

What is a Web Session?

Are you wondering "what is a web session?" You're not alone. Despite being a crucial part of the modern World Wide Web, web sessions aren't always understood as well as they should be.

Below, we'll discuss everything you need to know about web sessions: what a web session is, how web sessions work, and the difference between web sessions and cookies.

What is a web session?

In English, the word "session" refers to a discrete block of time during which an activity is performed. A **web session** is therefore the amount of time that a user spends browsing a given website: from the moment they arrive on the first page, to the moment they leave the site.

How do web sessions work?

In practice, a web session consists of the data or files that are persistent throughout the use of a website or web application. These resources are uniquely identified with a **session ID**. The user's browser is given this ID upon beginning a new session, and this ID is exchanged during each subsequent communication between the browser and the server.

A web session includes all the information that may be relevant during the user's visit. Depending on the purpose of the website or web application, this may include data such as:

- The pages the user has viewed
- The contact details that the user has entered into a form
- The items in the user's shopping cart

There is typically some upper time limit for web sessions, after which the session will time out. This maximum time limit depends on the implementation. For example, web sessions in [Google Analytics](#) expire after 30 minutes of inactivity; further user activity will be treated as a new session.

Websites and web applications with very high numbers of users often cache web sessions, so that they can be retrieved faster and more efficiently.

Why use web sessions?

The benefits of using web sessions are obvious: web sessions allow the website to have some form of "short-term memory" about a user's activity.

On one hand, having no memory of users at all would be extremely inconvenient. If an e-commerce website could not remember a user's actions, for example, users would have to place e-commerce orders all at once within a single action, rather than storing items in a shopping cart.

On the other hand, having a memory that is too long can also be impractical. For example, if a user returns to an e-commerce website after a month, they may not want to see the same items in their shopping cart as they had last time.

Web sessions represent a balance between these two extremes. Short-term web sessions give websites and web applications enough "memory" to build engaging, personalized user experiences over the course of a user's visit, without storing too much information that is irrelevant in the long run.

Web sessions vs. cookies

Web sessions are frequently compared to (and confused with) cookies. Although both cookies and web sessions store information about a user, their functions are different in practice.

Cookies are text files that are used to authenticate and track visitors to a website, and that are stored only on the user's machine. The lifespan of a cookie is typically much longer than that of a web session, on the order of months or even years. Cookies are how websites store long-term user information that should be preserved: for example, automatically logging the user in when arriving at the website, or automatically filling in a form with the user's details.

By contrast, web sessions are meant to store information about only the user's most recent activities. Web sessions are stored on the server rather than the client, which helps prevent malicious users from editing them. Both web sessions and cookies can be used in combination to keep track of users' long-term and short-term behavior.

Similar terms

[Data Grid](#)

[Geospatial Data](#)

[Key-Value Store](#)

[Microservices](#)

[Sharding](#)

[Time Series Database](#)

[Tomcat web session replication](#)