Same Origin Policy

Cross Origin Resource Sharing

Date: 28th July 2019

By: Taufiq A.k.a TAS

@p0wnsauc3

What stops …

- Myserver.com from reading the cookies of notmyserver.com stored in the browser?
- Myserver.com from reading/manipulating DOM of of notmyserver.com?
- Myserver.com from send a request & reading a response to sensitive api hosted on notmyserver.com
- Etc. Etc.

Definition of Same Origin Policy

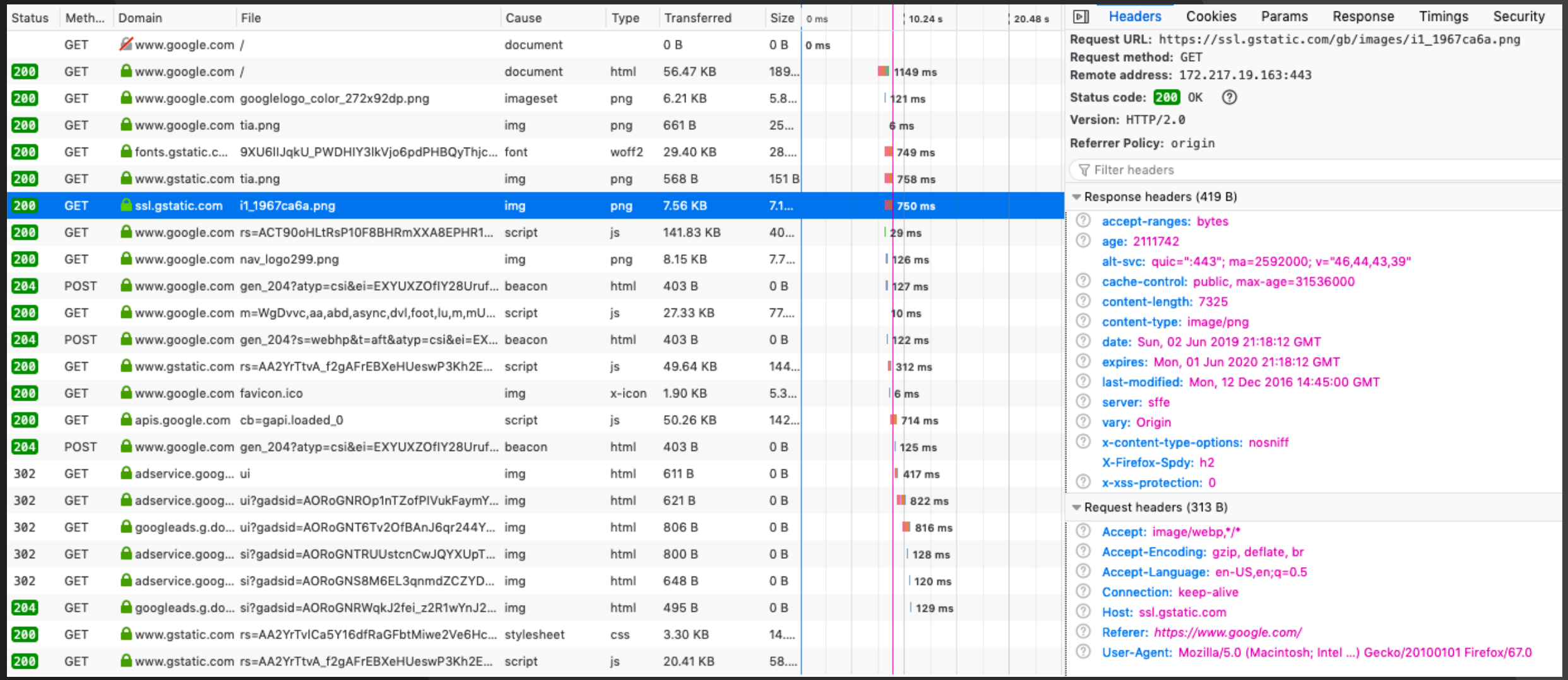
The same-origin policy is a critical security mechanism that restricts how a document or script loaded from one origin can interact with a resource from another origin. It helps isolate potentially malicious documents, reducing possible attack vectors.

