Network Working Group
Internet-Draft
Intended status: Informational
Expires: 11 October 2025

Y. Weiss
M. Metzger
Shopify

9 April 2025

HttpOnly cookie prefix
draft-httponlyprefix-weiss-http-01

Abstract

This draft introduces the __HttpOnly and __HostHttpOnly cookie name prefixes that ensure the cookie was set with an HttpOnly attribute.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://yoavweiss.github.io/httponly_prefix/draft-httponlyprefix-weiss-http.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-httponlyprefix-weiss-http/.

Source for this draft and an issue tracker can be found at https://github.com/yoavweiss/httponly_prefix.

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 https://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 11 October 2025.

Copyright Notice

Table of Contents

1. Introduction

There are cases where it's important to distinguish on the server side between cookies [COOKIES] that were set by the server and ones that were set by the client.

One such case is cookies that are normally _always_ set by the server, unless some unexpected code (an XSS exploit, a malicious extension, a commit from a confused developer, etc.) happens to set them on the client.

This draft add a signal that would enable servers to make such a distinction.

More specifically, it defines the __HttpOnly and __HostHttpOnly prefixes, that make sure that a cookie is not set on the client side using script.

1.1. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Server Requirements

These requirements apply to cookies set in Set-Cookie response headers by the server, as well as ones received in a Cookie request header from the client.

2.1. Cookie Name Prefixes

2.1.1. The "__HttpOnly-" prefix

2.1.1.1. Cookie creation

If a server creates a cookie whose name begins with a case-sensitive match for the string __HttpOnly-, then all the following MUST be true:

1. The Set-Cookie HTTP header MUST include the Secure attribute.

2. The Set-Cookie HTTP header MUST include the HttpOnly attribute.

2.1.1.2. Cookie processing

If a server processes a cookie received in a Cookie request header whose name begins with a case-sensitive match for the string __HttpOnly-, this indicates that *all* the following are true:

1. The cookie was originally created using a Set-Cookie HTTP header sent from this server.

2. The Set-Cookie HTTP header included the Secure attribute.

3. The Set-Cookie HTTP header included the HttpOnly attribute.

2.1.2. The "__HostHttpOnly-" prefix

2.1.2.1. Cookie creation

If a server uses a Set-Cookie HTTP header to create a cookie whose name begins with a case-sensitive match for the string __HostHttpOnly-, then all the following MUST be true:

1. The Set-Cookie HTTP header MUST include the Secure attribute.

2. The Set-Cookie HTTP header MUST include the HttpOnly attribute.

3. The Set-Cookie HTTP header MUST include the Path attribute with a value of /.

4. The Set-Cookie HTTP header MUST NOT include the Domain attribute.

2.1.2.2. Cookie processing

If a server processes a cookie received in a Cookie request header whose name begins with a case-sensitive match for the string __HostHttpOnly-, this indicates that *all* the following are true:

1. The cookie was originally created using a Set-Cookie HTTP header sent from this server

2. The Set-Cookie HTTP header included the Secure attribute.

3. The Set-Cookie HTTP header included the HttpOnly attribute.

4. The Set-Cookie HTTP header included the Path attribute with a value of /.

5. The Set-Cookie HTTP header did not include the Domain attribute.

3. User Agent Requirements

These requirements apply to cookies received in a Set-Cookie response header from the server.

3.1. Cookie Name Prefixes

User agents' requirements for cookie name prefixes differ slightly from servers', as UAs MUST match the prefix string case-insensitively.

3.1.1. Storage Model

Add the following steps after step 21 of section 5.7 in [COOKIES].

1. If the cookie-name begins with a case-insensitive match for the string "__HttpOnly-",

    1. Abort these steps and ignore the cookie entirely unless all the following conditions are true:

1. The cookie’s secure-only-flag is true.

2. The cookie’s http-only-flag is true.

3. The cookie-attribute-list contains an attribute with an attribute-name of "Path", and the cookie’s path is "/".

2. If the cookie-name begins with a case-insensitive match for the string "__HostHttpOnly-",

    1. Abort these steps and ignore the cookie entirely unless all the following conditions are true:

        1. The cookie’s secure-only-flag is true.

        2. The cookie’s http-only-flag is true.

        3. The cookie’s host-only-flag is true.

        4. The cookie-attribute-list contains an attribute with an attribute-name of "Path", and the cookie’s path is "/".

        5. The cookie-attribute-list does not contain an attribute with an attribute-name of "Domain".

4. Security Considerations

There are no particular security considerations. These new prefixes will only limit the ability of non-compliant cookies to be set. They do not open up new capabilities for server to set cookies where they previously could not.

5. IANA Considerations

This document has no IANA actions.

6. Normative References

[COOKIES] "Cookies HTTP State Management Mechanism", February 2025, <https://datatracker.ietf.org/doc/draft-ietf-httpbis-rfc6265bis/>.

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

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

Acknowledgments

Thanks to Rory Hewitt for his contributions to this draft. TODO acknowledge.

Authors' Addresses

Yoav Weiss
Shopify
Email: yoav@yoav.ws

Matthew Metzger
Shopify
Email: matthew.o.metzger@gmail.com