



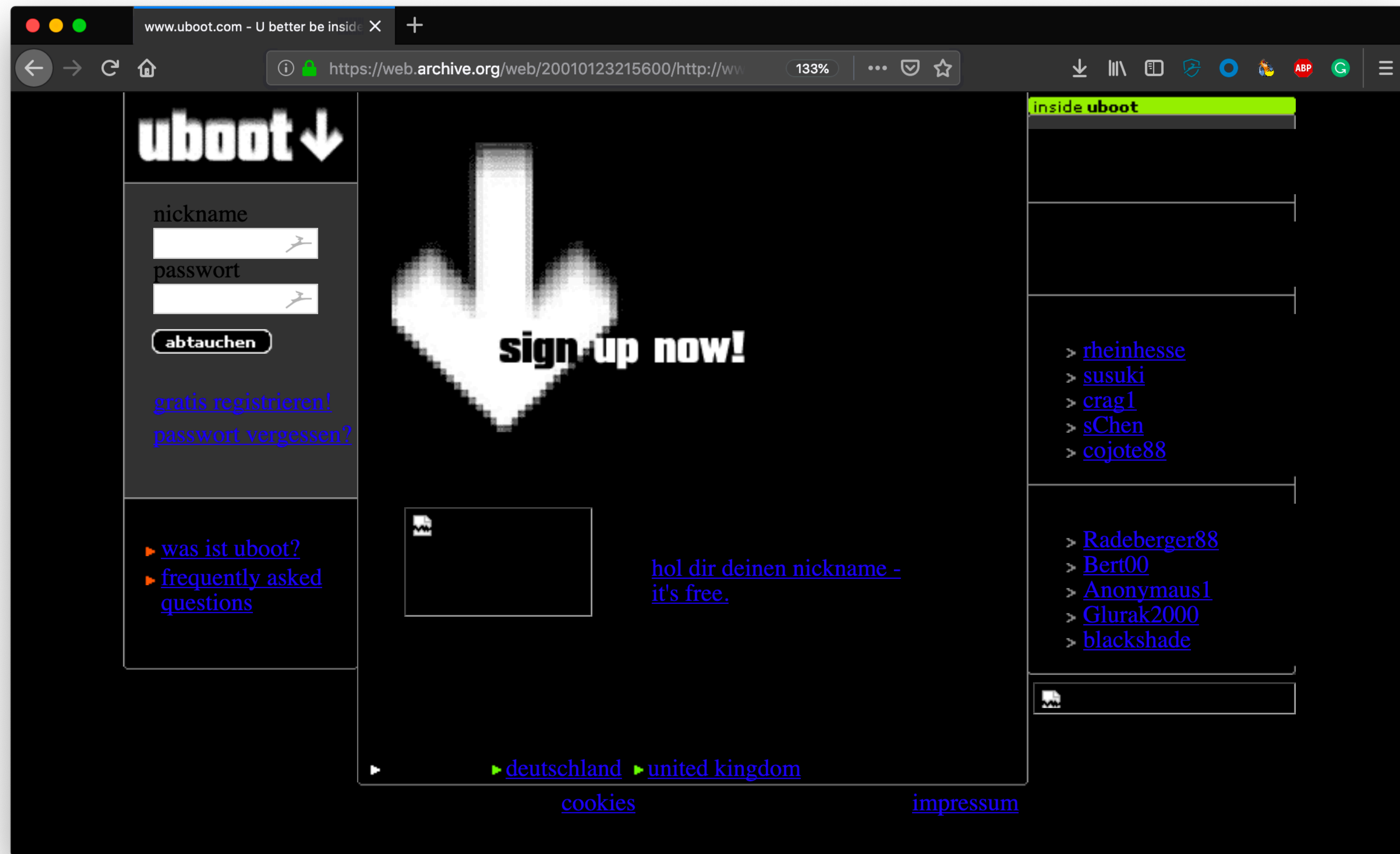
HTTP headers for the responsible developer

@stefanjudis



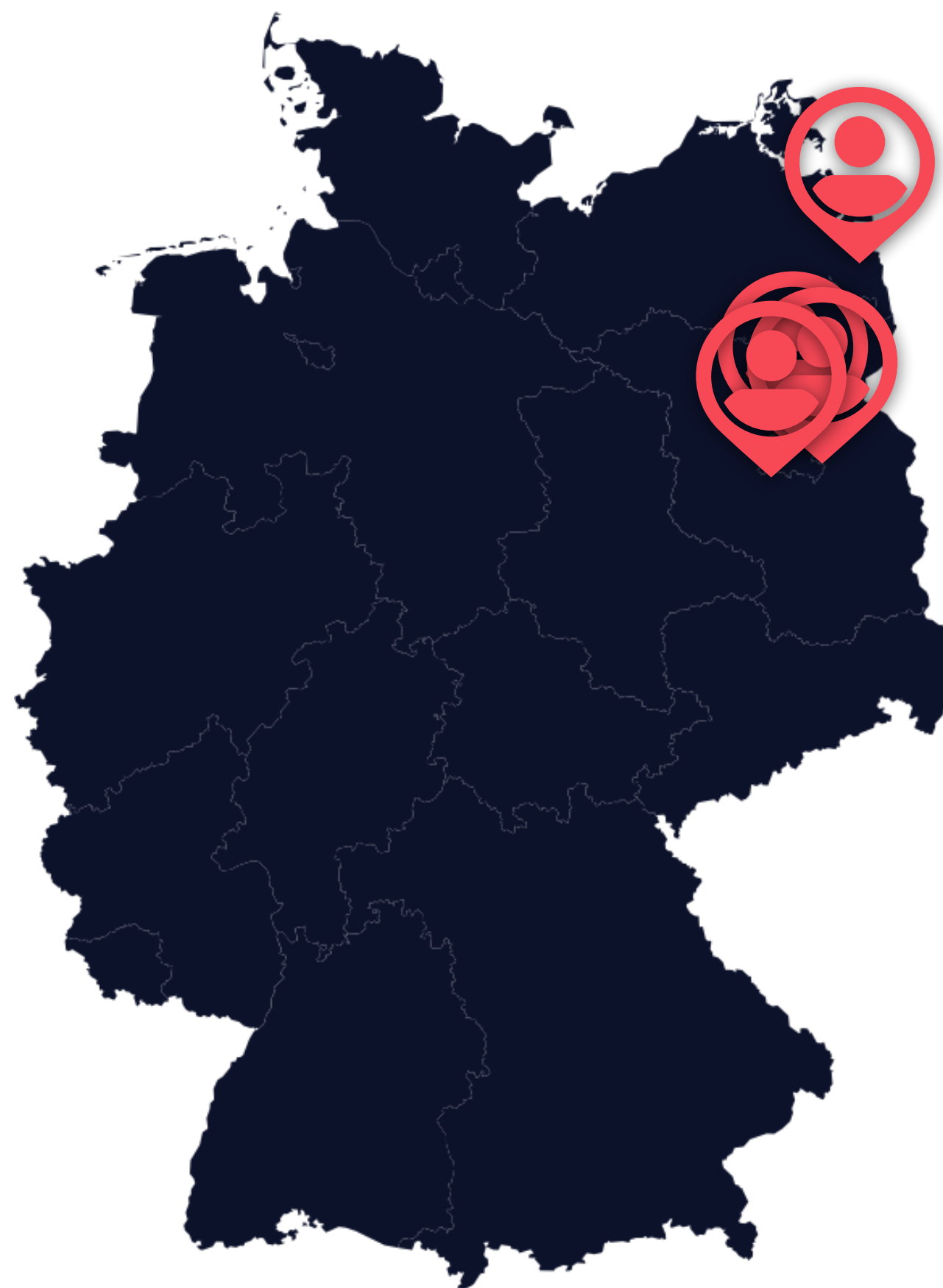
My journey on the web

uboot.com





1999





**The web
connects people**



2010





**The web
connects people**



We connect people!



We connect people!

We enable people!



We connect people!

We enable people!

We help people!



Heyo, I'm Stefan!

@stefanjudis
www.stefanjudis.com





**... and I want to be
a responsible developer**



1999



2019



2019



2019



2019



2019



2019



2019



2019



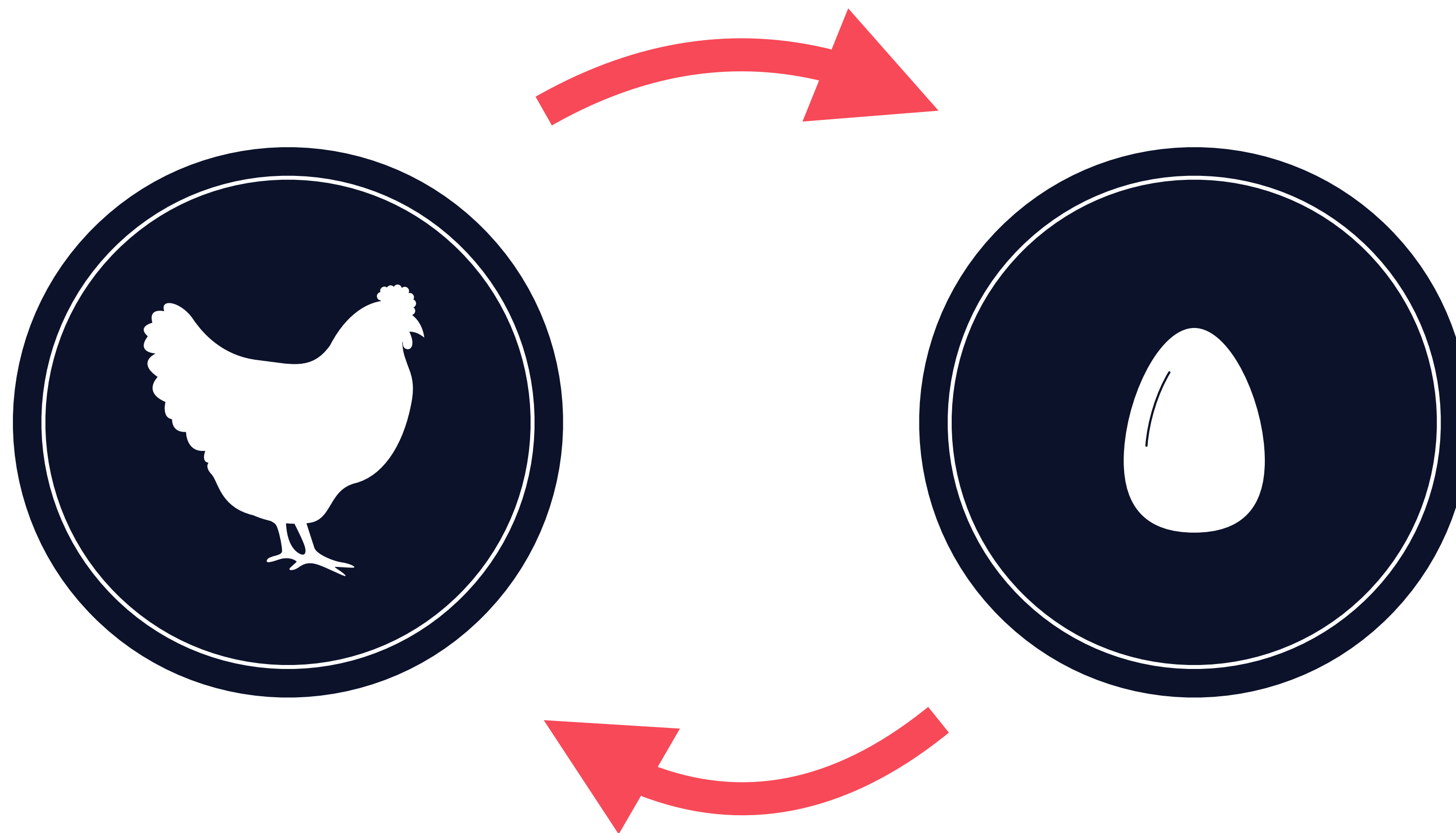
2019



**We should be building
for everybody**



***"We don't have
users in/that ..."***



"We don't have users in/that ..."



The challenge of building a "good" website



Design



Content



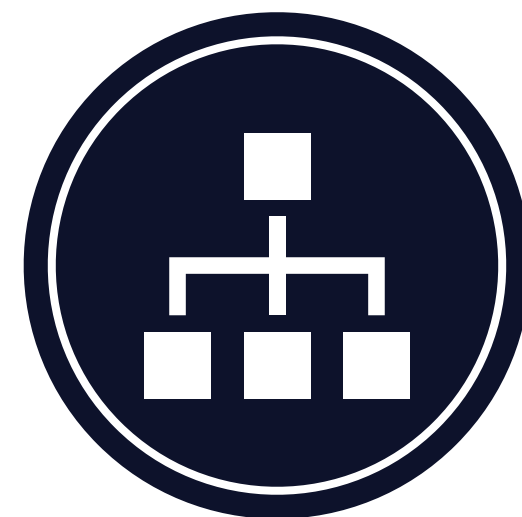
Performance



Accessibility



Frameworks



Network



Devices



Design



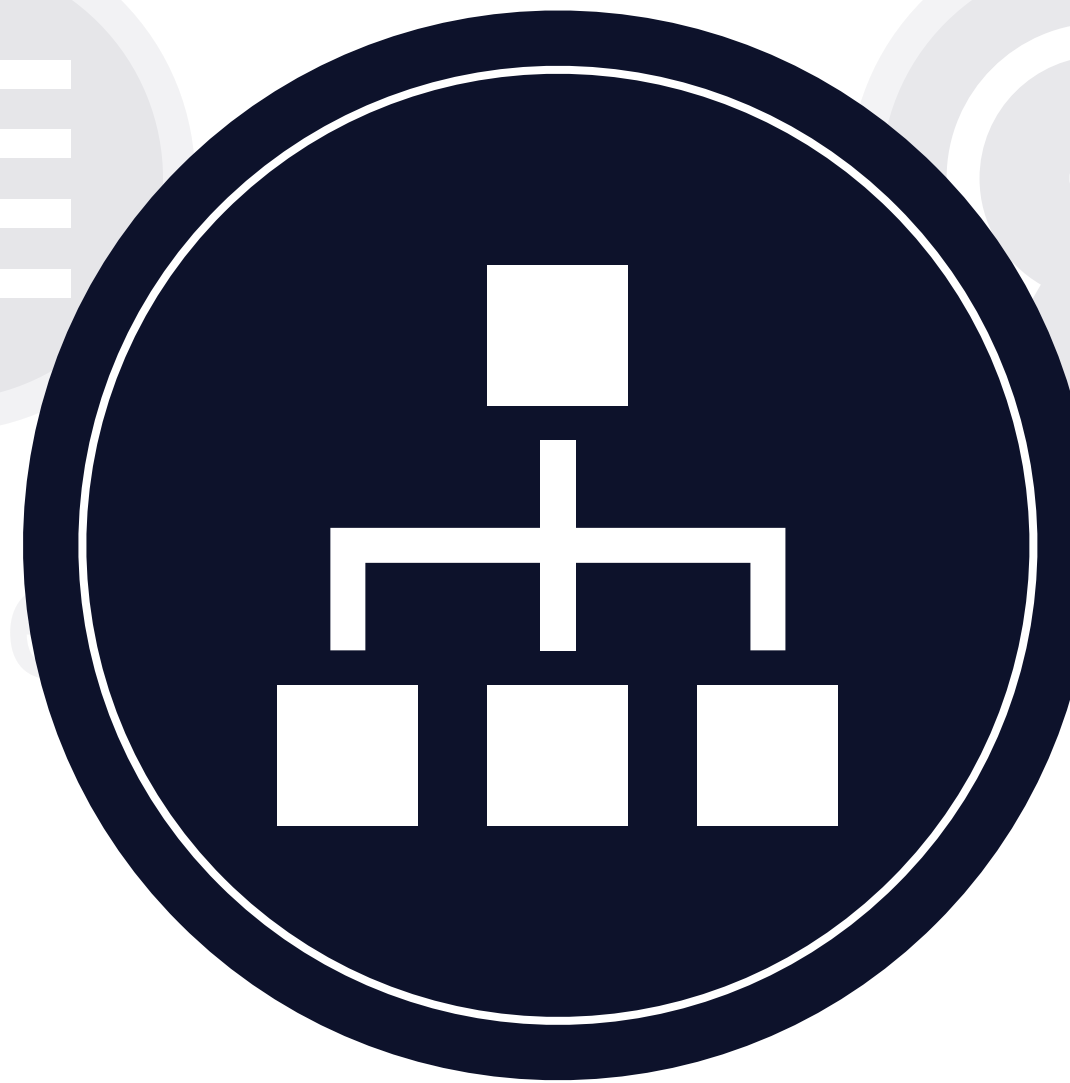
Content



Performance



Accessibility



Frameworks



Devices

Network



Let's talk HTTP



<https://the-responsible.dev/>

Accept: text/html,application/xhtml+xml,application/xml
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,de;q=0.7
...

Connection: keep-alive
Content-Type: text/html; charset=utf-8
Date: Mon, 11 Mar 2019 12:59:38 GMT
...

Response Body



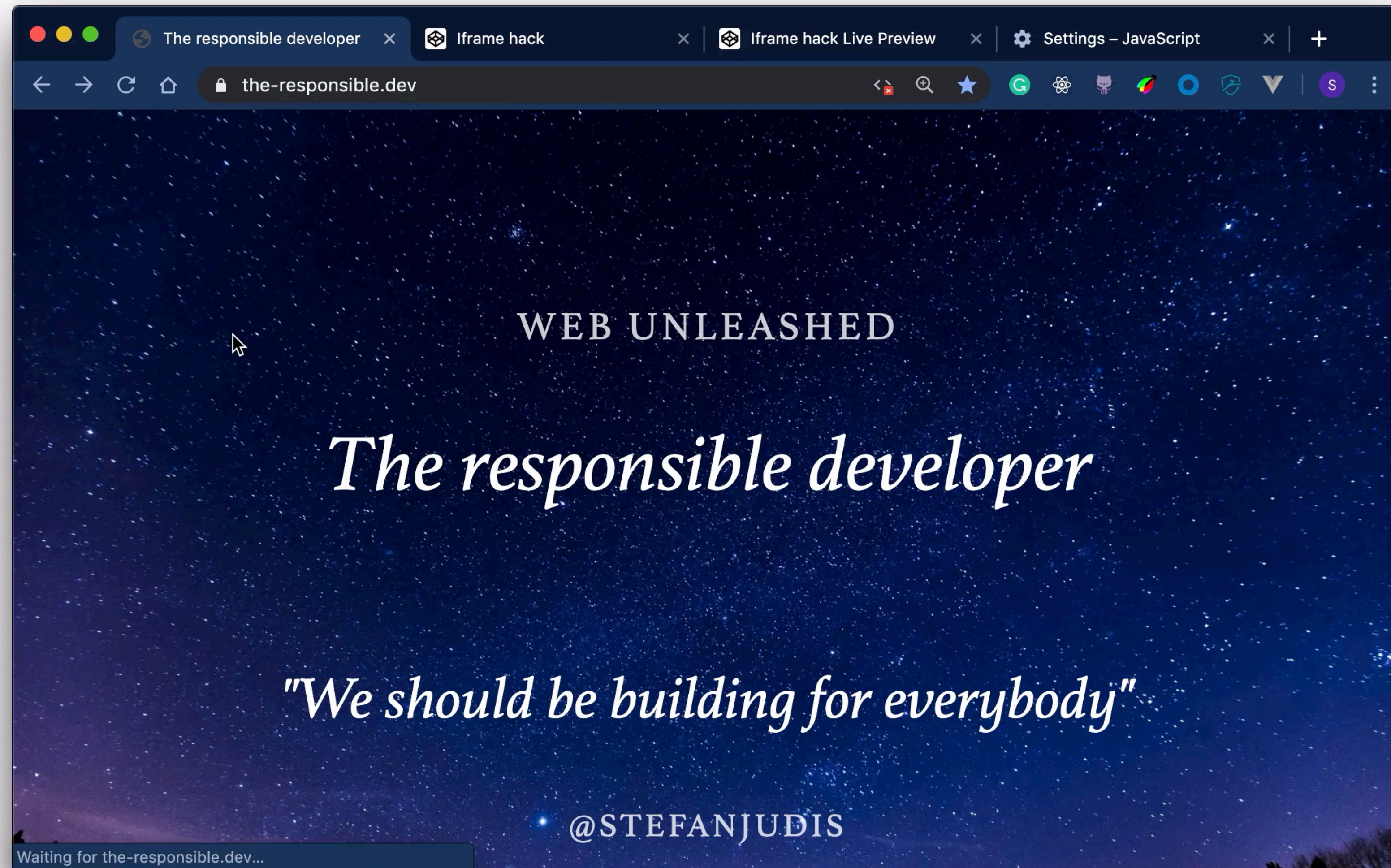
<https://the-responsible.dev/>

Accept: text/html,application/xhtml+xml,application/xml
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,de;q=0.7
...

Connection: keep-alive
Content-Type: text/html; charset=utf-8
Date: Mon, 11 Mar 2019 12:59:38 GMT
...

