The simple recipe for user authentication

1. **Ask the user for a login and password** and send it to the server (HTTP/POST request)

2. **Verify the login/password** based on information stored on the server (usually in the database)

3. **Start a session** once the user has been authenticated

4. **Grant access to resources** according to the session

The simple recipe for user authentication

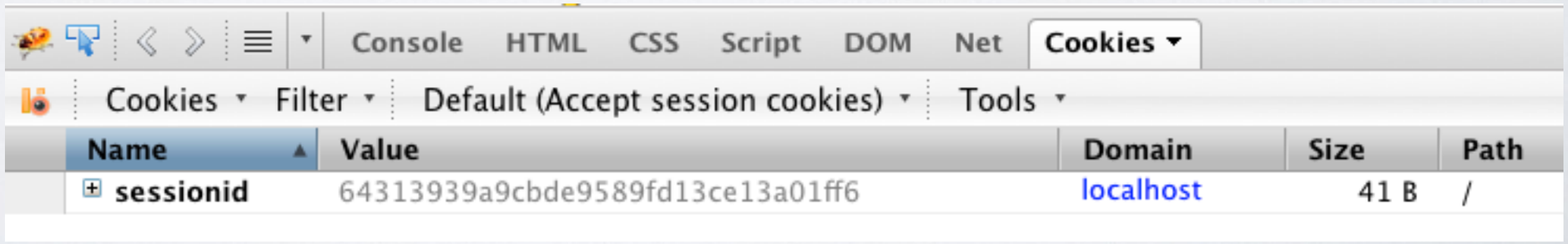
1. **Ask the user for a login and password** and send it to the server (HTTP/POST request)
2. **Verify the login/password** based on information stored on the server (usually in the database)
3. **Start a session** once the user has been authenticated
4. **Grant access to resources** according to the session

The concept of session

There is a **session id** (aka token)
between the browser and the web application

This session id should be **unique** and **unforgeable**
(usually a long random number or a hash)

➡ Stored in the cookie

The session id is bind to **key/value pairs data**

➡ Stored on the server