Same-Origin Policy

- Same-Origin Policy (SOP) restricts how resources loaded from a domain may interact with resources from another domain

- **Domain:** (Scheme, host, port) tuple

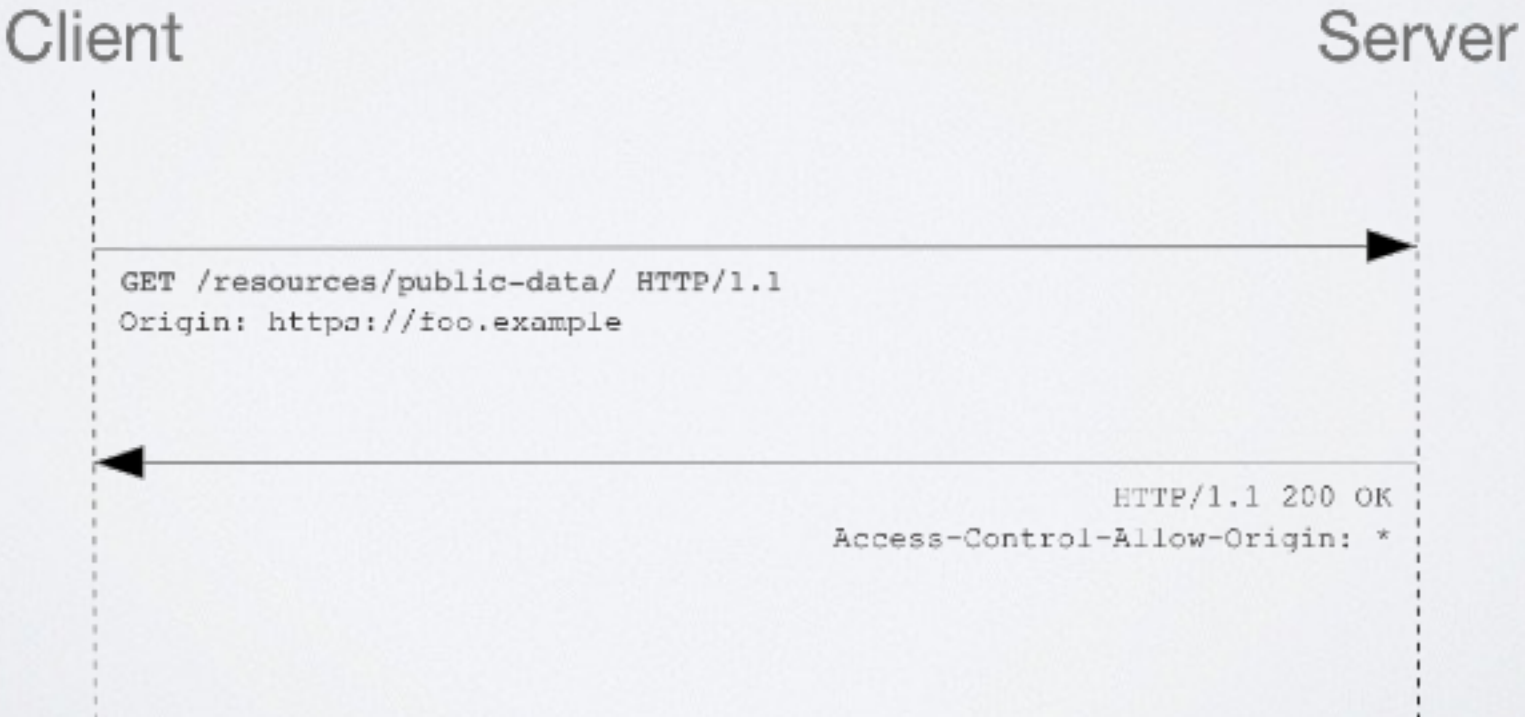
- http://utsc.utoronto.ca:80 =/= https://utsc.utoronto.ca:443

- E.g Malicious JS in one domain cannot access resources of other sites the user is visiting

Same-Origin Policy - CORS

- Very strict - often relaxed with Cross Origin Resource Sharing (CORS)

- Additional HTTP headers that specify permitted/trusted origins and access control e.g **Access-Control-Allow-Origin**



Client

Server

```
GET /resources/public-data/ HTTP/1.1
Origin: https://foo.example
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
```

https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS