A new security header: Feature Policy

July 16, 2018

We have a new Security Header!! Feature Policy will allow a site to enable or disable certain browser features and APIs in the interest of better security and privacy. Let's take a look!

Feature Policy

Feature Policy is being created to allow site owners to enable and disable certain web platform features on their own pages and those they embed. Being able to restrict the features your site can use is really nice but being able to restrict features that sites you embed can use is an even better protection to have.

HTTP Response Header

Delivering a Feature Policy via HTTP response header is just as simple as issuing the other various security headers we have available to us. You simply need to decide the restrictions you'd like to place on your page and build the policy to return. Here is a simple example:

```
Feature-Policy: vibrate 'self'; usermedia *; sync-xhr 'self' https://example.com
```

In the above example by specifying `vibrate` and allowing it for `self` the feature is disabled for all origins except our own. The `sync-xhr` feature is allowed by the current origin and `https://example.com` and `usermedia` is allowed by all origins. If you've had experience with Content Security Policy (https://scotthelme.co.uk/content-security-policy-an-introduction/) then this should be fairly familiar. The full list of features that can be restricted isn't final yet but here are a few things you could restrict:

- `geolocation`
- `midi`

- `notifications`
- `push`
- `sync-xhr`
- `microphone`
- `camera`
- `magnetometer`
- `gyroscope`
- `speaker`
- `vibrate`
- `fullscreen`
- `payment` (PaymentRequest)

This list can and will change so keep an eye on the documents linked at the bottom of the page for updates.

Controlling Origins

Controlling which origins can use which features can be done with the following values:

- `*`
- `'self'`
- `'none'`
- `<origin(s)>`

Let's break those down and look at exactly what each one will allow.

`*`
This will allow the current page to use the feature and any nested browsing contexts inside it like iframes.

`'self'`
This will allow the current page to use the feature and any nested browsing contexts like iframes only if they are on the same-origin, so for example if you frame your own site on your page.

`'none'`
This feature will be disabled for the current page and any nested browsing contexts like iframes.

`<origin(s)>`
Only the specified origins will be allowed to use this feature. For exmple `https://example.com` or `https://example.net https://example.org` .

Restricting iframes

Delivering a policy as a HTTP response header applies it to the page and embedded browsing contexts within it. You may wish to have a different policy applied to each of these so you can enable features on specific iframes.

```
<iframe src="https://example.com" allow="vibrate">
```

One thing to note is that if a parent disables a feature then it can be enabled again on any child. Thus, if we disable `vibrate` in our HTTP response header we can enable it only for a specific iframe. To demonstrate, if we issue the following header on our page it would result in the iframe on our page *not* having the vibrate feature but we can enable it specifically.

```
Feature-Policy: vibrate 'none'
```

```
<iframe src="https://example.com" allow="vibrate">
```

Of course, the other way we could specify this policy is to allow `example.com` access to vibrate in the response header, but that would grant it to all child contexts loaded from that origin.

```
Feature-Policy: vibrate 'self' example.com
```

```
<iframe src="https://example.com">
```

