Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 9, 2016

M. West
Google, Inc

October 7, 2015

Content Security Policy Directive Registry
draft-west-webappsec-csp-reg-01

Abstract

This document establishes an Internet Assigned Number Authority (IANA) registry for Content Security Policy directives. It populates the registry with the directives defined in the CSP specification.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 9, 2016.

Table of Contents

1. Introduction

The Content Security Policy specification [CSP] defines a mechanism by which web developers can control the resources which a particular page can fetch or execute, as well as a number of security-relevant policy decisions.

The policy language specified in that document consists of an extensible set of "directives", each of which controls a specific resource type or policy decision. This specification establishes a registry to ensure that extensions to CSP are listed and standardized.

2. Use of the Registry

Content Security Policy directives must be documented in a readily available public specification in order to be registered by IANA. This documentation must fully explain the syntax, intended usage, and semantics of the directive. The intent of this requirement is to assure interoperable independent implementations, and to prevent accidental namespace collisions between implementations of dissimilar features.

Documents defining new Content Security Policy directives must register them with IANA, as described in Section 3. The IANA registration policy for such parameters is "Specification Required" [RFC5226], and is further discussed in Section 3.2.

3. IANA Considerations

This specification creates a new top-level IANA registry named "Content Security Policy directives".

3.1. Content Security Policy directives Registry

New Content Security Policy directives, and updates to existing directives, must be registered with IANA.

When registering a new Content Security Policy directive, the following information must be provided:

- The directive's name, an ASCII string conforming to the "directive-name" rule specified in Section 4.1 of [CSP].
- A reference to the readily available public specification defining the new directive's syntax, usage, and semantics.

The following table contains the initial values for this registry:

Directive Name	Reference
base-uri	[CSP]
child-src	[CSP]
connect-src	[CSP]
default-src	[CSP]
font-src	[CSP]
form-action	[CSP]
frame-ancestors	[CSP]
frame-src	[CSP]
img-src	[CSP]
media-src	[CSP]
object-src	[CSP]
plugin-types	[CSP]
report-uri	[CSP]
sandbox	[CSP]
script-src	[CSP]
style-src	[CSP]

3.2. Registration Policy for Content Security Policy directives

The registration policy for Content Security Policy directives is "Specification Required" [RFC5226], which uses a designated expert to review the specification.

The designated expert, when deliberating on whether to include a new directive in the registry, should consider the following criteria. This is not an exhaustive list, but representative of the issues to consider when rendering a decision):

- Content Security Policy is a restrictive feature, which allows web developers to deny themselves access to resources and APIs which would otherwise be available. Deploying Content Security Policy is, therefore, a strict reduction in risk. The expert should carefully consider whether proposed directives would violate this property.

- Granular directives are valuable, but the expert should strive to strike a reasonable balance between providing developers with all the knobs and switches possible, and providing only those with known security implications.

4. Security Considerations

The registry in this document does not in itself have security implications. The directives specified, however, certainly do. The documents referenced when registering new directives must contain detailed security and privacy considerations sections, and should contain usage information which informs web developers as to the directive's expected implementation.

5. References

5.1. Normative References

[CSP] West, M. and D. Veditz, "Content Security Policy", n.d., <https://w3c.github.io/webappsec-csp/>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

5.2. Informative References

[RFC5341] Jennings, C. and V. Gurbani, "The Internet Assigned Number Authority (IANA) tel Uniform Resource Identifier (URI) Parameter Registry", RFC 5341, DOI 10.17487/RFC5341, September 2008, <http://www.rfc-editor.org/info/rfc5341>.

Appendix A. Acknowledgements

Much of this document's structure comes from [RFC5341]. Thank you to Cullen Jennings and Vijay K. Gurbani for giving me a reasonable template to work within, and to Barry Leiba for his helpful commentary and suggestions.

Author's Address

Mike West
Google, Inc

Email: mkwst@google.com
URI: https://mikewest.org/