



Cross-Origin Isolation and you

Frederik Braun



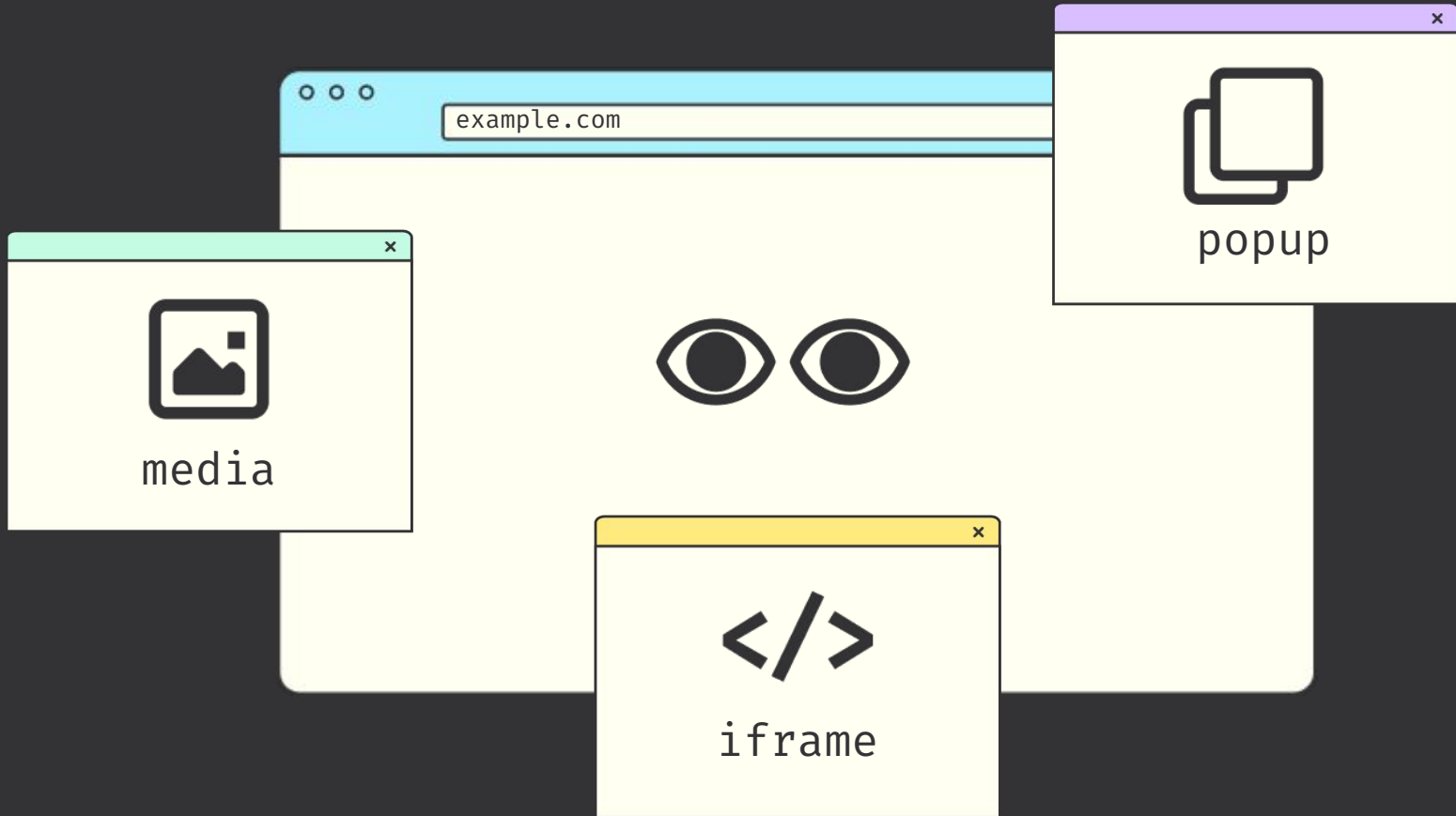
Getting to use SharedArrayBuffer

Frederik Braun

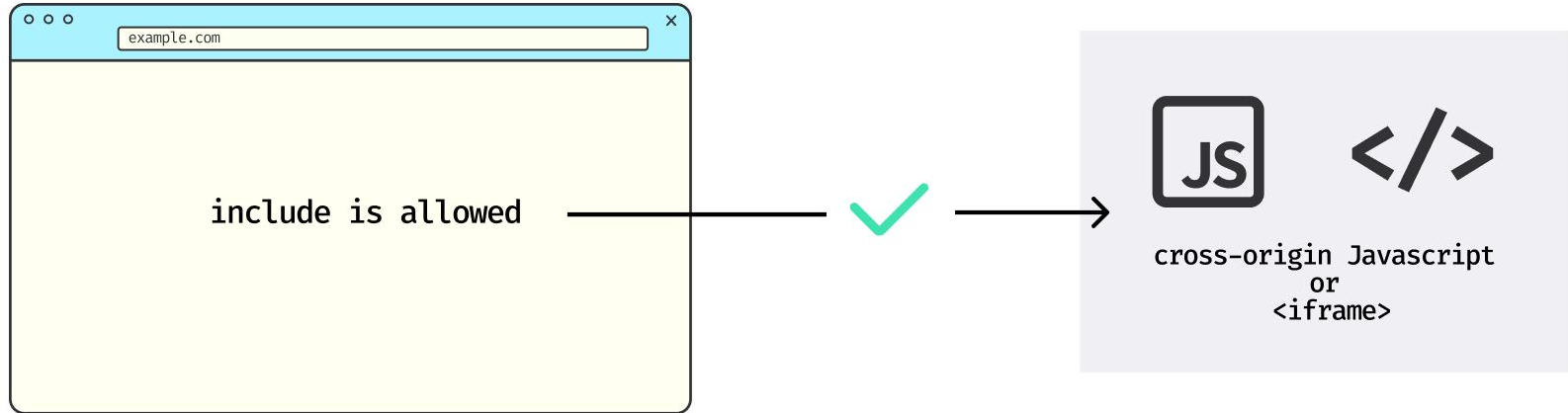


COOP & COEP & CORP & You

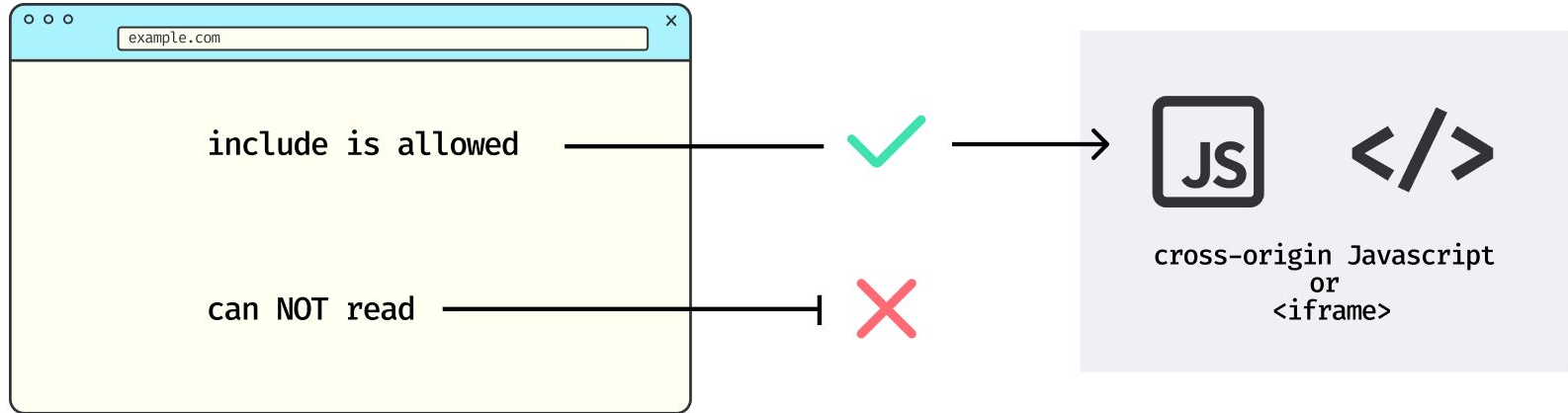
Frederik Braun



Same-Origin Policy



