# Security in Cookies

Community members have expanded access to our knowledge library. If you're not seeing the complete article, Log in (https://community.akamai.com/customers/s/login). Not a member? Register here (https://community.akamai.com/customers/s/login/SelfRegister).

May 18, 2018 · Knowledge

## Description

**What is a Cookie?**

A cookie is a small file sent by a website (or set by a web server) and stored by the end-user's browser. Cookies let us get around the statelessness of the HTTP protocol by storing data at the client-side. Cookies are set using the ***Set-Cookie*** HTTP Header, sent in an HTTP response from the web server. This header instructs the web browser to store the cookie and send it back in future requests to the server. In most cases, a cookie is primarily used as either an authentication token or data storage vehicle.

**The Problem with Cookies**

- Cookies are stored on the client-side and in some cases may contain sensitive data (e.g. an IP address of an internal server or PII) that is set in clear text. Therefore, the cookie data is in complete control of the client; it can be modified or overwritten or captured and reused.
- Cookies are passed over HTTP, and HTTP does not encrypt the headers in anyway. This leaves cookies susceptible for sniffing attacks.
- Cookies are used to store session data. These are known as Session cookies. They store the respective Session ID of the user. The real power of the session happens server side where the Session ID is used to pull data stored on the server that you don't want the client to have access or authorize an end-user for example. Imagine the damage that can be caused when a Session ID is sniffed and replayed again by a malicious attacker via a MITM or Replay attack.

**Identifying your Next Steps to Secure a Cookie**

To identify the security measures you should take to protect your cookie, you should ask yourself the following questions:

- Does my cookie contain any sensitive information? and how sensitive is it?
- Is my cookie passed over TLS? Does it need to persist if the user leaves an TLS portion of the site?
- Does the cookie need to work across different sub domains?
- What part of the my site really need to access my cookie?
- Does my cookie restrict access to Java scripts?

**Protecting your Cookie**

- **Encrypt cookies in the Browser** to protect them at-rest and in-transit. This can be done using a software of Javascript APIs. Encrypting the cookie itself will protect you against:
  - **Session Hijacking**: if the cookie is sent in an encrypted manner, attempts for hijacking attacks will be mitigated in this case, even if the cookies are sent over clear HTTP.
  - **Sniffing Attacks**: in case someone gains local access to your computer and scans for cookies OR someone sniffs your cookie while in-transit, encrypted cookies prevent the attacker from viewing the cookie contents.
  - **XSS Attacks:** in case a cookie gets captured via a cross site scripting attack, the information or data is going to be non-usable in encrypted format or will add a layer of complexity for the attacker to decrypt the captured info.Last but not least, "encrypting your cookies in the browser provides you with user privacy."
- **Pass your cookies over TLS** to protect your cookie in-transit.
- **Set the right attributes** for your cookies to secure them and make them safer. Below is a list of attributes that can be set on a per-cookie basis which makes them safer to use:

