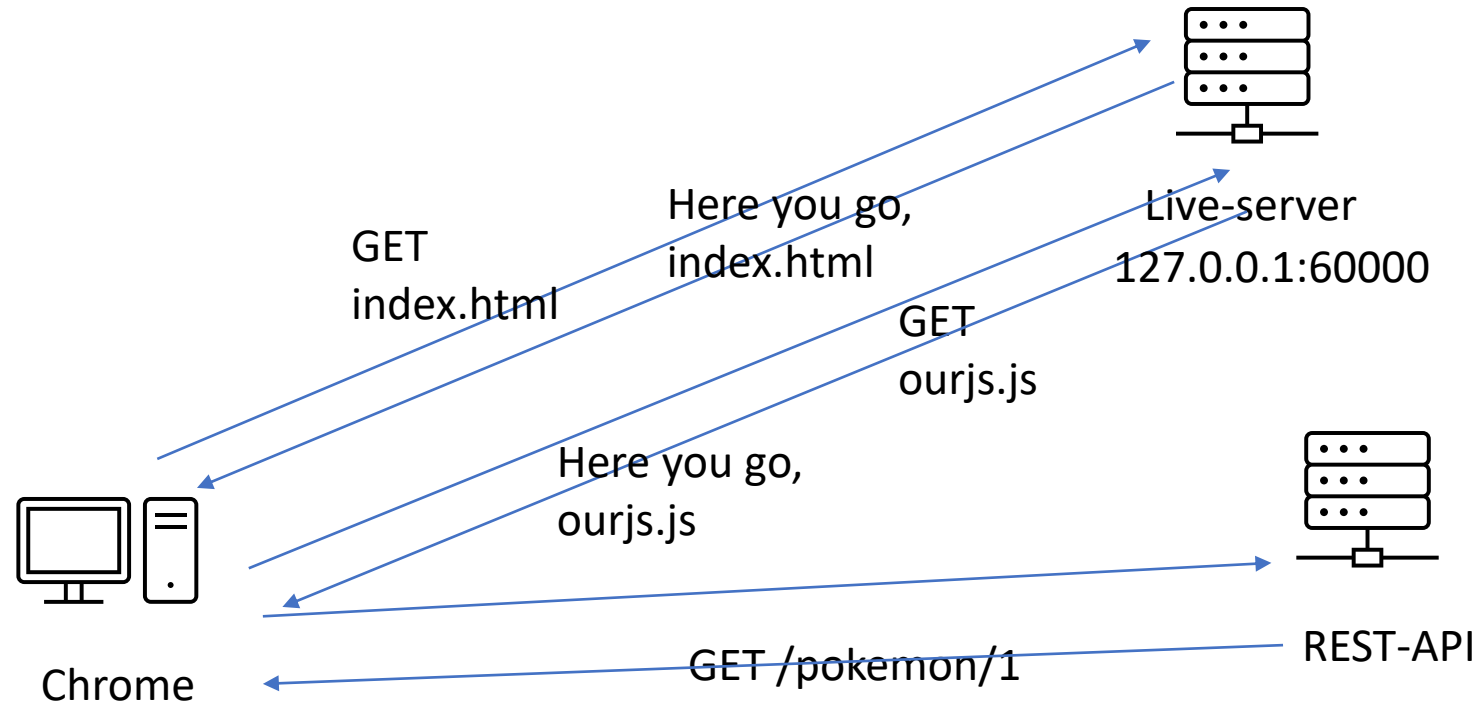


Cors

(Cross Origin Resource Sharing)



GET
index.html

Here you go,
index.html

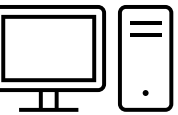
Live-server
127.0.0.1:60000

GET
ourjs.js

Here you go,
ourjs.js

GET /pokemon/1

REST-API



Chrome

“No, .js files
that send
requests to
us from
those
origins are
not allowed
to do so”

Browser will ask:
This request is
coming from a .js
file served from
some other server
(origin:
127.0.0.1:60000),
is that allowed?

The purpose of CORS is to protect the user from accidentally visiting random websites that might send .js files that could send arbitrary HTTP requests to websites the user uses, such as gmail, youtube, etc.

So over on the backend, it is important to enforce that only .js files originating from certain origins are allowed to send those requests (typically origins that that backend owner owns)