CSP – http header

(draft-gondrom-websec-csp-header)

Adam Barth, Tobias Gondrom

March 2012

Content Security Policy HTTP Header

1. Background
2. Draft and Questions

CSP - Background

- Content Security Policy:
  - Is developed by the W3C Web Application Security Working Group
  - W3C makes good progress towards CSP
  - During pre-formation stage of W3C WebAppSec WG, there was informal understanding that while the whole Content Security Policy semantics etc. would be done in W3C, the http header to communicate it, should be standardised in IETF-Websec.
  - As the CSP makes good progress towards completion, Adam and I filed an I-D strawman for the CSP http header.

CSP – http header

- strawman draft-gondrom-websec-csp-header
- using the W3C CSP specification
  - Basically put the http header part of specification in RFC format for http header definition
  - Very light-weight I-D: Refers for all semantics to W3C.
- Questions:
  - Does this approach still make sense (or should we leave the whole http header as well to be standardised by W3C) when they finish CSP?
  - Is websec WG still the place for it?

CSP - http header

- Some personal thoughts:
  - there is good value in IETF involvement in the http header definition by review and filing as RFC.
  - However, to be clear: discussion about semantics MUST be on W3C WebAppSec mailing-list and not on websec mailing-list.
  - I-D should be as light-weight as possible and refer to W3C CSP specification and only focus on the http header specification.
  - Additional reviews of CSP http header definition would be useful.

Thank you