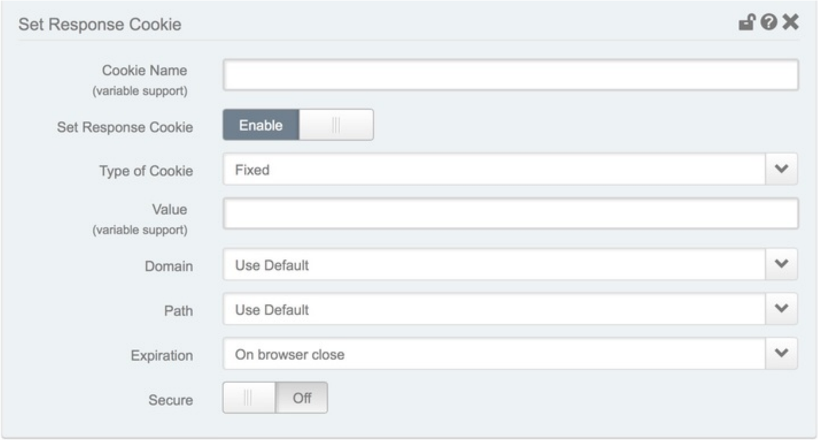
- ***Secure:*** informs the browser (or other http clients) to only send the cookie over secure connections (HTTPS or TLS). This means that the cookie will not be available to any part of the site that is not secure, it also makes it much less likely that you will accidentally send the cookie in clear text.
- ***HTTPOnly:*** informs the browser that it should not allow Java scripts to access the content of a cookie. This helps protect against XSS attacks as it will prevent hackers from being able to retrieve and use session or other type of info through such an attack.
- ***Domain:*** allows you to specify whether or not to send the cookie to sub-domains. Setting "www.foo.com (http://www.foo.com)" for instance will mean only the exact domain "www.foo.com (http://www.foo.com)" will be matched, while setting ".foo.com (http://foo.com)" will also match again any sub-domain (e.g. support.foo.com (http://support.foo.com), blog.foo.com (http://blog.foo.com), etc…)
- ***Path:*** specifies the location or path the cookie is valid for. For example, the default value of "/" means every request will get the cookie, while "/services/" would limit the cookie to just that path. This path is going to be based on the actual URL the browser uses, before any mod_rewrite or URL mapping. It is important when using this attribute to use as restrictive a path as possible to avoid attacks launched from co-located apps.
- ***Expires:*** offers strong protection against misuse of cookies because it erases the cookie when the expiration date is met. If this attribute is not set then the cookie will be erased when the browser is closed by the end-user.
- ***SameSite***: has been introduced by Google Chrome recently. This attribute offers a robust defense against CSRF attacks when deployed in strict mode, and when supported by the client. It basically requests the browser to only send the cookie in a first-party context (when you are using the web application directly). When another site tries to request something from the web application, the cookie is not sent. This effectively makes CSRF impossible, because an attacker can not use a user's session from his site anymore. This attribute might not be supported by Akamai at this point. *Please reach out to your account team to confirm.*

***Here are some good references on the SameSite attribute***:

- draft-west-first-party-cookies-07 - Same-site Cookies (https://ac.akamai.com/external-link.jspa?url=https%3A%2F%2Ftools.ietf.org%2Fhtml%2Fdraft-west-first-party-cookies-07)
- Preventing CSRF with the same-site cookie attribute (https://ac.akamai.com/external-link.jspa?url=https%3A%2F%2Fwww.sjoerdlangkemper.nl%2F2016%2F04%2F14%2Fpreventing-csrf-with-samesite-cookie-attribute%2F)

You will find some of the best practices or guidelines we discussed above under OWASP Secure Coding Practices Checklist - OWASP (https://ac.akamai.com/external-link.jspa?url=https%3A%2F%2Fwww.owasp.org%2Findex.php%2FOWASP_Secure_Coding_Practices_Checklist)

The Professional Services team (or yourself) can help improve the security of your cookie by setting the right attributes for your cookie at the edge in your Akamai configuration.



Set Response Cookie

| | |
|---|---|
| Cookie Name (variable support) | |
| Set Response Cookie | Enable |
| Type of Cookie | Fixed |
| Value (variable support) | |
| Domain | Use Default |
| Path | Use Default |
| Expiration | On browser close |
| Secure | Off |

Please reach out to you account team to discuss your cookies security posture in depth.

