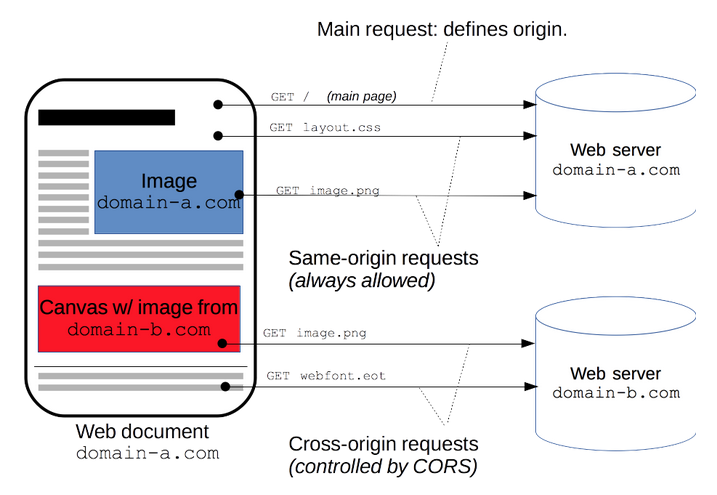
# AUTH AND CORS

* Auth is the abbreviation of authentication and it can be defined as the process or action of verifying the identity of a user or process.
* **Cross-Origin Resource Sharing** ([CORS](https://developer.mozilla.org/en-US/docs/Glossary/CORS)) is a mechanism that uses additional [HTTP](https://developer.mozilla.org/en-US/docs/Glossary/HTTP) headers to tell browsers to give a web application running at one [origin](https://developer.mozilla.org/en-US/docs/Glossary/origin), access to selected resources from a different origin. A web application executes a cross-origin HTTP request when it requests a resource that has a different origin (domain, protocol, or port) from its own.
* For security reasons, browsers restrict cross-origin HTTP requests initiated from scripts. For example, XMLHttpRequest and the [Fetch API](https://developer.mozilla.org/en-US/docs/Web/API/Fetch_API) follow the [same-origin policy](https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy). This means that a web application using those APIs can only request resources from the same origin the application was loaded from unless the response from other origins includes the right CORS headers.
* The CORS mechanism supports secure cross-origin requests and data transfers between browsers and servers. Modern browsers use CORS in APIs such as XMLHttpRequest or [Fetch](https://developer.mozilla.org/en-US/docs/Web/API/Fetch_API) to mitigate the risks of cross-origin HTTP requests.



* The Cross-Origin Resource Sharing standard works by adding new [HTTP headers](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers) that let servers describe which origins are permitted to read that information from a web browser. Additionally, for HTTP request methods that can cause side-effects on server data (in particular, HTTP methods other than [GET](https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/GET), or [POST](https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/POST) with certain [MIME types](https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types)), the specification mandates that browsers "preflight" the request, soliciting supported methods from the server with the HTTP [OPTIONS](https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/OPTIONS) request method, and then, upon "approval" from the server, sending the actual request. Servers can also inform clients whether "credentials" (such as [Cookies](https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies) and [HTTP Authentication](https://developer.mozilla.org/en-US/docs/Web/HTTP/Authentication)) should be sent with requests.