Same-Origin Policy



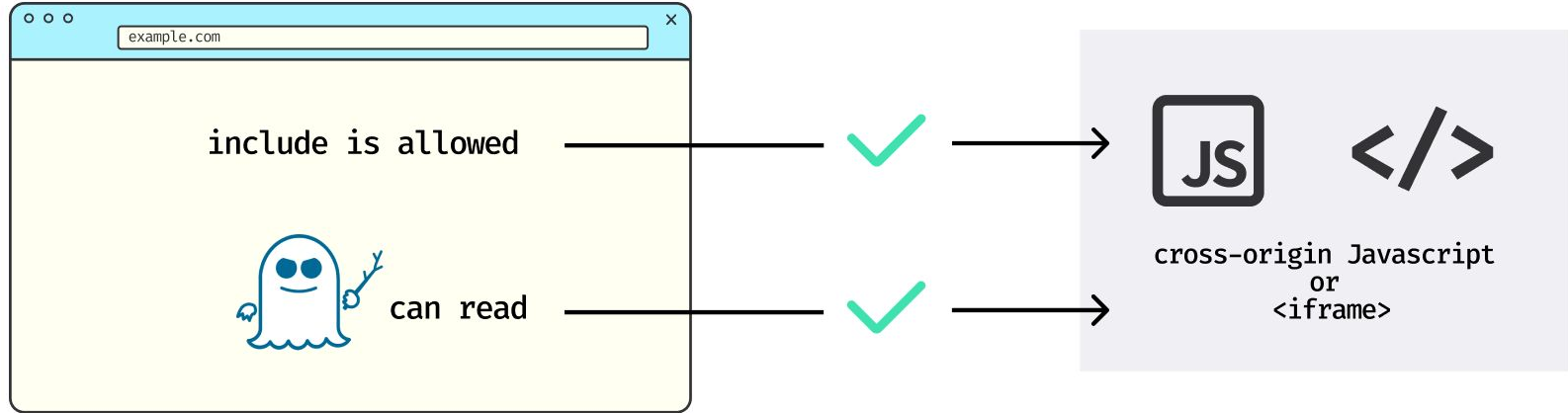
Spectre & Meltdown



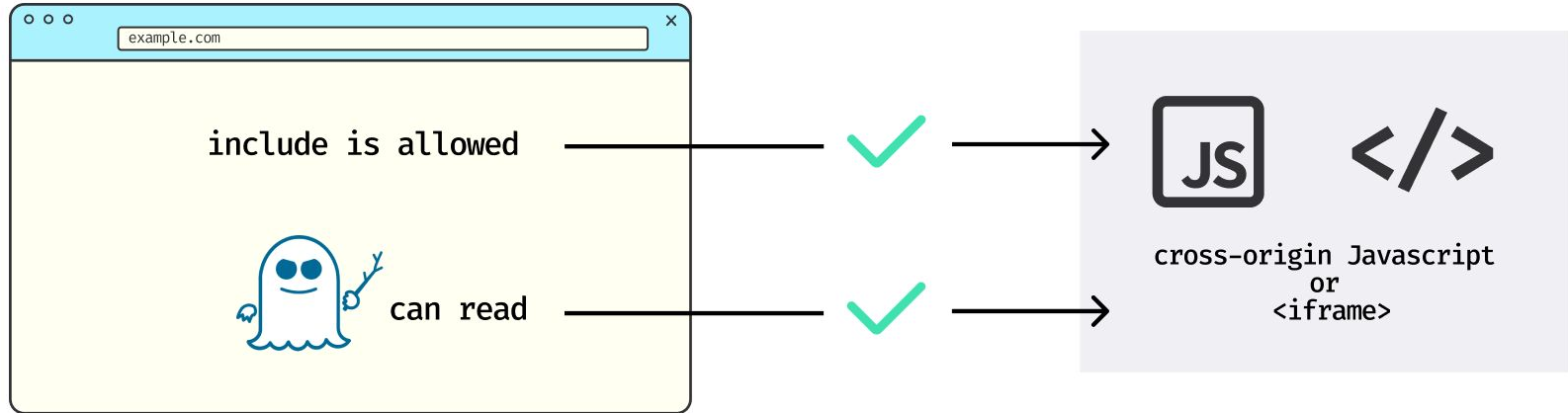
**Spectre & Meltdown
broke the web
security model.**



Spectre breaks the Same-Origin Policy



Spectre breaks the Same-Origin Policy



Using

`performance.now()` or

`SharedArrayBuffer()`



**A new Security
model for the web**

Browser Changes

Browser Changes

Mitigations (temporary)

Disabled dangerous APIs (e.g.,
`performance.now()` and
`SharedArrayBuffer`)

Site Isolation

Different process per site

Opaque Response Blocking (ORB)

