Haketilo - Feature #88

[Roadmap 6][Milestone] Allow payloads to also specify CSP rules that should be used instead of the original ones served by page

09/04/2021 07:36 PM - koszko

Status:	New	**Start date:**	09/04/2021
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Note that this concerns CSP rules other than those for scripts. For scripts we always use a nonce

Roadmap

History

#1 - 09/10/2021 05:07 PM - koszko

As this is somehow related, I'll write an update regarding our recent CSP change (where we are no longer modifying existing CSP headers but rather dropping them completely or leaving them as they were).

In the end, I didn't use the commit from your branch, Jahoti. I hope you don't mind that. After the change:

- No CSP headers get modified for pages where there is no payload being injected.
- All original CSP headers sent by server get removed for pages where we're going to inject some payload.
- I retained the code that injects our "x-hachette" header and retrieves it later in case of headers being cached by Firefox (I saw you removed on your branch but I don't know why; it is still needed, right?).
- We no longer differentiate between normal and report-only CSP headers.

The behavior I aimed for was slightly different from that on your branch + content/main.js was already very different from when you modified it with your commit. That's why I did it this way

#2 - 09/11/2021 12:14 PM - jahoti

I read this thread earlier today and had been meaning to reply, yet couldn't find it again- sorry!

> In the end, I didn't use the commit from your branch, Jahoti. I hope you don't mind that. After the change:

Not at all- whatever works best!

> - No CSP headers get modified for pages where there is no payload being injected.
> - All original CSP headers sent by server get removed for pages where we're going to inject some payload.
> - I retained the code that injects our "x-hachette" header and retrieves it later in case of headers being cached by Firefox (I saw you removed on your branch but I don't know why; it is still needed, right?).

It is still needed; that was what I now understand to be faulty reasoning, which also led to CSP headers being removed where scripts are blocked even if no payload was injected. Thank you for re-doing that change correctly!

- We no longer differentiate between normal and report-only CSP headers.

The behavior I aimed for was slightly different from that on your branch + content/main.js was already very different from when you modified it with your commit. That's why I did it this way

Indeed, it is for the best :).

#3 - 02/24/2022 12:49 PM - koszko

- Blocks Feature #73: [Roadmap 6] Implement a permissions system added

#4 - 02/24/2022 12:50 PM - koszko

- Subject changed from Allow payloads to also specify CSP rules that should be used instead of the original ones served by page to [Roadmap 6][Milestone] Allow payloads to also specify CSP rules that should be used instead of the original ones served by page

#5 - 02/24/2022 01:04 PM - koszko

- Description updated

#6 - 06/21/2022 02:27 PM - koszko

- Blocks deleted (Feature #73: [Roadmap 6] Implement a permissions system)