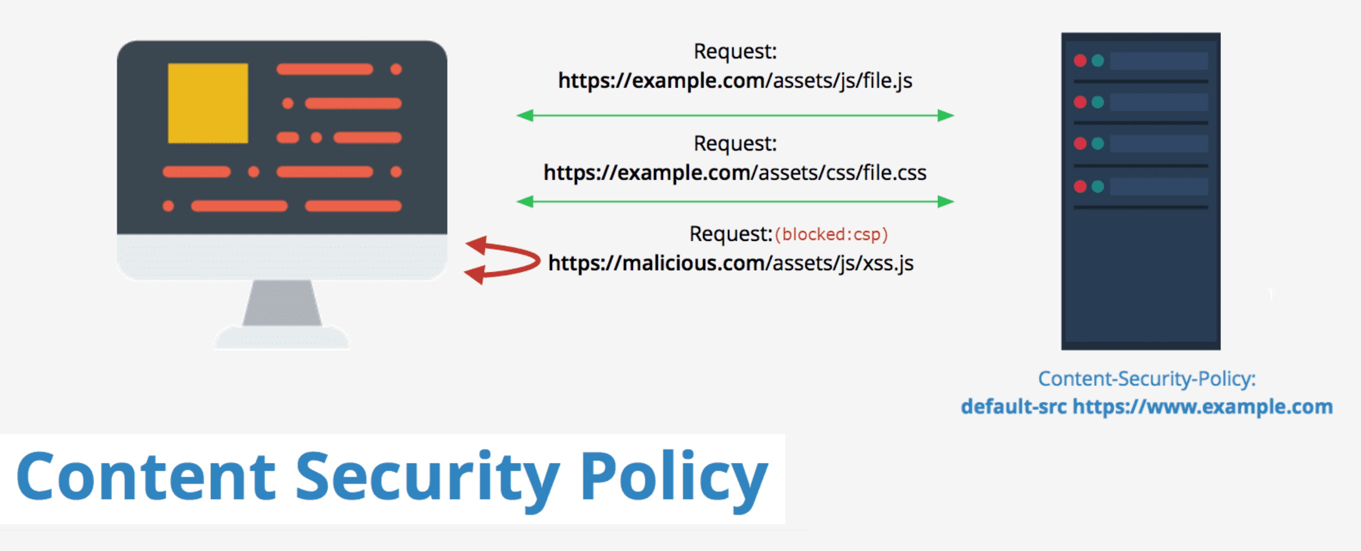
CSP and CORS

AGENDA

1. CSP - Content Security Policy
2. CORS - Cross-Origin Resource Sharing

1. CSP - Content Security Policy


Request:
https://example.com/assets/js/file.js
Request:
https://example.com/assets/css/file.css
Request:(blocked:csp)
https://malicious.com/assets/js/xss.js
Content-Security-Policy:
default-src https://www.example.com
Content Security Policy

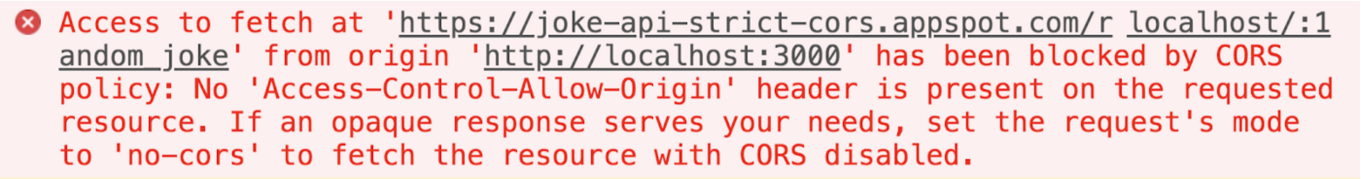
> Source: https://www.rahulpnath.com/blog/http-content-security-policy-csp/

```
// try to run this line of code on MDN and see
fetch('http://js-post-api.herokuapp.com/api/students?_page=1')

// error: Refused to connect to 'http://js-post-api.herokuapp.com/api/students?_page=1' because it violates the document's Content Security Policy
```

