Conquering CORS

Taming Cross-Origin Resource Sharing

Anton Nazarov

CORS in a Life of Developer

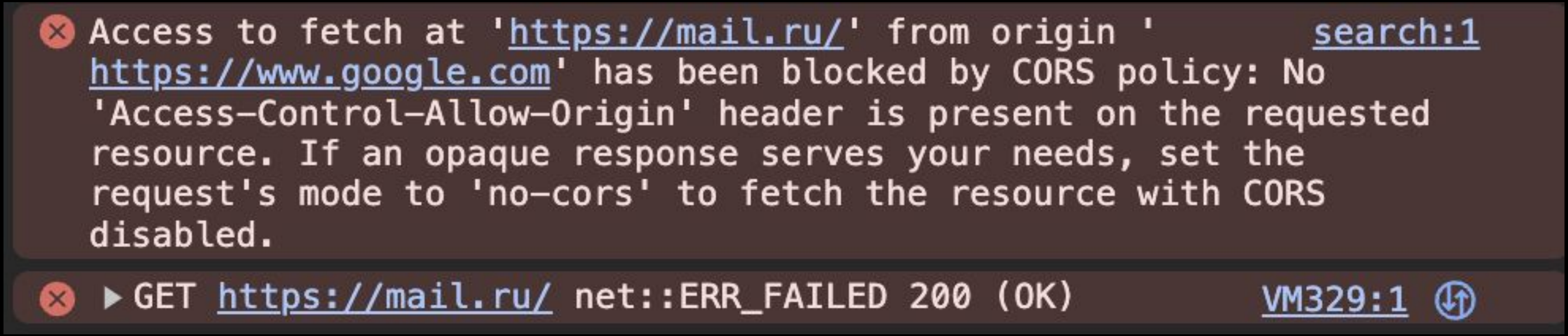
- What is CORS in general
- What is HTTP Request
- What methods we have in HTTP Request
- Methods that CORS use
- Preflight request (options)
- How to find preflight request throw DevTools
- Why browser sends this request
- What is CORS in details
- What is SOP
- What server does with headers
- Where to configure CORS policy on back-end
- What about Curl/Wget
- What about mobile app developers
- What about Selenium
- How to ignore CORS policy

What is a CORS in General?

- A security feature in a browser.
- Allows web servers to specify which origins can access their resources.

CORS in Action

Here is a typical example of how we can observe CORS in action:

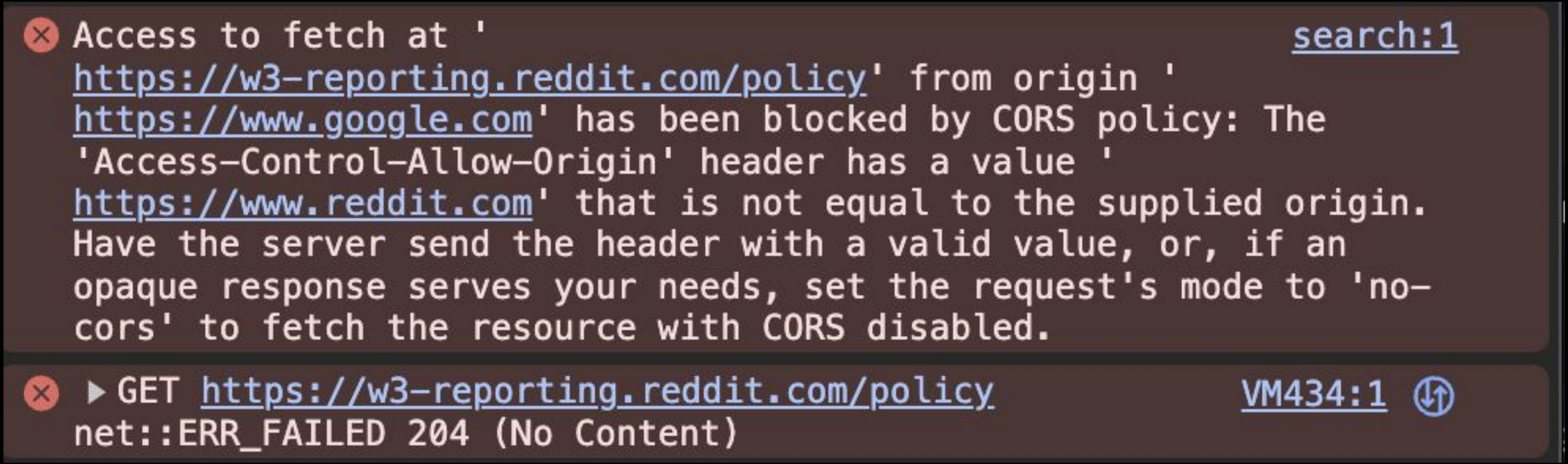


```
Access to fetch at 'https://mail.ru/' from origin '          search:1
https://www.google.com' has been blocked by CORS policy: No
'Access-Control-Allow-Origin' header is present on the requested
resource. If an opaque response serves your needs, set the
request's mode to 'no-cors' to fetch the resource with CORS
disabled.

▶ GET https://mail.ru/ net::ERR_FAILED 200 (OK)          VM329:1
```

