CORS: Cross Origin Resource Sharing

@ Sec_r0

SecurityZines.com

1 ORIGIN

Uniquely identifies a resource on the Web

WEB URI

http :// example.com : 8080 / foo

Protocol   domain   Port   Path

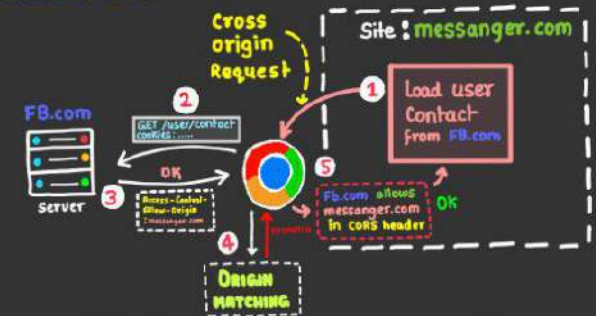ORIGIN   Defines the source of URI
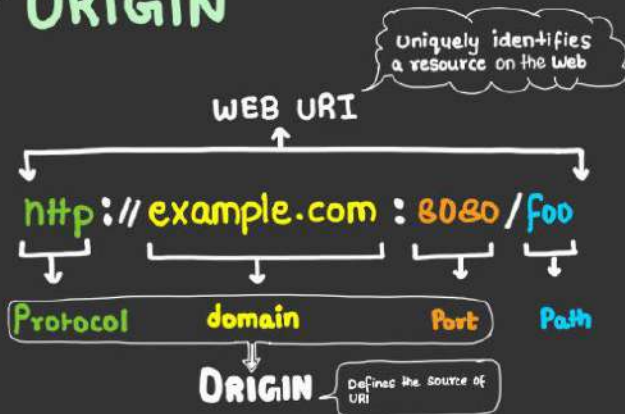
2 Same Origin Policy blocks 🚫

Cross Origin Requests

Cross origin Request

Site : evil.com

① Load user Contact from FB.com

FB.com

② GET /user/contact cookies :.....

Server

③ OK

④ ORIGIN MATCHING

ERROR ⚠
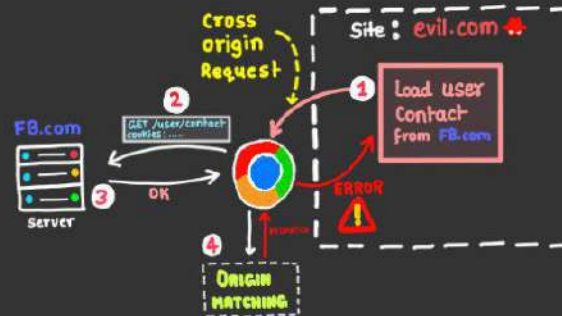
3 CORS Headers

* Headers set by server to allow cross domain interaction

Cross origin Request

Site : messanger.com

① Load user Contact from FB.com

FB.com

② GET /user/contact cookies :....

Server

③ Access-Control-Allow-Origin : messanger.com

④ ORIGIN MATCHING

⑤ Fb.com allows messanger.com in CORS header   Ok

4 Access-Control-Allow-Origin

GET /

example.com

Ok

Load user Contact from Server

Server

Access-Control-Allow-Origin : example.com

* Response header set by SERVER to indicate which site can access its data.

5 Access-Control-Allow-Credentials

If this request is initiated with cookies in it, then server need to make sure it allows credentials in request from origin

GET /

example.com

cookie : abcd....

Ok

Load user Contact from Server

Server

Access-Control-Allow-Origin : example.com

Access-Control-Allow-Credentials : true

Failure for server to send this will make browser to drop the request.

6 Pre Flight Request

* Request initiated by browser before making actual Cross Origin Request.

* Response of this request will tell browser about CORS header that a server may respond with.

— — —

Other CORS Headers

Access-Control-Allow-Methods
* which method server allow

Access-Control-Allow-Headers
* which headers server allow

Access-Control-Max-Age
* For how long response from preflight can be reused.