WEBSEC
Internet-Draft
Intended status: Informational
Expires: April 26, 2013

D. Ross
Microsoft
T. Gondrom

October 23, 2012

HTTP Header X-Frame-Options
draft-ietf-websec-x-frame-options-01

Abstract

To improve the protection of web applications against Clickjacking this standard defines an http response header that declares a policy communicated from a host to the client browser on whether the browser must not display the transmitted content in frames of other web pages. This drafts serves to document the existing use and specification of X-Frame-Options.

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 26, 2013.

Table of Contents

1. Introduction

In 2009 and 2010 many browser vendors ([Microsoft-X-Frame-Options], [CLICK-DEFENSE-BLOG], [Mozilla-X-Frame-Options]) introduced the use of a non-standard http header RFC 2616 [RFC2616] "X-Frame-Options" to protect against Clickjacking [Clickjacking]. This draft is to document the current use of X-Frame-Options header and shall in the future be replaced by the Frame-Options [FRAME-OPTIONS] standard.

Existing anti-ClickJacking measures, e.g. Frame-breaking Javascript, have weaknesses so that their protection can be circumvented as a study [FRAME-BUSTING] demonstrated.

Short of configuring the browser to disable frames and script entirely, which massively impairs browser utility, browser users are vulnerable to this type of attack.

The "X-Frame-Options" allows a secure web page from host B to declare that its content (for example a button, links, text, etc.) must not be displayed in a frame (<frame> or <iframe>) of another page (e.g. from host A). In principle this is done by a policy declared in the HTTP header and obeyed by conform browser implementations.

1.1. 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].

2. X-Frame-Options Header

The X-Frame-Options HTTP response header indicates a policy whether a browser MUST NOT allow to render a page in a <frame> or <iframe> . Hosts can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, by ensuring that their content is not embedded into other pages or frames.

2.1. Syntax

The header field name is:
X-Frame-Options

There are three different values for the header field. These values are exclusive, that is NOT more than one of the three values MUST be set.

DENY
A browser receiving content with this header MUST NOT display this content in any frame.

SAMEORIGIN
A browser receiving content with this header MUST NOT display this content in any frame from a page of different origin than the content itself.
If a browser or plugin can not reliably determine whether the origin of the content and the frame have the same origin, this MUST be treated as "DENY".
(Please note that current implementations may vary on the interpretation of this criteria: In some it only allows to be framed if the origin of the top-level browsing-context is identical, in other it compares with to the origin of the framing page.)

ALLOW-FROM (followed by a URI [RFC3986] of a trusted origin)
A browser receiving content with this header MUST NOT display this content in a frame from any page with a top-level browsing contex of different origin than the specified origin. While this can expose the page to risks by the trusted origin, in some cases it may be necessary to allow the framing by content from other domains.
For example: X-FRAME-OPTIONS: ALLOW-FROM: https://www.domain.com/

The ALLOW-FROM URI MUST be valid.
Any data beyond the domain address (i.e. any data after the "/" separator) is to be ignored. And the algorithm to compare origins from [RFC6454] SHOULD be used to verify a referring page is of the same origin as the content or that the referring page's origin is identical with the ALLOW-FROM URI.

Wildcards or lists to declare multiple domains in one ALLOW-FROM statement are not permitted.

Please note that in conflict with [RFC6454], current implementations do not consider the port as a defining component of the origin.

2.2. Backus-Naur Form (BNF)

The RFC 822 [RFC0822] EBNF of the X-Frame-Options header is:

```
X-Frame-Options = "Frame-Options" ":" "DENY"/ "SAMEORIGIN" /
                          ("ALLOW-FROM" ":" URI)
```

With URI as defined in [RFC3986]
[TBD] Or should we use the ABNF (RFC 2234) alternatively to EBNF or in addition?

2.3. Design Issues

2.3.1. Enable HTML content from other domains

There are three main direct vectors that enable HTML content from other domains:

- IFRAME Tag
- Frame tag
- The Object tag (requires a redirect)

Besides these, other ways to host HTML content can be possible. For example some plugins may host HTML views directly. If these plugins appear essentially as frames (as opposed to top-level windows), the plugins MUST conform to the X-FRAME-OPTIONS directive as specified in this draft as well.

2.3.2. Browser Behaviour and Processing

To allow secure implementations, browsers MUST behave in a consistent and reliable way.

If an HTTP Header prohibits framing, the user-agent of the browser MAY immediately abort downloading or parsing of the document.

When a browser discovers loaded content with the X-FRAME-OPTIONS header would be displayed in a frame against the specified origin orders of the header, the browser SHOULD redirect as soon as possible to a "No-Frame" page.