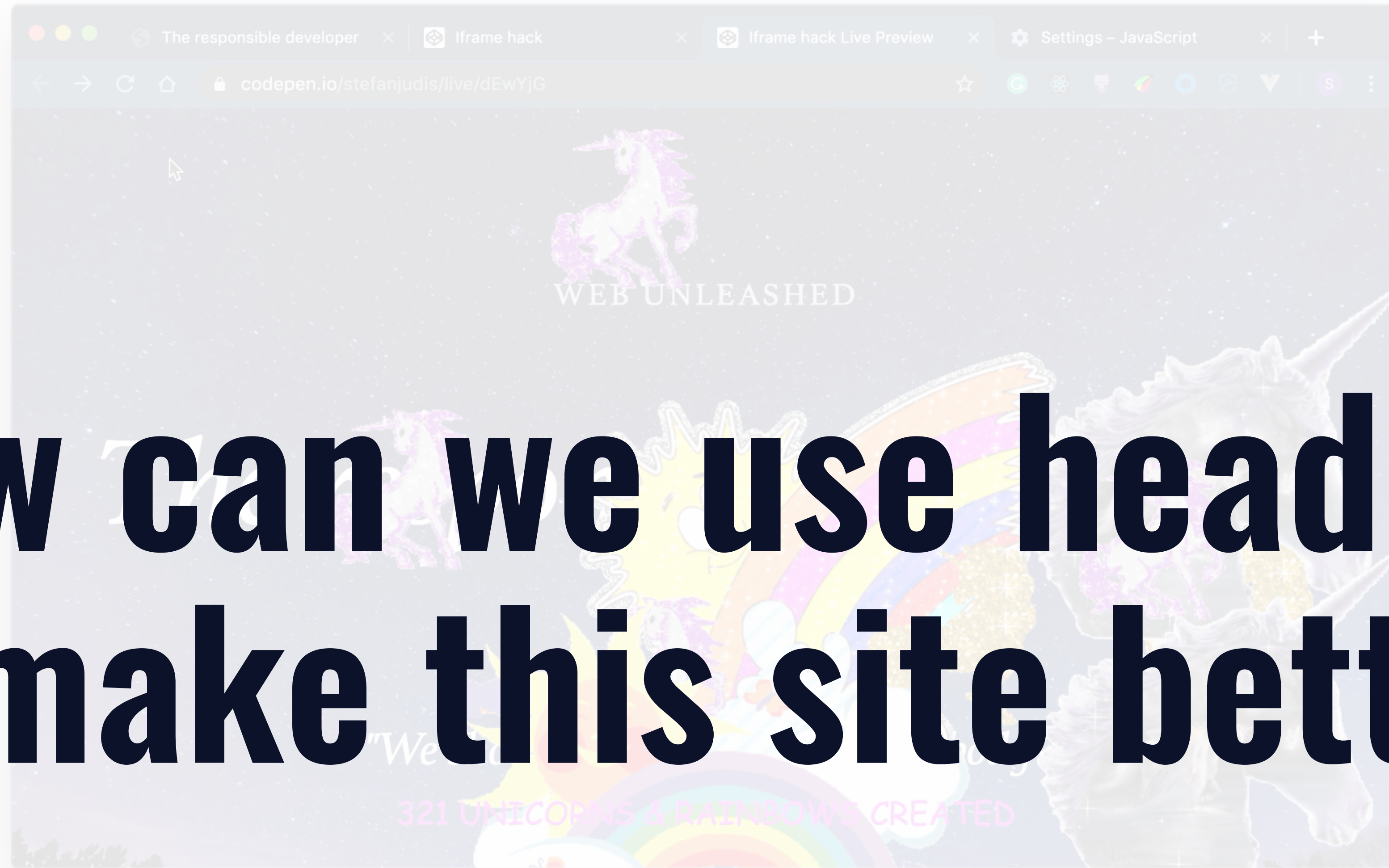
Response Body

the-responsible.dev



the-responsible.dev

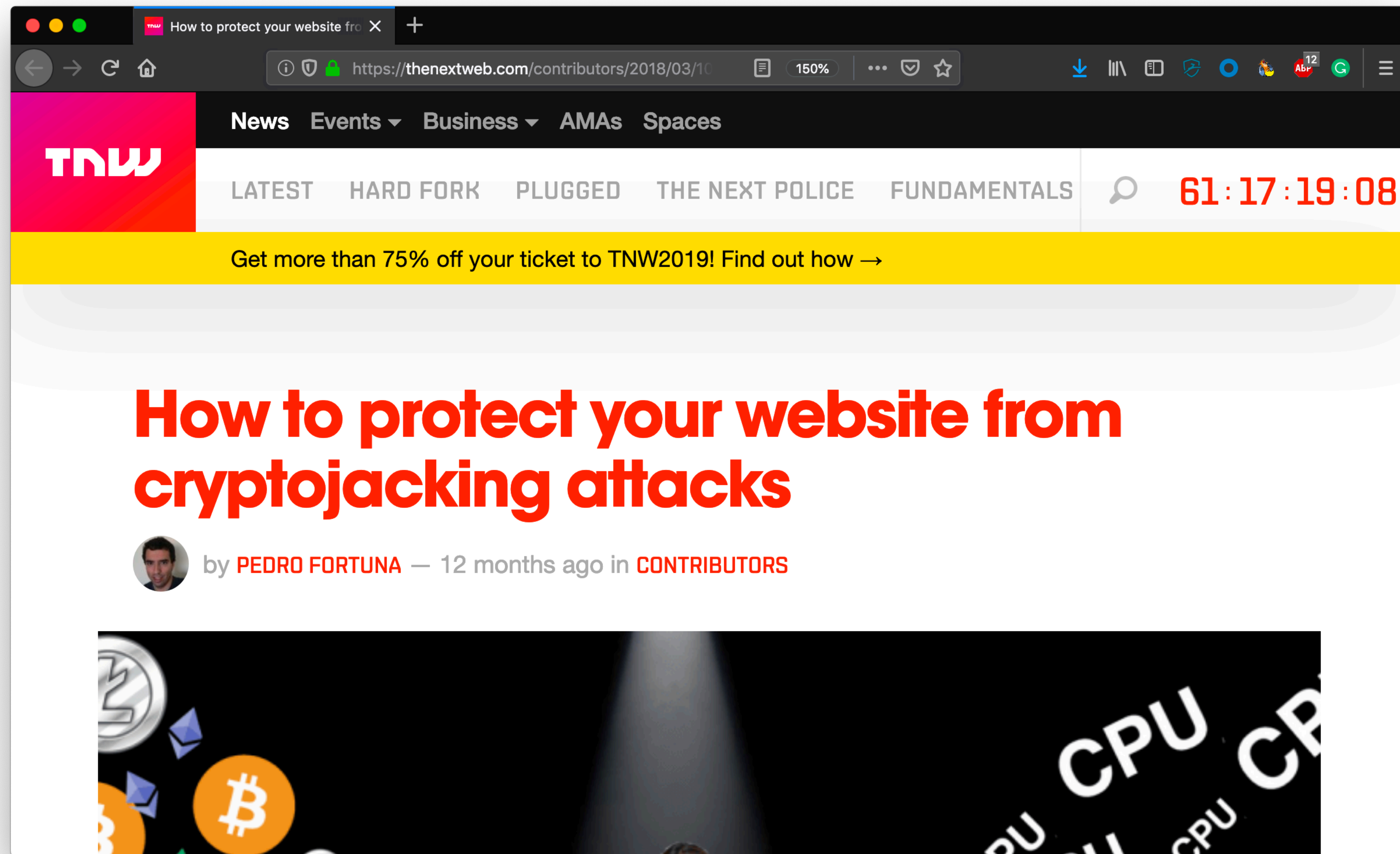
How can we use headers to make this site better?





**The web is
a scary place**

thenextweb.com/contributors/2018/03/10/protect-website-cryptojacking-attacks/



shoptalkshow.com/episodes/special-one-one-hacker/

The screenshot shows a web browser window with the URL `https://shoptalkshow.com/episodes/special-one-one-hackl` in the address bar. The page features a large orange 'Special' text and a black title 'One on One with a Hacker'. Navigation links for 'Previous Episode' and 'Next Episode' are visible. The episode details include the date 'March 24th, 2014', a duration of '00:55:43', and a 'Download' button. A video player is at the bottom with a play button and a progress bar showing '0:00 / 0:00'. On the right, there is a 'SHOPTALK SHOW' logo, a description of the show as an internet radio show starring Dave Rupert and Chris Coyier, and buttons for 'Subscribe on iTunes or RSS', 'Job Board', and 'Ask a Question'.

Special

One on One with a Hacker

← Previous Episode Next Episode →

March 24th, 2014 00:55:43 Download

0:00 / 0:00

SHOPTALK SHOW

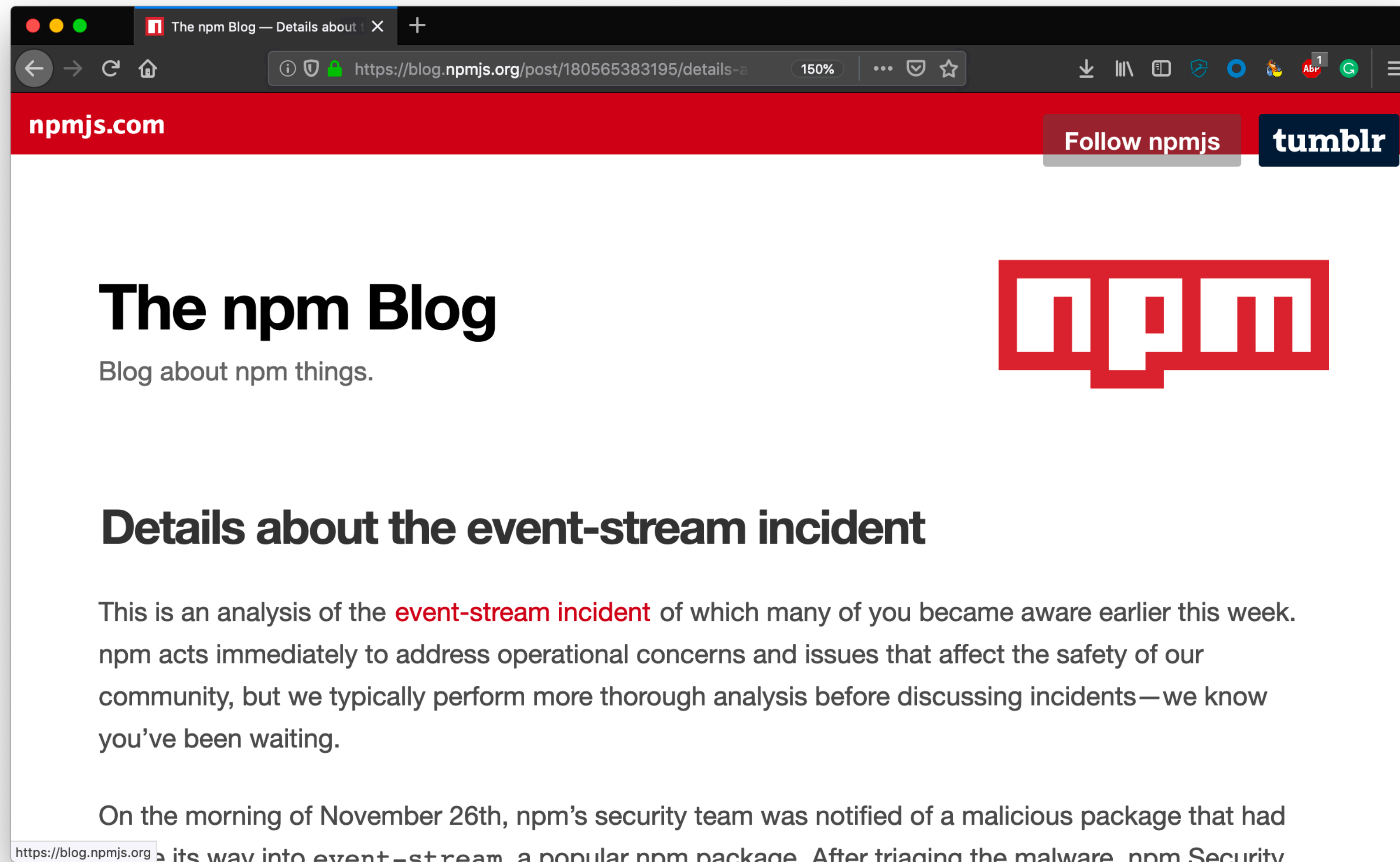
An internet radio show about the internet starring Dave Rupert and Chris Coyier.

Subscribe on iTunes or RSS

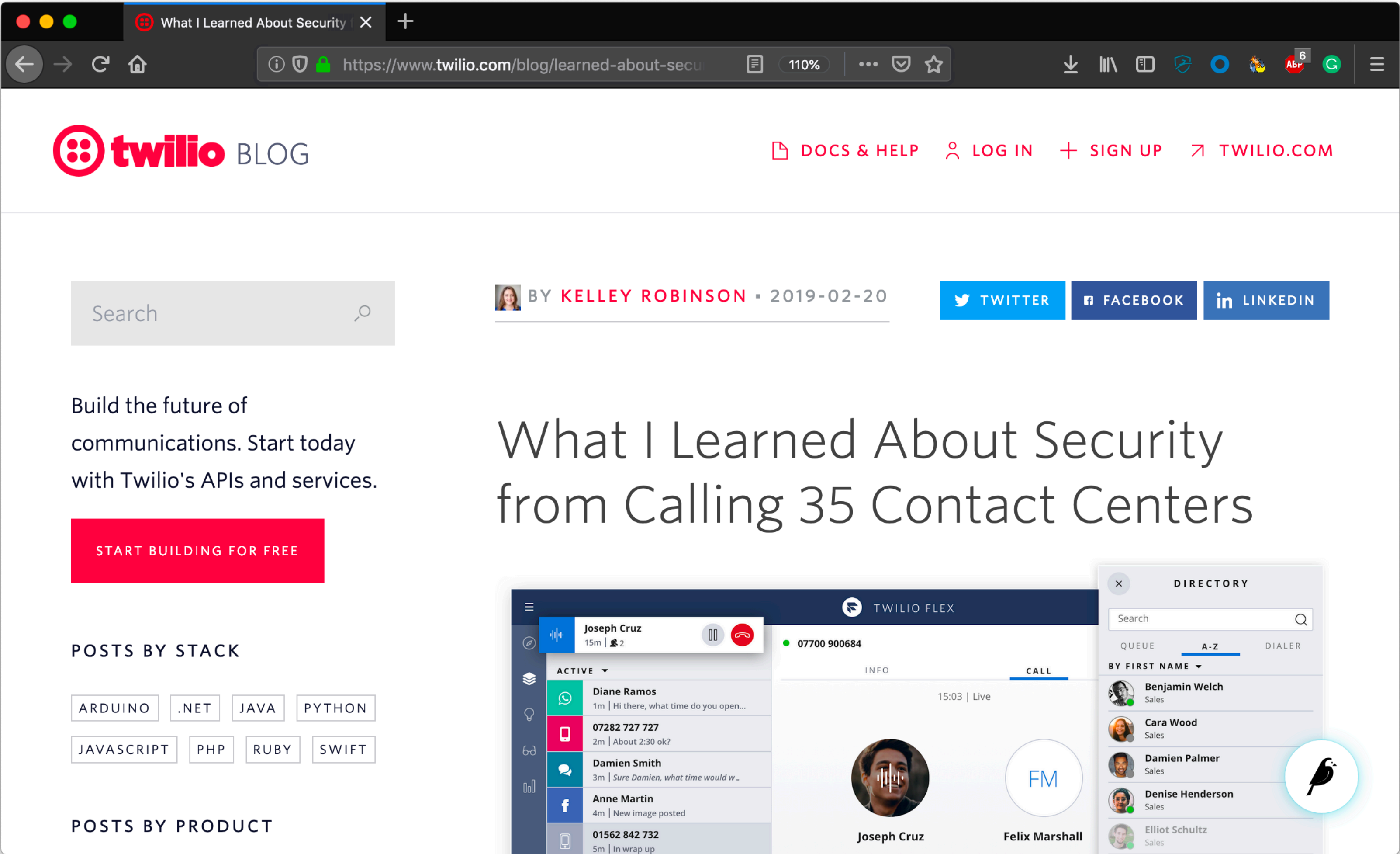
Job Board

Ask a Question

blog.npmjs.org/post/180565383195/details-about-the-event-stream-incident



www.twilio.com/blog/learned-about-security-from-calling-35-contact-centers



www.twilio.com/blog/learned-about-security-from-calling-35-contact-centers

We always
rely on others

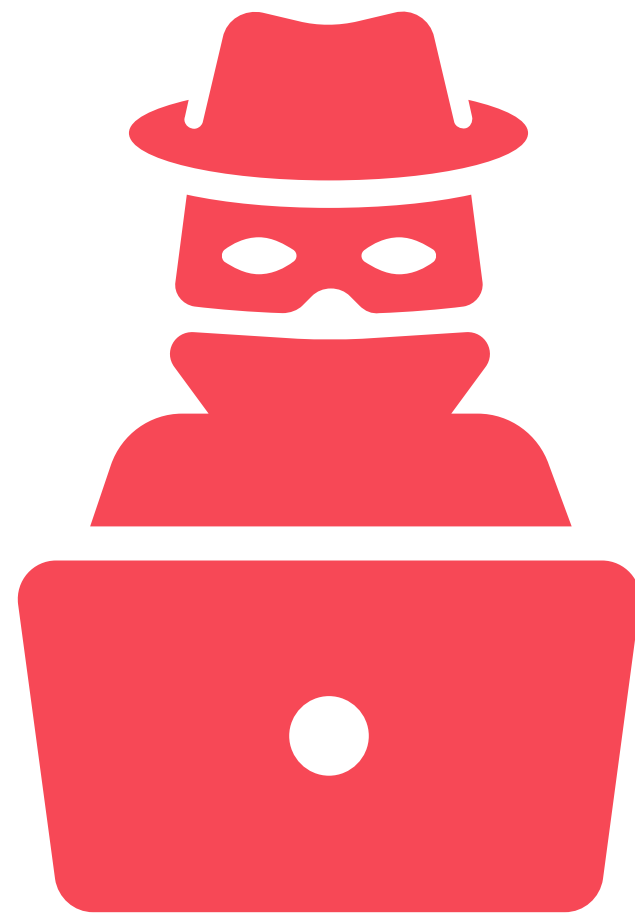




**The web
has to be safe!**

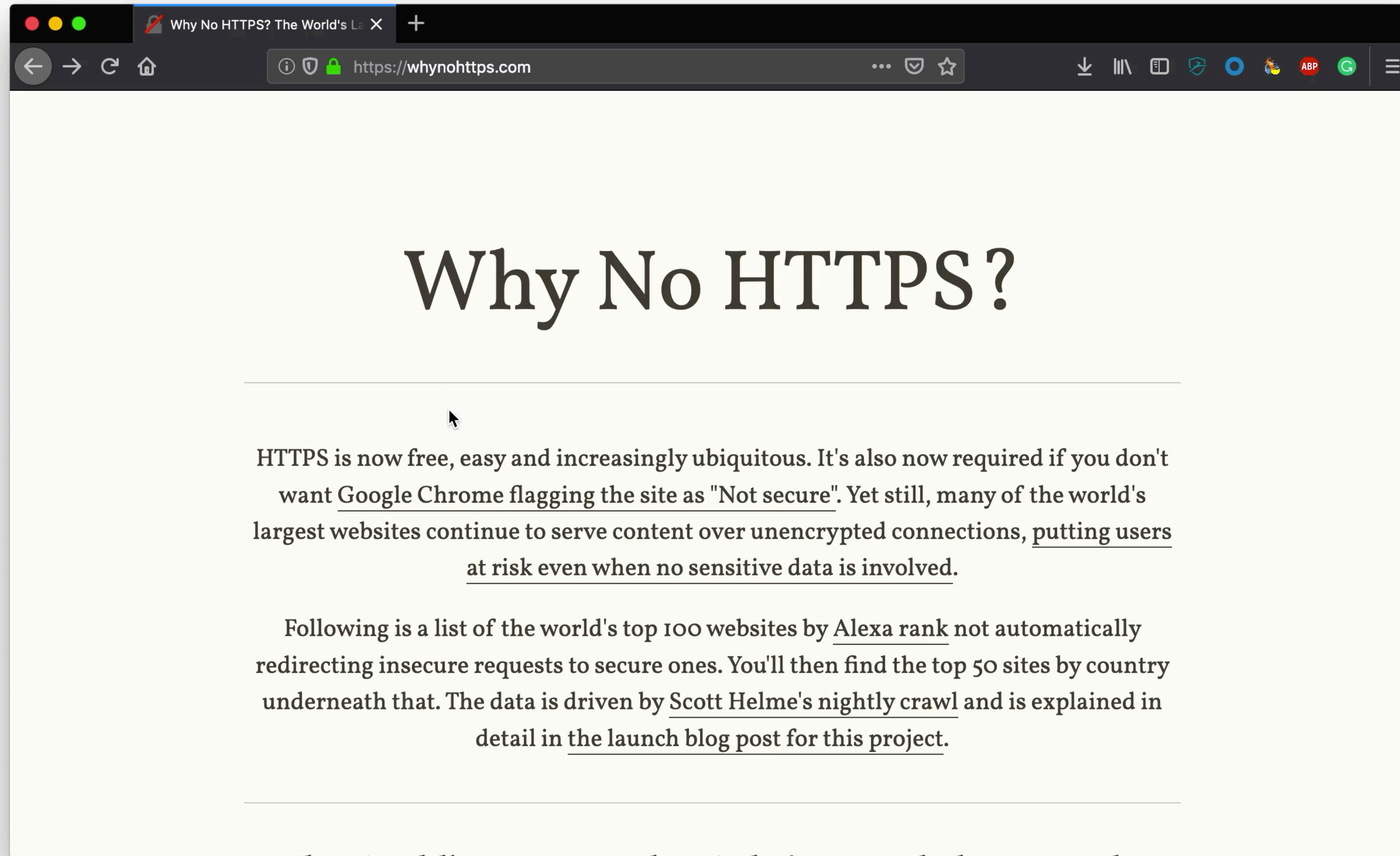


HTTPS



HTTP/2 ServiceWorker
getUserMedia() ...

whynohttps.com



←

→

↻

i

www.ard.de/home/ARD_Startseite/21920/index.html

...

☆

↓

≡

ARD Home

Nachrichten

Sport

Börse

Ratgeber

Wissen

Kultur

Kinder

Die ARD

Fernsehen

Radio


ARD Mediathek

ARD

ARD.de

Suche in der ARD Mediathek

Nachrichten



Nach Ankündigung von Zöllen

Trumps Drohung schockt Mexiko

Eigentlich war die Stimmung in Nordamerika gerade versöhnlich - umso schockierter ist Mexiko von Trumps Zoll-Drohung. Präsident López Obrador schrieb einen zweiseitigen Brief. Von Anne-Katrin Mellmann. | mehr

Mexiko: Abschiebung statt Arbeitsvisum, 17.05.2019

Mexikos Antwort auf Trumps Strafzoll-Drohung | audio

Strafzölle für Mexiko: Trump könnte US-Autobauer treffen

▼

Machtkampf in der SPD: Nahles wackelt

▼

Bundesregierung will IS-Waisen zurückholen

▼

Ärztetag positioniert sich klar in Sachen Impfpflicht

▼

EU-Wahl: Finanzdebakel für rechtsextreme NPD

▼

Neue Vorwürfe gegen Wirecard

▼

Sport



Ensure encryption



Strict-Transport-Security:
max-age=1000;
includeSubDomains;
preload

hstspreload.org

HSTS Preload List Submission

https://hstspreload.org

On GitHub

Enter a domain:

example.com

Check HSTS preload status and eligibility

Information

This form is used to submit domains for inclusion in Chrome's [HTTP Strict Transport Security \(HSTS\)](#) preload list. This is a list of sites that are hardcoded into Chrome as being HTTPS only.

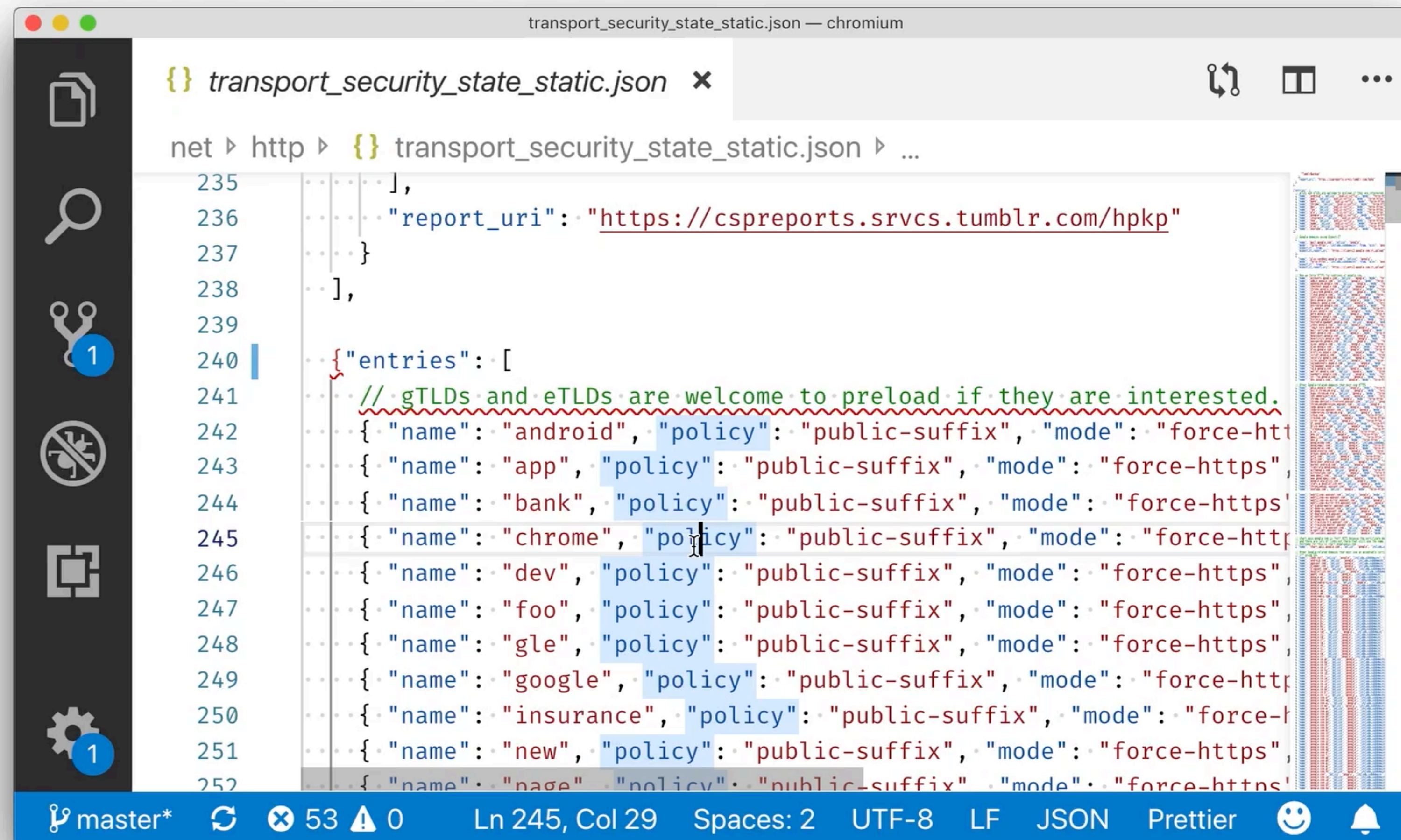
Most major browsers (Chrome, [Firefox](#), Opera, Safari, [IE 11 and Edge](#)) also have HSTS preload lists based on the Chrome list. (See the [HSTS compatibility matrix](#).)

Submission Requirements

If a site sends the `preload` directive in an HSTS header, it is considered to be requesting inclusion in the preload list and may be submitted via the form on this site.

In order to be accepted to the HSTS preload list through this form, your site must satisfy the following set of requirements:

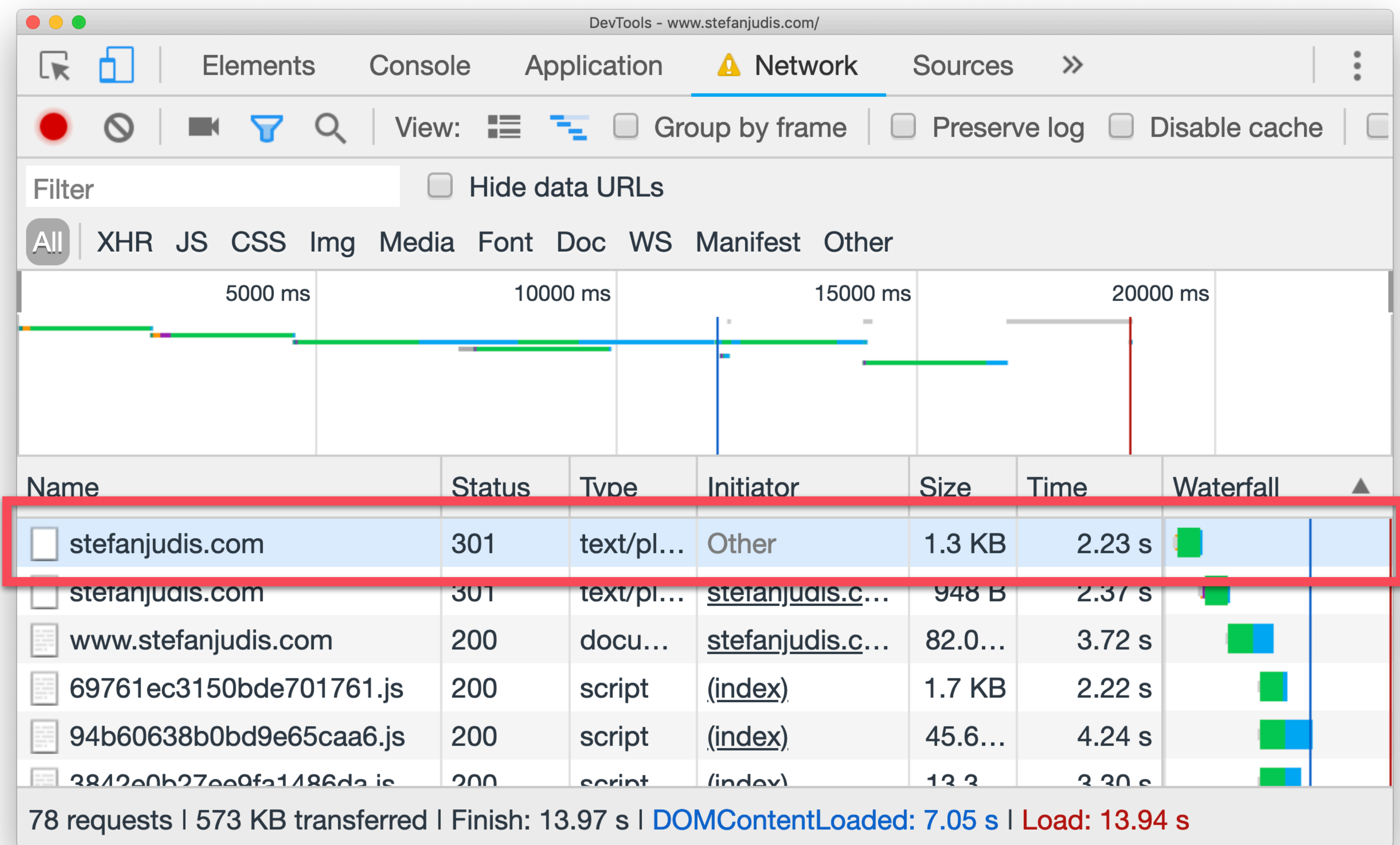
chromium.googlesource.com/chromium/src/net/+master/http/transport_security_state_static.json



The screenshot shows a web browser window with the title "transport_security_state_static.json — chromium". The browser's address bar shows the path "net > http > {} transport_security_state_static.json > ...". The main content area displays a JSON file named "transport_security_state_static.json". The JSON content is as follows:

```
{
  "report_uri": "https://cspreports.srvcs.tumblr.com/hpkp",
  "entries": [
    // gTLDs and eTLDs are welcome to preload if they are interested.
    { "name": "android", "policy": "public-suffix", "mode": "force-https" },
    { "name": "app", "policy": "public-suffix", "mode": "force-https" },
    { "name": "bank", "policy": "public-suffix", "mode": "force-https" },
    { "name": "chrome", "policy": "public-suffix", "mode": "force-https" },
    { "name": "dev", "policy": "public-suffix", "mode": "force-https" },
    { "name": "foo", "policy": "public-suffix", "mode": "force-https" },
    { "name": "gle", "policy": "public-suffix", "mode": "force-https" },
    { "name": "google", "policy": "public-suffix", "mode": "force-https" },
    { "name": "insurance", "policy": "public-suffix", "mode": "force-https" },
    { "name": "new", "policy": "public-suffix", "mode": "force-https" },
    { "name": "page", "policy": "public-suffix", "mode": "force-https" }
  ]
}
```

The editor interface includes a sidebar on the left with icons for file explorer, search, and other tools. The bottom status bar shows "master*", "53", "0", "Ln 245, Col 29", "Spaces: 2", "UTF-8", "LF", "JSON", "Prettier", and a bell icon.



caniuse.com/#feat=stricttransportsecurity





Upgrade HTTP requests

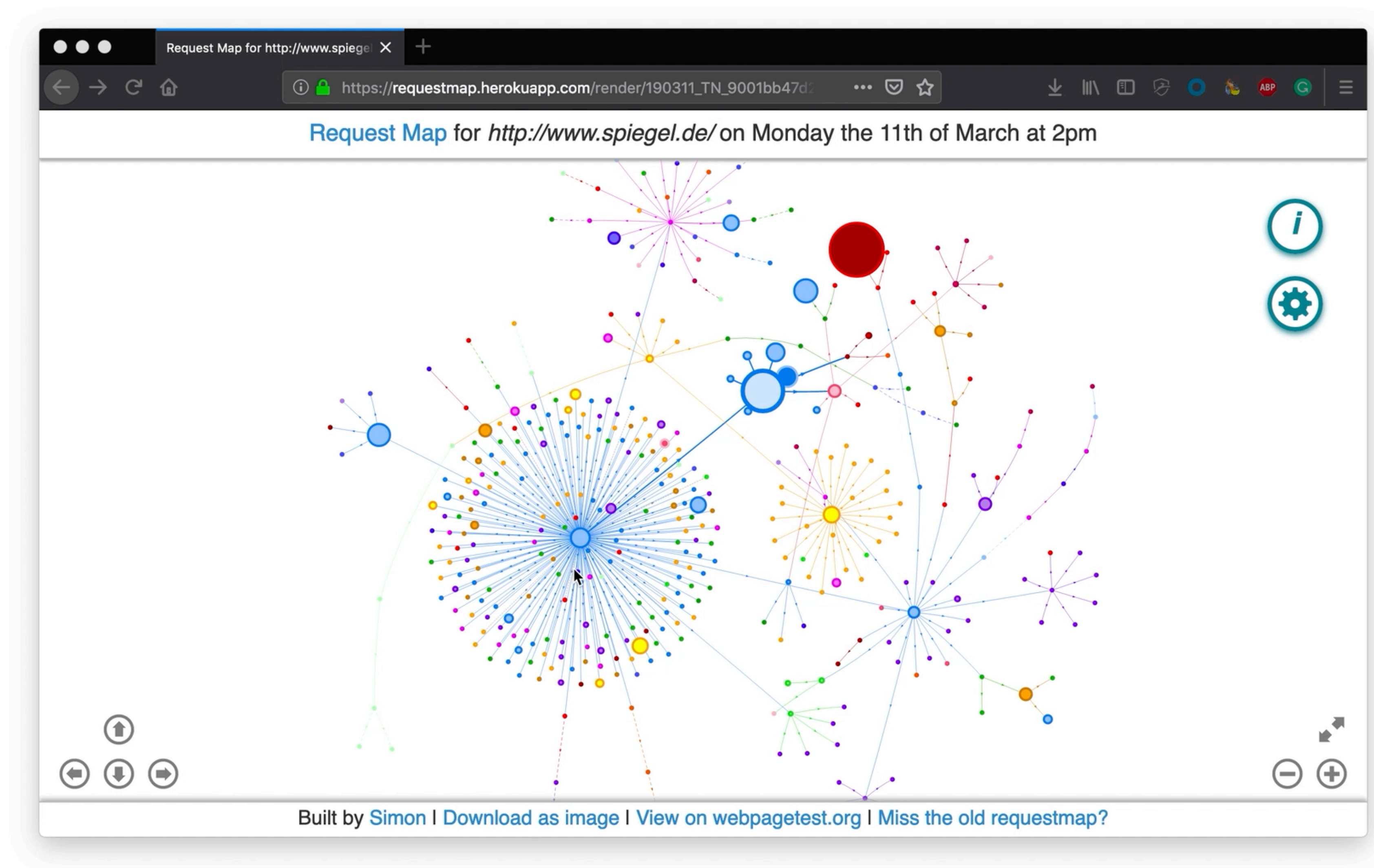


Content-Security-Policy:
upgrade-insecure-requests



Limit what's allowed

requestmap.webperf.tools



developer.mozilla.org/en-US/docs/Web/HTTP/CSP

base-uri

img-src

report-to

block-all-mixed-content

manifest-src

require-sri-for

connect-src

media-src

sandbox

default-src

navigate-to

script-src

font-src

object-src

strict-dynamic

form-action

plugin-types

style-src

frame-ancestors

prefetch-src

worker-src

frame-src

report-sample

upgrade-insecure-requests

developer.mozilla.org/en-US/docs/Web/HTTP/CSP

base-uri

img-src

report-to

block-all-mixed-content

manifest-src

require-sri-for 

connect-src

media-src

sandbox

default-src

navigate-to 

script-src

font-src

object-src

strict-dynamic

form-action

plugin-types

style-src

frame-ancestors

prefetch-src 

worker-src

frame-src

report-sample 

upgrade-insecure-requests



```
<meta http-equiv="Content-Security-Policy"  
      content="default-src 'self'; img-src https://*;">
```


Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' just-comments.com www.google-analytics.com production-assets.codepen.io storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data: images.contentful.com images.ctfassets.net www.gravatar.com www.google-analytics.com just-comments.com; font-src 'self' data:; connect-src 'self' cdn.contentful.com images.contentful.com videos.contentful.com images.ctfassets.net videos.ctfassets.net service.just-comments.com www.google-analytics.com; media-src 'self' videos.contentful.com videos.ctfassets.net; object-src 'self'; frame-src codepen.io; frame-ancestors 'self'; worker-src 'self'; block-all-mixed-content; manifest-src 'self' 'self'; disown-opener; prefetch-src 'self'; report-uri https://stefanjudis.report-uri.com/r/d/csp/reportOnly

Content-Security-Policy-Report-Only: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' just-comments.com www.google-analytics.com production-assets.codepen.io storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data: images.contentful.com images.ctfassets.net www.gravatar.com www.google-analytics.com just-comments.com; font-src 'self' data:; connect-src 'self' cdn.contentful.com images.contentful.com videos.contentful.com images.ctfassets.net videos.ctfassets.net service.just-comments.com www.google-analytics.com; media-src 'self' videos.contentful.com videos.ctfassets.net; object-src 'self'; frame-src codepen.io; frame-ancestors 'self'; worker-src 'self'; block-all-mixed-content; manifest-src 'self' 'self'; disown-opener; prefetch-src 'self'; report-uri https://stefanjudis.report-uri.com/r/d/csp/reportOnly

Content-Security-Policy-Report-Only: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' just-comments.com www.google-analytics.com production-assets.codepen.io storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data: images.contentful.com images.ctfassets.net www.gravatar.com www.google-analytics.com just-comments.com; font-src 'self' data:; connect-src 'self' cdn.contentful.com images.contentful.com videos.contentful.com images.ctfassets.net videos.ctfassets.net service.just-comments.com www.google-analytics.com; media-src 'self' videos.contentful.com videos.ctfassets.net; object-src 'self'; frame-src codepen.io; frame-ancestors 'self'; worker-src 'self'; block-all-mixed-content; manifest-src 'self' 'self'; disown-opener; prefetch-src 'self'; [report-uri https://stefanjudis.report-uri.com/r/d/csp/reportOnly](https://stefanjudis.report-uri.com/r/d/csp/reportOnly)

Content-Security-Policy-Report-Only: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' just-comments.com www.google-analytics.com production-assets.codepen.io storage.googleapis.com; style-src 'self' 'unsafe-inline'; img-src 'self' data: images.contentful.com images.ctfassets.net www.gravatar.com www.google-analytics.com just-comments.com; font-src 'self' data:; connect-src 'self' cdn.contentful.com images.contentful.com videos.contentful.com images.ctfassets.net videos.ctfassets.net service.just-comments.com www.google-analytics.com; media-src 'self' videos.contentful.com videos.ctfassets.net; object-src 'self'; frame-src codepen.io; frame-ancestors 'self'; worker-src 'self'; block-all-mixed-content; manifest-src 'self' 'self'; disown-opener; prefetch-src 'self'; report-uri https://stefanjudis.report-uri.com/r/d/csp/reportOnly



Content-Security-Policy:

```
default-src 'self';  
script-src 'sha256-blL...'
```

```
<script>  
  console.log('Inline script executing ...');  
</script>
```




Content-Security-Policy:

default-src 'self';

script-src 'nonce-abc...'

```
<script nonce="abcdef">  
  console.log('Inline script executing ...');  
</script>
```

caniuse.com/#feat=contentsecuritypolicy

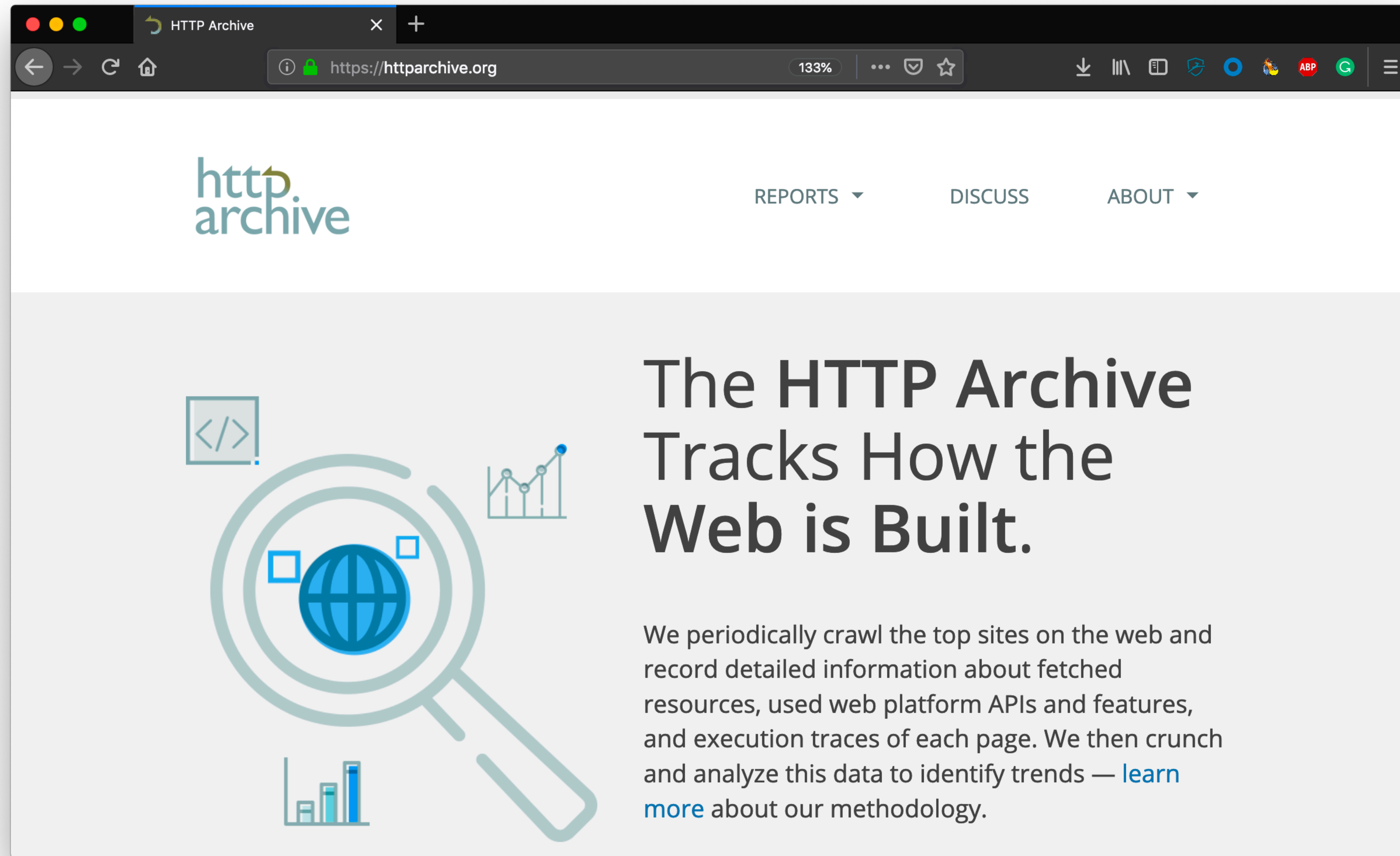


caniuse.com/#feat=contentsecuritypolicy2



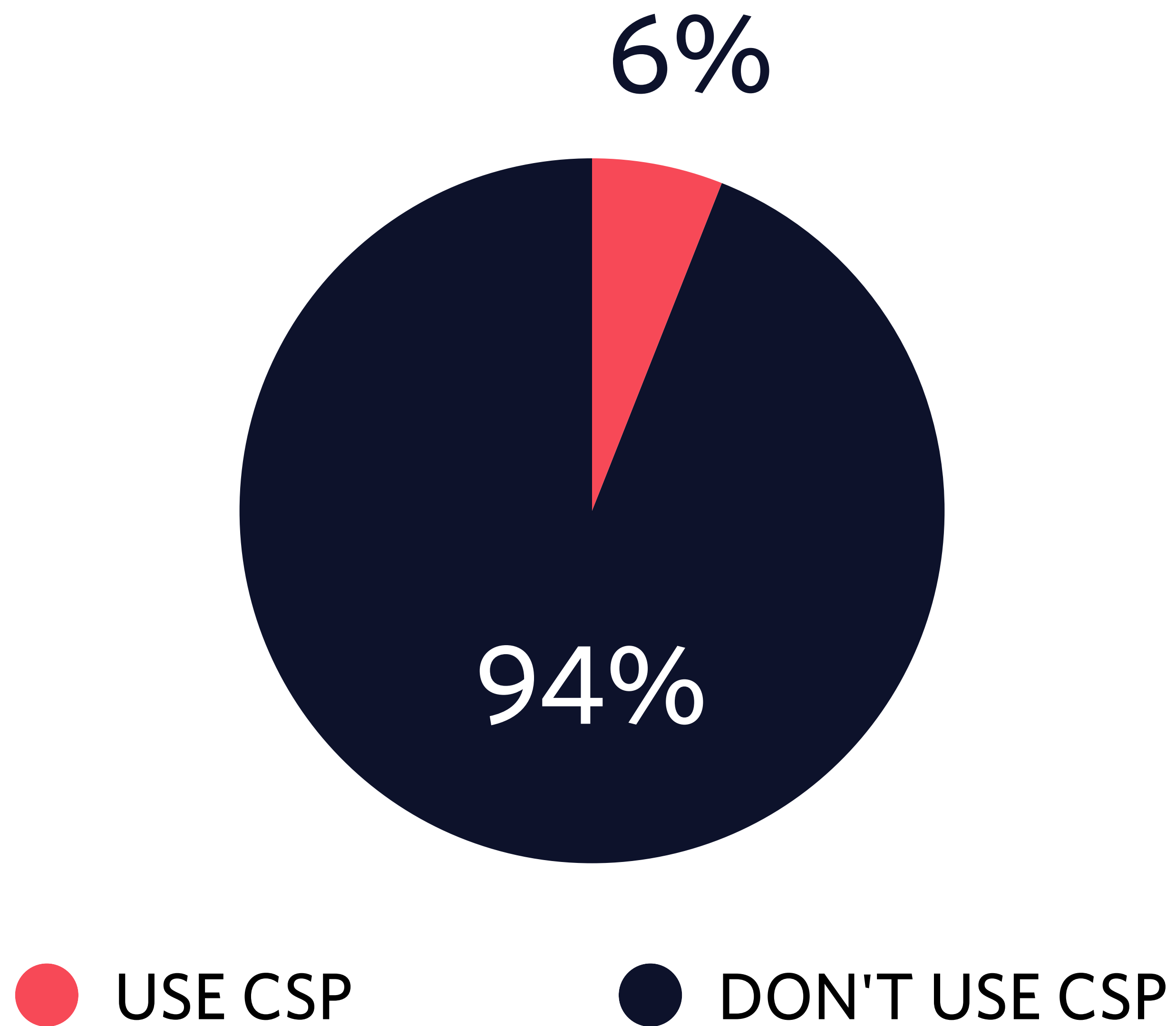
* not complete

httparchive.org





How many pages use CSP?

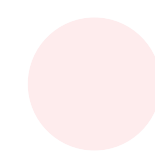


6%



94%

We can do better!