CORS in Action

Here is a typical example of how we can observe CORS in action:



```
Access to fetch at '                                                    search:1
https://w3-reporting.reddit.com/policy' from origin '
https://www.google.com' has been blocked by CORS policy: The
'Access-Control-Allow-Origin' header has a value '
https://www.reddit.com' that is not equal to the supplied origin.
Have the server send the header with a valid value, or, if an
opaque response serves your needs, set the request's mode to 'no-
cors' to fetch the resource with CORS disabled.

▶ GET https://w3-reporting.reddit.com/policy                      VM434:1
net::ERR_FAILED 204 (No Content)
```

What is Access-Control-Allow-Origin?

It is an HTTP header that specifies which domains are allowed to access resources on a web server.

It could include:

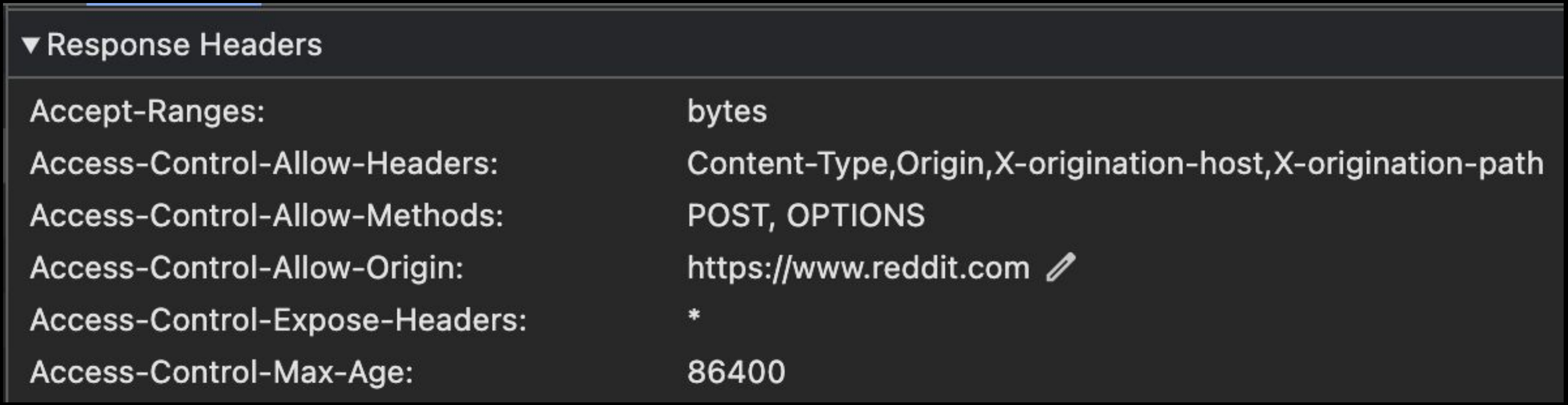
A list of domains for access from specific domains

OR

A wildcard: (*) for access from any domain

How to Find the Access-Control-Allow-Origin header?

It can be found in headers in response from the server.



▼ Response Headers

Accept-Ranges:	bytes
Access-Control-Allow-Headers:	Content-Type,Origin,X-origination-host,X-origination-path
Access-Control-Allow-Methods:	POST, OPTIONS
Access-Control-Allow-Origin:	https://www.reddit.com
Access-Control-Expose-Headers:	*
Access-Control-Max-Age:	86400

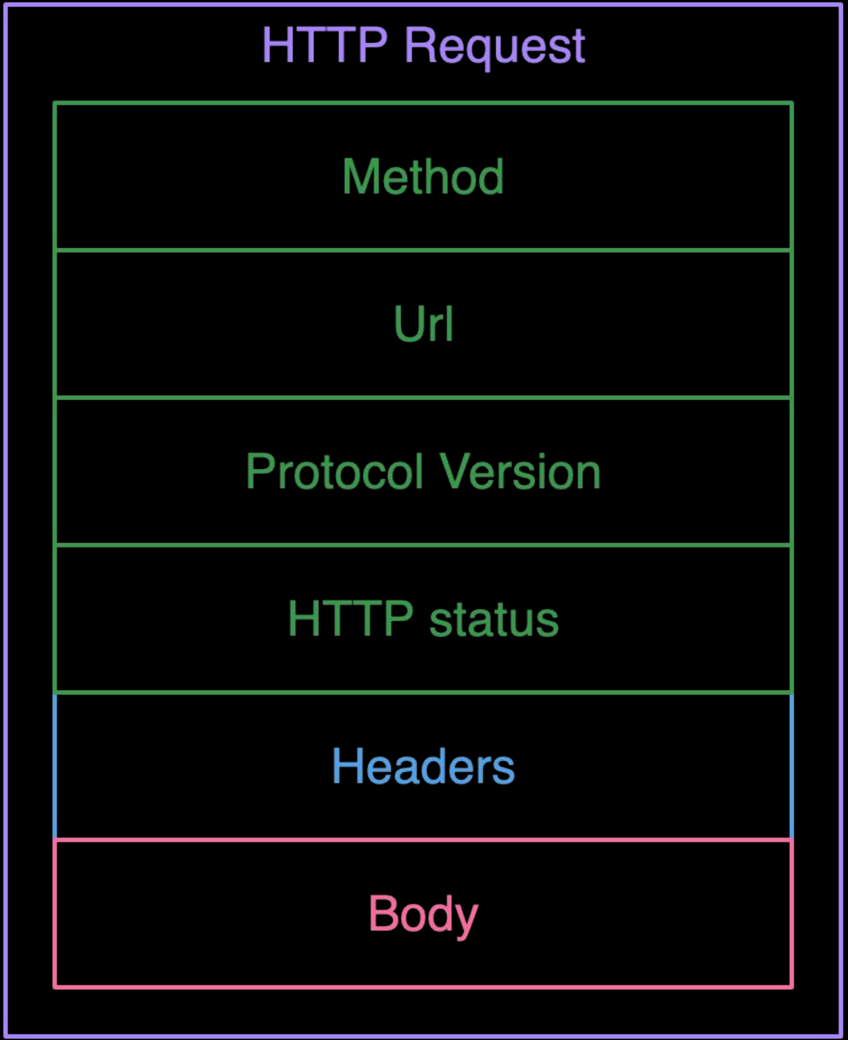
What is a Header?

Header is a part of HTTP-request message

HTTP-request is a message sent by a client (such as a web browser) to a server.

It includes:

- Method
- Url
- Protocol Version
- Http Status
- **Headers**
- Body



Anton Nazarov

How We Can Observer HTTP-request?

Chrome: Press F12 on Windows; ⌘ + Option + I on macOS.

Firefox: Press Ctrl + Shift + I or F12 on Windows, Linux; ⌘ + Option + I on macOS

