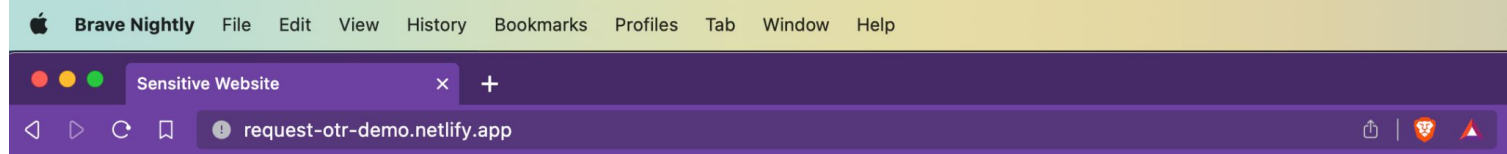


Request Off-The-Record HTTP Header

Shivan Kaul Sahib
Anton Lazarev
Brave Browser

Threat Model

1. **Attacker:** local “UI-bound adversary”
 - a. Authenticated access to a victim’s device via standard user interfaces [0]
 - b. Examples: browsing history, URL autocomplete, cookies
 - c. **Non-examples:** network snooping, malware, websites
2. **The attack:** identify if the victim has been to a “sensitive” site
3. **Victim:** hide evidence that they’ve visited a “sensitive” site while in a stressful environment
4. **Sensitive:** self-reported by website



This site may contain sensitive content.

Would you like to visit this site in Off-The-Record mode?

`https://request-otr-demo.netlify.app`


Brave wants to protect you when visiting sensitive sites. Sites you visit in Off-The-Record mode won't show up in your browsing history, and cookies will not be saved.

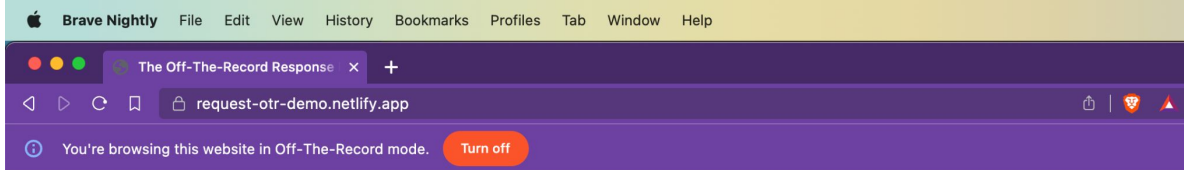
☐ Don't ask me again

You can change this later in Brave Settings in the Privacy and Security section

Proceed Normally

Proceed Off-The-Record

✕	Headers	Preview	Response	Initiator	Timing
Remote Address:		[2600:1f1c:471:9d01::c8]:443			
Referrer Policy:		strict-origin-when-cross-origin			
▼ Response Headers					
Accept-Ranges:		bytes			
Age:		106			
Cache-Control:		public, max-age=0, must-revalidate			
Content-Encoding:		br			
Content-Length:		13779			
Content-Type:		text/html; charset=UTF-8			
Date:		Sun, 23 Jul 2023 20:27:31 GMT			
Etag:		"9f4ffcce41ee6003110b1edfa167965e-ssl-df"			
Request-Otr:		1 			
Server:		Netlify			
Strict-Transport-Security:		max-age=31536000; includeSubDomains; preload			
Vary:		Accept-Encoding			
X-Nf-Request-Id:		01H626Z42G3CX1G6WR38Y3KVPB			
▼ Request Headers					



Workgroup: HTTP
Internet-Draft: draft-sahib-httpbis-off-the-record-latest
Published: 22 July 2023
Intended Status: Standards Track
Expires: 23 January 2024
Author: S. K. Sahib
Brave Software

The Off-The-Record Response Header Field

Abstract

This document specifies an HTTP response header field that enables a server to inform the client that the requested website should be treated as "off-the-record." The purpose is to indicate that the server considers the content sensitive in some way, and the client should not retain any record of accessing it.

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://brave-experiments.github.io/draft-sahib-httpbis-off-the-record/#go.draft-sahib-httpbis-off-the-record.html>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-sahib-httpbis-off-the-record/>.

Discussion of this document takes place on the HTTP Working Group mailing list (<mailto:ietf-http-wg@w3.org>), which is archived at <https://lists.w3.org/Archives/Public/ietf-http-wg/>.

Source for this draft and an issue tracker can be found at <https://github.com/brave-experiments/draft-sahib-httpbis-off-the-record>.

Status of This Memo

Table of Contents

- 1. Introduction
- 2. Conventions and Definitions
- 3. Request-OTR Response
 - 3.1. Definition
 - 3.2. Operation
- 4. Off-The-Record Session
- 5. Comparisons With Other Approaches
 - 5.1. Private Browsing
 - 5.2. Manual Editing
 - 5.3. Clear-Site-Data
- 6. Security Considerations
 - 6.1. Navigation History
 - 6.2. Malicious Websites
 - 6.3. Consent
 - 6.4. Doesn't Protect Against
 - 6.5. Third Parties on the Same Site
 - 6.6. Only Applicable for Attacker
 - 6.7. Fingerprinting
 - 6.8. Self-Identification
- 7. IANA Considerations
- 8. References
 - 8.1. Normative References
 - 8.2. Informative References
- Acknowledgments
- Author's Address