USE CSP



DON'T USE CSP



***Always monitor your CSP reports
and "test in production" with
report-only before enforcing them!***

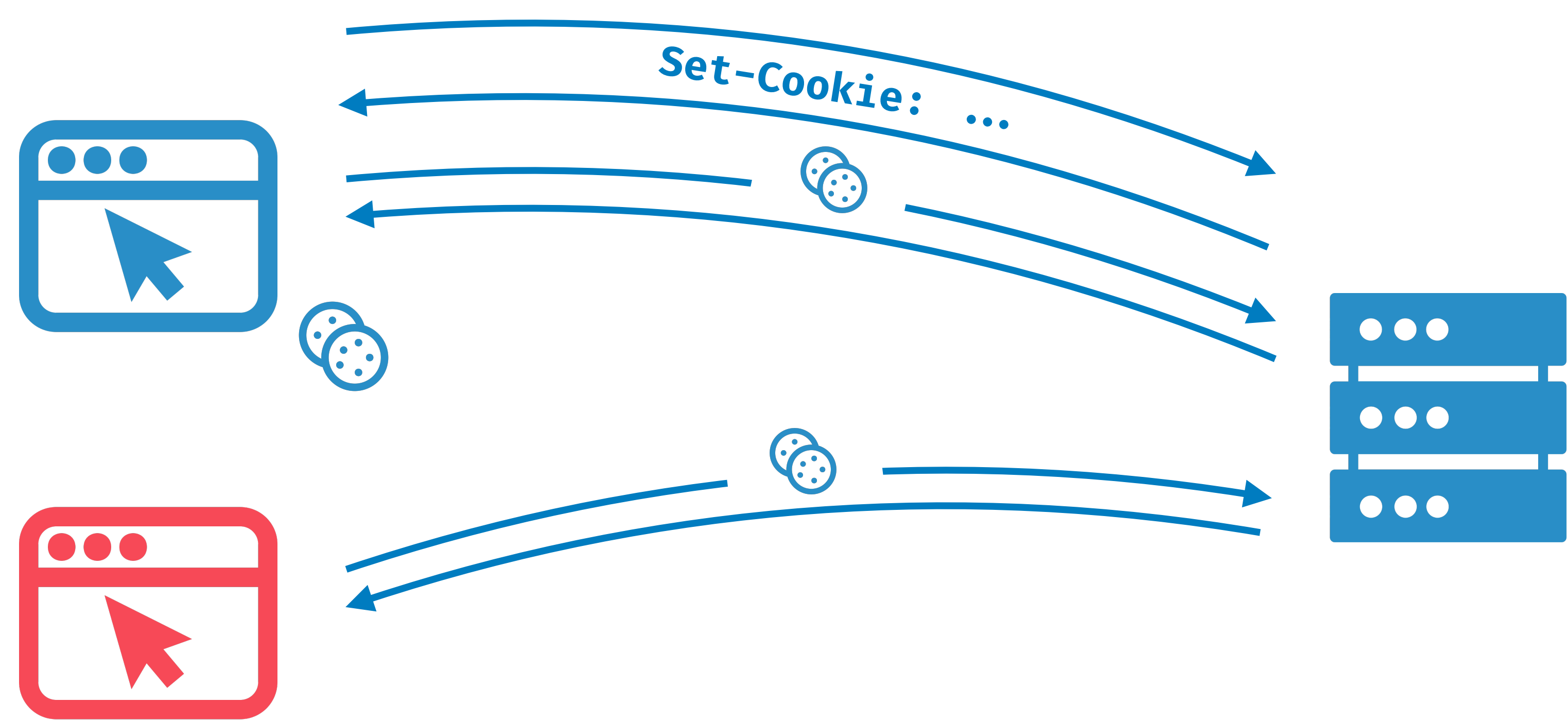
Troy Hunt



**Disallow
third-party cookies!**



Set-Cookie: widget_session=abc123;





Set-Cookie: widget_session=abc123;

**This behaviour leads to
security and privacy concerns**





Set-Cookie: widget_session=abc123; SameSite=None; Secure

Set-Cookie: widget_session=abc123; SameSite=Lax; Secure

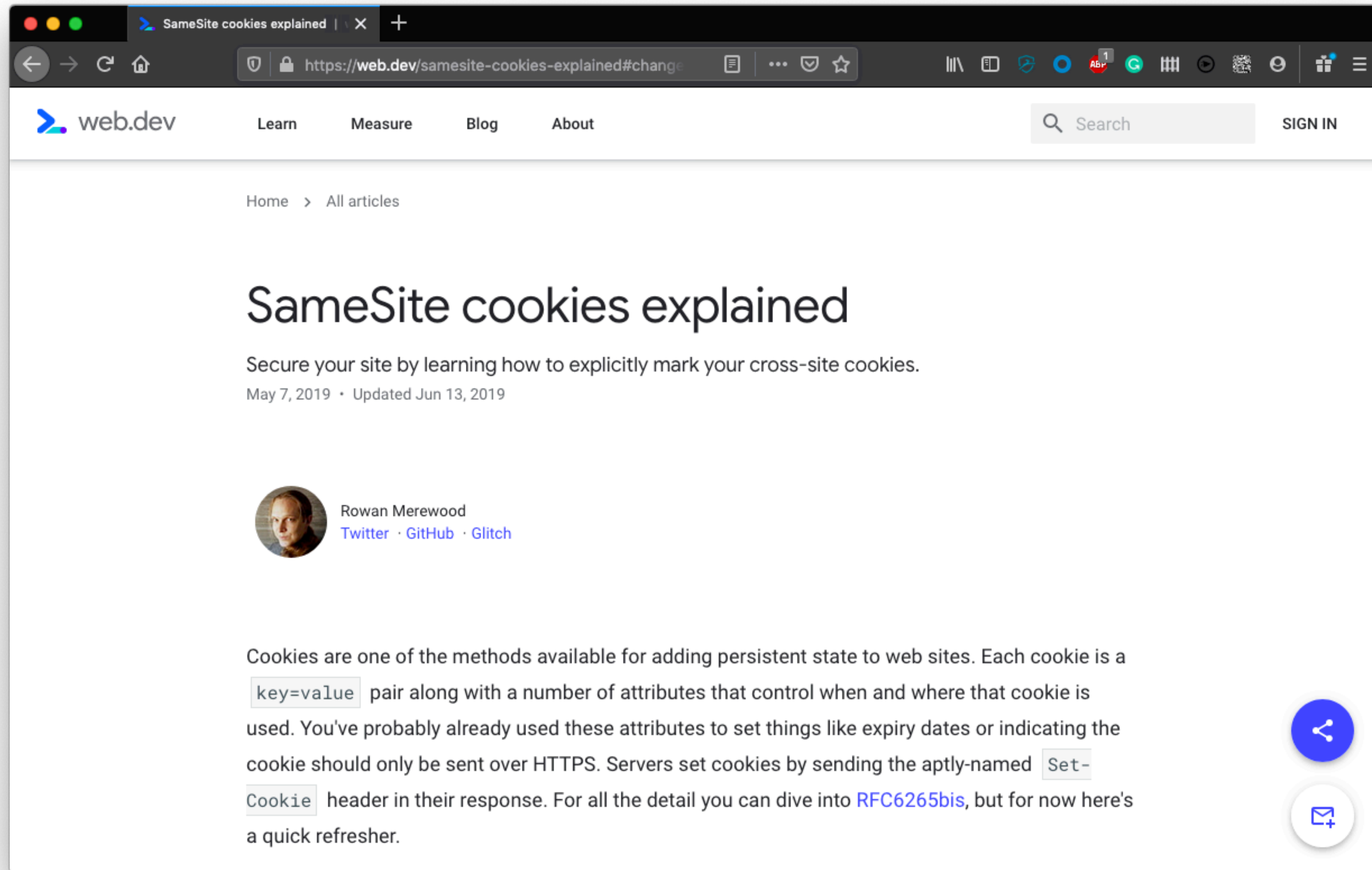
Set-Cookie: widget_session=abc123; SameSite=Strict; Secure

caniuse.com/#feat=same-site-cookie-attribute

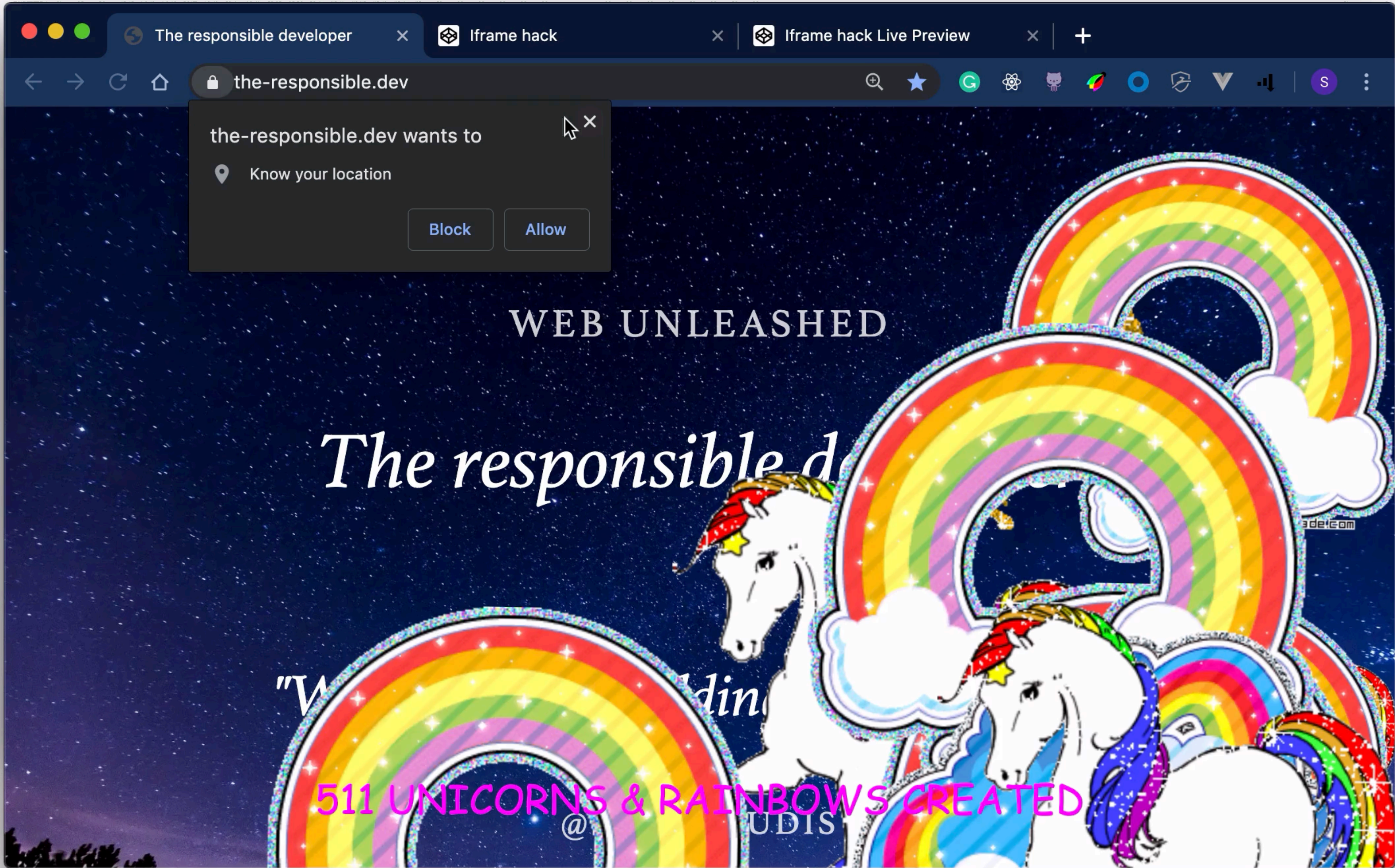


* somewhat ready but maybe buggy

web.dev/samesite-cookies-explained



the-responsible.dev/safe/



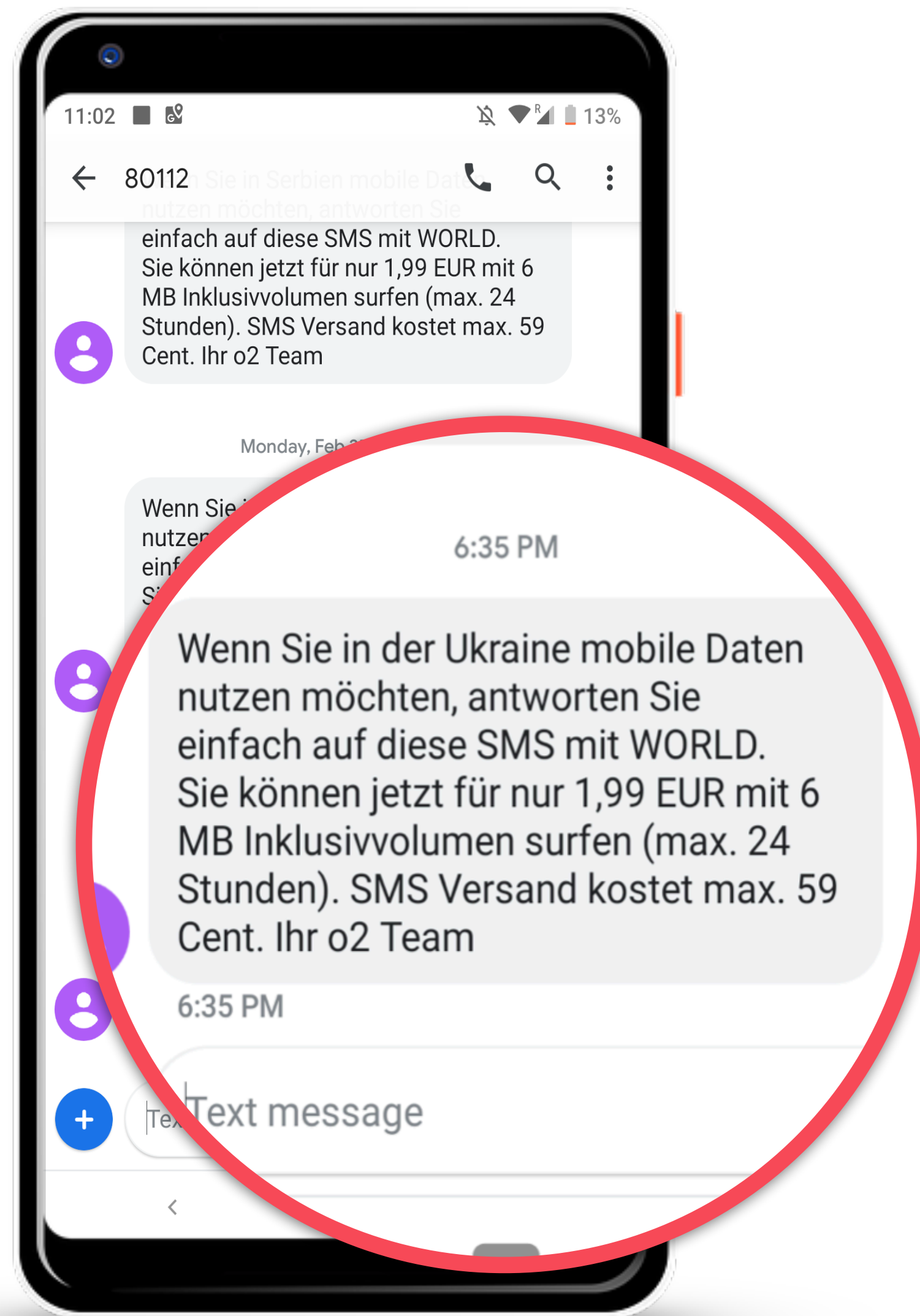


**The web is crucial
for people.**



***Your sh** doesn't
work in Africa.***

William Imoh

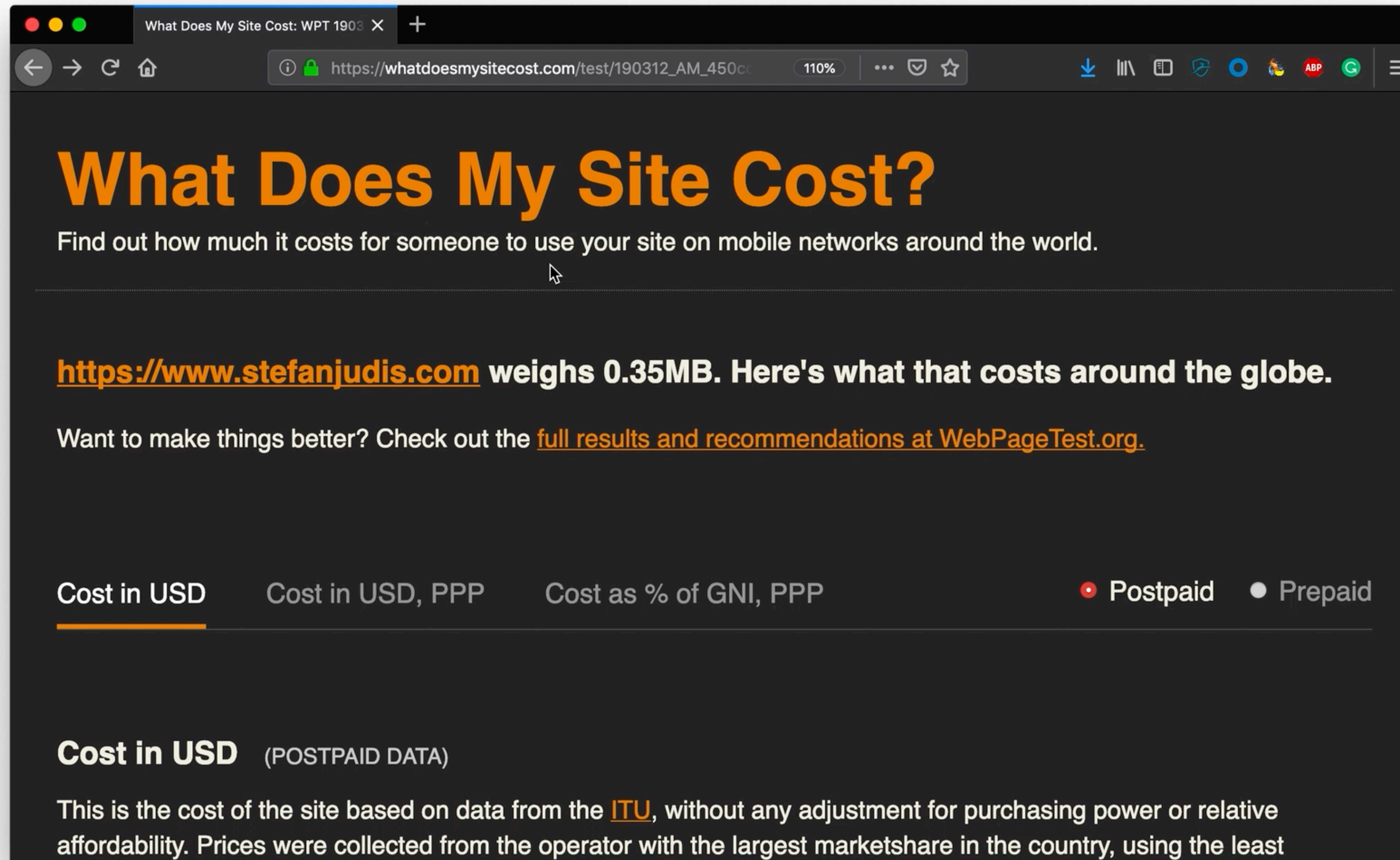




**You get 6MB for 2Euros
but you have only 24h to
use them! Right...**



whatdoesmysitecost.com



The screenshot shows a web browser window with the title 'What Does My Site Cost: WPT 1903'. The address bar shows the URL 'https://whatdoesmysitecost.com/test/190312_AM_450cc' and a zoom level of 110%. The main heading is 'What Does My Site Cost?' in large orange text. Below it, a subtitle reads 'Find out how much it costs for someone to use your site on mobile networks around the world.' The test results for 'https://www.stefanjudis.com' are displayed, stating it weighs 0.35MB. A link to 'full results and recommendations at WebPageTest.org' is provided. At the bottom, there are tabs for 'Cost in USD', 'Cost in USD, PPP', and 'Cost as % of GNI, PPP', with 'Cost in USD' selected. A legend indicates 'Postpaid' is selected over 'Prepaid'. The 'Cost in USD' section is titled '(POSTPAID DATA)' and includes a disclaimer about the data source (ITU) and methodology.

What Does My Site Cost?

Find out how much it costs for someone to use your site on mobile networks around the world.

<https://www.stefanjudis.com> weighs 0.35MB. Here's what that costs around the globe.

Want to make things better? Check out the [full results and recommendations at WebPageTest.org](#).

Cost in USD Cost in USD, PPP Cost as % of GNI, PPP ☒ Postpaid ☐ Prepaid

Cost in USD (POSTPAID DATA)

This is the cost of the site based on data from the [ITU](#), without any adjustment for purchasing power or relative affordability. Prices were collected from the operator with the largest marketshare in the country, using the least



**The web
has to be affordable!**



**Don't request
the same content
over and over again**



Cache-Control:
`max-age=31536000, public`



Cache-Control:

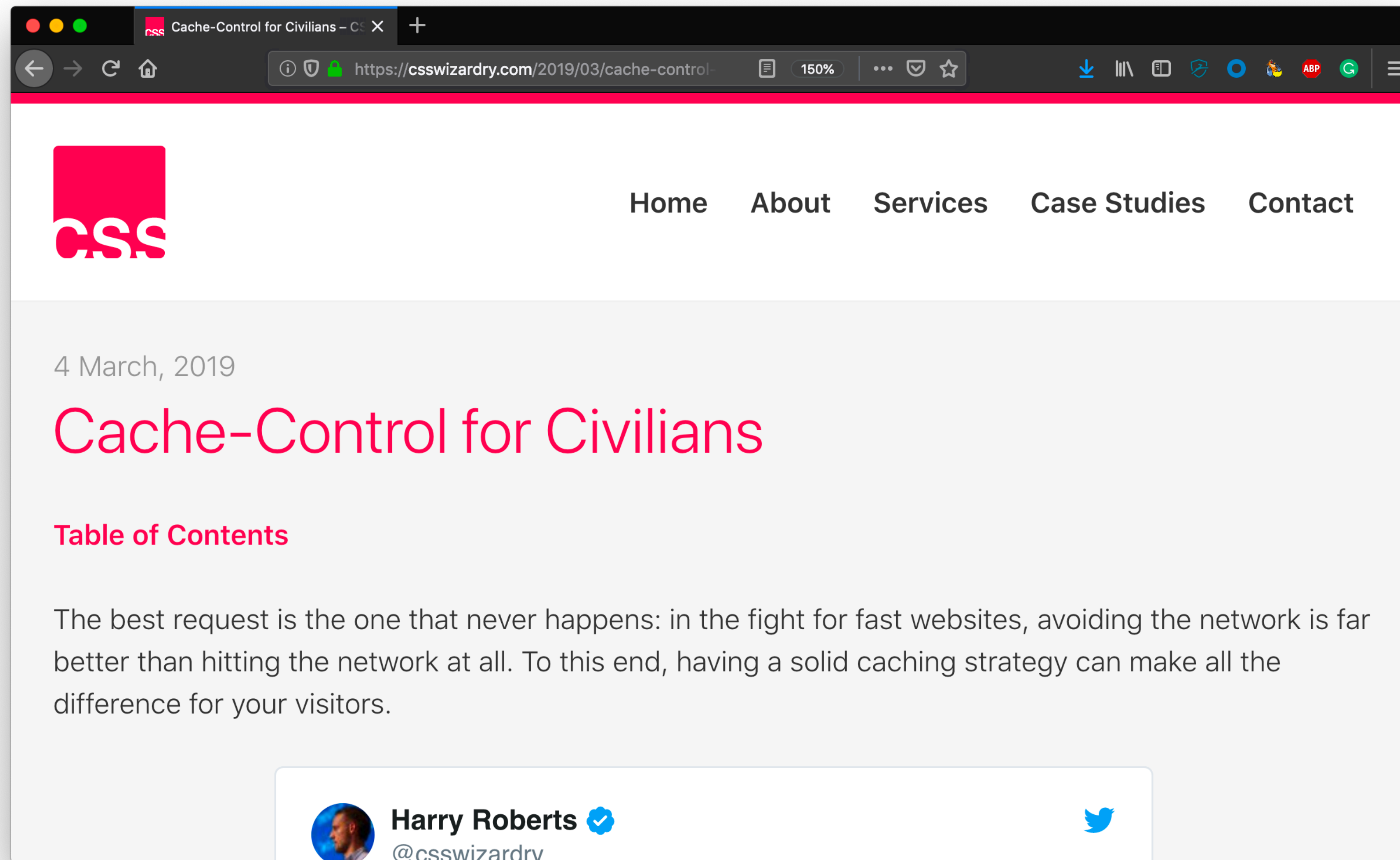
max-age=31536000, public, immutable

immutable

developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control



csswizardry.com/2019/03/cache-control-for-civilians/





Send the right data



Accept-Encoding:
gzip, deflate, br

```
2. sjudis@7510: ~/Projects/the-responsible-developer-express/public (zsh)

🐟 → ll [19:46:56]
-rw-r--r-- 101k sjudis 11 Mar  0:53 styles.12345.css
-rw-r--r--  9.4k sjudis 10 Mar 21:12 styles.12345.css.br
-rw-r--r--  15k sjudis 10 Mar 21:12 styles.12345.css.gz
```



Stefan Judis
@stefanjudis



I love these kind of stats. ❤️

A reduction of 9KB for the shipped JavaScript on Wikipedia's scale will lead to 1.4 Terrabytes that don't need to go over the wire. 😲

phabricator.wikimedia.org/phame/live/7/p...

