Session and Persistent Cookies

In this lesson, we'll study two types of cookies, persistent and session.

We'll cover the following

Session cookies

When a server sends a cookie without setting its `Expires` or `Max-Age`, browsers treat it as a *session cookie*. Rather than guessing its time-to-live or applying funny heuristics, the browser deletes it when it shuts down.

Persistent cookies

A *persistent cookie*, on the contrary, is stored on the client until the deadline set by its `Expires` or `Max-Age` directives.

Session restoring

It is worth noting that browsers might employ a mechanism known as *session restoring*, where session cookies can be recovered after the client shuts down. Browsers have implemented this kind of mechanism to conveniently let users resume a session after a crash.

Session restoring could lead to unexpected issues if we're expecting session cookies to expire within a certain timeframe (e.g., we're absolutely positive a session would not last longer than X amount of time). From a browser's perspective, session restoring is a perfectly valid feature, as those cookies are left in the hands of the client, without an expiration date.

What the client does with those cookies does not affect the server, who is unable to detect whether the client shut down at any point in time. If the client wishes to keep session cookies alive forever that's no concern for the server. It would definitely be a questionable implementation, but there's nothing the server could do about it.

Session vs persistent cookies

I don't think there is a clear-cut winner between session and persistent cookies, as both might serve different purposes very well. What I've observed, though, is that Facebook, Google, and similar services will use persistent cookies. From personal experience, I've always used persistent cookies, but never had to tie critical information, such as a social security number or a bank account's balance, to a session.

In some contexts, you might be required to use session cookies due to compliance requirements. I've seen auditors asking to convert all persistent cookies to session ones. When people ask me "*should I use X or Y?*" my answer is "it depends on the context." Building a guestbook for your blog carries different security ramifications than building a banking system. As we will see later in the course, I would recommend understanding your context and trying to build a system that's *secure enough*: Absolute security is a utopia, just like a 100% SLA.

In the next lesson, we'll study the `Host-only` cookie.