**Title**

Security in Cookies

**URL Name**

Security-in-Cookies

**Created Date**
4/12/2017 9:16 PM

Home (/customers/s/) Explore Support More from Akamai Log in

Files

**Related Articles**

| | |
|---|---|
| mPulse FAQ (/customers/s/article/mPulse-FAQ) | 32.12K |
| AnswerX & Resolver DNS (rDNS) Security - Resisting Attacks, Threat, & Denial of Service (DOS) (/customers/s/article/AnswerX-Resolver-DNS-rDNS-Security-Resisting-Attacks-Threat-Denial-of-Service-DOS) | 1.39K |
| Is Your Akamaized Property Ready for the new TLS Security Requirements for PCI Compliance? (/customers/s/article/Is-Your-Akamaized-Property-Ready-for-the-new-TLS-Security-Requirements-for-PCI-Compliance) | 6.23K |
| Security considerations regarding the Akamai debug HTTP headers (/customers/s/article/Security-considerations-regarding-the-Akamai-debug-HTTP-headers) | 3.54K |
| End of Life (EOL):Windows® Media Streaming” and “QuickTime® Streaming - Migration Path Options (/customers/s/article/End-of-Life-EOL-Windows-Media-Streaming-and-QuickTime-Streaming-Migration-Path-Options) | 6.12K |

**Akamai Confidential.** The information in this knowledge base article is believed to be accurate as of the date of this publication but is subject to change without notice. You understand and agree that use of this content is at your own discretion and risk and that you will be solely responsible for any damage that results from your use of it. The information is subject to the confidentiality provisions of the Terms & Conditions governing your use of Akamai services.

**Your cookie choices for this website**

Manage Preferences Accept Cookies

We use cookies to ensure the proper function of this website and to improve your website experience. Click “Accept Cookies” to agree to the current cookie settings or click “Manage Preferences” to make individual choices and get details on the cookies in use. For additional information relating to your privacy take a look at our Privacy Statement (https://www.akamai.com/us/en/multimedia/documents/akamai/akamai-privacy-statement.pdf)

COMPANY
Leadership (https://www.akamai.com/us/en/about/leadership/)
Our History (https://www.akamai.com/us/en/about/company-history.jsp)
Locations (https://www.akamai.com/us/en/locations.jsp)
Investor Relations (https://www.ir.akamai.com/)
Diversity (https://www.akamai.com/us/en/about/careers/workplace-diversity.jsp)
Corporate Responsibility (https://www.akamai.com/us/en/about/corporate-responsibility/)
Compliance (https://www.akamai.com/us/en/about/compliance/)
Events (https://www.akamai.com/us/en/about/events/)
Our Partners (https://www.akamai.com/us/en/partners/)

CAREERS
Students (https://akamaijobs.referrals.selectminds.com/info/page1)
Working at Akamai (https://www.akamai.com/us/en/about/careers/working-at-akamai.jsp)

NEWSROOM
Media Resources (https://www.akamai.com/us/en/about/news/media-resources.jsp)
Press Contacts (https://www.akamai.com/us/en/about/news/press-contacts.jsp)

RESOURCES
akamai.com (https://www.akamai.com/)
For Developers (https://developer.akamai.com/)
Akamai Blog (https://blogs.akamai.com/)

SOCIAL
Facebook (https://www.facebook.com/AkamaiTechnologies/)
LinkedIn (https://www.linkedin.com/company/akamai-technologies)
Twitter (https://twitter.com/Akamai)
YouTube (https://www.youtube.com/user/akamaitechnologies)

PRIVACY TRUS
Policy Details (https://www.
policies/)
Cookie Settin
(https://www.
policies/mana

Akamai secures and delivers digital experiences for the world’s largest companies. Akamai’s intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the pov architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai’s portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world’s top brands trus (https://www.akamai.com), blogs.akamai.com (https://blogs.akamai.com), or @Akamai (https://twitter.com/Akamai) on Twitter. You can find our global contact information at www.akamai.com/locations (https://www.akamai.com/us/en/locations.jsp).

| Privacy & Policies (https://www.akamai.com/us/en/privacy-policies/) | EMEA Legal Notices (https://www.akamai.com/us/en/privacy-policies/legal-notices.jsp) | Support (https://www.akamai.com/us/en/support/) | Community Manager (mailto:c
Sitemap (/customers/s/sitemap)