[Tweet übersetzen](#)

We have around 363,000 page views a minute in total on Wikipedia and sister projects. That's 21.8M an hour, or 523 million every day ([User pageview stats](#)). This week's deployment saves around 1.4 Terabytes a day. In total, the year-long effort is saving **ALT** rabytes a day of bandwidth on our users' page views.


```
2. sjudis@7510: ~/Projects/the-responsible-developer-express/public (zsh)

🐟 → ll [19:46:56]
-rw-r--r-- 101k sjudis 11 Mar  0:53 styles.12345.css
-rw-r--r--  9.4k sjudis 10 Mar 21:12 styles.12345.css.br
-rw-r--r--  15k sjudis 10 Mar 21:12 styles.12345.css.gz
```

***But Brotli compression
is so slow!***



GZIP

vs

Brotli

GZIP

vs

Brotli



GZIP

vs

Brotli



GZIP

vs

Brotli



6

Default
Mode



11

GZIP

vs

Brotli

Default
Mode



6

11

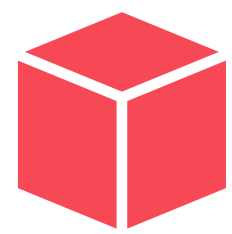


GZIP

vs

Brotli

Default
Mode



6

11



GZIP

vs

Brotli

Optimal
middle
ground



6

4



GZIP

vs

Brotli

**Brotli tends to
compress better
with the same speed**

4

6

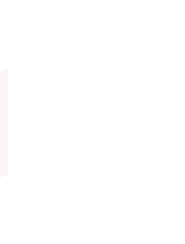
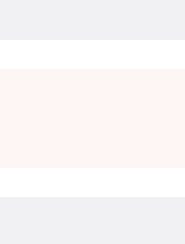
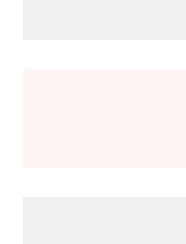
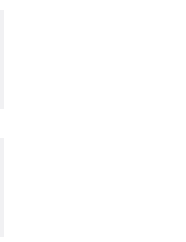
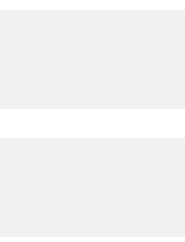
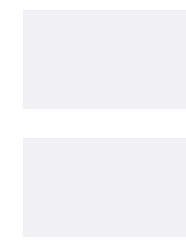
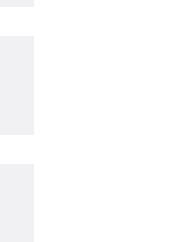


GZIP

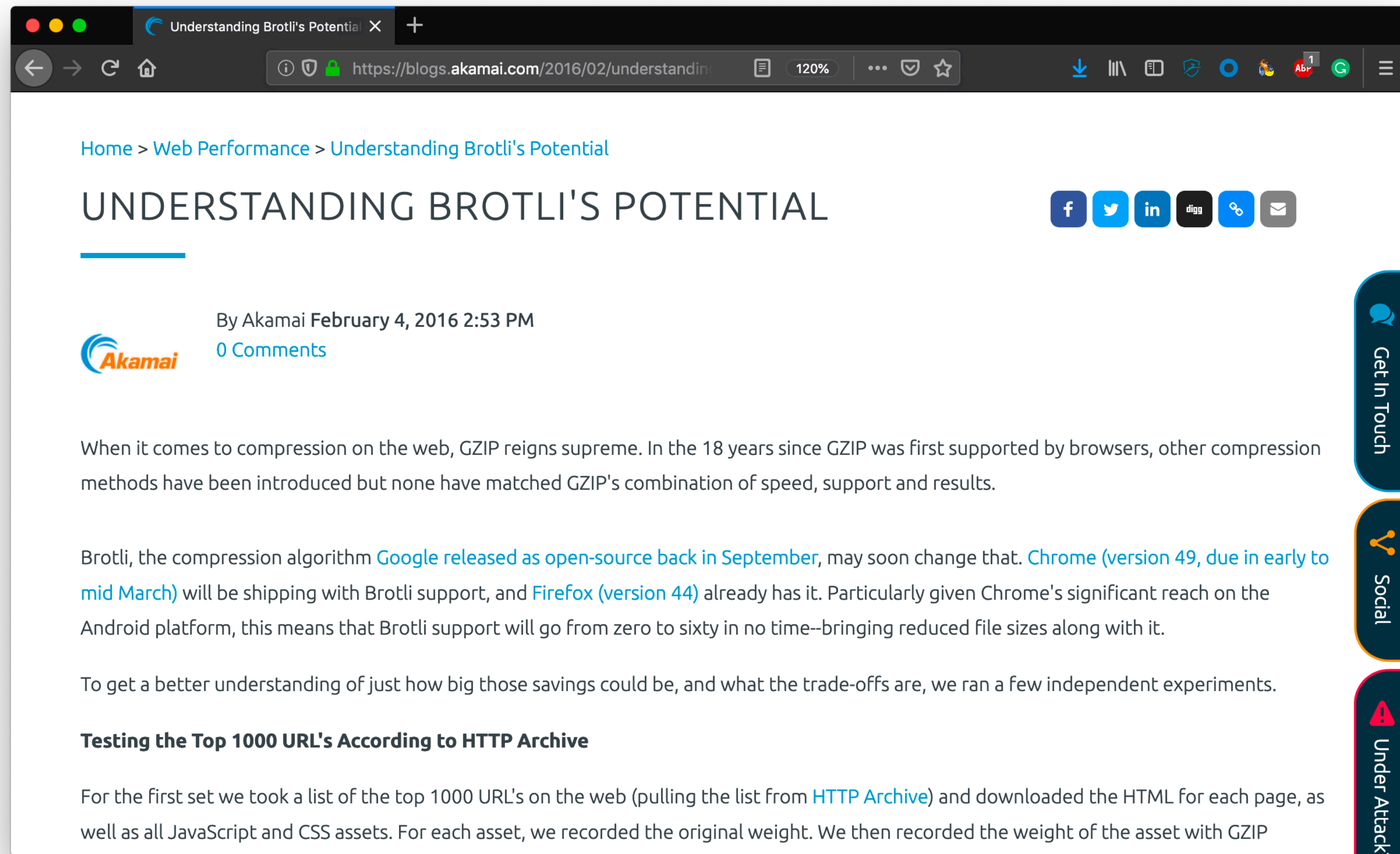
vs

Brotli

**You don't have
to do it on the fly...**



blogs.akamai.com/2016/02/understanding-brotli-potential.html



caniuse.com/#feat=brotli





Facebook

Search

Stefan Home Create

Morela Zulauf Chat

Inspector Console Debugger Network

Filter URLs

Persist Logs Disable cache

All HTML CSS JS XHR Fonts Images Media WS Other

Stat...	Met...	File	Type	Transferred	Size	C
200	GET	/	html	179.82 kB	1.57 MB	br
200	POST	bz	html	7.23 kB	0 B	
200	POST	bz	html	3.17 kB	0 B	
200	POST	bz	html	4.09 kB	0 B	
200	GET	CTOU17YZVwh.css?_nc_x=kRPDusB...	css	8.64 kB	67.25 kB	br
200	GET	lwnCL9T3TvH.css?_nc_x=kRPDusB9...	css	4.22 kB	20.10 kB	br
200	GET	zHWCd luswD.css?_nc_x=kRPDusB...	css	15.05 kB	101.98 kB	br
287 requests				16.53 MB / 5.67 MB transferred		Finish: 24.02 s

DOMContentLoaded

Google

w.google.com

Console Network

Persist Logs Disable cache

XHR Fonts Images Media WS Other

	Type	Transferred	Size	C		
	html	61.67 kB	212.49 kB	br		
0.png	png	24.05 kB	23.64 kB			
archbox_sprites302_hr.png	png	1.03 kB	665 B			
webhp&t=aft&atyp=csi...	html	370 B	0 B			
0.png	png	8.15 kB	7.77 kB			
	jpeg	4.26 kB	3.76 kB			
an-grams-166th-birthda...	png	53.48 kB	53.09 kB			
13 requests				1.10 MB / 436.95 kB transferred		Finish: 901 ms

DOMContentLoaded



Serve tailored media


```
<picture>
  <!-- serve WebP to Chrome and Opera -->
  <source
    media="(min-width: 50em)"
    sizes="50vw"
    srcset="/image/thing-200.webp 200w, /image/thing-400.webp 400w,
      /image/thing-800.webp 800w, /image/thing-1200.webp 1200w,
      /image/thing-1600.webp 1600w, /image/thing-2000.webp 2000w"
    type="image/webp">
  <source
    sizes="(min-width: 30em) 100vw"
    srcset="/image/thing-crop-200.webp 200w, /image/thing-crop-400.webp 400w,
      /image/thing-crop-800.webp 800w, /image/thing-crop-1200.webp 1200w,
      /image/thing-crop-1600.webp 1600w, /image/thing-crop-2000.webp 2000w"
    type="image/webp">
  <!-- serve JPEG to others -->
  <source
    media="(min-width: 50em)"
    sizes="50vw"
    srcset="/image/thing-200.jpg 200w, /image/thing-400.jpg 400w,
      /image/thing-800.jpg 800w, /image/thing-1200.jpg 1200w,
      /image/thing-1600.jpg 1600w, /image/thing-2000.jpg 2000w">
  <source
```



Accept:
image/webp,
image/apng,
image/*,*/*; q=0.8

caniuse.com/#feat=webp





Accept-CH: Width, Viewport-Width
Accept-CH-Lifetime: 100



Accept-CH: Width, Viewport-Width
Accept-CH-Lifetime: 100

Request URL: https://.../header.jpg
Viewport-Width: 980
Width: 980



```

```



```

```

Accept: image/webp,image/apng,image/*,*/*;q=0.8

Request URL: https://.../header.jpg

Viewport-Width: 980

Width: 980



```

```



```

```

Accept: image/webp,image/apng,image/*,*/*;q=0.8

Request URL: https://.../header.jpg

Viewport-Width: 980

Width: 1960



```

```

**Serve a tailored version
via server/service worker**

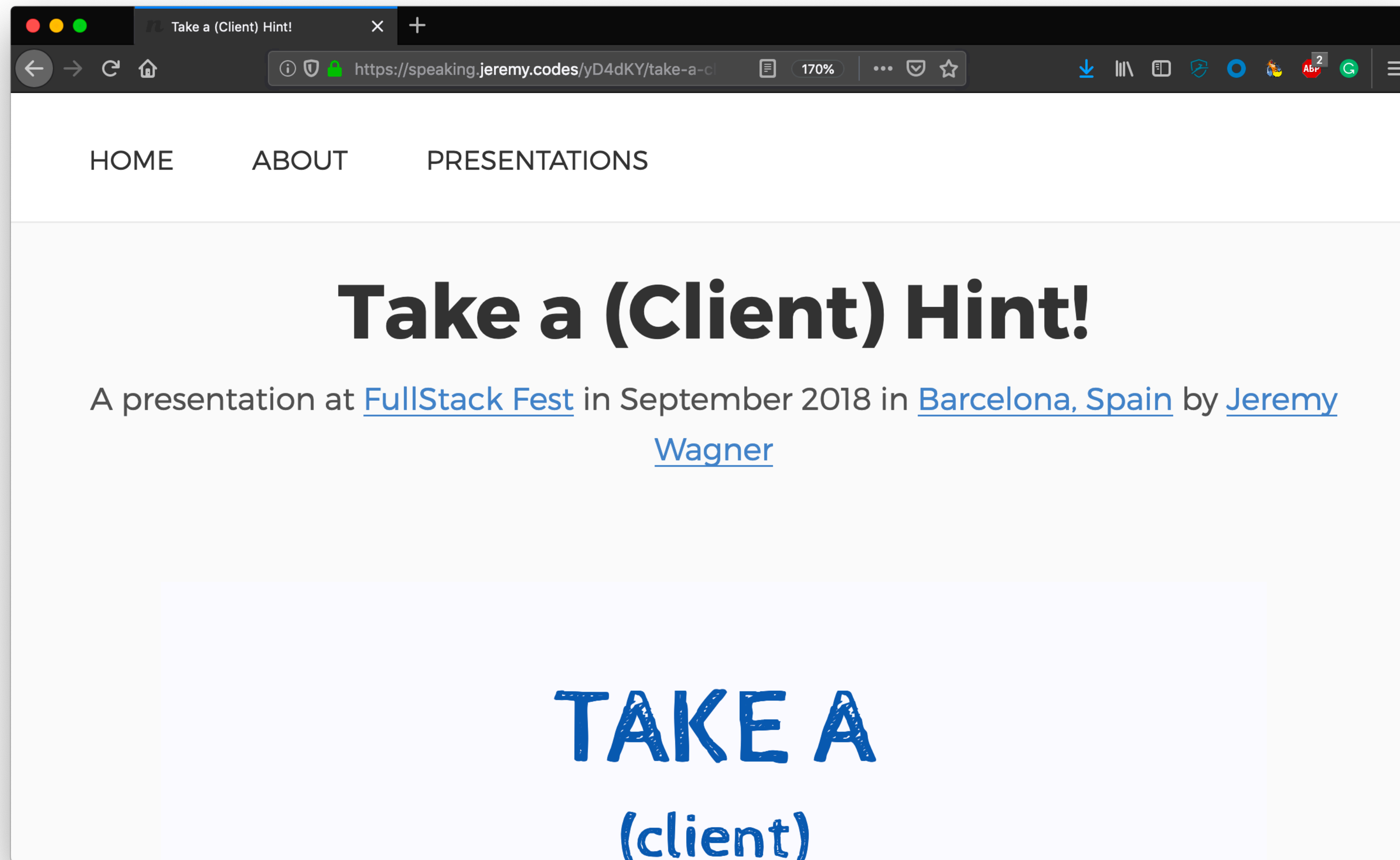
Accept: image/webp, image/apng, image/*;q=0.8

Request URL: https://.../header.jpg

viewport: 330px

Width: 1064

speaking.jeremy.codes/yD4dKY/take-a-client-hint





Save data



save-data: on



save-data: on

```
if ("connection" in navigator) {  
    if (navigator.connection.saveData === true) {  
        // Implement data saving operations here.  
    }  
}
```





**Let's use the platform
and make these
features more visible**



https://....



Save
data?



https://....

**We should provide an
easy way to save data!**

Save
data?



https://....



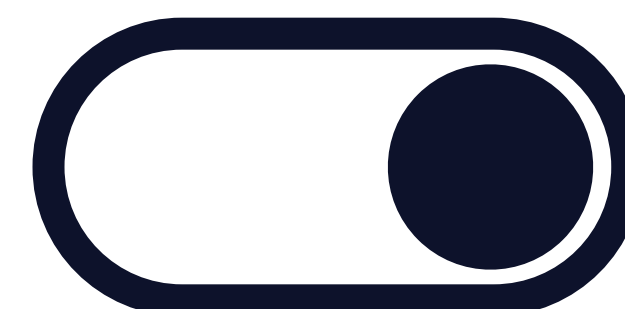
Save
data?



https://....



Prefer a dark
interface?



Prefer reduced
motion?

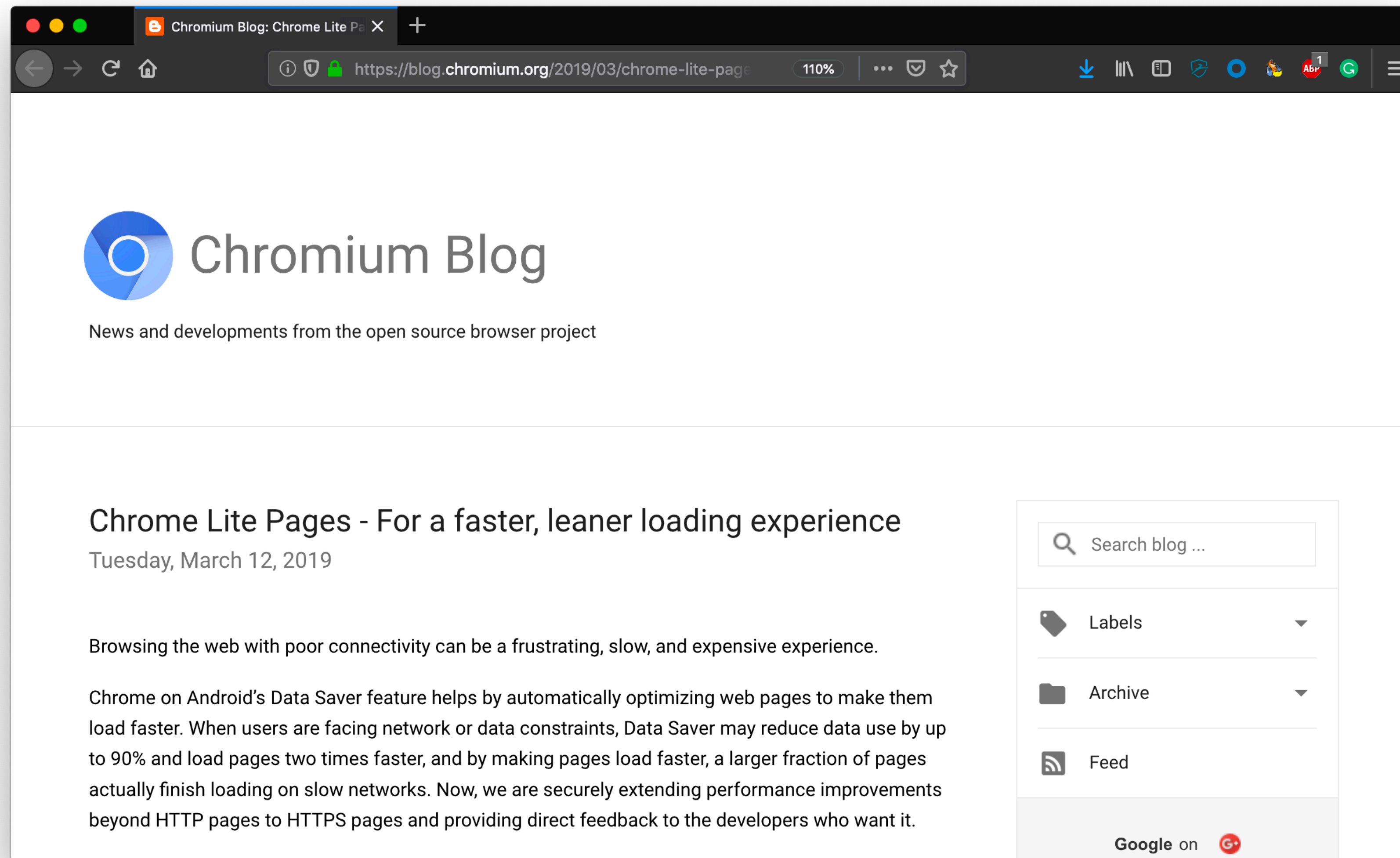


Save
data?

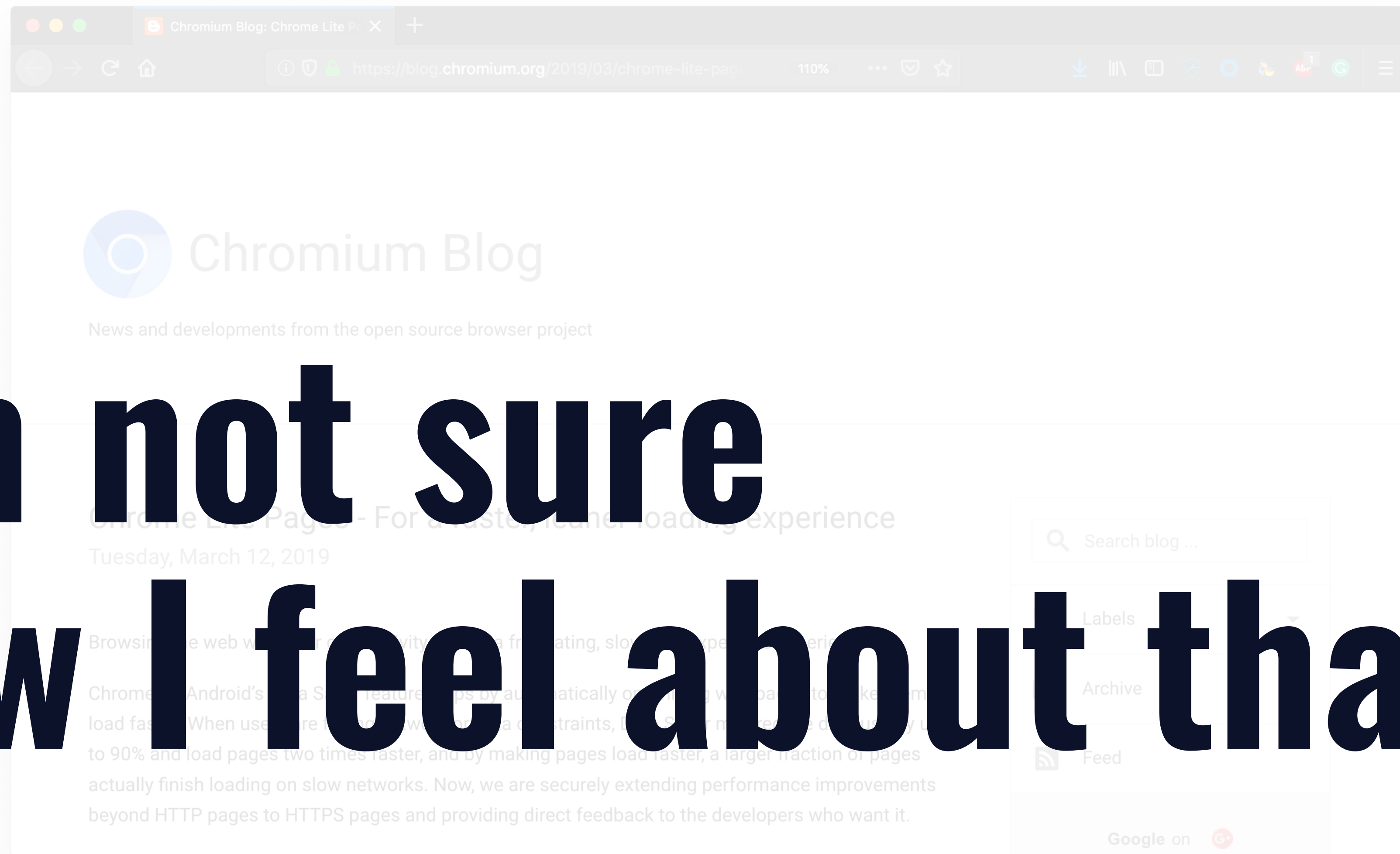


**All these settings should
be easily accessible all
the time!**

blog.chromium.org/2019/03/chrome-lite-pages-for-faster-leaner.html



blog.chromium.org/2019/03/chrome-lite-pages-for-faster-leaner.html



**I'm not sure
how I feel about that...**



Cache-Control:

max-age=31536000, public, no-transform



**Be aware of CDNs and
proxies – use vary**



Brendan Abbott

@brend0



[@tkadlec shopify.com](#) is now Save-Data aware. About a 13% reduction in page weight, [webpagetest.org/video/compare....](#)

Early data shows 20% of Indian/Brazilian requests contain this header so happy days [#webperf](#) 🎉

[Tweet übersetzen](#)