Move the network stack to a
separate process



Cross-Origin Isolation



Cross-Origin Isolation

**Prevent your website
from being opened**

Cross-Origin-Opener-Policy

**Restrict your website
from using cross-origin
content**

Cross-Origin-Embedder-Policy

**CDNs can declare
resources to be
readable across origins**

Cross-Origin-Resource-Policy



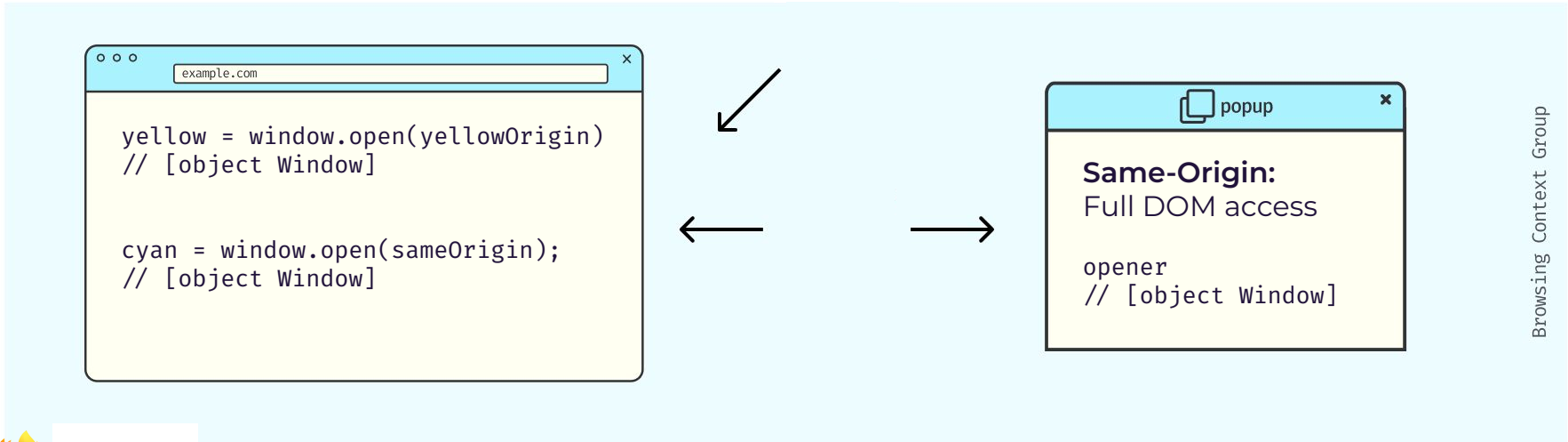
**Plugging window
handle leaks.**



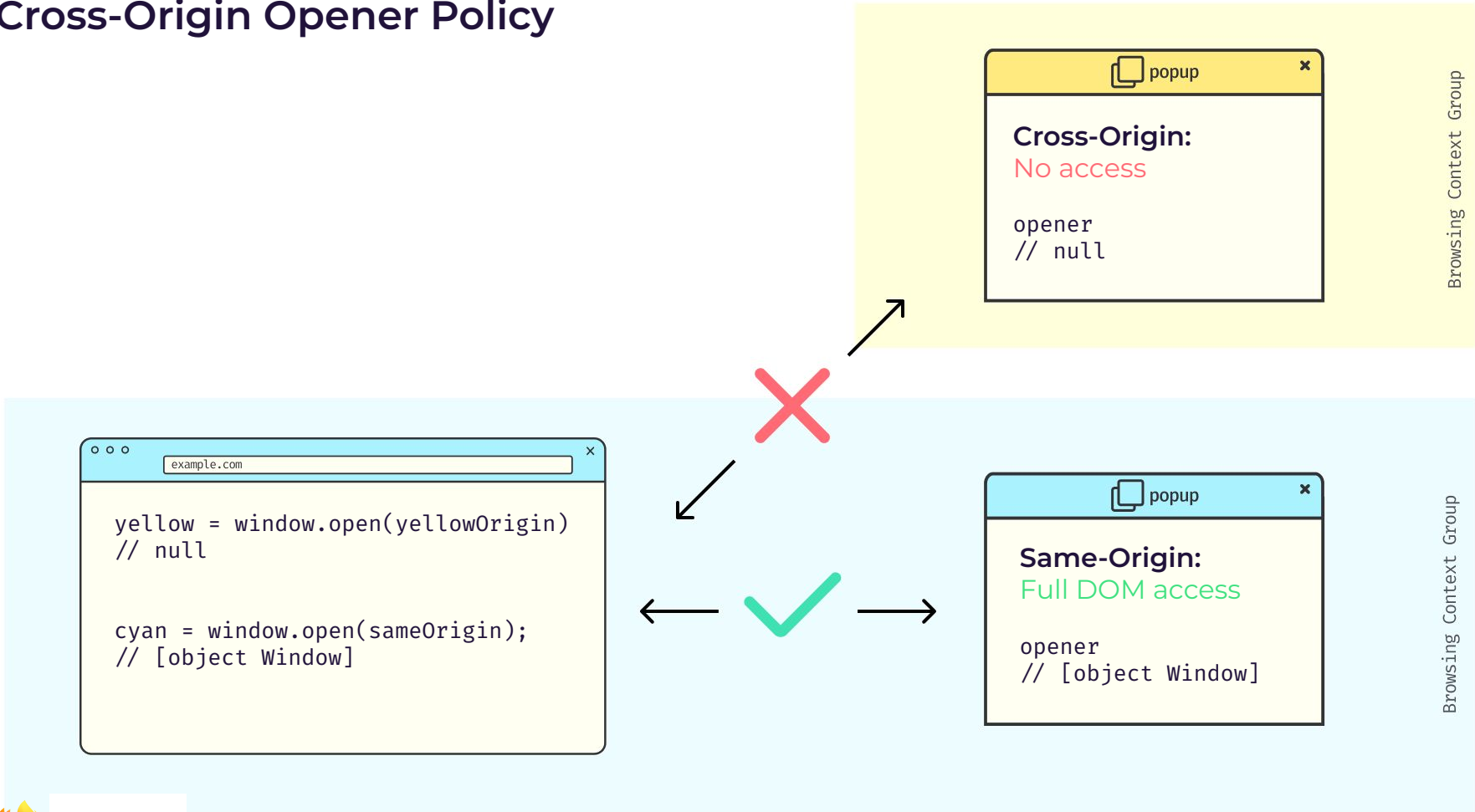
**Plugging window
handle leaks with
COOP.**



