Haketilo - Feature #83

Also add ability to selectively block other types of content (e.g. fonts)

08/31/2021 01:36 PM - koszko

Status:	New	**Start date:**	08/31/2021
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Google uses fonts sites load from its servers for snooping. Blocking them causes relatively little issues (compared to blocking JS) and greatly improves privacy, so it would be a good idea to add support for it

History

#1 - 09/03/2021 10:16 AM - jahoti

To summarise from the full list of CSP directives, we can block/restrict the following with CSP (which would only require refactoring the storage structure and UI):

- loading from script interfaces (i.e. link pinging, beacons, fetch(), XMLHttpRequest, WebSocket, and EventSource)
- fonts
- frames
- images (including favicons)
- application manifests
- multimedia files
- objects
- prefetching (currently tied to scripts)
- scripts
- stylesheets
- workers
- CSP violation reporting
- HTTP (i.e. auto-upgrade to HTTPS)

There is also the option to restrict inclusion of the referer header on navigation, using the referrer-policy header, and CSP directives which do something I don't entirely understand involving a trusted types framework for JavaScript.

#2 - 09/03/2021 11:44 AM - koszko

I am not entirely sure the actual fetching of resources is also prevented by CSP. What I am sure would work, though, is using webRequest to, for example, block certain requests with "font" type. And it seems this could be also achieved in the new declarativeNetRequest ^^

jahoti wrote:

> CSP directives which do something I don't entirely understand involving a trusted types framework for JavaScript.

This makes me even more confident we'd be better off just removing all served CSP rules for pages we intend to inject something to... Otherwise, it might be impossible to keep up with the browsers and at some point something will block our stuff :/

#3 - 09/03/2021 12:18 PM - jahoti

> I am not entirely sure the actual fetching of resources is also prevented by CSP. What I am sure would work, though, is using webRequest to, for example, block certain requests with "font" type. And it seems this could be also achieved in the new declarativeNetRequest ^

Good point- both approaches can be combines, in any case.

> jahoti wrote:
>
> CSP directives which do something I don't entirely understand involving a trusted types framework for JavaScript.
>
> This makes me even more confident we'd be better off just removing all served CSP rules for pages we intend to inject something to... Otherwise, it might be impossible to keep up with the browsers and at some point something will block our stuff :/

I'm starting to agree now, and try and do that while modifying the CSP filtering.