# Web Cookies

The web is not private by default. Websites often use **cookies** to track user actions on their site and even across other sites.

**What's a cookie?**

An **HTTP cookie** is a small amount of text that helps a website track information about a user across multiple pages of the website and personalize the user's experience on the website. If you've ever logged into a website, a cookie kept you logged in across multiple pages.

## The cookie process

### ***Step 1: Browser requests a website***

Imagine a user that navigates to a website for the first time--or at least, the first time from that particular browser. The browser sends an HTTP request to the server that hosts the website.

GET /index.html HTTP/1.1

Host: www.shoopshop.com

### ***Step 2: Server sends cookie with response***

The server sends back an HTTP response and includes a Set-Cookie header in that response.

HTTP/1.0 200 OK

Content-type: text/html

Set-Cookie: sessionId=abc123; Expires=Wed, 09 Jun 2021 10:18:14 GMT

...

The cookie contains a name (sessionId) and a value (abc123), plus an expiration date for the browser to clear this cookie from its memory.

If it wants to set multiple cookies, it adds more Set-Cookie headers to the response.

### ***Step 3: Browser stores cookie***

The browser saves the cookie information, storing it on the user's hard drive. That way, the data will persist even after restarting the browser or computer. That's why this type of cookie is called a "**persistent cookie**".

There are also "**session cookies**", cookies with no expiration date which are always deleted when the browser is shut down.

### ***Step 4: Browser sends cookies with requests***

When the user navigates to a different page on the website, the browser sends along the stored cookies with each HTTP request.

GET /shop.html HTTP/1.1

Cookie: sessionId=abc123

### ***Step 5: Server personalizes response***

When the server receives the HTTP request, it inspects the cookies and sees that this request is coming from a user with a known sessionId. It can then look up that session ID in its database and use any information about the session to personalize the response.

**Third-party cookies**

Each cookie stored by a browser is associated with a domain and path. When you visit a website and its server sends back an HTTP response with a cookie, the browser associates that cookie with the domain of the server. That's called a **first-party cookie**.

However, a website can also include resources from other domains, like an image, iframe, or script. When the browser requests those resources, their servers can also send back cookies, which will now be associated with their domain. These are called **third-party cookies**.