Brendan Abbott

@brend0

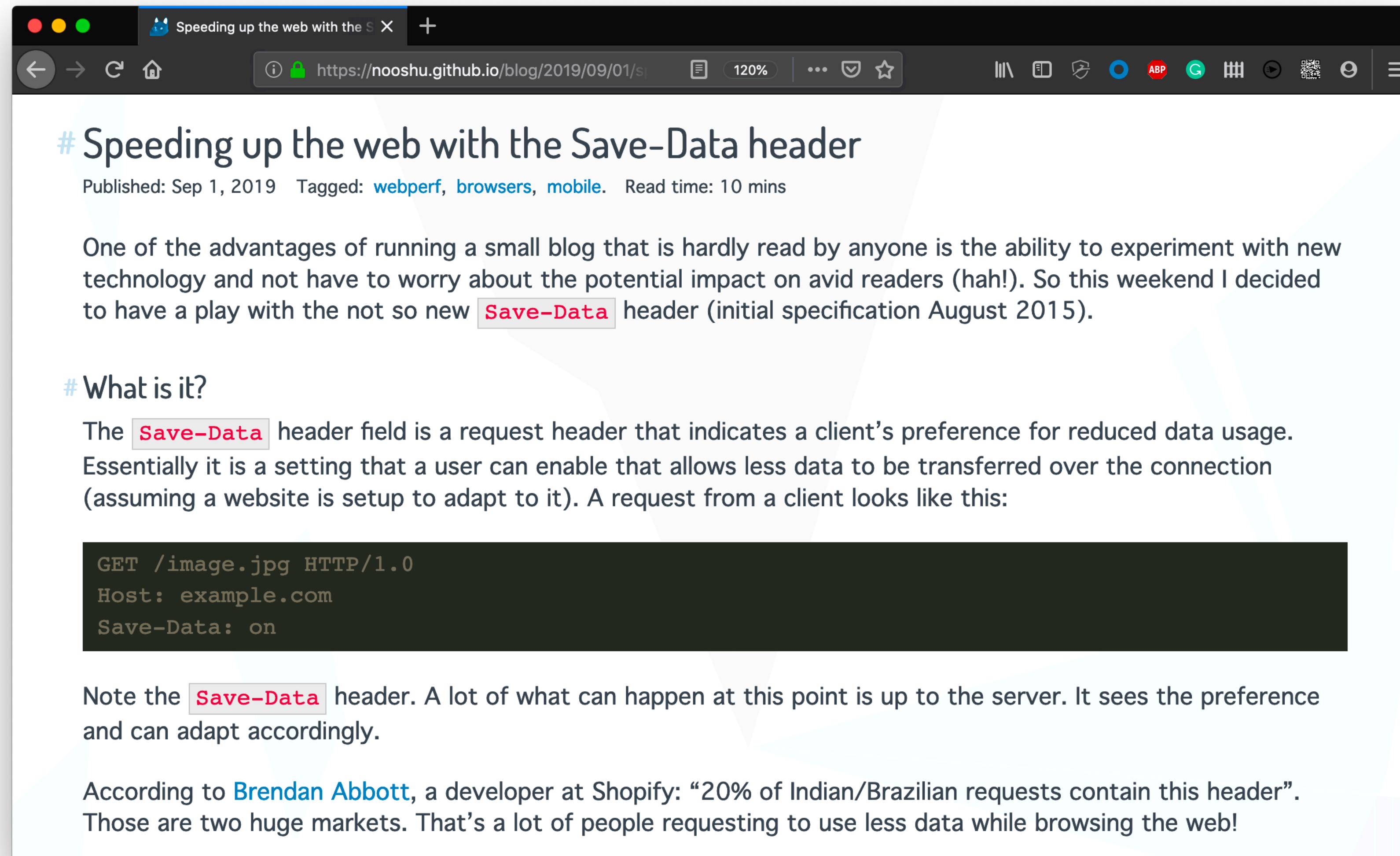
@tkadlec [shopify.com](#) is now Save-Data aware. About a 13% reduction in page weight, [webpagetest.org/video/compare....](#)

Early data shows 20% of Indian/Brazilian requests contain this header so happy days [#webperf](#) 🎉

20% of requests...



<https://nooshu.github.io/blog/2019/09/01/speeding-up-the-web-with-save-data-header/>

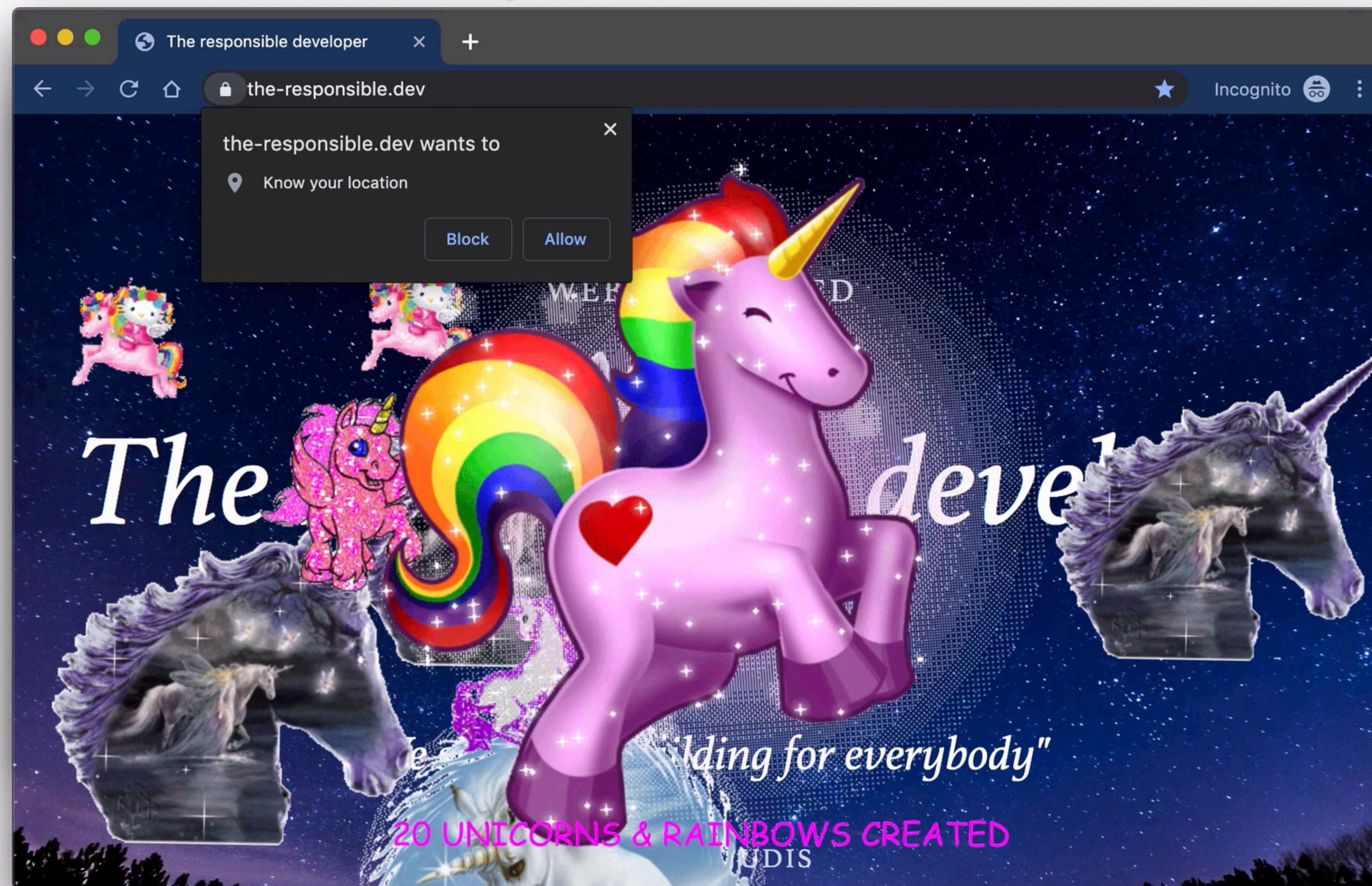




Less Data Doesn't Mean a Lesser Experience

@tkadlec

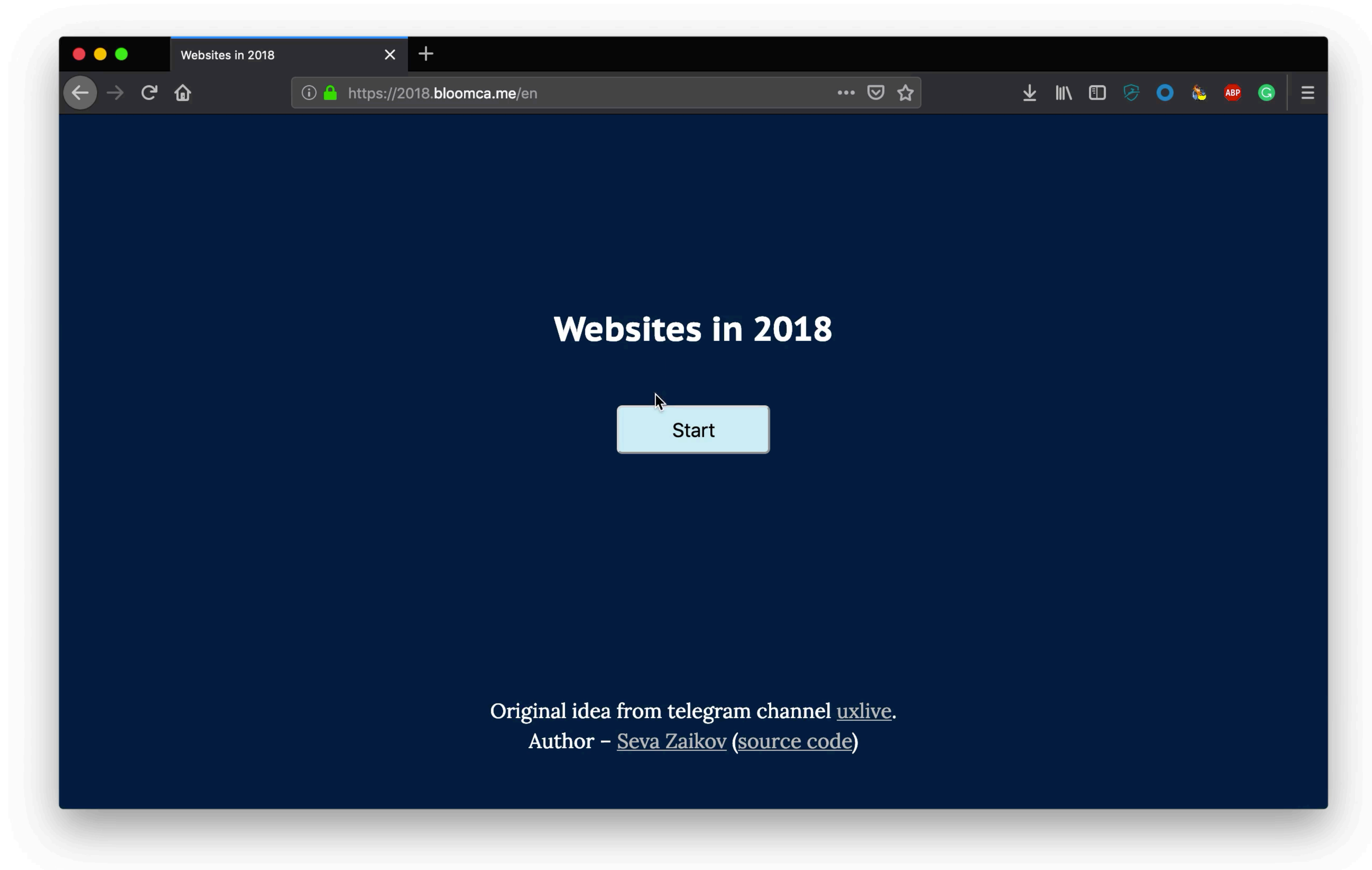
the-responsible.dev/affordable/





**The web is
with us every day**

2018.bloomca.me





It has to be respectful!



**Get stuff "down" as
quickly as possible**



```
<link rel="preload" href="/unleashed.jpg" as="image">
```

Link:

```
</unleashed.jpg>; rel=preload; as=image
```



```
<link rel="preload" href="/unleashed.jpg" as="image">
```

Link:

```
</unleashed.jpg>; rel=preload; as=image; no-push
```



```
<link rel="preload" href="/unleashed.jpg" as="image">
```

**This is great to speed
up critical resources**

Link:

```
<link rel="preload" href="/unleashed.jpg" as="image" no-push>
```


caniuse.com/#feat=link-rel-preload




* behind a flag




**Don't annoy the user
(aka. the AMP reaction)**


speakerdeck.com/stefanjudis/amp-tries-to-fix-the-web-what-can-we-learn-from-it?slide=112

AMP tries to fix the web - What can we learn from it



AMP tries to fix the web - What can we learn from it






"We need to come up with a standard alternative real quick"

Yoav Weiss
Akamai

<https://twitter.com/yoavweiss/status/659141410990350336>

 stefan judis

November 12, 2016

Technology

☆ 2

👁 300

📄



Feature-Policy:
vibrate 'none'; geolocation 'none'

developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

accelerometer

gyroscope

picture-in-picture

ambient-light-sensor

legacy-image-formats

speaker

autoplay

layout-animations

sync-xhr

camera

magnetometer

unoptimized-images

document-domain

microphone

unsized-media

encrypted-media

midi

usb

fullscreen

oversized-images

vibrate

geolocation

payment

vr

developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

accelerometer 

ambient-light-sensor 

autoplay 

camera 

document-domain 

encrypted-media 

fullscreen 

geolocation 

gyroscope 

legacy-image-formats 

layout-animations 

magnetometer 

microphone 

midi 

oversized-images 

payment 

picture-in-picture 

speaker 

sync-xhr 

unoptimized-images 

unsized-media 

usb 

vibrate 

vr 

developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

accelerometer 

ambient-light-sensor 

autoplay 

camera 

document-domain 

encrypted-media 

fullscreen 

geolocation 

gyroscope 

legacy-image-formats 

layout-animations 

magnetometer 

microphone 

midi 

oversized-images 

payment 

picture-in-picture 

speaker 

sync-xhr 

unoptimized-images 

unsized-media 

usb 

vibrate 

vr 



feature-policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment 'none'; usb 'none'



```
<iframe allow="camera 'none'; microphone 'none'">
```

```
document.featurePolicy.allowedFeatures();  
// → ["geolocation", "midi", ...]
```

```
document.featurePolicy.allowsFeature('geolocation');  
// → true
```

```
document.featurePolicy.getAllowlistForFeature('geolocation');  
// → ["https://example.com"]
```



**What happened to the
most annoying one?**

<https://github.com/w3c/webappsec-feature-policy/issues/243>

The screenshot shows a web browser window displaying a GitHub issue page. The browser's address bar shows the URL `https://github.com/w3c/webappsec-` and the page title is "What happened to 'notifications'? #243". The GitHub navigation bar at the top includes a search bar, "Pull requests", "Issues", "Marketplace", and "Explore". The repository path is `w3c / webappsec-feature-policy`, with 40 watchers, 173 stars, and 39 forks. The "Issues" tab is selected, showing 101 issues. The issue title is "What happened to 'notifications'? #243", marked as "Open", and was opened by `annevk` on 14 Nov 2018 with 9 comments. The issue body contains two comments from `annevk`, both dated 14 Nov 2018. The first comment, with a "Member" role, asks if a feature was dropped during migration. The second comment, with "Author" and "Member" roles, asks if the problem is primarily with push notifications. The right sidebar shows sections for "Assignees" (No one assigned), "Labels" (None yet), "Projects" (None yet), and "Milestone".

What happened to "notifications"? #243

Open `annevk` opened this issue on 14 Nov 2018 · 9 comments

`annevk` commented on 14 Nov 2018 Member

It was added in [#3](#) / [#33](#), but got dropped since then. Maybe while migrating the features out of the main document it got lost?

cc [@johannhof](#)

`annevk` commented on 14 Nov 2018 Author Member

Is the problem here perhaps primarily with push notifications, which you cannot really delegate? (This

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone

caniuse.com/#feat=feature-policy

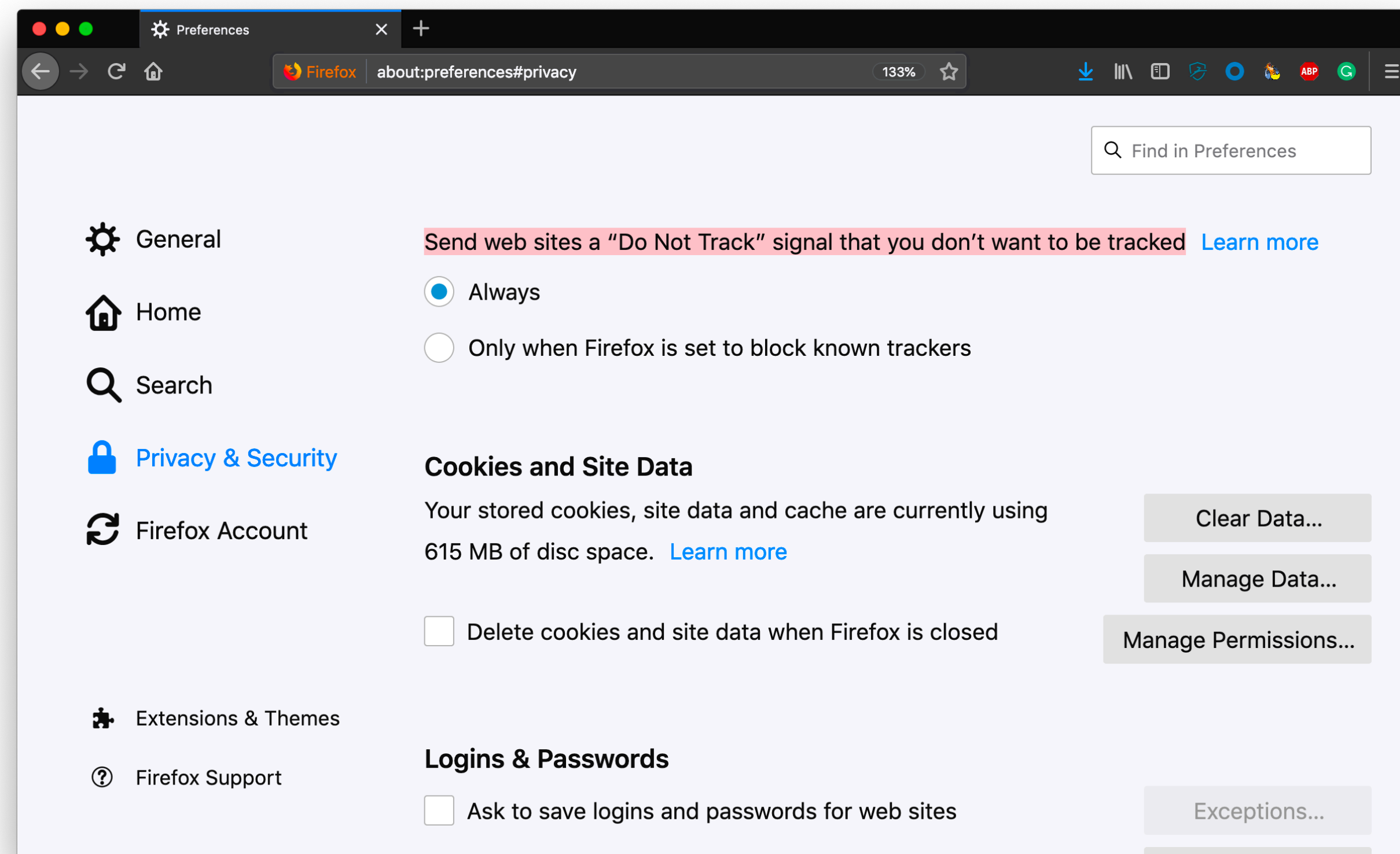
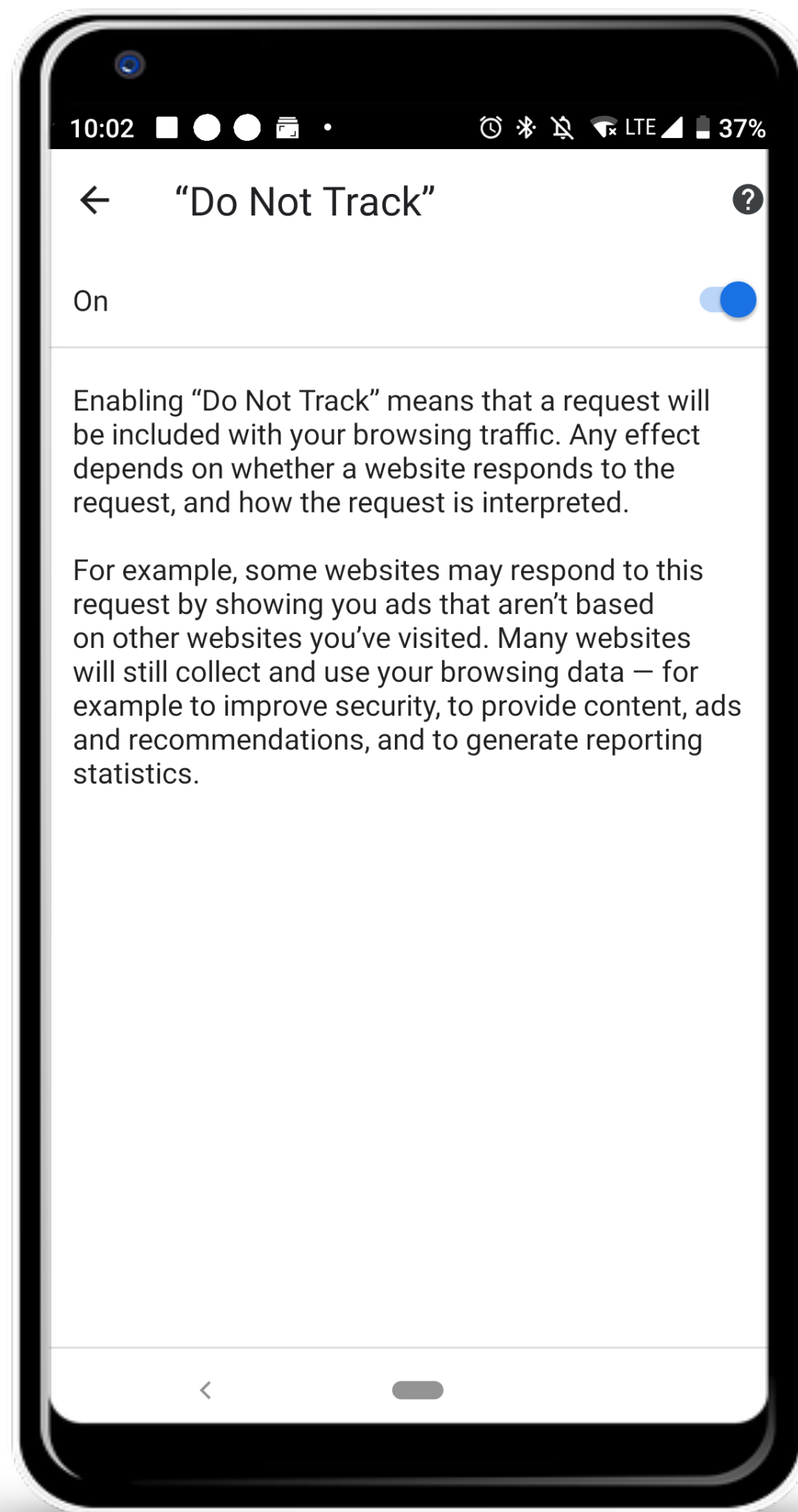


* support for **Feature-Policy** header, **allow** on iframes, and JS API behind a flag

