Introduction HTTP Cookies

In this lesson, we'll get a quick introduction to cookies.

We'll cover the following

- Why are they important?

What are cookies?

Imagine you are a backend developer who needs to implement *sessions* in an application. The first thing that comes to your mind is to issue a *token* to clients and ask them to send this token with their subsequent requests. From there onwards you are going to be able to identify clients based on the token included in their request.

HTTP cookies were born to standardize this sort of mechanism across browsers. They're nothing more than a way to store data sent by the server and send it along with future requests. The server sends a cookie, which contains small bits of data, the browser stores it and sends it along with future requests to the same server.

Why are they important?

Why would we bother learning about cookies in a security course? Because the data they contain is, more often than not, extremely sensitive. Cookies are generally used to store session IDs or access tokens, an attacker's holy grail. Once they are exposed or compromised, attackers can impersonate users or escalate their privileges on your application.

Securing cookies is one of the most important aspects when implementing sessions on the web. This chapter will, therefore, give you a better understanding of cookies, how to secure them, and what alternatives can be used.

cookies, how to secure them, and what alternatives can be used.

In the next lesson, we’ll dive a little deeper into how cookies work.