Definition of Origin

Two URLs have the same origin if the protocol, port (if specified), and host are the same for both.

URL	Outcome	Reason
`http://store.company.com/dir2/other.html`	Same origin	Only the path differs
`http://store.company.com/dir/inner/another.html`	Same origin	Only the path differs
`https://store.company.com/page.html`	Failure	Different protocol
`http://store.company.com:81/dir/page.html`	Failure	Different port (`http://` is port 80 by default)
`http://news.company.com/dir/page.html`	Failure	Different host

So what is going on here?



Status	Meth...	Domain	File	Cause	Type	Transferred	Size	0 ms / 10.24 s / 20.48 s
	GET	www.google.com	/	document		0 B	0 B	0 ms
200	GET	www.google.com	/	document	html	56.47 KB	189...	1149 ms
200	GET	www.google.com	googlelogo_color_272x92dp.png	imageset	png	6.21 KB	5.8...	121 ms
200	GET	www.google.com	tia.png	img	png	661 B	25...	6 ms
200	GET	fonts.gstatic.c...	9XU6lIJqkU_PWDHIY3lkVjo6pdPHBQyThjc...	font	woff2	29.40 KB	28....	749 ms
200	GET	www.gstatic.com	tia.png	img	png	568 B	151 B	758 ms
200	GET	ssl.gstatic.com	i1_1967ca6a.png	img	png	7.56 KB	7.1...	750 ms
200	GET	www.google.com	rs=ACT90oHLtRsP10F8BHRmXXA8EPHR1...	script	js	141.83 KB	40...	29 ms
200	GET	www.google.com	nav_logo299.png	img	png	8.15 KB	7.7...	126 ms
204	POST	www.google.com	gen_204?atyp=csi&ei=EXYUXZOfIY28Uruf...	beacon	html	403 B	0 B	127 ms
200	GET	www.google.com	m=WgDvvc,aa,abd,async,dvl,foot,lu,m,mU...	script	js	27.33 KB	77....	10 ms
204	POST	www.google.com	gen_204?s=webhp&t=aft&atyp=csi&ei=EX...	beacon	html	403 B	0 B	122 ms
200	GET	www.gstatic.com	rs=AA2YrTtvA_f2gAFrEBXeHUeswP3Kh2E...	script	js	49.64 KB	144...	312 ms
200	GET	www.google.com	favicon.ico	img	x-icon	1.90 KB	5.3...	6 ms
200	GET	apis.google.com	cb=gapi.loaded_0	script	js	50.26 KB	142...	714 ms
204	POST	www.google.com	gen_204?atyp=csi&ei=EXYUXZOfIY28Uruf...	beacon	html	403 B	0 B	125 ms
302	GET	adservice.goog...	ui	img	html	611 B	0 B	417 ms
302	GET	adservice.goog...	ui?gadsid=AORoGNROp1nTZofPlVukFaymY...	img	html	621 B	0 B	822 ms
302	GET	googleads.g.do...	ui?gadsid=AORoGNT6Tv2OfBAnJ6qr244Y...	img	html	806 B	0 B	816 ms
302	GET	adservice.goog...	si?gadsid=AORoGNTRUUstcnCwJQYXUpT...	img	html	800 B	0 B	128 ms
302	GET	adservice.goog...	si?gadsid=AORoGNS8M6EL3qnmdZCZYD...	img	html	648 B	0 B	120 ms
204	GET	googleads.g.do...	si?gadsid=AORoGNRWqkJ2fei_z2R1wYnJ2...	img	html	495 B	0 B	129 ms
200	GET	www.gstatic.com	rs=AA2YrTvlCa5Y16dfRaGFbtMiwe2Ve6Hc...	stylesheet	css	3.30 KB	14....	
200	GET	www.gstatic.com	rs=AA2YrTtvA_f2gAFrEBXeHUeswP3Kh2E...	script	js	20.41 KB	58....	

