Initial Assignment for the Content Security Policy Directives Registry

Abstract

   This document establishes an Internet Assigned Number Authority
   (IANA) registry for Content Security Policy directives and populates
   that registry with the directives defined in the Content Security
   Policy Level 2 specification.

Status of This Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Not all documents
   approved by the IESG are a candidate for any level of Internet
   Standard; see Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc7762.

Table of Contents

1. Introduction

   The Content Security Policy (CSP) specification [CSP] defines a
   mechanism that web developers can use to control the resources that a
   particular page can fetch or execute, as well as a number of
   additional 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. Terminology

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in [RFC2119].

3. 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.

4. IANA Considerations

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

4.1. 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:

   o The directive's name, an ASCII string conforming to the
      "directive-name" rule specified in Section 4.1 of [CSP]. The ABNF
      [RFC5234] is as follows:

          directive-name = 1*(ALPHA / DIGIT / "-")

   o 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]     |
            +-----------------+-----------+
```

4.2. 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.

   When appointing an Expert (or Experts), the IESG SHOULD draw from the
   W3C's security community, coordinating through the liaison.

   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:

   o Content Security Policy is a restrictive feature, which allows web
      developers to deny themselves access to resources and APIs that
      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.

   o 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.

5. 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 that informs web developers as to the
   directive's expected implementation.

6. References

6.1. Normative References

   [CSP]   West, M., Barth, A., and D. Veditz, "Content Security
              Policy Level 2", July 2015, <https://www.w3.org/TR/CSP2>.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <http://www.rfc-editor.org/info/rfc2119>.

   [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., Ed. and P. Overell, "Augmented BNF for Syntax
              Specifications: ABNF", STD 68, RFC 5234,
              DOI 10.17487/RFC5234, January 2008,
              <http://www.rfc-editor.org/info/rfc5234>.

6.2. 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>.

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/