** support only for **allow** on iframes



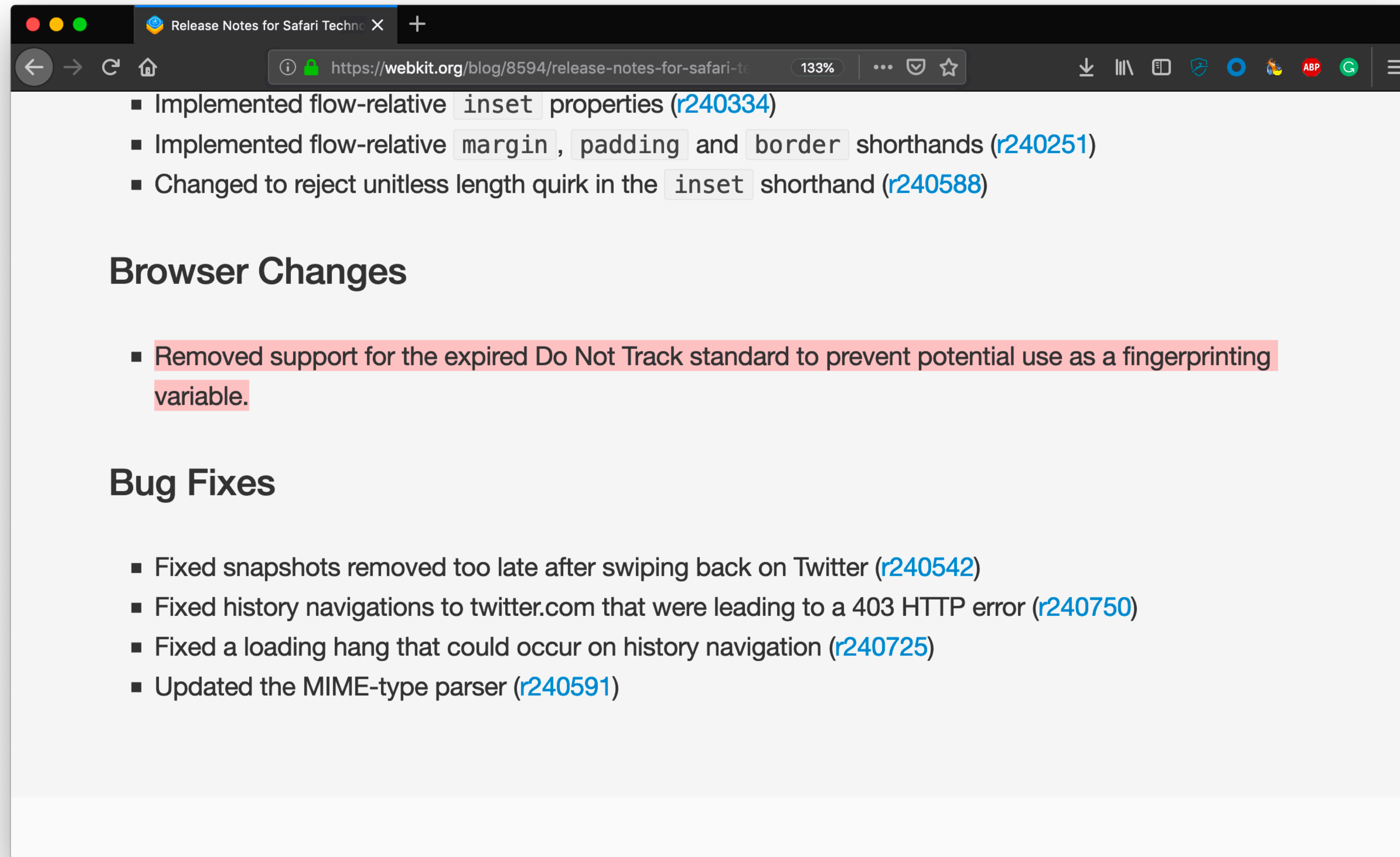
Respect privacy



caniuse.com/#feat=do-not-track



webkit.org/blog/8594/release-notes-for-safari-technology-preview-75/

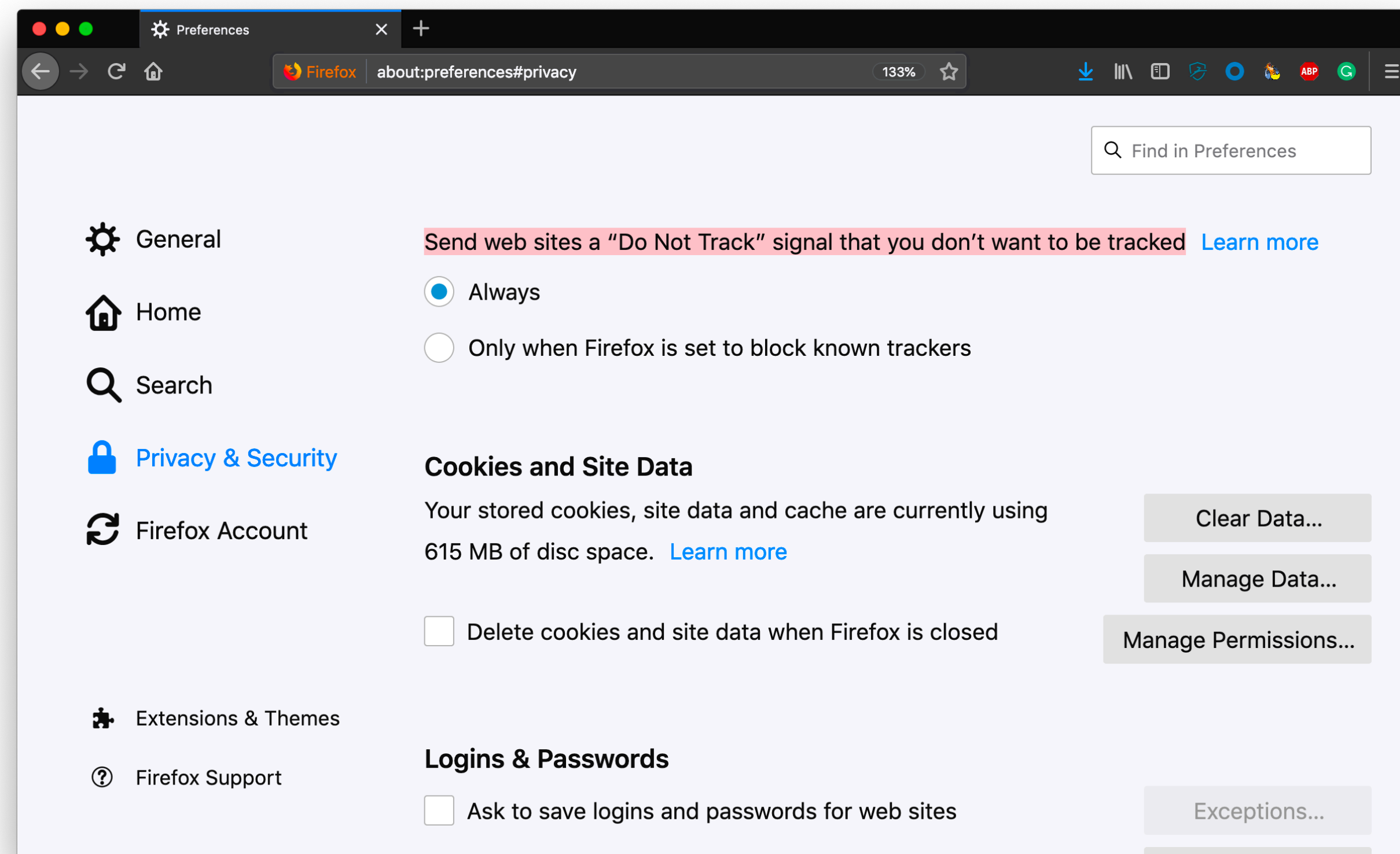
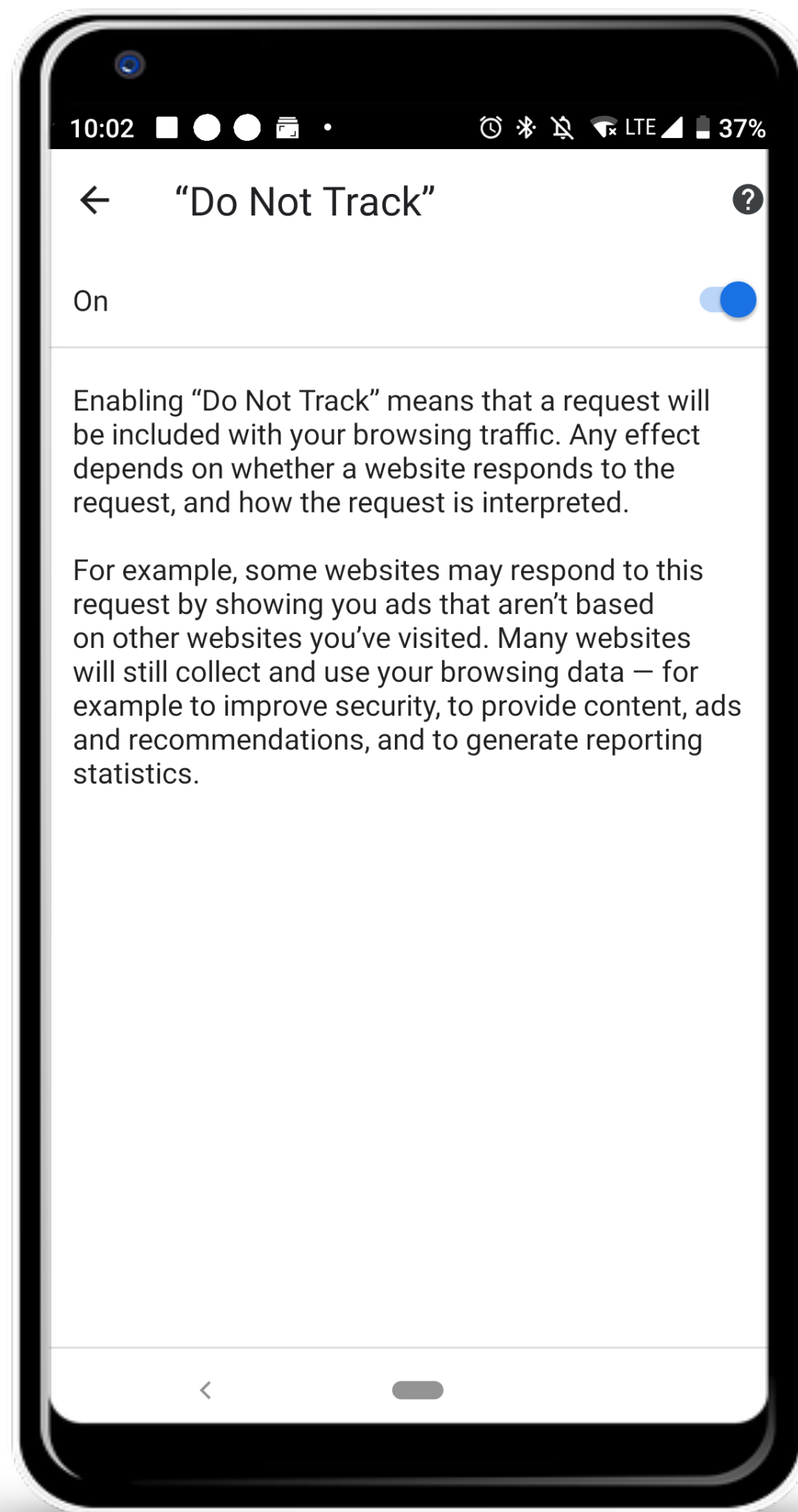


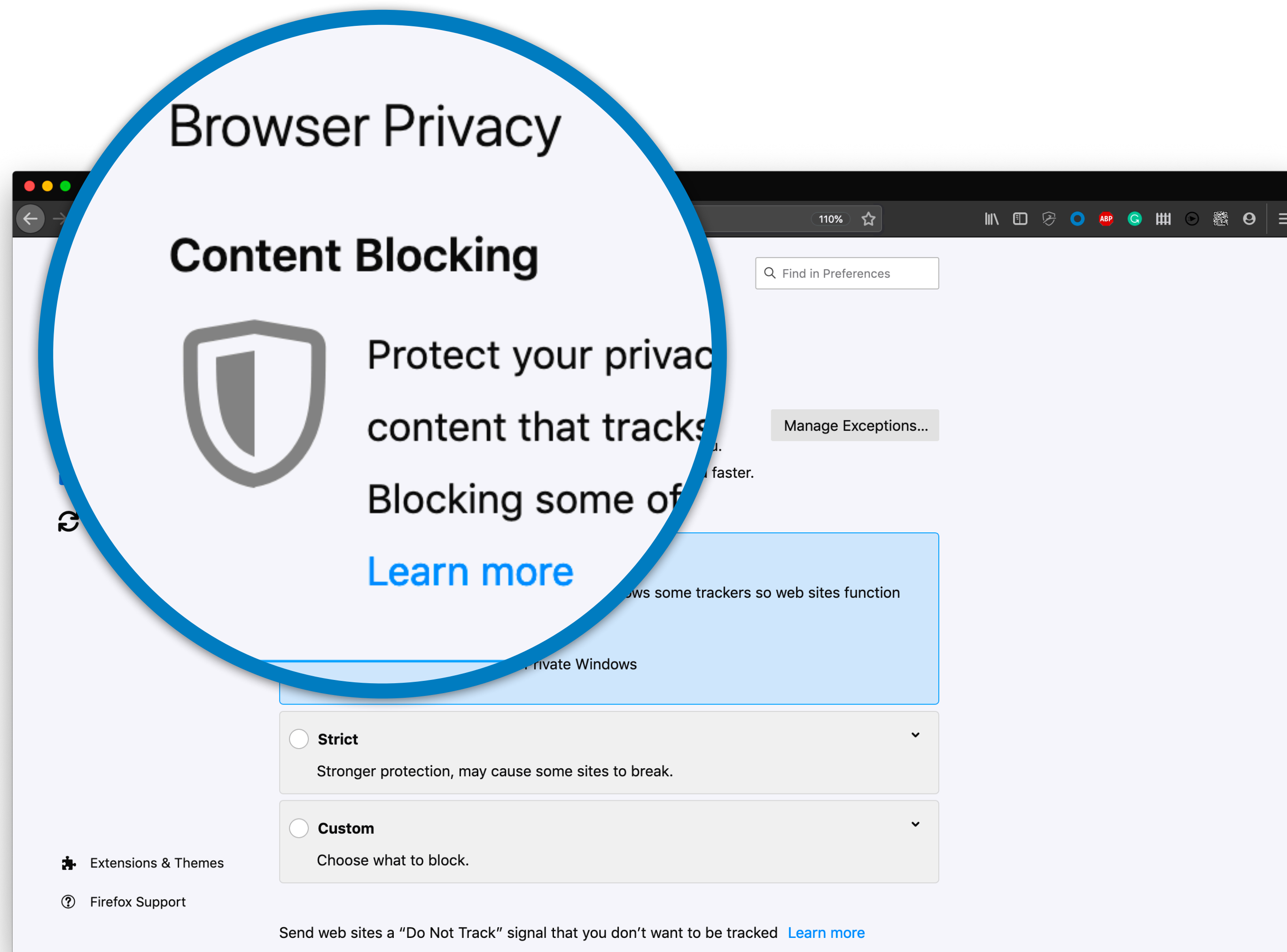
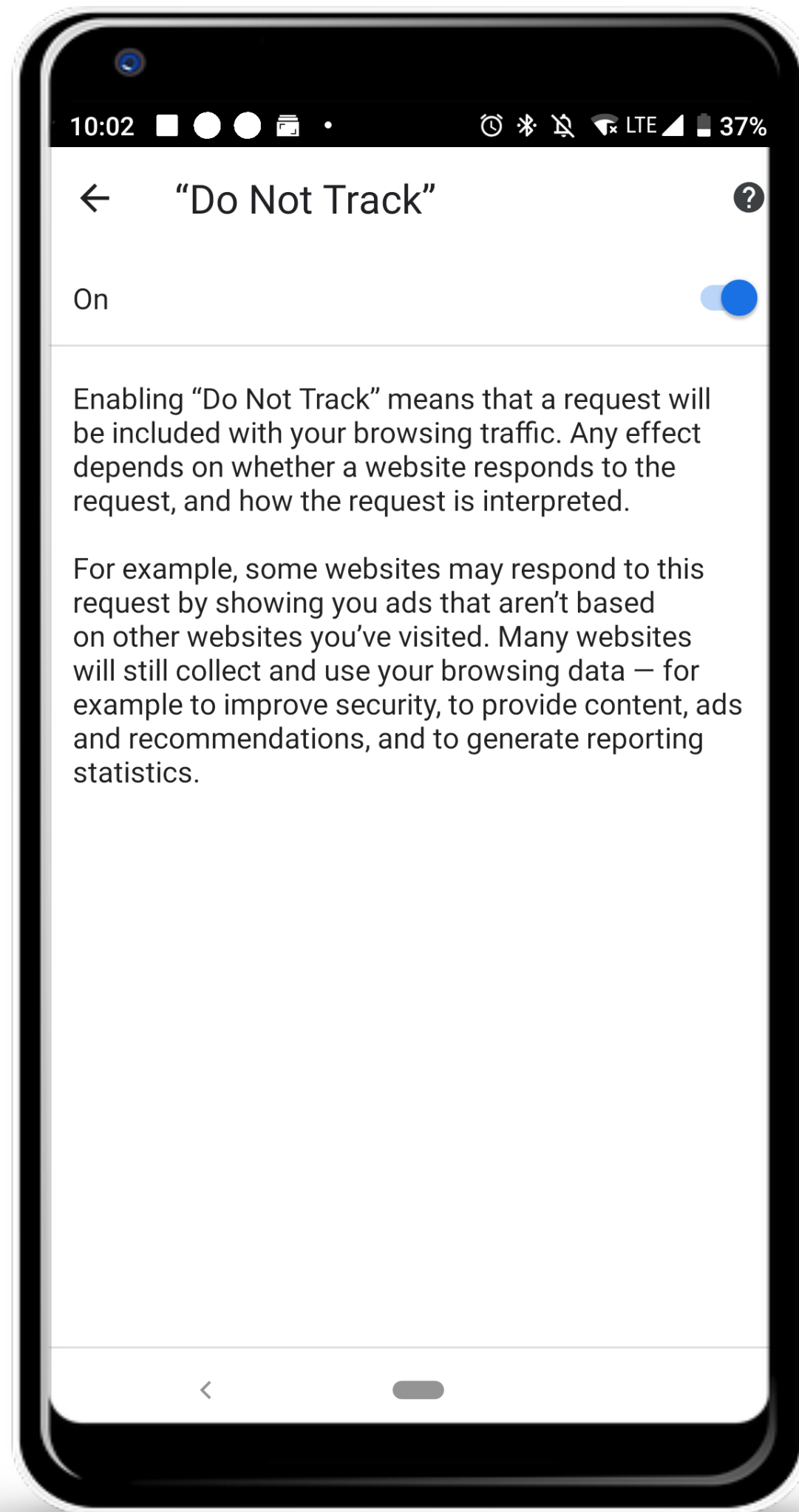
caniuse.com/#feat=do-not-track

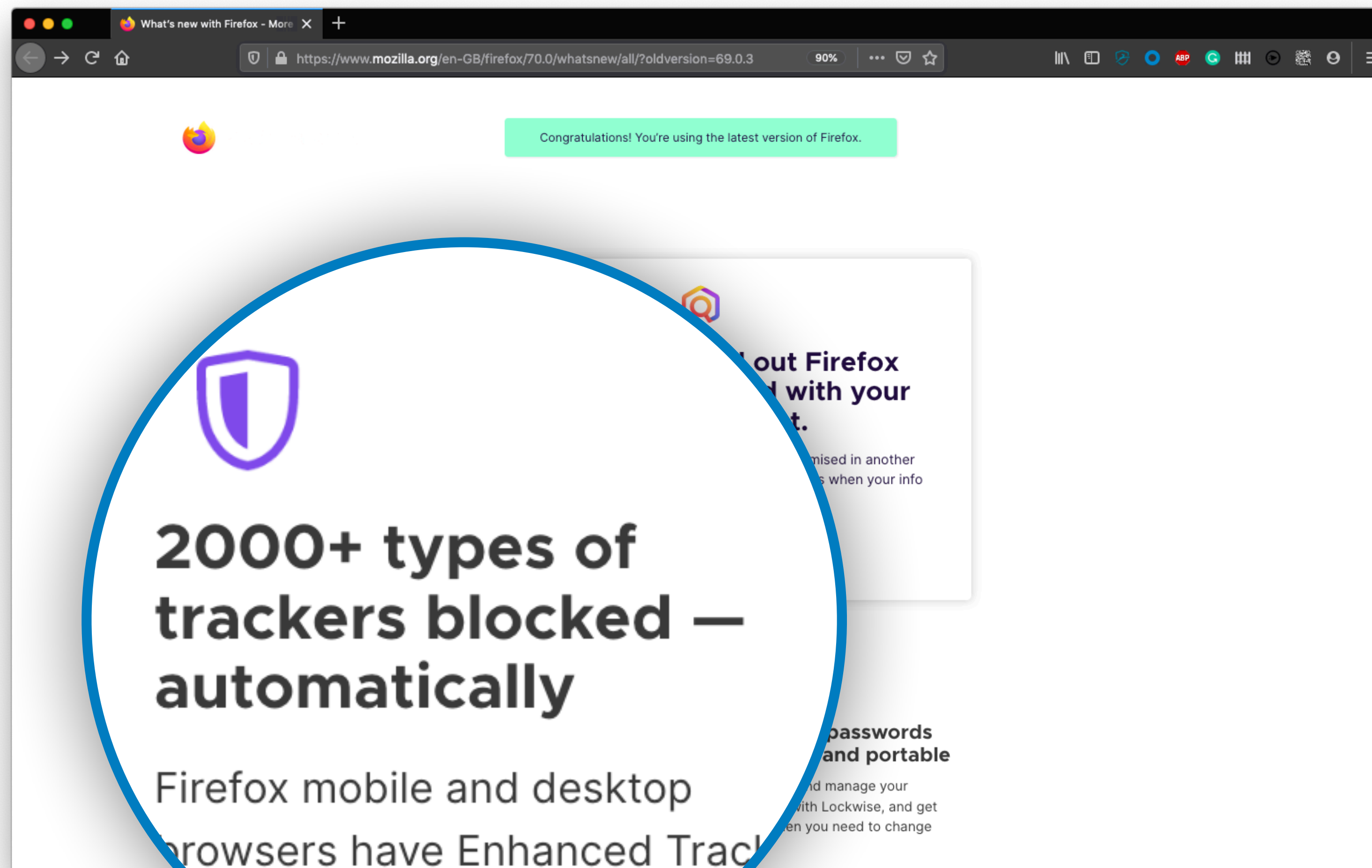


caniuse.com/#feat=do-not-track

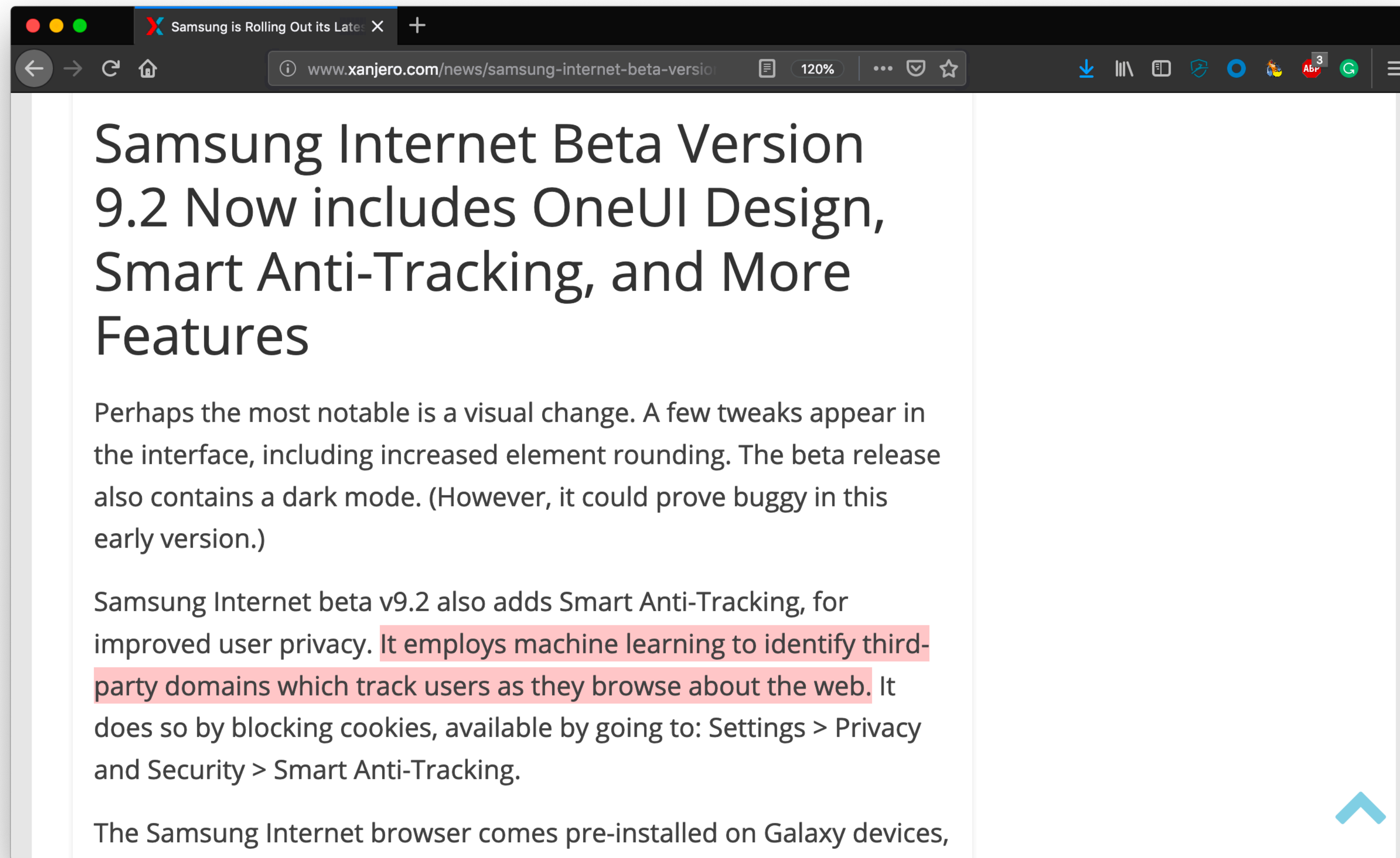
**It was a nice try,
but I don't really see
that happening...**



