Alternatives

In this lesson, we'll study the alternatives to cookies.

We'll cover the following

- localStorage
- JWT

Reading all of this material about cookies and security you might be tempted to say, “I really want to stay away from cookies!”. The reality is that, as of now, cookies are your best bet if you want to implement some sort of session mechanism over HTTP. Every now and then I’m asked to evaluate alternatives to cookies, so I’m going to try and summarize a couple of things that often get mentioned:

localStorage

Especially in the context of single-page applications (SPA), localStorage is sometimes mentioned when discussing where to store sensitive tokens. The problem with this approach, though, is that localStorage does not offer any kind of protection against XSS attacks. If an attacker is able to execute a simple `localStorage.getItem('token')` on a victim’s browser, it’s game over. `HttpOnly` cookies easily overcome this issue.

JWT

JSON Web Tokens define a way to securely exchange data between two clients, in the form of a token. JWT is a specification that defines what an access token would look like but does not define where the token is going to be stored. In other words, you could store a JWT in a cookie, localStorage or even in memory so it doesn’t make sense to consider JWTs an alternative to cookies.

In the next lesson, we’ll look at a quick conclusion to this chapter.