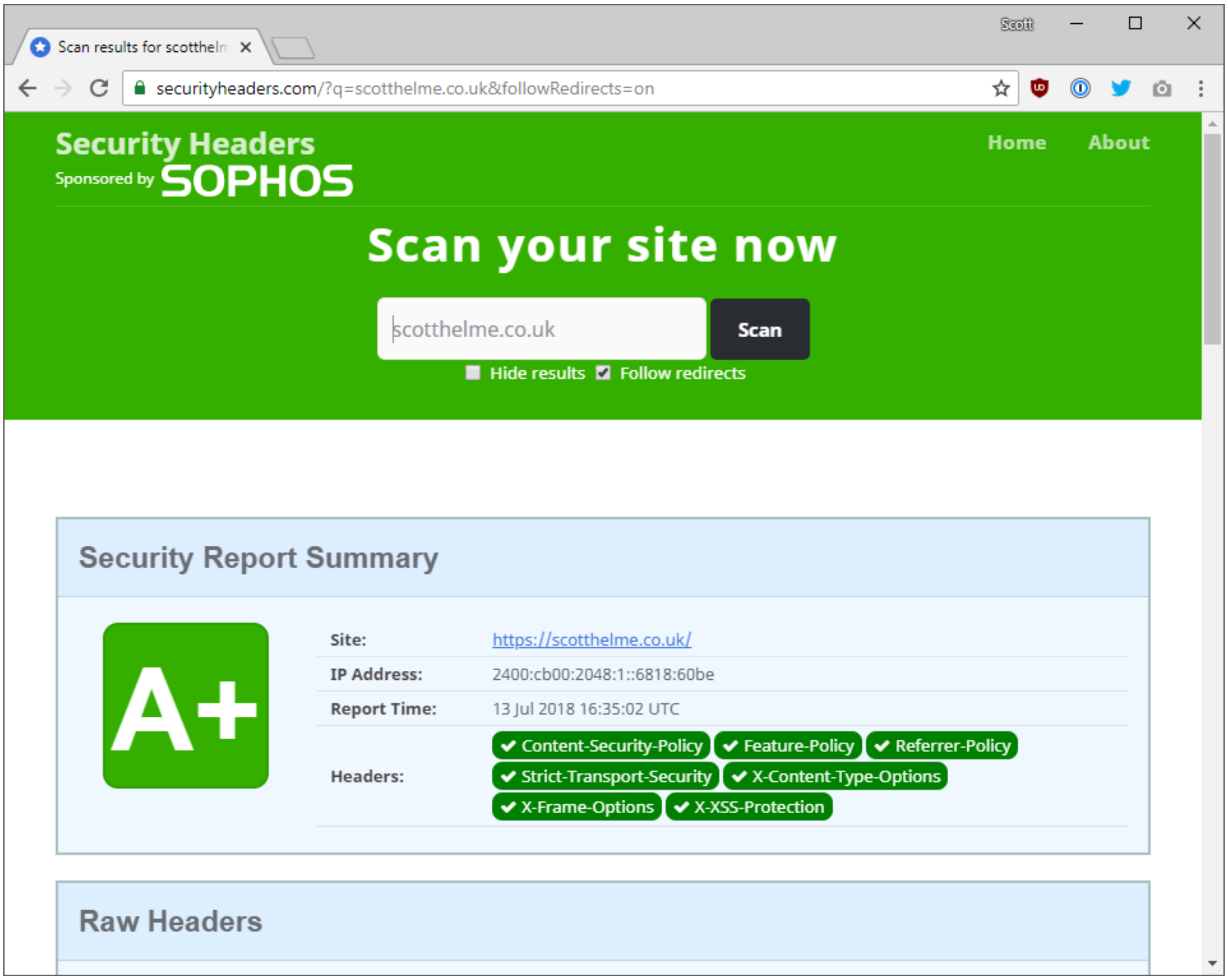
Feature Policy provides a fair amount of flexibility in this regard so it should be easy enough to deploy in a manner that affords real protection.

Support

Even though it is still early days we already have support (https://caniuse.com/#search=feature%20policy) in Chrome and Safari. I'd like to start getting visibility of these new features out there so we can start increasing adoption and as browser support follows, we will only get more and more benefit from deploying them.

Security Headers

To further the exposure of the header I will be adding detection to Security Headers (https://securityheaders.com). The header will not have a weight to impact the grade but it will be flagged as required. I can start to track utilisation and make people aware of its existence to drive adoption!


Scan results for scotthelm
Scott
securityheaders.com/?q=scotthelme.co.uk&followRedirects=on
Security Headers
Sponsored by SOPHOS
Home
About
Scan your site now
scotthelme.co.uk
Scan
□ Hide results ☑ Follow redirects

Security Report Summary

A+

Site:	https://scotthelme.co.uk/
IP Address:	2400:cb00:2048:1::6818:60be
Report Time:	13 Jul 2018 16:35:02 UTC
Headers:	✓ Content-Security-Policy ✓ Feature-Policy ✓ Referrer-Policy ✓ Strict-Transport-Security ✓ X-Content-Type-Options ✓ X-Frame-Options ✓ X-XSS-Protection

Raw Headers

Links

FP RFC: https://wicg.github.io/feature-policy/ (https://wicg.github.io/feature-policy/)

List of FP features: https://github.com/WICG/feature-policy/blob/master/features.md (https://github.com/WICG/feature-policy/blob/master/features.md)

Chromium Source list of features supported: https://cs.chromium.org/chromium/src/third_party/blink/renderer/platform/feature_policy/feature_polic
l=138&rcl=ab90b51c5b60de15054a32b0bd18e4839536a1c9 (https://cs.chromium.org/chromium/src/third_party/blink/renderer/platform/feature_policy/feature_poli
l=138&rcl=ab90b51c5b60de15054a32b0bd18e4839536a1c9)

Chrome Platform Status: https://www.chromestatus.com/features#component%3A Blink>FeaturePolicy (https://www.chromestatus.com/features#component%3A%20Blink%3EFeaturePolicy)

Feature Policy Explainer: https://docs.google.com/document/d/1k0Ua-ZWlM_PsFCFdLMa8kaVTo32PeNZ4G7FFHqpFx4E/edit (https://docs.google.com/document/d/1k0Ua-ZWlM_PsFCFdLMa8kaVTo32PeNZ4G7FFHqpFx4E/edit)