Recap: Window Handles

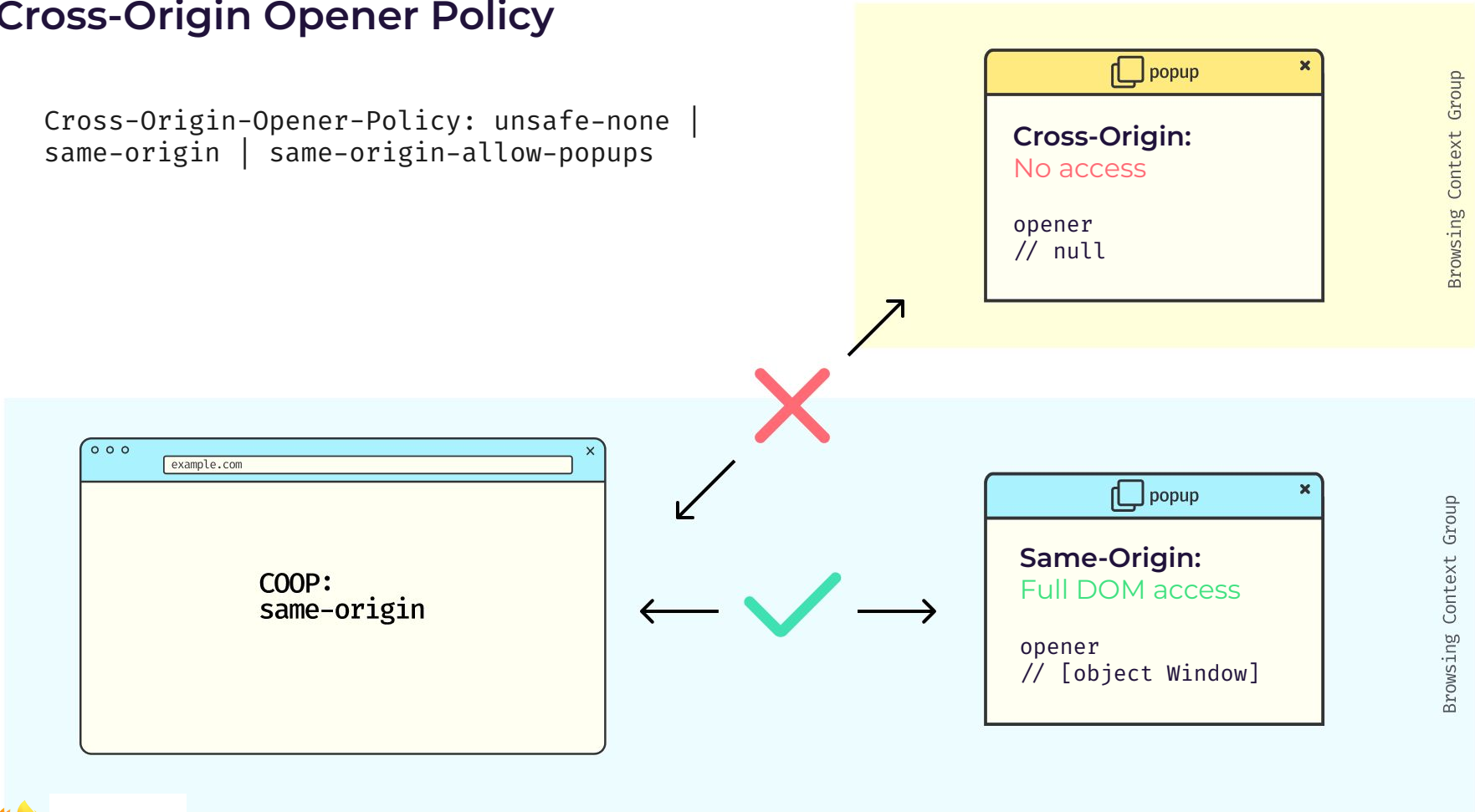


Cross-Origin Opener Policy



Cross-Origin Opener Policy

Cross-Origin-Opener-Policy: unsafe-none | same-origin | same-origin-allow-popups



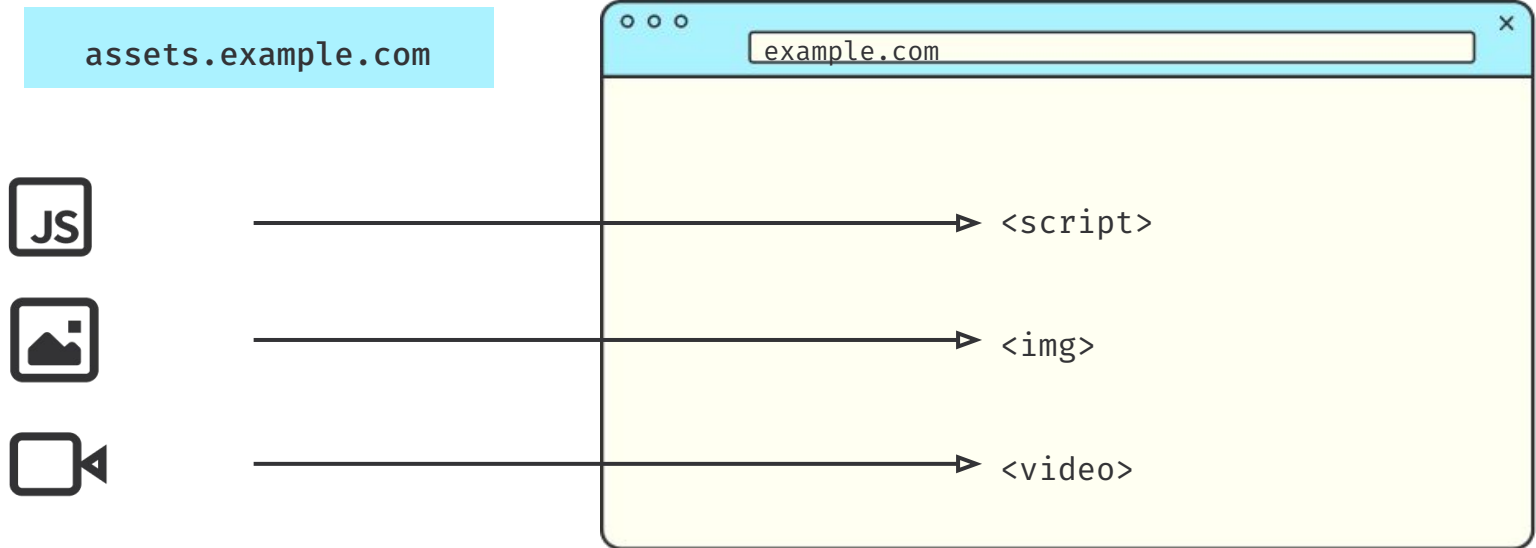
**Embedding only
what's allowed.**



**Embedding only
what's allowed with
COEP & CORP.**

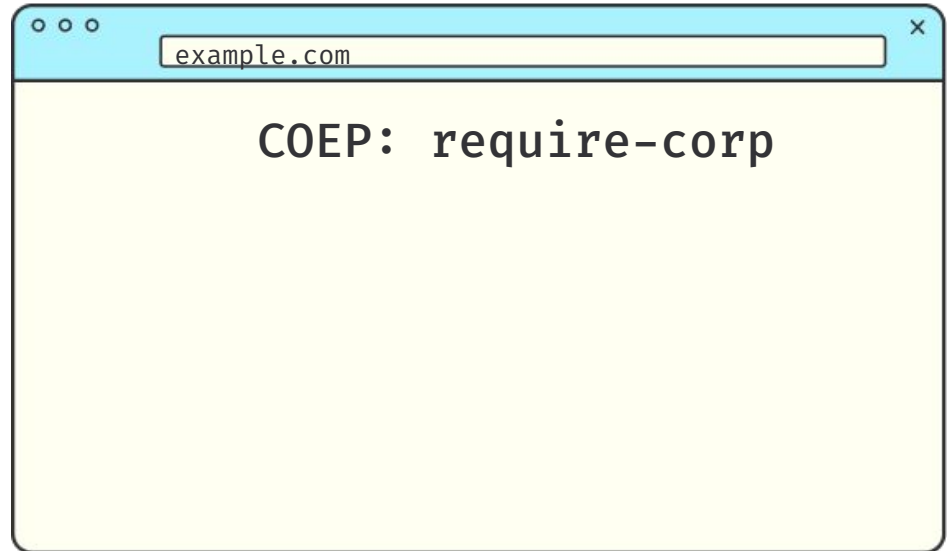


Cross-Origin-Embedder-Policy & Cross-Origin-Resource-Policy



Cross-Origin-Embedder-Policy (COEP)

Cross-Origin-Embedder-Policy: unsafe-none |
require-corp | credentialless



Cross-Origin-Resource-Policy (CORP)

Cross-Origin-Resource-Policy: same-site |
same-origin | cross-origin

assets.example.com



CORP:cross-origin



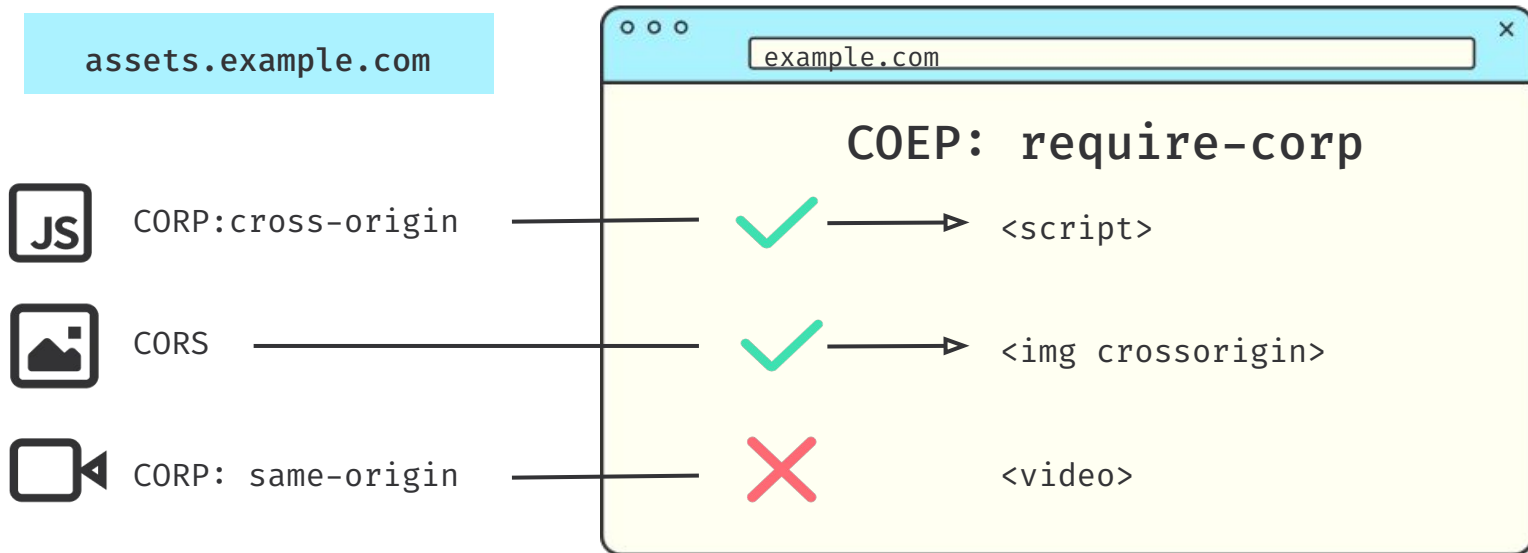
CORS



CORP: same-origin



Again: Cross-Origin-Embedder-Policy & Cross-Origin-Resource-Policy



Cross-Origin Isolation

Prevent websites from being opened

Cross-Origin-Opener-Policy

Restrict website from using cross-origin content

Cross-Origin-Embedder-Policy

Declare a resources to be readable across origins

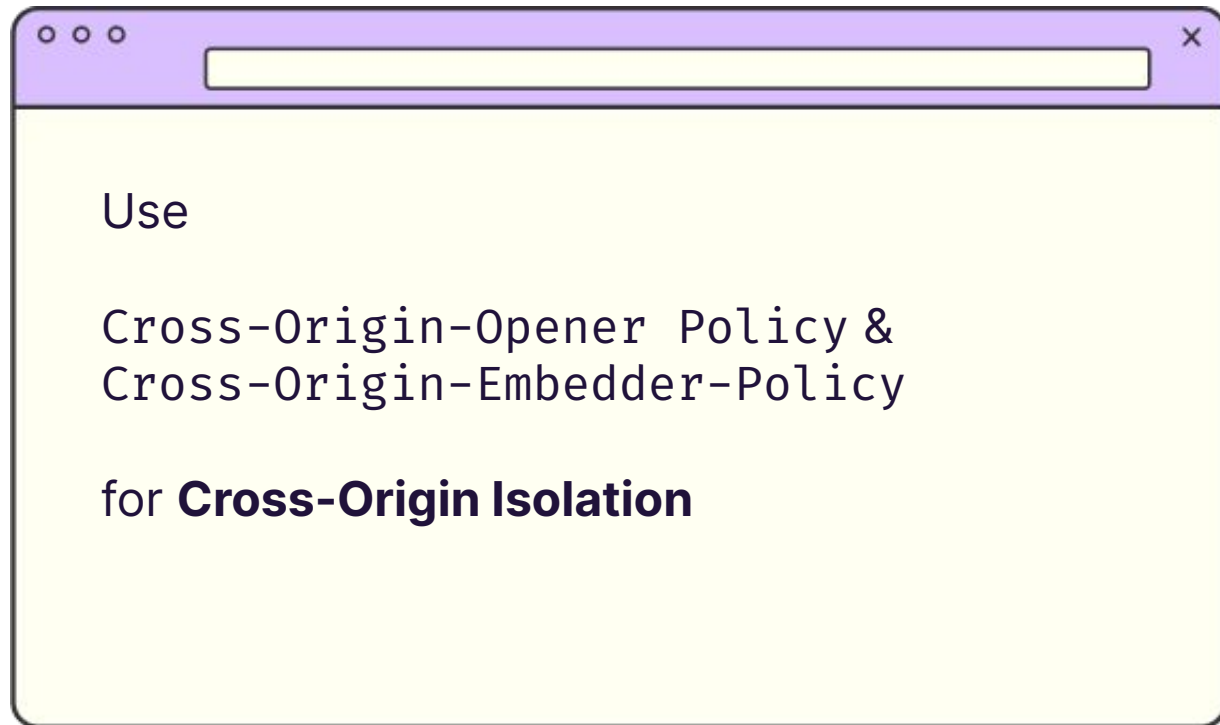
Cross-Origin-Resource-Policy

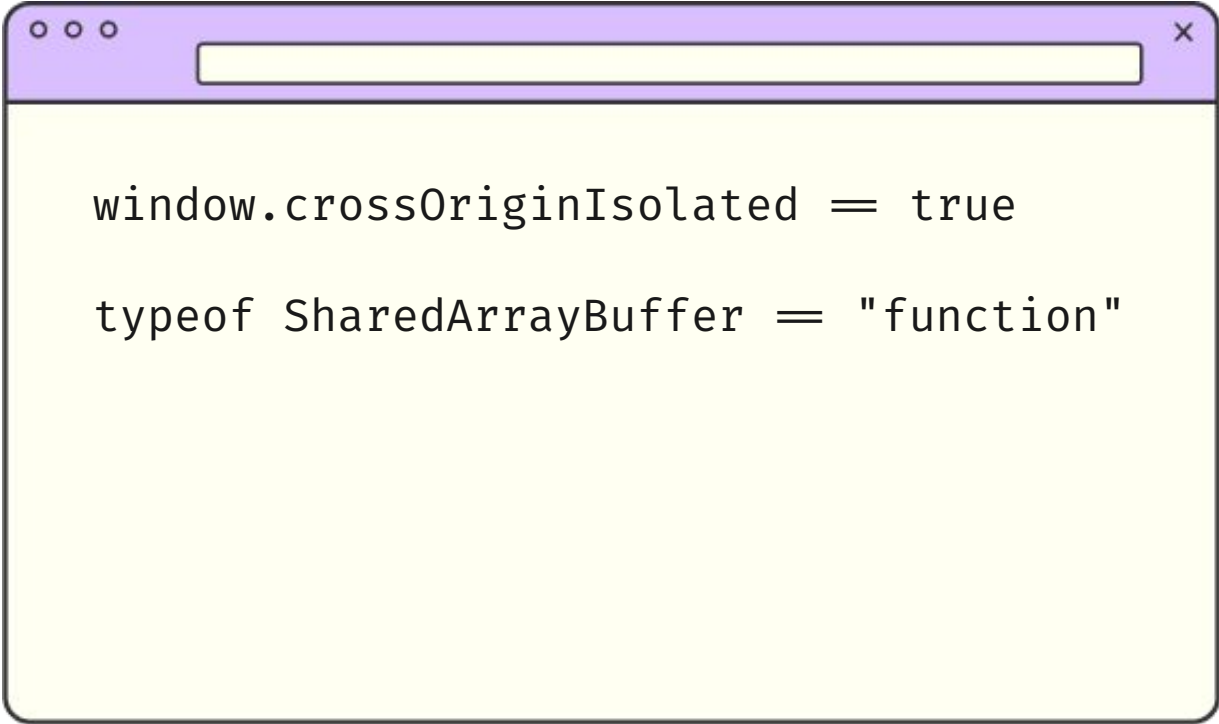


Full isolation with COEP & COOP



In Summary





```
window.crossOriginIsolated = true
```

```
typeof SharedArrayBuffer = "function"
```



Demo

<https://coop.on.web.security.plumbing/>



Credit & Acknowledgements

- Spectre & Meltdown: logos by Natascha Eibl
- Illustrations & color theming by Céline Villaneau



Further reading

- [Mitigations landing for new class of timing attack - Mozilla Security Blog](#)
- [Fantastic Timers and Where to Find Them:](#)
[High-Resolution Microarchitectural Attacks in JavaScript](#)
- [Safely reviving shared memory - Mozilla Hacks](#)
- [Frederik Braun : Neue Methoden für Cross-Origin Isolation: Resource, Opener & Embedding Policies mit COOP, COEP, CORP und CORB \(German\)](#)





Thank you



Frederik Braun

 @freddy@security.plumbing

 freddy@mozilla.com



Slides