Headers | Cookies | Params | Response | Timings | Security

Request URL: https://ssl.gstatic.com/gb/images/i1_1967ca6a.png
Request method: GET
Remote address: 172.217.19.163:443
Status code: 200 OK
Version: HTTP/2.0
Referrer Policy: origin

Filter headers

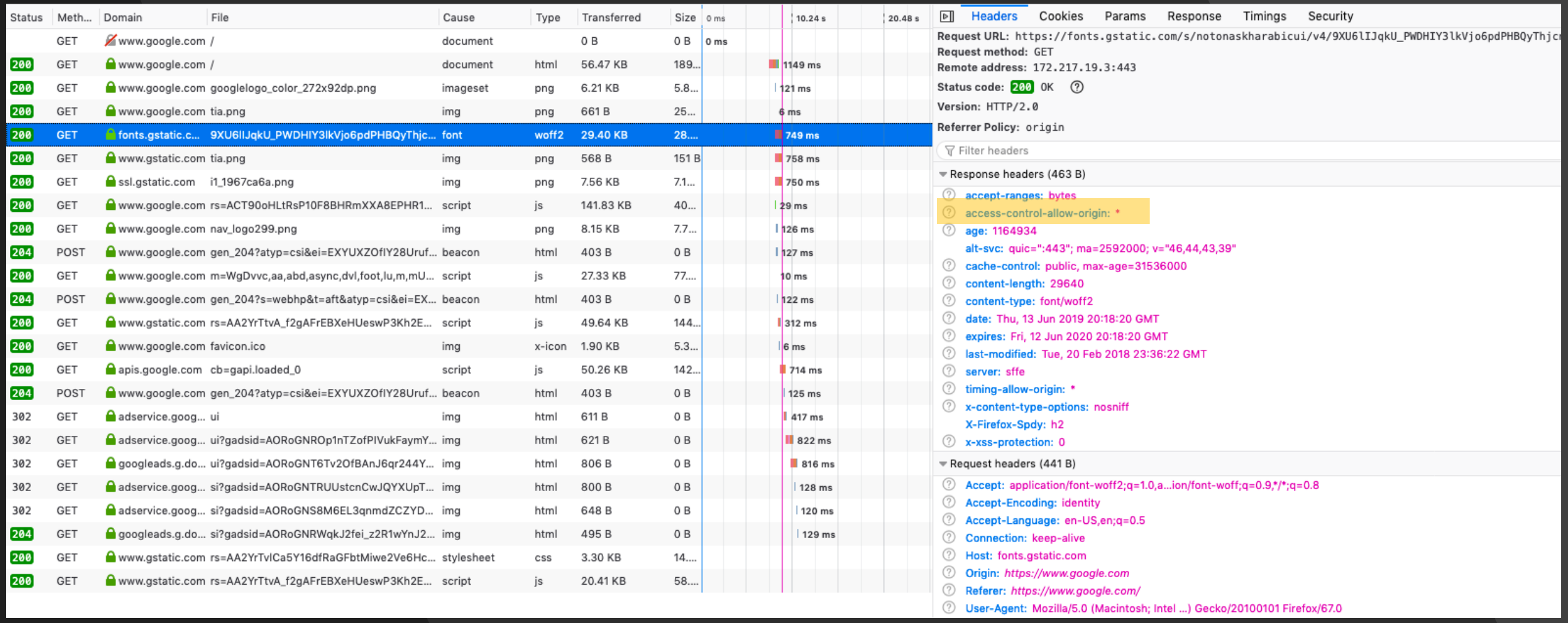
Response headers (419 B)

accept-ranges: bytes
age: 2111742
alt-svc: quic=":443"; ma=2592000; v="46,44,43,39"
cache-control: public, max-age=31536000
content-length: 7325
content-type: image/png
date: Sun, 02 Jun 2019 21:18:12 GMT
expires: Mon, 01 Jun 2020 21:18:12 GMT
last-modified: Mon, 12 Dec 2016 14:45:00 GMT
server: sffe
vary: Origin
x-content-type-options: nosniff
X-Firefox-Spdy: h2
x-xss-protection: 0

Request headers (313 B)

Accept: image/webp,*/*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Host: ssl.gstatic.com
Referer: *https://www.google.com/*
User-Agent: Mozilla/5.0 (Macintosh; Intel ...) Gecko/20100101 Firefox/67.0

Wait, what?



Status	Meth...	Domain	File	Cause	Type	Transferred	Size	0 ms	10.24 s	20.48 s
	GET	www.google.com	/	document		0 B	0 B	0 ms		
200	GET	www.google.com	/	document	html	56.47 KB	189...		1149 ms	
200	GET	www.google.com	googlelogo_color_272x92dp.png	imageset	png	6.21 KB	5.8...		121 ms	
200	GET	www.google.com	tia.png	img	png	661 B	25...		6 ms	
200	GET	fonts.gstatic.c...	9XU6lIJqkU_PWDHIY3lkVjo6pdPHBQyThjc...	font	woff2	29.40 KB	28....		749 ms	
200	GET	www.gstatic.com	tia.png	img	png	568 B	151 B		758 ms	
200	GET	ssl.gstatic.com	i1_1967ca6a.png	img	png	7.56 KB	7.1...		750 ms	
200	GET	www.google.com	rs=ACT90oHLtRsP10F8BHRmXXA8EPHR1...	script	js	141.83 KB	40...		29 ms	
200	GET	www.google.com	nav_logo299.png	img	png	8.15 KB	7.7...		126 ms	
204	POST	www.google.com	gen_204?atyp=csi&ei=EXYUXZOfIY28Uruf...	beacon	html	403 B	0 B		127 ms	
200	GET	www.google.com	m=WgDvvc,aa,abd,async,dvl,foot,lu,m,mU...	script	js	27.33 KB	77....		10 ms	
204	POST	www.google.com	gen_204?s=webhp&t=aft&atyp=csi&ei=EX...	beacon	html	403 B	0 B		122 ms	
200	GET	www.gstatic.com	rs=AA2YrTtvA_f2gAFrEBXeHUeswP3Kh2E...	script	js	49.64 KB	144...		312 ms	
200	GET	www.google.com	favicon.ico	img	x-icon	1.90 KB	5.3...		6 ms	
200	GET	apis.google.com	cb=gapi.loaded_0	script	js	50.26 KB	142...		714 ms	
204	POST	www.google.com	gen_204?atyp=csi&ei=EXYUXZOfIY28Uruf...	beacon	html	403 B	0 B		125 ms	
302	GET	adservice.goog...	ui	img	html	611 B	0 B		417 ms	
302	GET	adservice.goog...	ui?gadsid=AORoGNROp1nTZofPIVukFaymY...	img	html	621 B	0 B		822 ms	
302	GET	googleads.g.do...	ui?gadsid=AORoGNT6Tv2OfBAnJ6qr244Y...	img	html	806 B	0 B		816 ms	
302	GET	adservice.goog...	si?gadsid=AORoGNTRUUstcnCwJQYXUpT...	img	html	800 B	0 B		128 ms	
302	GET	adservice.goog...	si?gadsid=AORoGNS8M6EL3qnmdZCZYD...	img	html	648 B	0 B		120 ms	
204	GET	googleads.g.do...	si?gadsid=AORoGNRWqkJ2fei_z2R1wYnJ2...	img	html	495 B	0 B		129 ms	
200	GET	www.gstatic.com	rs=AA2YrTvlCa5Y16dfRaGFbtMiwe2Ve6Hc...	stylesheet	css	3.30 KB	14....			
200	GET	www.gstatic.com	rs=AA2YrTtvA_f2gAFrEBXeHUeswP3Kh2E...	script	js	20.41 KB	58....			