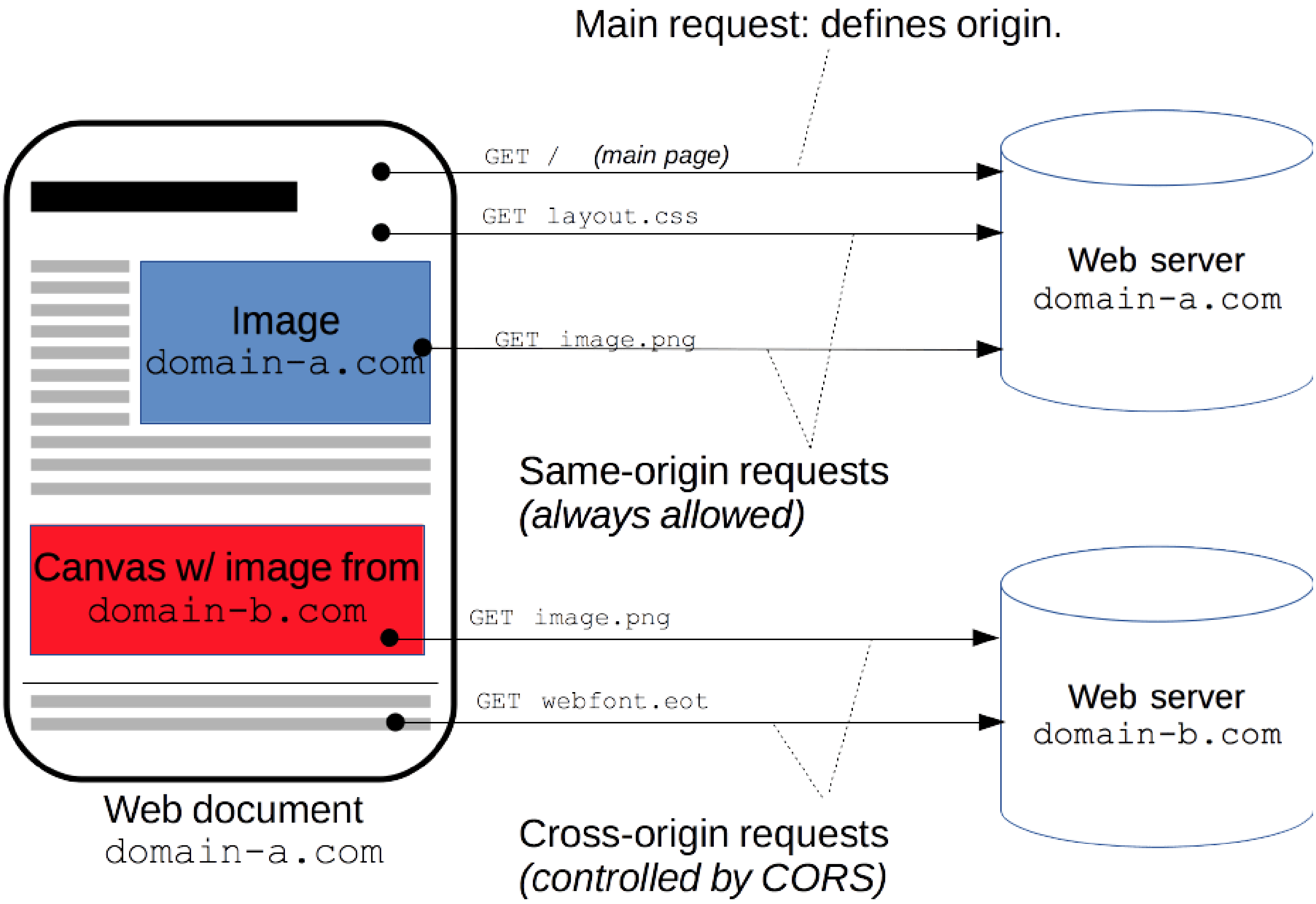
> Source: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

2. CORS - Cross-Origin Resource Sharing



```
ⓧ Access to fetch at 'https://joke-api-strict-cors.appspot.com/random_joke' from origin 'http://localhost:3000' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource. If an opaque response serves your needs, set the request's mode to 'no-cors' to fetch the resource with CORS disabled.   localhost/:1
```

