Alpha Anywhere Q&A

MAY 11, 2022

Webinar Schedule

May 18 - UX Component Watch Events

May 25 - Panels, Layouts, and Navigation

June 1 - Ship it! Deploying your App on Alpha Cloud

June 8 - Mobile Deployment with Alpha Launch

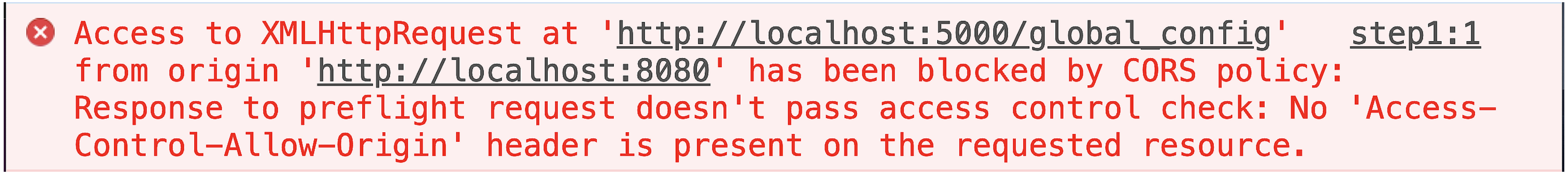
Alpha DevCon 2022

OCTOBER 18 - 22

REGISTER AT www.alphasoftware.com/devcon2022

CORS

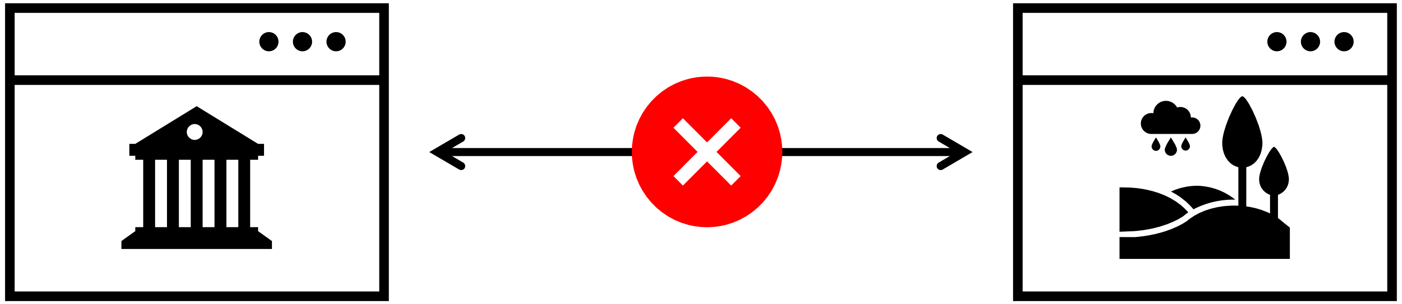
CROSS ORIGIN RESOURCE SHARING



```
Access to XMLHttpRequest at 'http://localhost:5000/global_config'    step1:1
from origin 'http://localhost:8080' has been blocked by CORS policy:
Response to preflight request doesn't pass access control check: No 'Access-
Control-Allow-Origin' header is present on the requested resource.
```

Same-Origin Policy

Rule enforced by web browsers to control access to data between web applications



Same-Origin Policy

Prevents reading data between web applications

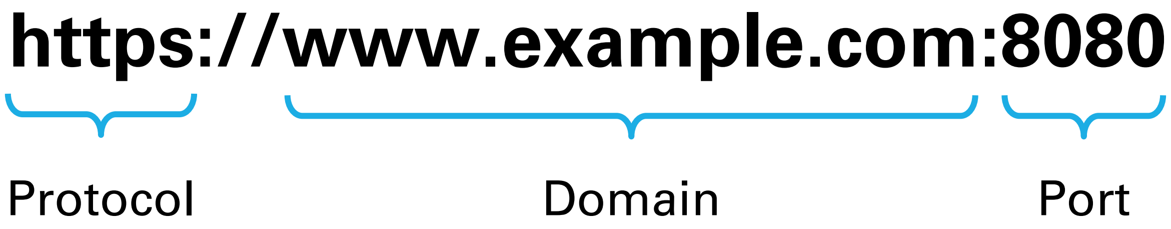
Access to data is based on the origin

If origins do not match, access is denied

What is an Origin

An origin is composed of three parts:

- The Protocol
- The Domain
- The Port



https://www.example.com:8080

Protocol

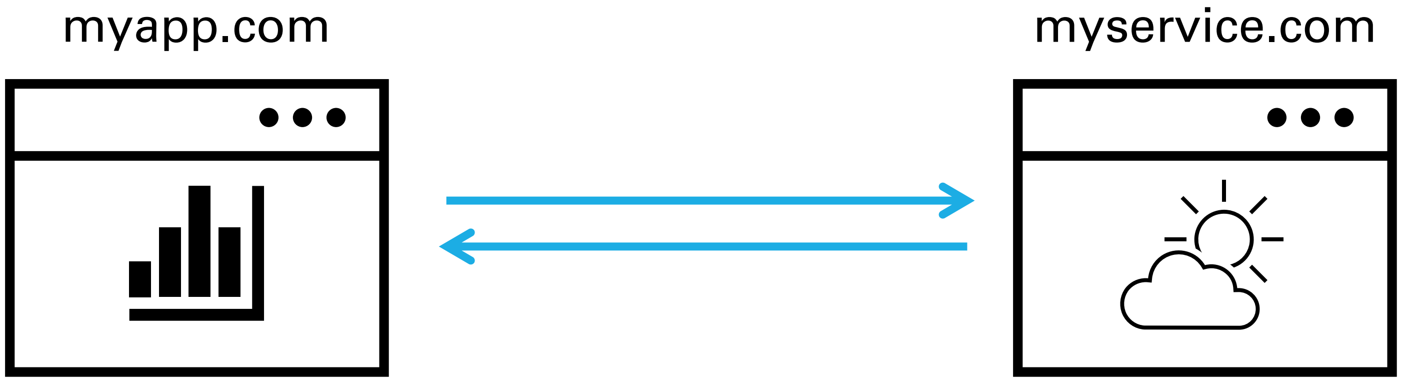
Domain

Port

CORS

Cross Origin Resource Sharing (CORS)

A method using HTTP headers to specify origins that are allowed to access resources



myapp.com

myservice.com

How is CORS Configured?

CORS is configured using HTTP headers:

- Access-Control-Allow-Origin
- Access-Control-Allow-Credentials
- Access-Control-Allow-Methods

Access-Control-Allow-Origin

Defines what origins have permission to access the resource

Specifying origins:

```
Access-Control-Allow-Origin: *

Access-Control-Allow-Origin: <origin>

Access-Control-Allow-Origin: null
```

Access-Control-Allow-Credentials

Allows cookies to be included in cross-origin requests

Can only be used with Access-Control-Allow-Origin: <origin> or Access-Control-Allow-Origin: null

Specifying credentials:

```
Access-Control-Allow-Credentials: true
```

Access-Control-Allow-Methods

Restrict allowed methods

Common methods: POST, GET, PUT, PATCH, DELETE, OPTIONS

Specifying Methods:

```
Access-Control-Allow-Methods: POST, GET, OPTIONS

Access-Control-Allow-Methods: *
```

SameSite Cookies

Controls whether or not a cookie is sent with a request to a third-party site

CORS Misconfiguration

THINGS TO WATCH OUT FOR

Dynamic Access-Control-Allow-Origin

Using code to dynamically populate Access-Control-Allow-Origin

Matching using a Regex

- Starts with "www.mydomain"
- Ends with "mydomain.com"

Access-Control-Allow-Origin: null

Easily Spoofed

```
<iframe sandbox></iframe>
```

Avoid it

Access-Control-Allow-Origin: *
on Internal Networks

JetBrains IDE Remote Code Execution and Local File Disclosure - Jordan Milne

A malicious website could gain access to the JetBrains' IDE and perform remote code execution.

Affected IDEs including PyCharm, Android Studio, WebStorm, IntelliJ IDEA, etc

*Access-Control-Allow-Origin was configured to allow **

CORS Best Practices

Ensure	Ensure Proper Configuration
Use	Use a Whitelist to restrict access to trusted sites
Avoid	Avoid using Access-Control-Allow-Origin: null
Avoid	Avoid using Access-Control-Allow-Origin: * on Internal Networks

Resources

Cross-Origin Resource Sharing (CORS) | Complete Guide

Rana Khalil

https://www.youtube.com/watch?v=t5FBwq-kudw

Live Demo

CONFIGURING CORS FOR A WEB SERVICE IN ALPHA ANYWHERE

Questions?

guides@alphasoftware.com