WEBSEC
Internet-Draft
Intended status: Standards Track
Expires: September 7, 2012

A. Barth
Google, Inc.
T. Gondrom

March 6, 2012

HTTP Header Content Security Policy
draft-gondrom-websec-csp-header-00

Abstract

To communicate the Content Security Policy (CSP) as defined by the W3C, the web server needs to send a HTTP header to the browser (client) to inform it about the content security policies that SHALL be applied on the client. This draft outlines the header to communicate the CSP with its fields. The definition of the semantic of the directives will be done by the Web Application Security Working Group at the W3C.

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 September 7, 2012.

Table of Contents

1. Introduction

In 2011 the W3C started the working group "Web Application Security Working Group" to work on a future Content Security Policy. A policy language intended to enable web designers or server administrators to declare web application content security policy. The goal of the specification is to reduce attack surface by specifying overall rules for what content may or may not do, thus preventing violation of security assumptions by attackers who are able to partially manipulate that content.

The goal of this drafts is only to document and specify the HTTP header used to communicate the Content Security Policy as specified by the W3C working group.

2. Requirements Language

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 RFC 2119 [RFC2119].

3. Content Security Policy Header

The Content Security Policy (CSP) HTTP response header indicates a policy to be enforced by the browser on from which sources different types of content will be allowed to load and possibly execute. Hosts can declare this policy in the header of their HTTP responses to prevent Cross Site Scripting, Cross-Site Request Forgery and clickjacking attacks, by ensuring that content from untrusted sources is not loaded/executed in web pages or frames.

4. Overview

The header field name is:
Content-Security-Policy

Please note, that previous experimental implementations prior to this standard may use the header name X-Content-Security-Policy, which does not indicate any conformance with this standard.

The server transmits its security policy for a particular resource using a HTTP header with the label "Content-Security-Policy" followed by a collection of directives, each of which controls a specific set of privileges for a document rendered by a user-agent. More details are provided in the directives section.

In general any directive consists of a directive name, which specifies the privileges controlled by the directive, and its directive value, which specifies the restrictions the policy imposes on those privileges.

[TBD] do we need to mention the HTML meta tag here as well?
The CSP SHOULD be delivered from the server to the client via an HTTP response header. Another less recommended alternative is an HTML meta element. Servers should use the HTTP response header mechanism whenever possible because, when using the meta element mechanism, there is a period of time between when the user agent begins to process the document and when the user agent encounters the meta element when the document is not protected by the policy.

4.1. Content-Security-Policy

A server may supply one or more CSP policies in HTTP response header fields named Content-Security-Policy along with the protected content. Upon receiving an HTTP response containing more than one Content-Security-Policy header field, the user agent MUST enforce the most combination of all the policies contained in these header fields. [TBD] should this be the most restrictive combination?

4.2. Content-Security-Policy-Report-Only

As an alternative, the server can also use the HTTP header "Content-Security-Policy-Report-Only" header field to experiment with CSP by only monitoring (instead of enforcing) the policy. This feature allows server operators to develop their security policy in iterations. They can deploy a report-only policy based on their best estimate of how their site behaves. And if the site violates this policy, instead of breaking the site, the user agent(s) will send violation reports to a URI specified in the policy. Once a server has confidence that the policy is appropriate, it can promote the report-only policy to full "Content-Security-Policy" (blocking) mode. As with "Content-Security-Policy", a server may supply one or multiple of these policies in HTTP response header fields named Content-Security-Policy-Report-Only along with the protected content. Upon receiving an HTTP response containing more than one Content-Security-Policy-Report-Only header field, the user agent MUST enforce the most combination of all the policies contained in these header fields. [TBD] should this be the most restrictive combination?

A server MUST NOT provide Content-Security-Policy header field(s) and Content-Security-Policy-Report-Only header field(s) in the same HTTP response. If a client received both header fields in a response, it MUST discard all Content-Security-Policy-Report-Only header fields and MUST enforce the Content-Security-Policy header field. A warning

SHOULD be send to the report URI as specified in the Content-Security-Policy, if the report address is specified.

5. Augmented Backus-Naur Form (ABNF)

The RFC 5234 [RFC5234] ABNF of the CSP header is as follows:

6. ABNF

The ABNF is as follows:

```
csp-header   = "Content-Security-Policy:" OWS policy OWS

policy            = directive-list
directive-list    = [ directive *( ";" [ directive ] ) ]
directive         = *WSP [ directive-name [ WSP directive-value ] ]
directive-name    = 1*( ALPHA / DIGIT / "-" )
directive-value   = *( WSP / <VCHAR except ";"> )
```

7. Source List

Many CSP directives may refer to sources from which content / resources may be loaded. These sources are defined as a value defined by a source list. Each source expression in the source list represents a location from which content of the specified type can be retrieved. The source expression 'self' represents the set of URIs which are in the same origin (as defined by SAMEORIGIN [RFC6454]) as the protected document and the source expression 'unsafe-inline' represents content supplied inline in the document itself.

```
source-list       = *WSP [ source-expression
                    *( 1*WSP source-expression ) *WSP ]
                    / *WSP "'none'" *WSP
source-expression = scheme-source / host-source / keyword-source
scheme-source     = scheme ":"
host-source       = ( [ scheme "://" ] host [ port ] )
keyword-source    = "'self'" / "'unsafe-inline'" / "'unsafe-eval'"
scheme            = <scheme> production from RFC 3986
host              = "*" / [ "*." ] 1*host-char *( "." 1*host-char )
host-char         = ALPHA / DIGIT / "-"
port              = ":" ( 1*DIGIT / "*" )
```

8. Directives

The following CSP directives are defined:

default-src
: If this directive is set, it it sets the default source for all directives that are not explicitely specified.

script-src

object-src

style-src

img-src

media-src

frame-src

font-src

connect-src

sandbox
: [TBD]???

report-uri
: Reports of violations of the CSP will be send to this URI

policy-uri
: URI to load the CSP

9. Examples

Example Cases

10. Acknowledgements

This document was derived its input from specifications published by W3C and developed by various browser vendors like Mozilla, Google, Microsoftm Opera and Apple.

11. IANA Considerations

This memo a request to IANA to include the specified HTTP header in registry as outlined in Registration Procedures for Message Header Fields [RFC3864]

11.1. Registration Template

PERMANENT MESSAGE HEADER FIELD REGISTRATION TEMPLATE:

Header field name: Content-Security-Policy

Applicable protocol: http [RFC2616]

Status: Standard

Author/Change controller: IETF

Specification document(s): draft-gondrom-websec-CSP-header

Related information:

Figure 1

12. Security Considerations

The introduction of the CSP http header improves the protection against Cross Site Scripting, CSRF and Clickjacking, however it is not self-sufficient on its own but MUST be used in conjunction with other security measures like secure coding, the Same-Origin Policy, Frame-Options, etc,

13. References

13.1. Normative References

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

13.2. Informative References

[CLICK-DEFENSE-BLOG]
Microsoft, "Clickjacking Defense", 2009, <http://blogs.msdn.com/b/ie/archive/2009/01/27/ie8-security-part-vii-clickjacking-defenses.aspx>.

[CSRF] OWASP (Open Web Application Security Project), "OWASP Top-10: Cross-Site Request Forgery (CSRF)", 2010, <http://www.owasp.org/index.php/Top_10_2010-A5>.

[Clickjacking] OWASP (Open Web Application Security Project), "Clickjacking", 2010, <http://www.owasp.org/index.php/Clickjacking>.

[FRAME-OPTIONS] IETF, "The Frame-Options", December 2010, <http://tools.ietf.org/id/draft-gondrom-frame-options-02.txt>.

[RFC0822] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, September 2004.

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

[RFC6454] Barth, A., "The Web Origin Concept", RFC 6454, December 2011.

[W3C] W3C, "W3C: DRAFT Web Application Security Working Group Charter", 2012, <http://www.w3.org/2011/07/appsecwg-charter.html>.

[W3C-CSP] W3C, "W3C: CSP", 2012, <http://www.w3.org/TR/CSP/#policies>.

Authors' Addresses

Adam Barth
Google, Inc.

Email: ietf@adambarth.com
URI: http://www.adambarth.com/

Tobias Gondrom
Kruegerstr. 5A
Unterschleissheim,
Germany

Phone: +44 7521003005
Email: tobias.gondrom@gondrom.org