Feature Policy (/tag/feature-policy/), *Security Headers (/tag/security-headers/)*

s://twitter.com/share?
0new%20security%20header%3A%20Feature%20Policy&url=https://scotthelme.co.uk/a-new-security-
eature-policy/)
s://www.facebook.com/sharer/sharer.php?u=https://scotthelme.co.uk/a-new-security-header-feature-

s://plus.google.com/share?url=https://scotthelme.co.uk/a-new-security-header-feature-policy/)
s://pinterest.com/pin/create/button/?url=https://scotthelme.co.uk/a-new-security-header-feature-
media=https://scotthelme.co.uk/content/images/2018/07/fp.png&description=%5Bobject%20Object%5D)
s://www.linkedin.com/shareArticle?mini=true&url=https://scotthelme.co.uk/a-new-security-header-
olicy/&title=A%20new%20security%20header%3A%20Feature%20Policy)
s:////www.reddit.com/submit?url=https://scotthelme.co.uk/a-new-security-header-feature-policy/)
s://news.ycombinator.com/submitlink?u=https://scotthelme.co.uk/a-new-security-header-feature-
=A%20new%20security%20header%3A%20Feature%20Policy)

‹ Previous Post : Proxying traffic to Report URI with Cloudflare Workers (/report-uri-proxy/)

Next Post : Fast scaling with DigitalOcean › (/fast-scaling-with-digitalocean/)

The Author

Hi, I'm Scott Helme, a Security Researcher, international speaker and author of this blog. I'm also the founder of the popular securityheaders.com (https://securityheaders.com) and report-uri.com (https://report-uri.com), free tools to help you deploy better security!

Follow

f (https://www.facebook.com/scott.helme) (https://twitter.com/Scott_Helme)

(https://google.com/+ScottHelme) in (https://www.linkedin.com/in/scotthelme)

(skype:scott.helme87?add) (https://uk.pinterest.com/scotthelme/)

(https://www.youtube.com/user/ScottHelme) (https://vimeo.com/scotthelme)

(https://www.flickr.com/photos/scotthelme/)

t (https://www.tumblr.com/blog/scotthelme) (https://github.com/ScottHelme)

(https://www.instagram.com/scotthelme/)

(https://stackoverflow.com/users/1414715/scott-helme)

(https://stackexchange.com/users/1513078/scott-helme)

฿ (bitcoin:1ScottkY3kbPi6fQEgAaGQoRfz4MxJLGZ) (https://www.paypal.me/scotthelme)

(mailto:scotthelme@hotmail.com) (https://scotthelme.co.uk/rss/)

Support

Enjoy my blog or find it useful? Please consider supporting me on Patreon (https://www.patreon.com/ScottHelme)!

Upcoming Events

NDC Security: (Gold Coast - Australia) (https://ndcsecurity.com.au/)
14th - 16th May

InfoShare: (Gdańsk - Poland) (https://infoshare.pl/)
22nd - 23rd May

BSides London: (London - UK) (https://www.securitybsides.org.uk/)
6th June

NDC Oslo: (Oslo - Norway) (https://ndcoslo.com/)
11th - 15th June

SteelCon: (Sheffield - England) (https://www.steelcon.info/)
3rd - 7th July

Subscribe

You can use this IFTTT recipe (https://ifttt.com/recipes/457742-send-me-an-email-when-scott-helme-blogs) to get an email when I publish a new blog!

There's also my RSS Feed (https://scotthelme.co.uk/rss/).

Cheat Sheets

CSP Cheat Sheet (https://scotthelme.co.uk/csp-cheat-sheet/)

HSTS Cheat Sheet (https://scotthelme.co.uk/hsts-cheat-sheet/)

HPKP Cheat Sheet (https://scotthelme.co.uk/hpkp-cheat-sheet/)

HTTPS Cheat Sheet (https://scotthelme.co.uk/https-cheat-sheet/)

Performance Cheat Sheet (https://scotthelme.co.uk/performance-cheat-sheet/)

Projects

https://report-uri.com (https://report-uri.com)

Real-time security reporting for your site.

https://securityheaders.com (https://securityheaders.com)

Analyse your HTTP response headers.

https://scotthel.me (https://scotthel.me)

My short URL service.

Popular Tags

HTTPS (/tag/https/) CSP (/tag/csp/) HSTS (/tag/hsts/) HPKP (/tag/hpkp/) HSTS-Preload (/tag/hsts-preload/) Let's Encrypt (/tag/lets-encrypt/) securityheaders.io (/tag/securityheaders-io/) report-uri.io (/tag/report-uri-io/) 2FA (/tag/2fa/) 2SV (/tag/2sv/) CSRF (/tag/csrf/) XFO (/tag/xfo/) XXSSP (/tag/xxssp/) XCTO (/tag/xcto/) CDN (/tag/cdn/) Wardriving (/tag/wardriving/) RSA (/tag/rsa/) ECDSA (/tag/ecdsa/) Table Storage (/tag/table-storage/) Performance (/tag/performance/)

Must Read

Alexa Top 1 Million Crawl - August 2017 (https://scotthelme.co.uk/alexa-top-1-million-analysis-aug-2017/)

29th August 2017

Year In Review | 2017 (https://scotthelme.co.uk/year-in-review-2017/)

29th December 2017

My week in Vegas (https://scotthelme.co.uk/my-week-in-vegas/)

14th August 2017