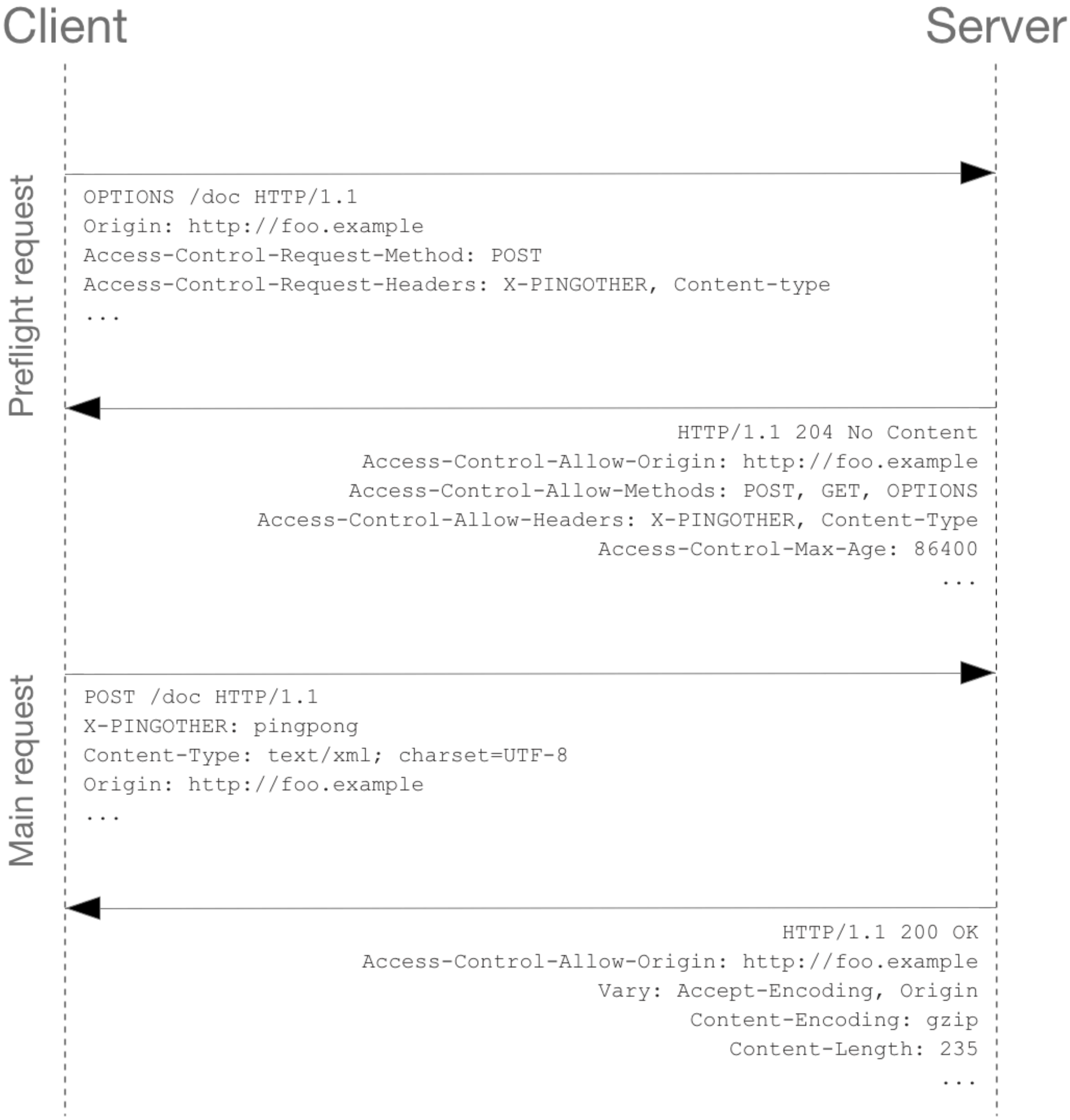
> Source: https://medium.com/@dtkatz/3-ways-to-fix-the-cors-error-and-how-access-control-allow-origin-works-d97d55946d9



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

```
// access this from google.com console
fetch('https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS/bcd.json')

// Access to fetch at 'https://developer.mozilla.org/en-
US/docs/Web/HTTP/CORS/bcd.json' from origin 'https://www.google.com' has
been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is
present on the requested resource. If an opaque response serves your
needs, set the request's mode to 'no-cors' to fetch the resource with CORS
disabled.
```



```
OPTIONS /doc HTTP/1.1
Origin: http://foo.example
Access-Control-Request-Method: POST
Access-Control-Request-Headers: X-PINGOTHER, Content-type
...
```

```
                      HTTP/1.1 204 No Content
         Access-Control-Allow-Origin: http://foo.example
          Access-Control-Allow-Methods: POST, GET, OPTIONS
 Access-Control-Allow-Headers: X-PINGOTHER, Content-Type
                          Access-Control-Max-Age: 86400
                                                     ...
```

```
POST /doc HTTP/1.1
X-PINGOTHER: pingpong
Content-Type: text/xml; charset=UTF-8
Origin: http://foo.example
...
```

```
                                   HTTP/1.1 200 OK
         Access-Control-Allow-Origin: http://foo.example
                        Vary: Accept-Encoding, Origin
                              Content-Encoding: gzip
                                 Content-Length: 235
                                                 ...
```

Khoá học Javascript cho người mới bắt đầu 2021 🎉

- Tác giả: **Hậu Nguyễn** - Founder Easy Frontend
- Khoá học chỉ được published trên Udemy, không thông qua trung gian.
- Khoá học không bán dạng videos upload trên Google Drive hay bất cứ hình thức nào tương tự.
- Khoá học có nhóm discord để hỗ trợ trong quá trình học tập.

☎️ Liên hệ tác giả để được hỗ trợ:

- ✅ Facebook: https://www.facebook.com/nvhauesmn/
- ✅ Fanpage: https://www.facebook.com/learn.easyfrontend
- ✅ Youtube Channel: https://www.youtube.com/easyfrontend