"No-Frame" Page
If the display of content is denied by the X-FRAME-OPTIONS header an error page SHOULD be displayed. For example this can be a noframe.html page also stating the full URL of the protected page and the hostname of the protected page.

The NoFrame page MAY provide the user with an option to open the target URL in a new window.

Variation in current browser behaviour
There are currently variations in the implementation of the X-FRAME-OPTIONS header. For example not all browsers may support the "ALLOW-

FROM" option.
And the criteria for SAMEORIGIN option is not evaluated unanimously: one implementation may evaluate the SAMEORIGIN option based on the origin of the framed page and the framing page, while another may evaluate based on the framed page and the top-level browsing-context

These variations in the evaluation of the header by different implementations impair the useage and reliability of this http header. A revised version of frame-options [FRAME-OPTIONS] shall unify the behaviour and replace this document in the future.

2.4. Examples of X-Frame-Options Headers

2.4.1. Example scenario for the ALLOW-FROM parameter

1. Inner IFRAME suggests via a querystring parameter what site it wants to be hosted by. This can obviously be specified by an attacker, but that's OK.

2. Server verifies the hostname meets whatever criteria. For example, for a Facebook "Like" button, the server can check to see that the supplied hostname matches the hostname expected for that Like button.

3. Server serves up the hostname in X-FRAME-OPTIONS: ALLOW-FROM if the proper criteria was met in step #2.

4. Browser enforces the X-FRAME-OPTIONS: ALLOW-FROM domain.com header.

3. Acknowledgements

This document was derived from input from specifications published by various browser vendors like Microsoft (Eric Lawrence, David Ross), Mozilla, Google, Opera and Apple.

4. 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]

4.1. Registration Template

PERMANENT MESSAGE HEADER FIELD REGISTRATION TEMPLATE:

Header field name: X-Frame-Option

Applicable protocol: http [RFC2616]

Status: Standard

Author/Change controller: IETF

Specification document(s): draft-ietf-websec-x-frame-options

Related information:

Figure 1

5. Security Considerations

The introduction of the http header X-FRAME-OPTIONS does improve the protection against Clickjacking, however it is not self-sufficient on its own but MUST be used in conjunction with other security measures like secure coding and Content Security Policy (CSP)

The parameter ALLOW-FROM allows a page to guess who is framing it. This is by design, but may lead to data leakage or data protection concerns.

6. References

6.1. Normative References

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

6.2. 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>.

[Clickjacking]
OWASP (Open Web Application Security Project),

"Clickjacking", 2010,
<http://www.owasp.org/index.php/Clickjacking>.

[FRAME-BUSTING]
Stanford Web Security Research, "Busting frame busting: a study of clickjacking vulnerabilities at popular sites", 2010, <http://seclab.stanford.edu/websec/framebusting/>.

[FRAME-OPTIONS]
IETF, "The Web Origin Concept", July 2012, <http://tools.ietf.org/id/draft-ietf-websec-frame-options-00.txt>.

[Microsoft-X-Frame-Options]
Microsoft, "Combating ClickJacking With X-Frame-Options", 2010, <http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx>.

[Mozilla-X-Frame-Options]
Mozilla, "The X-Frame-Options response header", 2010, <https://developer.mozilla.org/en-US/docs/The_X-FRAME-OPTIONS_response_header>.

[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.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

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

Appendix A. Description of a Clickjacking attack

More detailed explanation of Clickjacking scenarios

A.1. Shop

An Internet Marketplace/Shop offering a feature with a link/button to "Buy this" Gadget
The marketplace wants their affiliates (who could be bad guys) to be able to stick the "Buy such-and-such from XYZ" IFRAMES into their pages. There is a ClickJack possibility here, which is why the marketplace/onlineshop needs to then immediately navigate the main browsing context (or a new window) to a confirmation page which is protected by anti-CJ protections.

A.2. Confirm Purchase Page

Onlineshop "Confirm purchase" anti-CSRF page
The Confirm Purchase page must be shown to the end user without possibility of overlay or misuse by an attacker. For that reason, the confirmation page uses anti-CSRF tokens and contains the X-FRAME-OPTIONS directive, mitigating ClickJack attacks.

A.3. Flash Configuration

Macromedia Flash configuration page
Macromedia Flash configuration settings are set by a Flash object which can run only from a specific configuration page on Macromedia's site. The object runs inside the page and thus can be subject to a ClickJacking attack. In order to prevent ClickJacking attacks against the security settings, the configuration page uses the X-FRAME-OPTIONS directive.

Authors' Addresses

David Ross
Microsoft
U.S.

Phone:
Email:

Tobias Gondrom
Kruegerstr. 5A
Unterschleissheim,
Germany

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