Headers | Cookies | Params | Response | Timings | Security

Request URL: https://fonts.gstatic.com/s/notonaskharabicui/v4/9XU6lIJqkU_PWDHIY3lkVjo6pdPHBQyThjc
Request method: GET
Remote address: 172.217.19.3:443
Status code: 200 OK
Version: HTTP/2.0
Referrer Policy: origin

Filter headers

Response headers (463 B)

accept-ranges: bytes
access-control-allow-origin: *
age: 1164934
alt-svc: quic=":443"; ma=2592000; v="46,44,43,39"
cache-control: public, max-age=31536000
content-length: 29640
content-type: font/woff2
date: Thu, 13 Jun 2019 20:18:20 GMT
expires: Fri, 12 Jun 2020 20:18:20 GMT
last-modified: Tue, 20 Feb 2018 23:36:22 GMT
server: sffe
timing-allow-origin: *
x-content-type-options: nosniff
X-Firefox-Spdy: h2
x-xss-protection: 0

Request headers (441 B)

Accept: application/font-woff2;q=1.0,a...ion/font-woff;q=0.9,*/*;q=0.8
Accept-Encoding: identity
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Host: fonts.gstatic.com
Origin: https://www.google.com
Referer: https://www.google.com/
User-Agent: Mozilla/5.0 (Macintosh; Intel ...) Gecko/20100101 Firefox/67.0

Inherited origins

Scripts executed from pages with an about:blank or javascript: URL inherit the origin of the document containing that URL, since these types of URLs do not contain information about an origin server.

For e.g. if window.Open() was used on www.myserver.com, If this popup also contains JavaScript, that script would inherit the origin of www.myserver.com

Exceptions in Internet Explorer

Internet Explorer has two major exceptions to the same-origin policy:

1. Trust Zones - *If both domains are in the highly trusted zone (e.g. corporate intranet domains), then the same-origin limitations are not applied*

2. Port - *Internet Explorer doesn't include port into same-origin checks*.

Therefore, https://myserver.com:81/index.html and https://myserver.com/index.html are considered the same origin and no restrictions are applied.
These exceptions are nonstandard and unsupported in any other browser.

Changing origin

- Yes, a page may change its own origin, but with some limitations
- A script can set the value of document.domain
  - to its current domain
  - or a super domain of its current domain
- For example, assume a script from the document at http://abc.myserver.com/dir/other.html executes the following: document.domain = ”myserver.com"; this page will pass the same-origin check with http://myserver.com/dir/page.html

- Note: document.domain needs to be set by both, subdomain and domain

Demo

Cross-origin network access

- Browser can send the request to different origin, but cannot read the response for it
- These interactions are typically placed into three categories:
  - Cross-origin *writes* .(e.g. links, redirects, form submissions. Etc.)
  - Cross-origin *embedding* (e.g. href, src attributes etc.)
  - Cross-origin *reads* are not allowed (unless CORS is implemented)

Cross Origin Resource Embedding Examples

- JavaScript with <script src="…"></script
- CSS applied with <link rel="stylesheet" href="…">
- Images displayed by <img>.
- Media played by <video> and <audio>.
- Plugins embedded with <object>, <embed>, and <applet>.
- Fonts applied with @font-face.
- Anything embedded by <frame> and <iframe>.

Protect from Cross Origin Access

- To prevent Cross Origin write can be protected using CSRF tokens, Referrer checks, Origin validations etc.
- To prevent Cross origin embedding, ensure resource is not interpreted as any of the formats discussed earlier
- To prevent Cross origin reads, implement CORS
- Use X-Frame-Options to control access to the page

Cross-origin data storage access

- Access to data stored in the browser such as localStorage and IndexedDB are separated by origin
- Each origin gets its own separate storage
- JavaScript in one origin cannot read from or write to the storage belonging to another origin

What about Cookies?

- Cookies use a separate definition of origins
- A page can set a cookie for its own domain or any parent domain (as long as the parent domain is not a public suffix)
- The browser will make a cookie available to the given domain including any sub-domains, no matter which protocol (HTTP/HTTPS) or port is used

Securing Cookies

- When you read a cookie, you cannot see from where it was set
- Even if you use only secure https connections, any cookie you see may have been set using an insecure connection
- When you set a cookie, you can limit its availability using
  - Domain
  - Path,
  - Secure
  - Http-Only flags

How do you relax the SOP

Cross Origin Resource Sharing (CORS)

The CORS mechanism supports secure cross-origin requests and data transfers between browsers and web servers. Modern browsers use CORS in an API container such as XMLHttpRequest or Fetch to help mitigate the risks of cross-origin HTTP requests.

References

- https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
- https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS