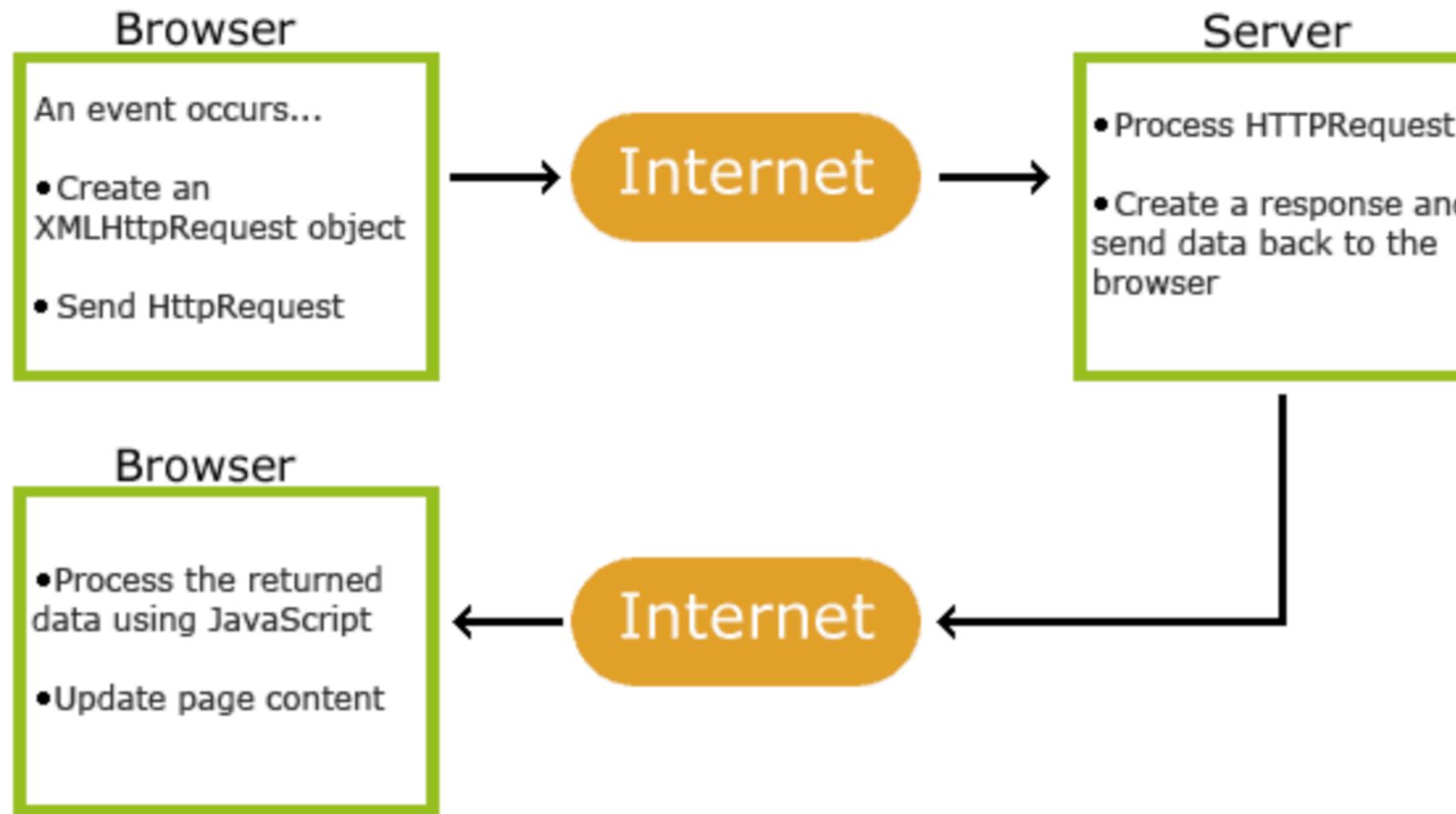




# **CSRF - token bypass**

# How AJAX Works

AJAX



ASYNCHRONISME <---> REACTIVITE

**AJAX** = Asynchronous JavaScript And XML.

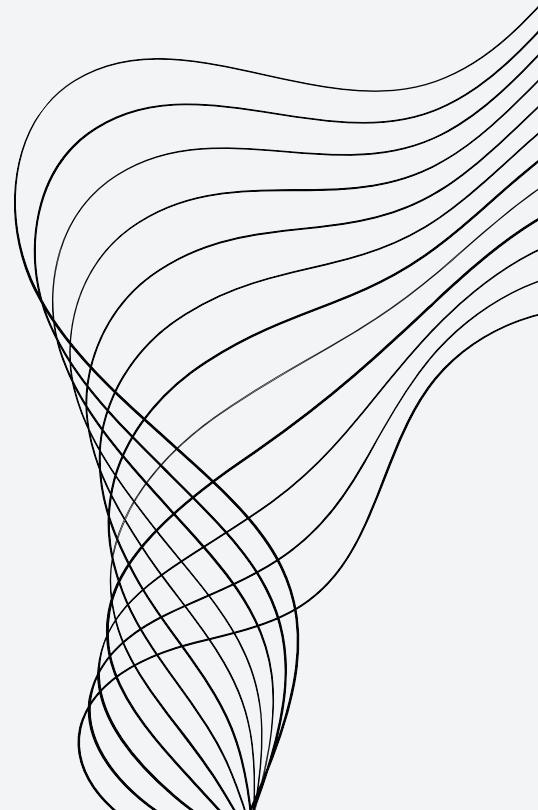
AJAX is not a programming language.

AJAX just uses a combination of:

- A browser built-in XMLHttpRequest object (to request data from a web server)
- JavaScript and HTML DOM (to display or use the data)

# XHR

XMLHttpRequest (**XHR**) objects are used to interact with servers. You can retrieve data from a URL without having to do a full page refresh. This enables a Web page to update just part of a page without disrupting what the user is doing. XMLHttpRequest is used heavily in AJAX programming.

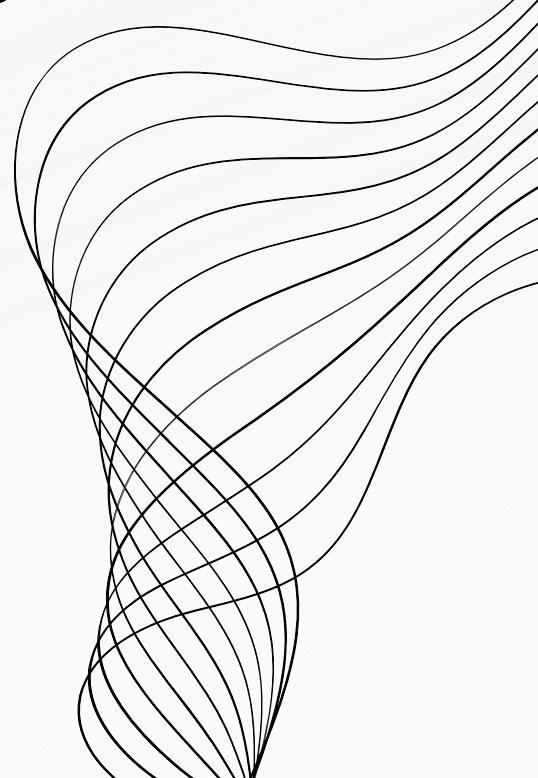


# SAME ORIGIN POLICY

En informatique, la **SOP** est un concept important dans le modèle de sécurité des applications Web. Selon cette politique, un navigateur Web autorise les scripts contenus dans une première page Web à accéder aux données d'une deuxième page Web, mais uniquement si les deux pages Web ont la même origine.



# CORS



[Cross-origin resource sharing](#) is a mechanism that allows restricted resources on a web page to be accessed from another domain outside the domain from which the first resource was served. A web page may freely embed cross-origin images, stylesheets, scripts, iframes, and videos.

**CORS est une technologie qui permet de créer des exceptions à la SOP**



**MERCI**