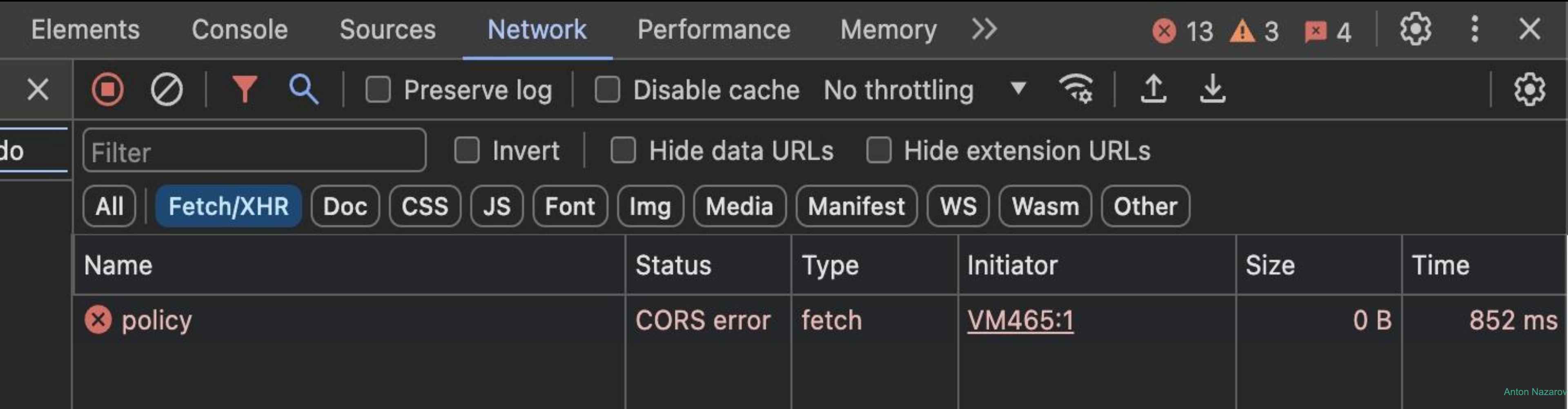
Safari: Open Safari

- Select Safari | Preferences.
- Select Advanced.
- Check the Show Develop menu in menu bar box. The Safari developer tools are now available from the Develop menu in the menu bar.

How We Can Observer HTTP-request?

In all browsers the pathway more or less similar:

- Select the tab Network
- Select the filter Fetch/XHR

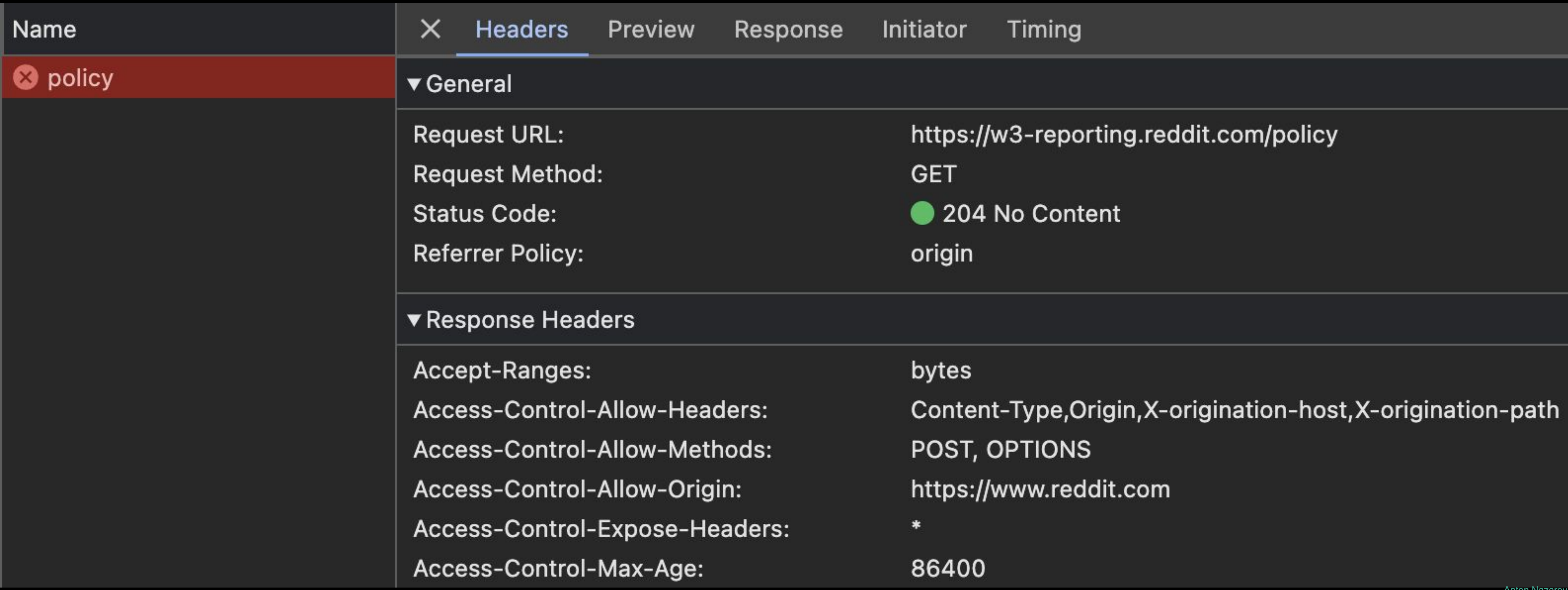


Name	Status	Type	Initiator	Size	Time
policy	CORS error	fetch	VM465:1	0 B	852 ms

Anton Nazarov

How to Find The Response Headers in DevTools?

Click on the request and in headers you find the block Response Headers



▼General

Request URL: https://w3-reporting.reddit.com/policy
Request Method: GET
Status Code: ● 204 No Content
Referrer Policy: origin

▼Response Headers

Accept-Ranges: bytes
Access-Control-Allow-Headers: Content-Type,Origin,X-origination-host,X-origination-path
Access-Control-Allow-Methods: POST, OPTIONS
Access-Control-Allow-Origin: https://www.reddit.com
Access-Control-Expose-Headers: *
Access-Control-Max-Age: 86400

Why Browsers Send Preflight Request?

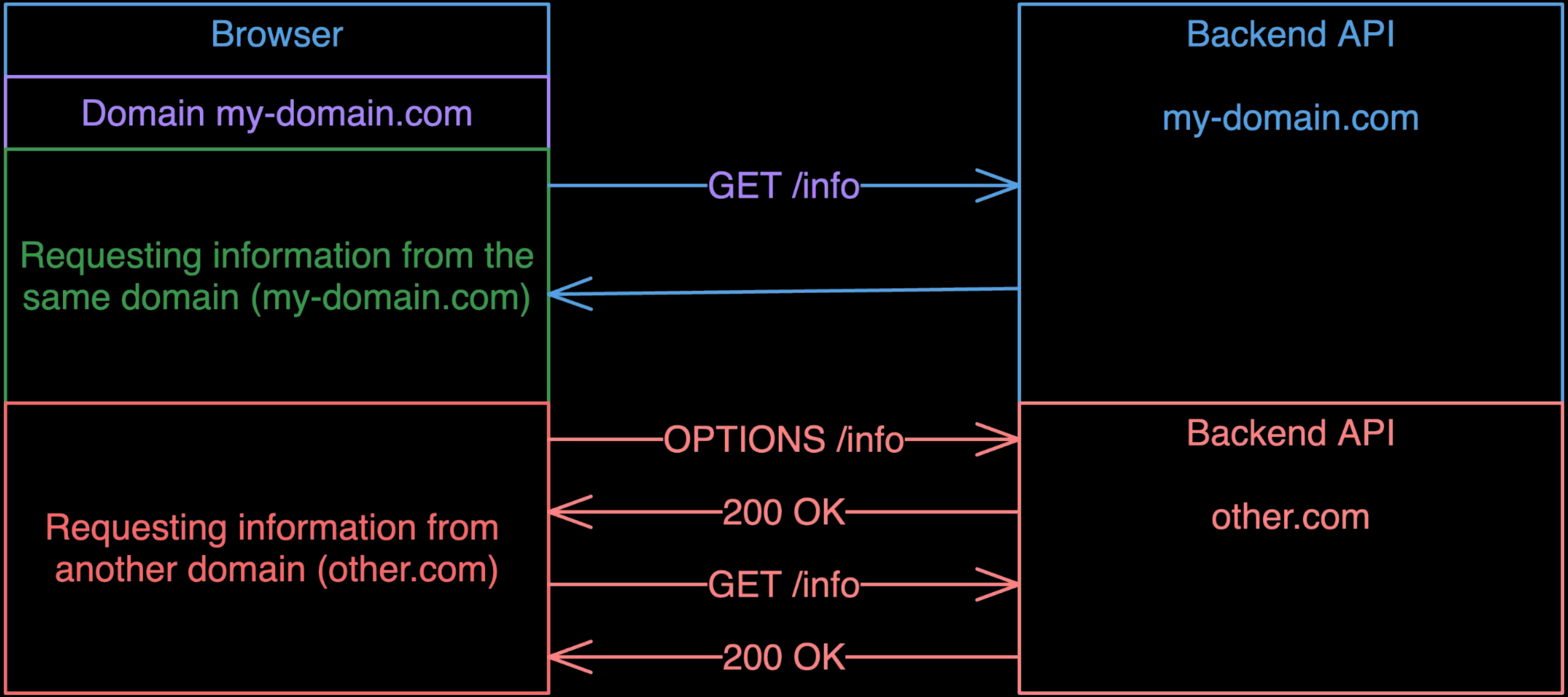
This cross-origin sharing standard can enable cross-origin HTTP requests for:

