Same Origin

The "same origin" policy in web browsers prevents requests from different origins, protecting users from security threats like CSRF and XSS attacks.

Origin: An origin is defined by a combination of the following three components:

- **Protocol**: This is typically either HTTP or HTTPS.
- **Domain**: The domain is the hostname (e.g., example.com).
- **Port**: The port number, if specified (e.g., :80 or :443). Most web traffic uses the default ports (80 for HTTP and 443 for HTTPS).
-

Same Origin-Two web pages are said to have the same origin if their protocols, domains, and ports all match. For example, "https://example.com" and "https://example.com:8080" have the same origin because they share the same protocol (HTTPS) and domain (example.com).

Cross-Origin: Any request made from a web page to a different origin is considered a cross-origin request.

Iframe

An iframe(in-line)is an HTML element that embeds another document within the current page, enabling direct display of content from a different source.

<iframe src="https://www.example.com"></iframe>

Iframe: wrong document pitfall

The "wrong document" issue is a common issue encountered by web developers when using JavaScript to manipulate or access iframe content in HTML, causing unexpected behavior and errors.

The sandbox

The `sandbox` attribute allows for the exclusion of certain actions inside an `<iframe>` in order to prevent it executing untrusted code. It "sandboxes" the iframe by treating it as coming from another origin and/or applying other limitations.

There's a "default set" of restrictions applied for `<iframe sandbox src="...">`. But it can be relaxed if we provide a space-separated list of restrictions that should not be applied as a value of the attribute, like this: `<iframe sandbox="allow-forms allow-popups">`.

In other words, an empty `"sandbox"` attribute puts the strictest limitations possible, but we can put a space-delimited list of those that we want to lift.

Here's a list of limitations:

`allow-same-origin`

By default `"sandbox"` forces the "different origin" policy for the iframe. In other words, it makes the browser to treat the `iframe` as coming from another origin, even if its `src` points to the same site. With all implied restrictions for scripts. This option removes that feature.

`allow-top-navigation`

Allows the `iframe` to change `parent.location`.

`allow-forms`

Allows to submit forms from `iframe`.

`allow-scripts`

Allows to run scripts from the `iframe`.

`allow-popups`

Allows to `window.open` popups from the `iframe`

See the manual for more.

The example below demonstrates a sandboxed iframe with the default set of restrictions: `<iframe sandbox src="...">`. It has some JavaScript and a form.