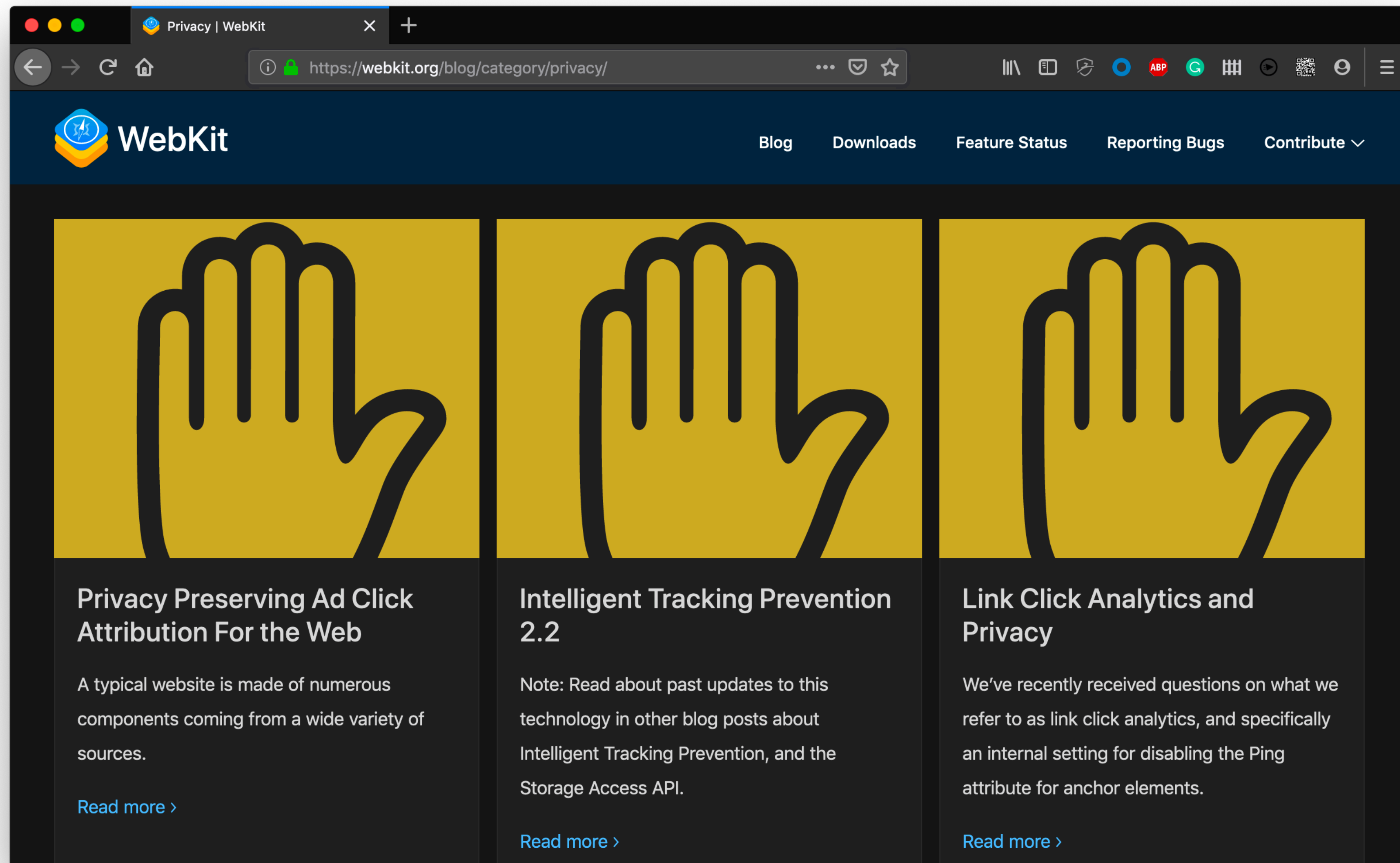




www.xanjero.com/news/samsung-internet-beta-version-9-2-now-includes-oneui-design-smart-anti-tracking-and-more-features/



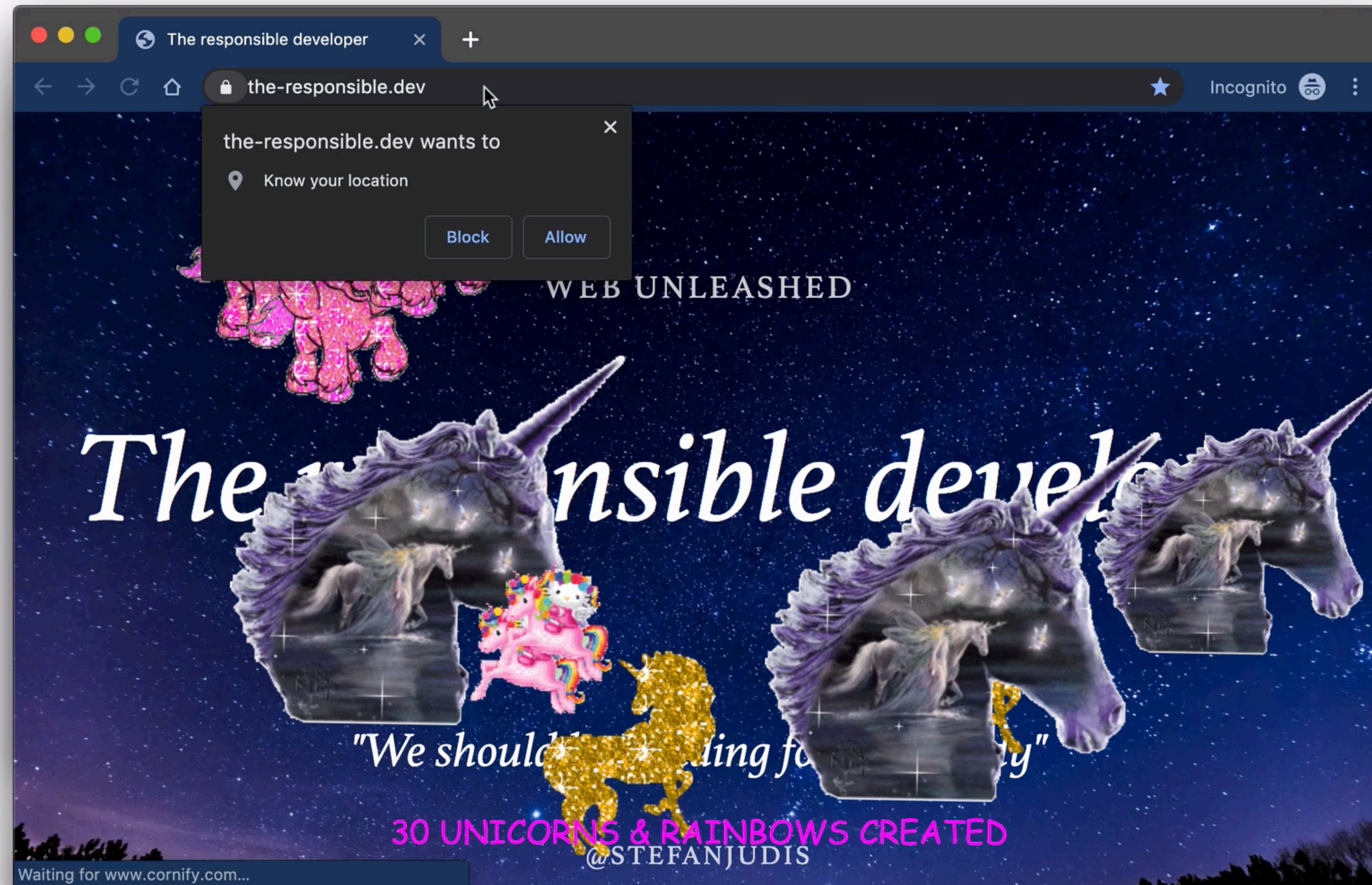
<https://webkit.org/blog/category/privacy/>





**The next browser war
is on its way...**

the-responsible.dev/respectful/





***Building for
the web is very hard***



Design



Content



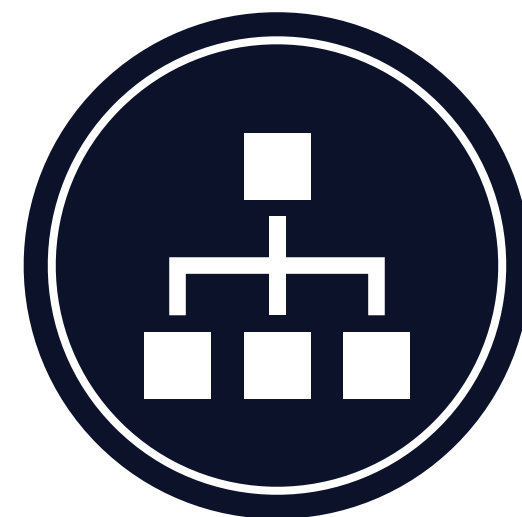
Performance



Accessibility



Frameworks

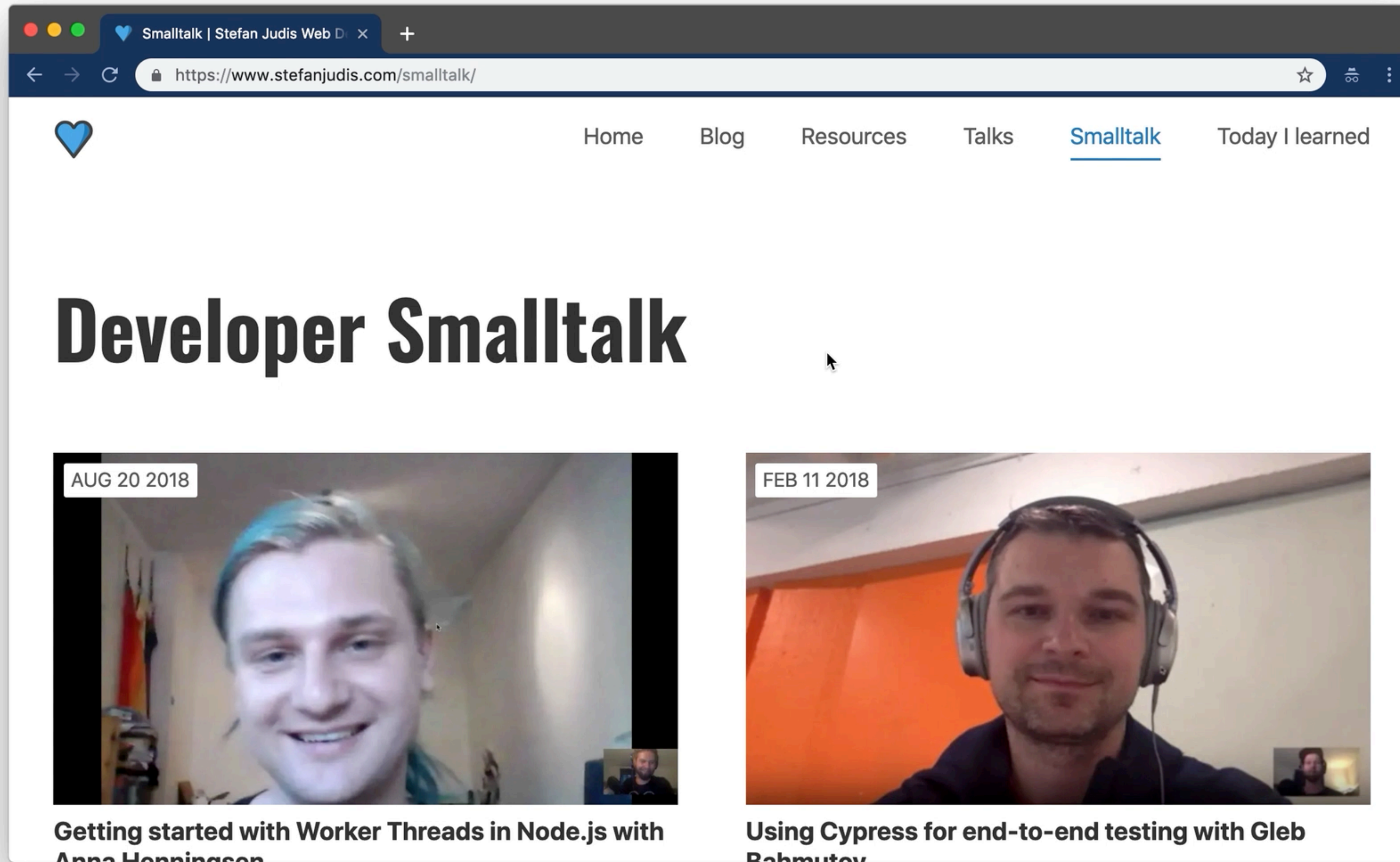


Network

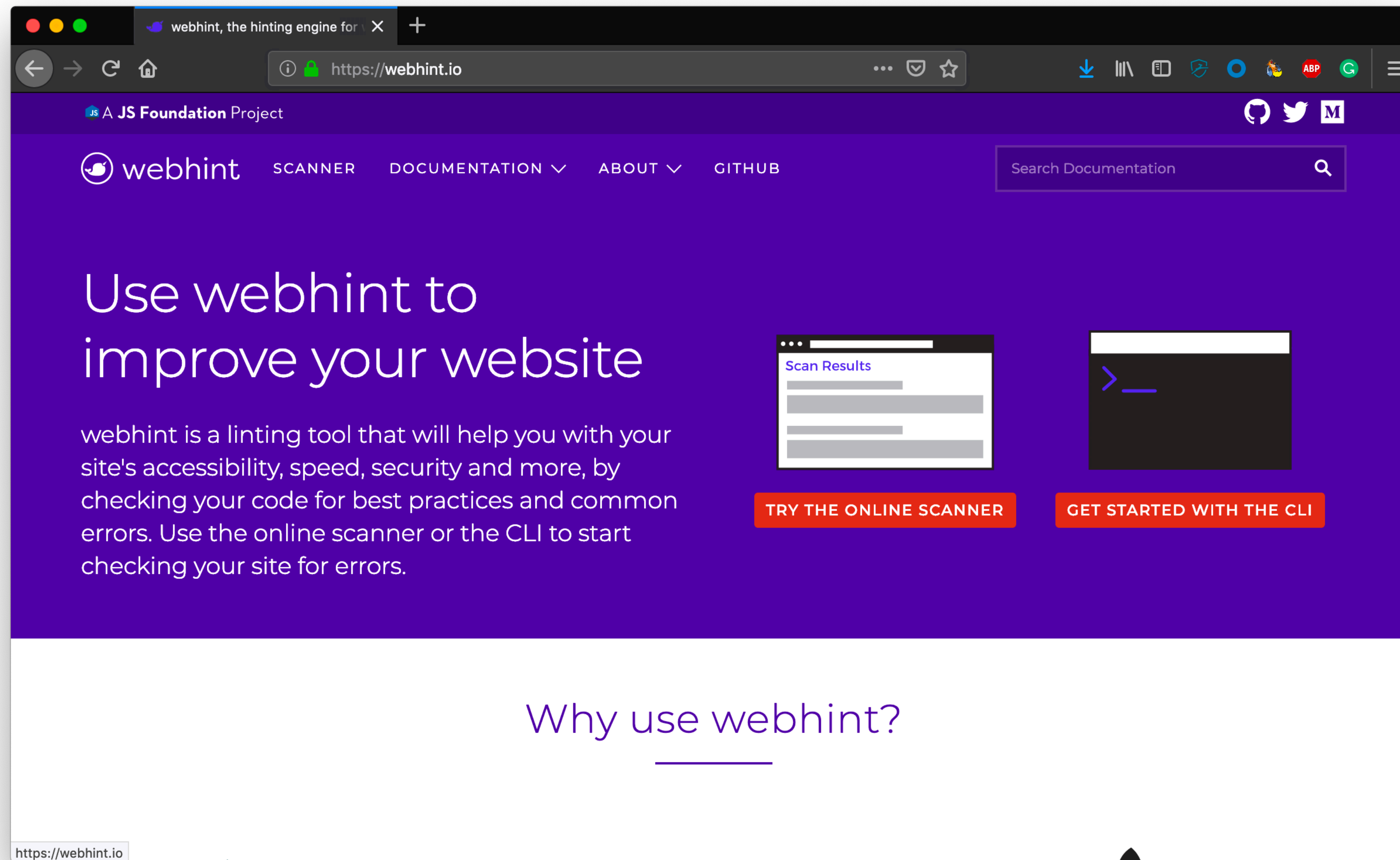


Devices

Lighthouse



webhint.io






**If you want to get a more
complete overview...**

<https://securityheaders.com>

Security Headers

Sponsored by  Report URI


Home About

Scan your site now

Scan

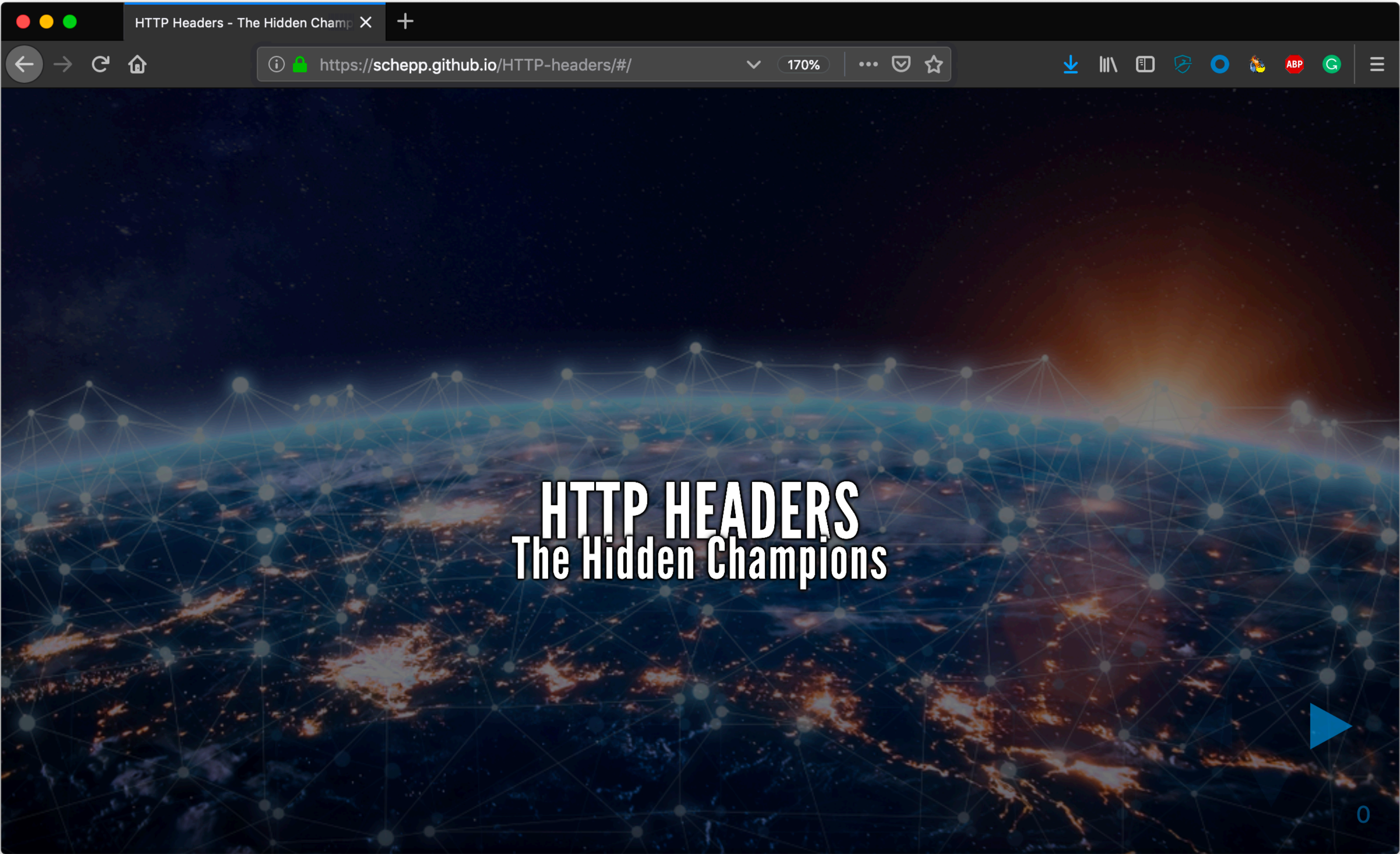
☐ Hide results ☒ Follow redirects

Security Report Summary



Site:	https://www.stefanjudis.com/
IP Address:	2604:a880:2:d0::21e9:c001
Report Time:	13 Sep 2019 12:22:32 UTC
Headers:	<div><div>✓ Content-Security-Policy</div><div>✓ Feature-Policy</div><div>✓ Referrer-Policy</div><div>✓ Strict-Transport-Security</div><div>✓ X-Content-Type-Options</div><div>✓ X-Frame-Options</div></div>
Warning:	Grade capped at A, please see warnings below.

schepp.github.io/HTTP-headers



youtu.be/1l9m9_esNZc

The screenshot shows a web browser window with a single tab titled "Nordic.js 2018 • Andrew Betts". The address bar displays the URL "https://www.youtube.com/watch?v=1l9m9_esNZc" with a 133% zoom level. The YouTube interface includes a search bar with the text "Suchen" and a user profile icon. The video player shows a presentation slide with a blue laptop icon, the text "Nordic.js", and logos for "Qlik Playground", "OPSIO", and "Confetti". A play button is centered over the video. The video progress bar at the bottom indicates a duration of 3:36 / 30:26. Below the video, the title "Nordic.js 2018 • Andrew Betts - Headers for Hackers" is visible, along with a partially obscured view count of "289 Aufrufe".

Nordic.js 2018 • Andrew Betts - Headers for Hackers

289 Aufrufe



The web has to be
safe...



**The web has to be
safe, affordable...**



**The web has to be
safe, affordable and
respectful...**



**... so that it really is
for everybody!**



Thanks.

@stefanjudis

www.stefanjudis.com

Slides:

my-links.online/the-responsible-dev

