# Sessions and Cookies

## Cookies

### Storage Location:

**Client-side** (stored as small text files in the user's web browser).

### Data Stored

Small amounts of data (typically up to 4KB per cookie). They store key-value pairs.

### Purpose

Primarily for **remembering user preferences**, tracking user behaviour, "remember me" login functionality, or storing non-sensitive identifiers. They can also be used for session management (by storing a Session ID).

### Lifespan

#### Session Cookies:

Last only for the duration of the browser session (deleted when the browser is closed).

#### Persistent Cookies:

Can be set with an expiration date, allowing them to persist on the user's device for days, months, or even years, or until manually deleted by the user.

### Visibility

Cookies are visible and accessible to the client's browser (and potentially client-side JavaScript, unless HttpOnly flag is set). Users can inspect, delete, or block cookies through browser settings.

### Security

Less secure than sessions for sensitive data because they are stored on the client side and are vulnerable to certain client-side attacks (like Cross-Site Scripting if not properly secured with HttpOnly).

### Server Load:

Do not directly consume server memory for data storage, reducing server load.

### Transmission

Sent automatically by the browser with every subsequent HTTP request to the same domain.

## Sessions

### Storage Location:

**Server-side** (stored in the web server's memory, file system, or a database). Only a small **Session ID** is typically stored on the client side (usually as a session cookie or via URL rewriting) to identify the server-side session.

### Data Stored:

Can store larger amounts and more complex data structures, as the data resides on the server.

### Purpose:

Primarily for **maintaining user state and context** during a single period of interaction (a "session"). This includes user authentication status, shopping cart contents, temporary form data, and other sensitive or frequently changing information.

### Lifespan:

Typically lasts for a **single Browse session** (until the user logs out or closes the browser).

Can have a **timeout** period of inactivity (e.g., 30 minutes), after which the server-side session is automatically invalidated.

### Visibility:

The actual session data is **not directly exposed to the client**. Only the Session ID is visible.

### Security:

Generally, **more secure** for sensitive data because the data itself never leaves the server. This reduces risks like data tampering or exposure through client-side vulnerabilities.

### Server Load:

Each active session consumes server resources (memory, CPU), which can become a concern for very large-scale applications with many concurrent users.

### Transmission:

The client sends the Session ID (e.g., via a cookie), and the server uses this ID to retrieve the associated session data from its storage.

|  |  |  |
| --- | --- | --- |
| Feature | Cookies | Sessions |
| Storage | Client-side (browser) | Server-side (with ID on client) |
| Data Size | Small (up to 4KB per cookie) | Can be larger, limited by server resources |
| Primary Use | Preferences, "Remember Me", tracking | Authentication, shopping carts, sensitive data |
| Lifespan | Session-based or persistent (set expiry) | Session-based (browser close or timeout) |
| Visibility | Visible to client, can be inspected | Data hidden from client, only ID visible |
| Security | Less secure (client-side exposure) | More secure (data remains on server) |
| Server Load | Low (data on client) | Higher (consumes server memory/resources) |
| Transmission | Entire cookie sent with each request | Only Session ID sent with each request |