.lorem.com
www.ipsum.com
Browser
Server
Pre flight: OPTIONS /file.txt
Origin: https://lorem.com
Response
Access-Control-Allow-Origin: *
Actual Request: PUT /file.txt
Response

The pre-flight request contains information about the actual request that is about to be sent, such as path, request method, headers etc so that the server can decide whether or not to allow it.