- fetch() or XMLHttpRequest methods calls.
- Web Fonts (for cross-domain font usage in @font-face within CSS), so that servers can deploy TrueType fonts that can only be loaded cross-origin and used by websites that are permitted to do so.
- WebGL textures.
- Images/video frames drawn to a canvas using drawImage().
- CSS Shapes from images.

Why Browsers Send Preflight Request?

- Preflight request with OPTIONS method (Fetch specs)
- If preflight request get 200 in response then the whole request goes to the server.
- If preflight request do no passes checks requests will be stopped.

What is CORS in a Picture?



Anton Nazarov

CORS Headers

Access-Control-Allow-Origin: Specifies which origins are allowed to access the resource. It can be a specific origin (e.g., `https://example.com`) or "*" to allow any origin.

Access-Control-Allow-Methods: Indicates which HTTP methods (GET, POST, PUT, DELETE, etc.) are permitted when accessing the resource.

Access-Control-Allow-Headers: Specifies which headers can be used in the actual request.

Access-Control-Allow-Credentials: Indicates whether the response to the request can include credentials (such as cookies and authorization headers). This header is set to "true" to allow credentials.

Access-Control-Expose-Headers: Specifies which headers are exposed to the browser in the response. This is used when the client needs to access headers other than the simple response headers.

Access-Control-Max-Age: Specifies how long the results of a preflight request (OPTIONS request) can be cached.

https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS#the_http_response_headers

CORS on Server Side

CORS can be configured

- NGINX / Apache / etc …
- Application level in a code
- In console of AWS/Azure

CURL/WGET

- What if I send a request from the Terminal using curl, wget, or any other tool?
- CORS works only in browsers; no preflight request would be sent.

CORS for Mobile App Developers

In mobile applications, CORS does not apply, despite the presence of Web Views within mobile applications.

- App use native programming languages which rely on own native code.
- WebViews do not achieve cross-platform compatibility to the extent that browsers do.
- No SOP (Same Origin Policy) applicable.

SOP (Same Origin Policy)

The same-origin policy is a vital security measure that limits interactions between a document or script loaded from one origin and resources from a different origin.

https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy

How CORS Could be Ignored by Chrome

To disable CORS it possible to run Chrome with:

- --disable-web-security
- --user-data-dir

These options will disable all CORS-related checks in a browser.

Documentation

https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS

https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy

https://fetch.spec.whatwg.org/#http-cors-protocol

https://www.w3.org/TR/2014/REC-cors-20140116/#terminology - !**old cors specification!**

https://docs.aws.amazon.com/AmazonS3/latest/userguide/cors.html

https://docs.aws.amazon.com/AmazonS3/latest/userguide/ManageCorsUsing.html

https://learn.microsoft.com/en-us/rest/api/storageservices/cross-origin-resource-sharing--cors--support-for-the-azure-storage-services

https://learn.microsoft.com/en-us/azure/container-apps/cors?tabs=arm&pivots=azure-portal

Useful Links

https://enable-cors.org/server.html

https://css-tricks.com/dont-snore-on-cors/

https://www.browserstack.com/docs/automate/selenium/disable-cors-restriction#BrowserStack_SDK

Thank you

Tony Nazarov

LinkedIn:
https://linkedin.com/in/tonynazarov

Email:
tonynazarov.nz@gmail.com

Presentations:
https://linktr.ee/tonynazarov.nz

SCAN ME

My Contacts: