State Management

Cookies and Sessions
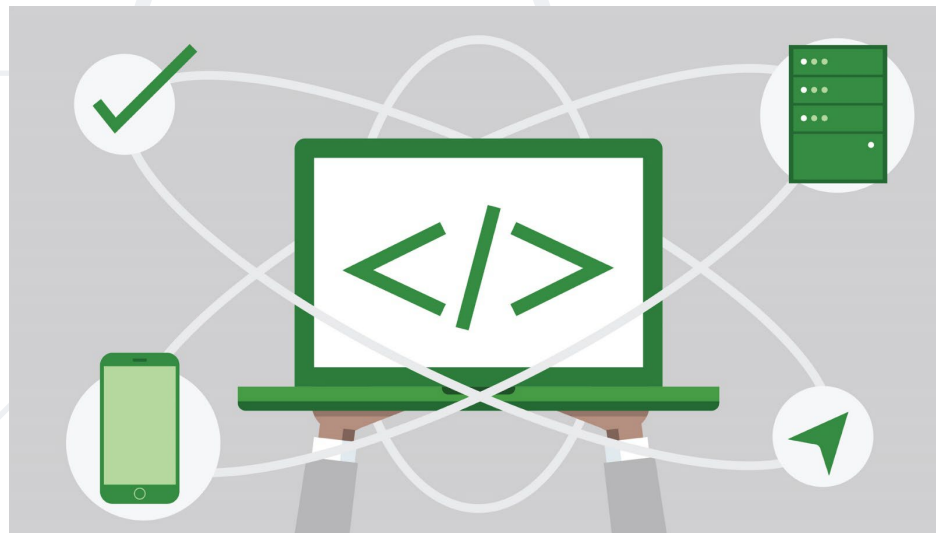
SoftUni Team

Technical Trainers

Software
University

SoftUni
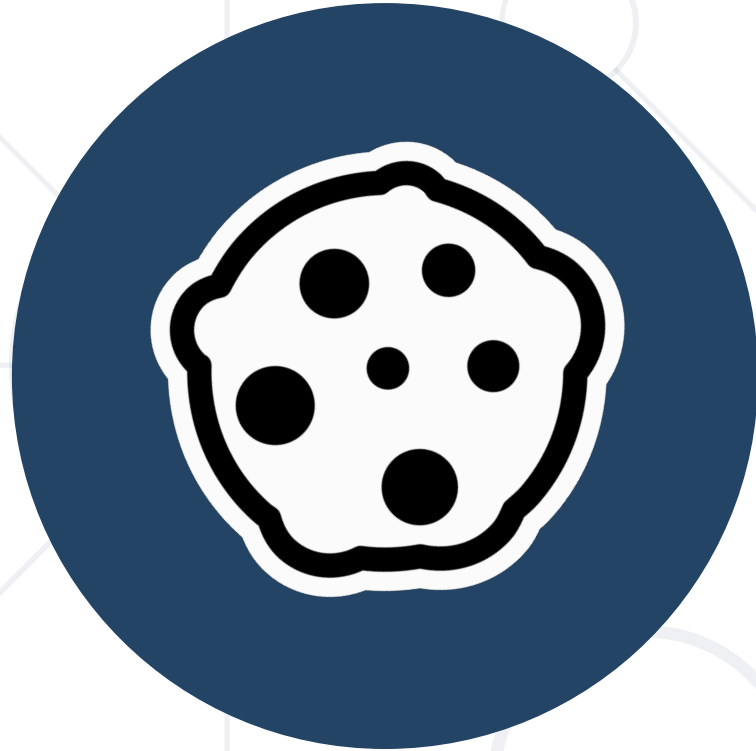
Software University

https://softuni.bg

Table of Content

sli.do

#java-web

HTTP Cookies

Usages and Control

What Are Cookies?

- A **small file** of **plain text** with no executable code

    - Sent by the server to the client's browser

    - Stored by the browser on the client's device (computer, tablet, etc.)

    - Hold small piece of data for a particular client and a website

What Are Cookies Used for?

- **Session management**

  - Logins, shopping carts, game scores, or anything else the server should remember

- **Personalization**

  - User preferences, themes, and other custom settings
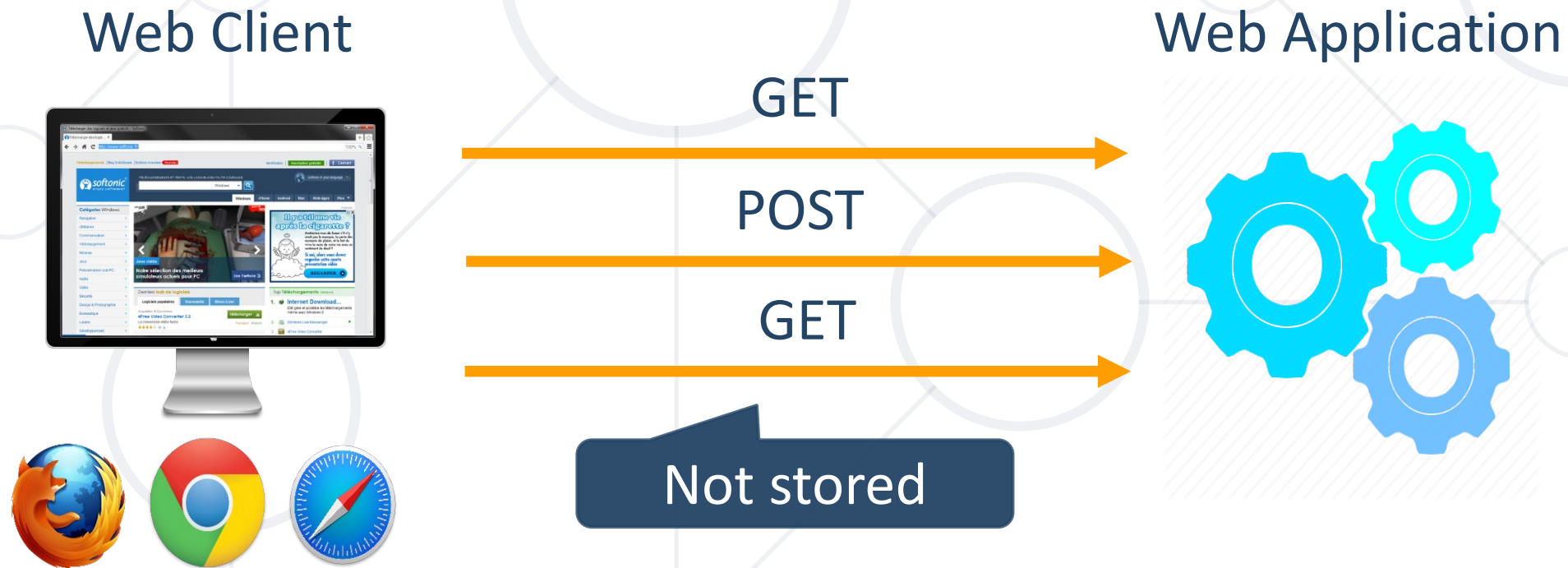
- **Tracking**

  - Recording and analyzing user behavior

- Breakfast

  - But that's not what we are currently talking about

Session Management

- The HTTP object is **stateless**
  - It **doesn't store** information about the requests

Web Client

Web Application

GET

POST

GET

Not stored

Stateless HTTP – the Problem

- The **server does not know** if two requests come from the same client

- **State management** problems
    - Navigation through pages requires **authentication each time**
    - Information about the pages is lost **between the requests**
    - **Harder personalization** of page functionality

Stateless HTTP – the Cookie Solution

- A reliable **mechanism** for websites to **remember stateful information**

  - to know whether the user is **logged in or not**

  - to know **which account** the user is logged in with

  - to record the user's **browsing activity**

  - to remember pieces of information **previously entered** into form fields (usernames, passwords, etc.)

How Are Cookies Used?

- The response holds the cookies to be saved within the **Set-Cookie** header

```
HTTP/1.1 200 OK
Set-Cookie: lang=en
```

- The request holds the specific web site cookie within the **Cookie** header

```
GET /index HTTP/1.1
Cookie: lang=en
```

Server-Client Cookies Exchange

Software University

http://www.example.bg/

Web Client

Web Application

GET /index HTTP/1.1

HTTP/1.1 200 OK Set-Cookie: lang=en

GET /index HTTP/1.1

Cookie: lang=en

Cookie Structure

- The cookie consists of **Name**, **Value** and **Attributes** (optional)

- The attributes are **key-value pairs** with additional information

- Attributes are not included in the requests

- Attributes are used by the client to control the cookies

Name=Value

Attributes

```
Set-Cookie: SSID=Ap4P…GTEq; Domain=foo.com; Path=/;
Expires=Wed, 13 Jan 2021 22:23:01 GMT; Secure; HttpOnly
```

Scope

- Defined by the attributes **Domain** and **Path**

- **Domain** – defines the website that the cookie belongs to

- **Path** – Indicates a **URL** path that must exist in the requested resource before sending the **Cookie** header

```
Set-Cookie: SSID=Ap4P…GTEq; Domain=foo.com; Path=/;
Expires=Wed, 13 Jan 2021 22:23:01 GMT; Secure; HttpOnly
```

Lifetime

- Defined by the attributes **Expires** and **Max-Age**

- **Expires** – defines the date that the browser should delete the cookie

- By default the cookies are deleted after the end of the session

- **Max-Age** – interval of seconds before the cookie is deleted

```
Set-Cookie: SSID=Ap4P…GTEq; Domain=foo.com; Path=/;
Expires=Wed, 13 Jan 2021 22:23:01 GMT; Secure; HttpOnly
```

Security

- Security flags do not have associated values

- **Security** - tells the browser to use cookies only via **secure/encrypted** connections

- **HttpOnly** – defines that the cookie cannot be accessed via client-side scripting languages

```
Set-Cookie: SSID=Ap4P…GTEq; Domain=foo.com; Path=/;
Expires=Wed, 13 Jan 2021 22:23:01 GMT; Secure; HttpOnly
```

What is in the Cookie?

- The cookie file contains a table with **key-value** pairs

Name:	ELOQUA
Content:	GUID=50B3A712CDAA4A208FE95CE1F2BA7063
Domain:	.oracle.com
Path:	/
Send for:	Any kind of connection
Accessible to script:	Yes
Created:	Monday, August 15, 2016 at 11:38:50 PM
Expires:	Wednesday, August 15, 2018 at 11:38:51 PM

Remove

Examine Your Cookies (1)

- Most cookies are stored in a **RDBMS**, usually **SQLite**

- Download **SQLite browser** from **here**

- Location of Mozilla cookies

```
C:\Users\{username}\AppData\Roaming\Mozilla\Firefox\Profiles\{name}.default\cookies.sqlite
```

- Location of Chrome cookies

```
C:\Users\{username}\AppData\Local\Google\Chrome\User Data\Default\Cookies
```

Examine Your Cookies (2)

- Open the file with the **SQLite browser**
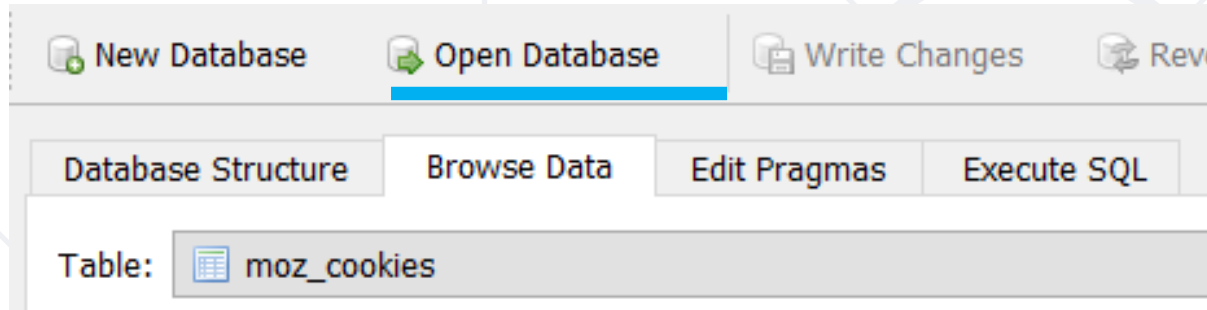
- Browse the cookies table

Control Your Cookies – Firefox Browser (1)

🔍 Find in Settings

⚙ **General**

🏠 **Home**

🔍 **Search**

🔒 **Privacy & Security**

🔄 **Sync**

m **More from Mozilla**

Send websites a "Do Not Track" signal that you don't want to be tracked   Learn more

◯ Always

🔵 Only when Firefox is set to block known trackers

Cookies and Site Data

Calculating site data and cache size...   Learn more

Clear Data...

☐ Delete cookies and site data when Firefox is closed

Manage Data...

Manage Exceptions...

Logins and Passwords

☑ Ask to save logins and passwords for websites

Exceptions...

☑ Autofill logins and passwords

Saved Logins...

☑ Suggest and generate strong passwords

☑ Suggest Firefox Relay email masks to protect your email address   Learn more

☑ Show alerts about passwords for breached websites   Learn more

🖉 Extensions & Themes

☐ Use a Primary Password   Learn more

Change Primary Password...

❓ Firefox Support

Formerly known as Master Password

☐ Allow Windows single sign-on for Microsoft, work, and school accounts   Learn more

19

Control Your Cookies – Firefox Browser (2)
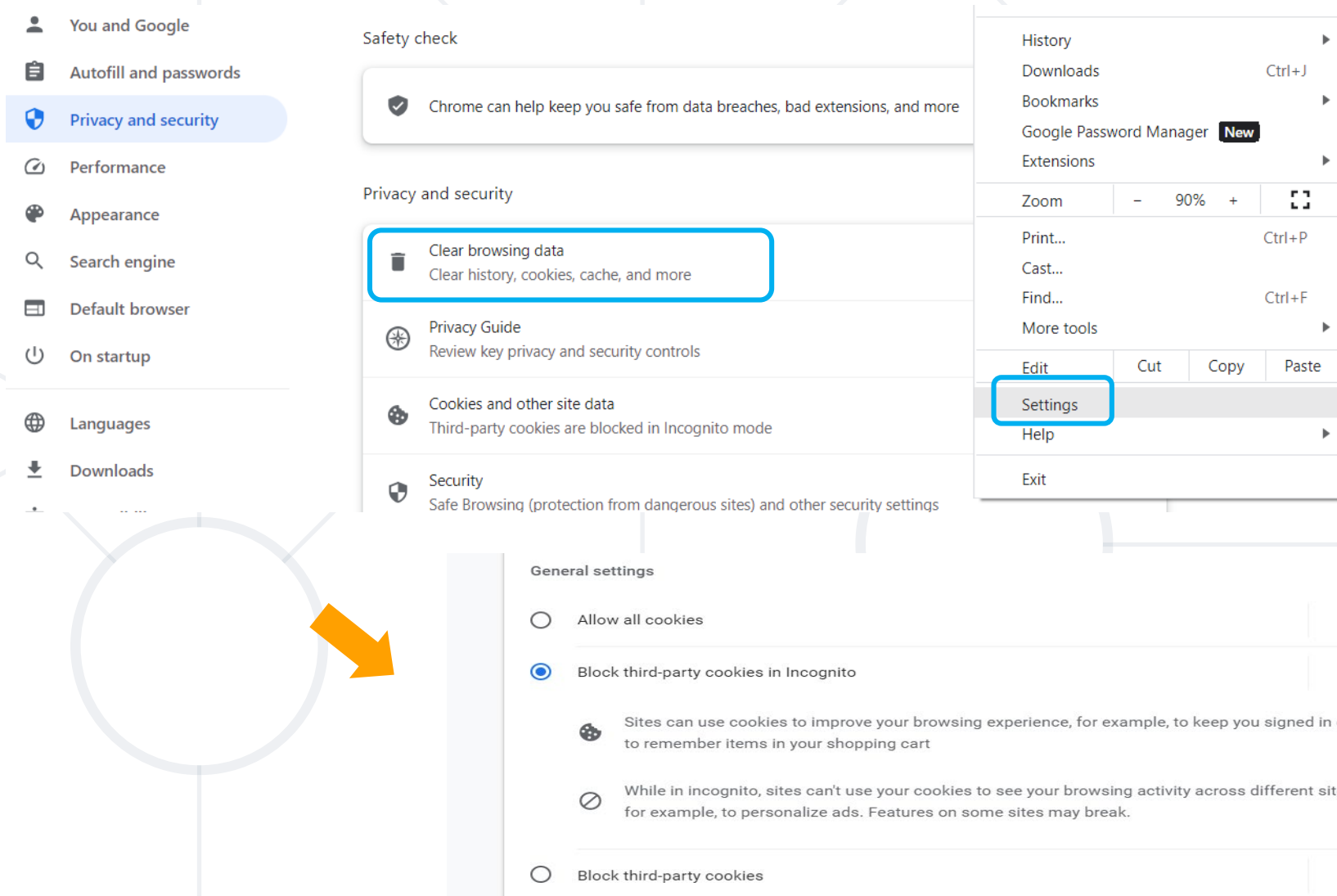
Browse cookies from a selected website

Delete a particular cookie or all cookies

Control Your Cookies – Chrome Browser

Third Party Cookies

- Cookies stored by an **external party** (different **domain**)

- Mainly used for advertising and tracking across the web

- By the end of 2023, Google will stop the use of third-party cookies.

Web Client

`http://stackoverflow.com/`

Web Application

Cookie transfer

Cookie transfer

Third Party

Cookies

Live Demo

Web Storage
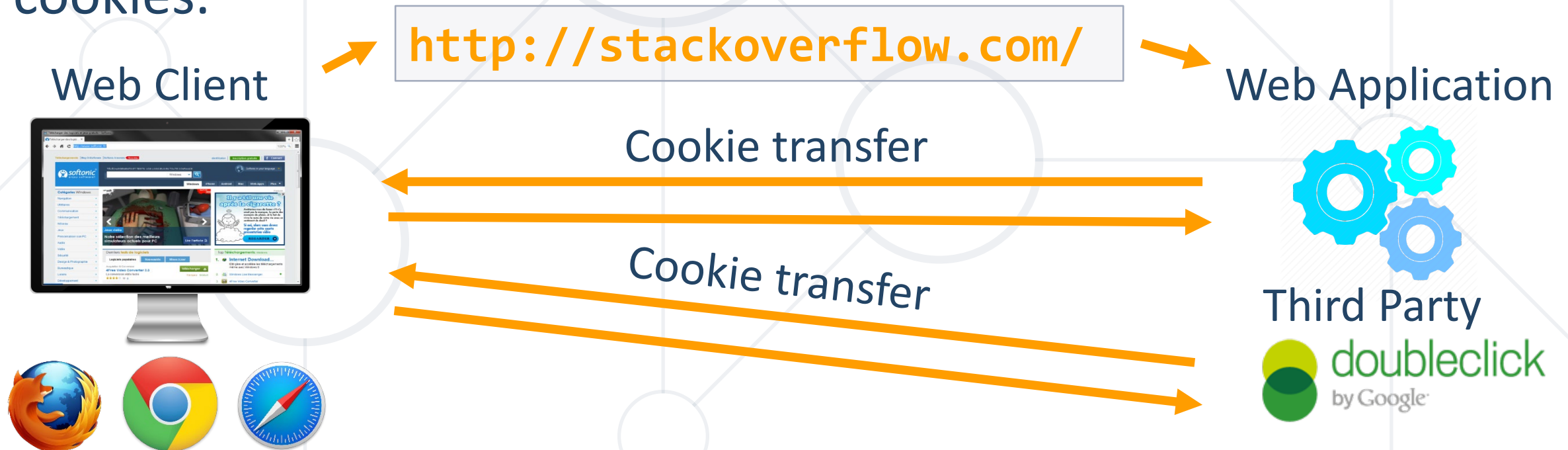
- Data is stored in **local storage** objects that have no expiration dates.

- Data is stored for one session in a **session storage** object (data is lost when the browser tab is closed).

Local Storage

- Pros
  - There is no expiration date for the data kept in local storage.
  - The storage limitation is approximately 10MB.
  - Data from local storage is never sent to the server.
- Cons
  - Since local storage data is in plain text, it is not designed to be secure.
  - Since the data type is restricted to strings, serialization is required.
  - Only the client side, not the server side, is capable of reading data.

Session Storage

- **Session Storage** is a way of storing data on the client side of an application. It's similar to local storage, but with a few key differences:

  - Data is only available to the site that created it.

  - Data is not shared with other sites.

  - Data is not persistent, meaning it is only available for the duration of the user's session on a site.

 - Data is specific to the browser tab in which it was created.

Differences

| Local Storage	Session Storage	Cookies
It allows **10MB** of data to be stored.	It allows **5MB** of data to be stored.	The storage capacity is limited to 4KB of data.
The stored data is not deleted when the browser is closed.	The data is stored only for the session and will be deleted when the browser is closed.	The data can be set to expire at a certain time.
Introduced in **HTML5.**	Introduced in **HTML5.**	Cookies are the oldest (**HTML4**) and most well known mechanism.
Useful for storing data that the user will need to access later, such as offline Data.	Great way to improve the performance of your web applications.	Cookies are a good choice for storing data that should not be persisted for a long time, such as session IDs.
The data is not sent with the request from the client to the server.	The data is not sent with the request from the client to the server.	The data is sent with the request from the client to the server.

HTTP Sessions

What Are Sessions?

- A way to store information about a user to be used across **multiple pages**
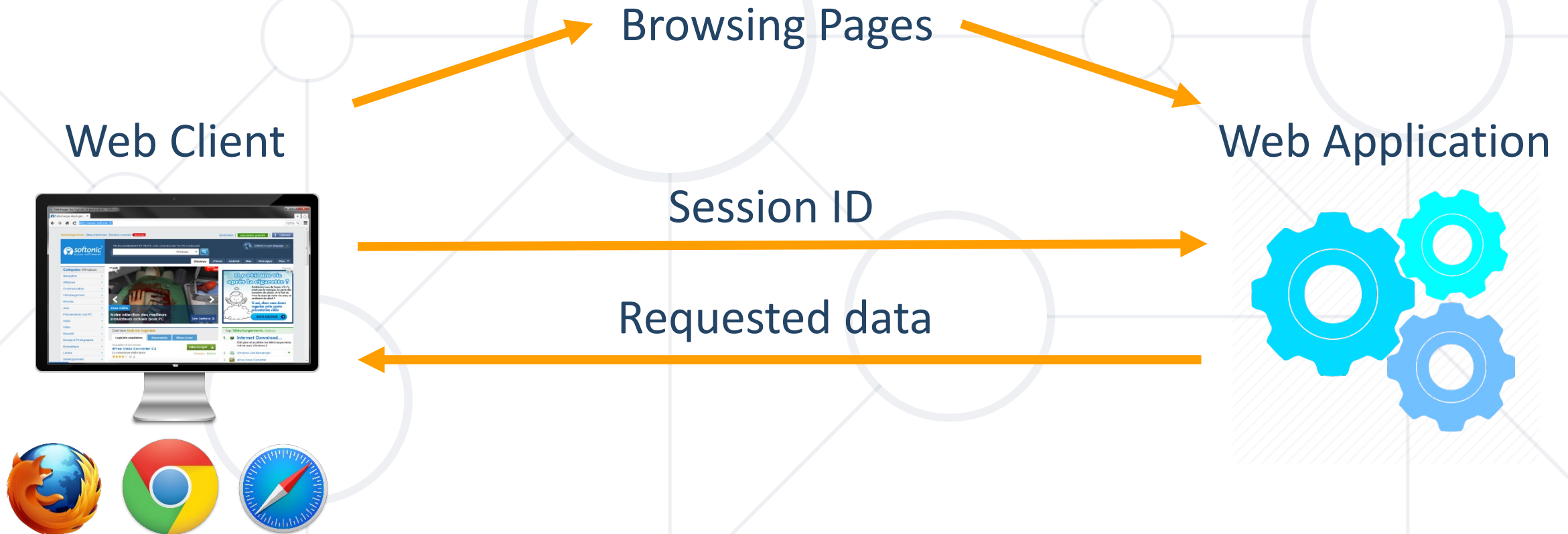
Web Application

Session

user: Teo

/login

/home

/products
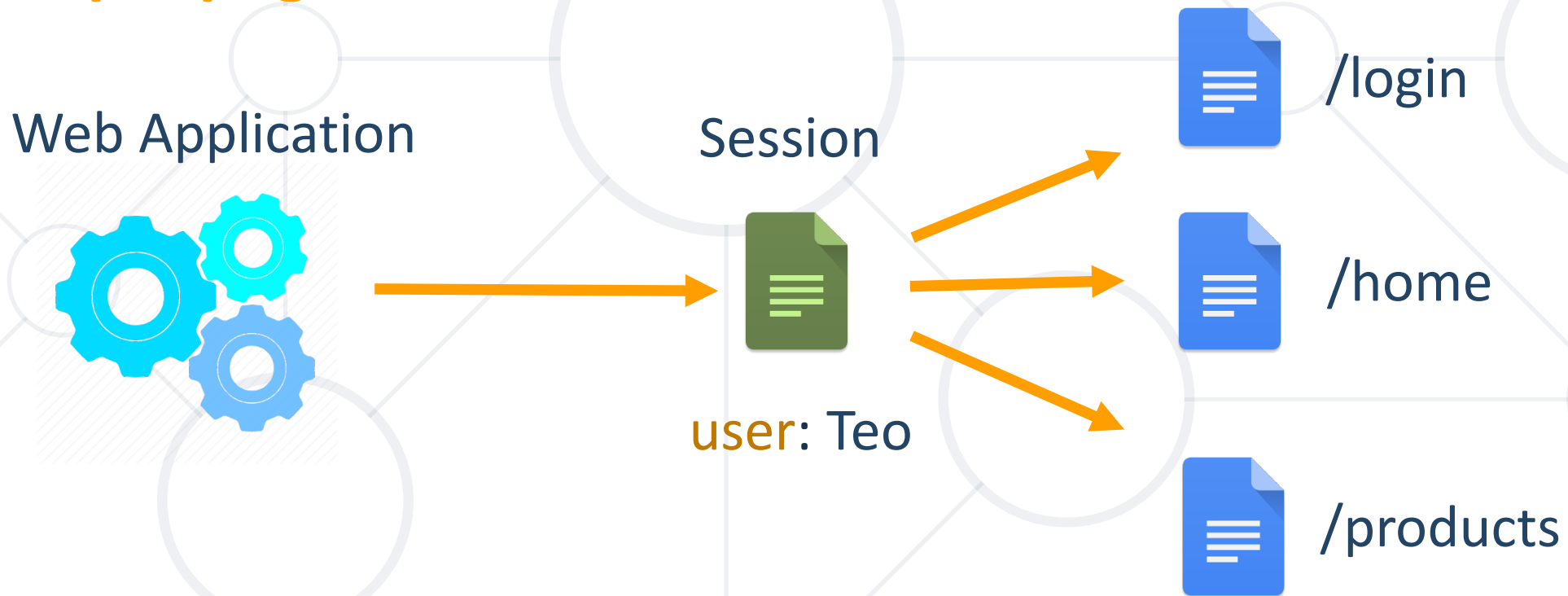
Session Management (1)

- The exchange mechanism be used between the user and the web application

First Time Login

Web Client

Web Application

User credentials
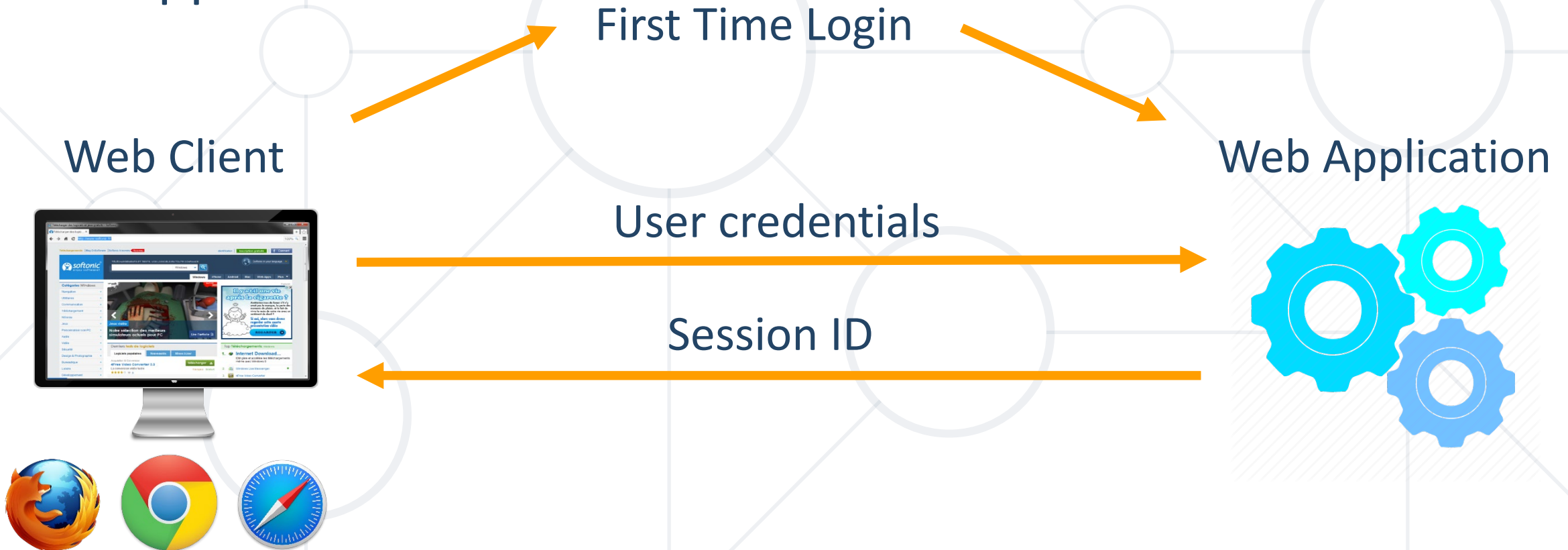
Session ID

Session Management (2)

■ The exchange mechanism be used between the user and the web application

Browsing Pages

Web Client

Web Application

Session ID

Requested data

- The exchange mechanism be used between the user and the web application

Browsing pages after
the server is restarted

Web Client

Web Application

Session ID

Requested data
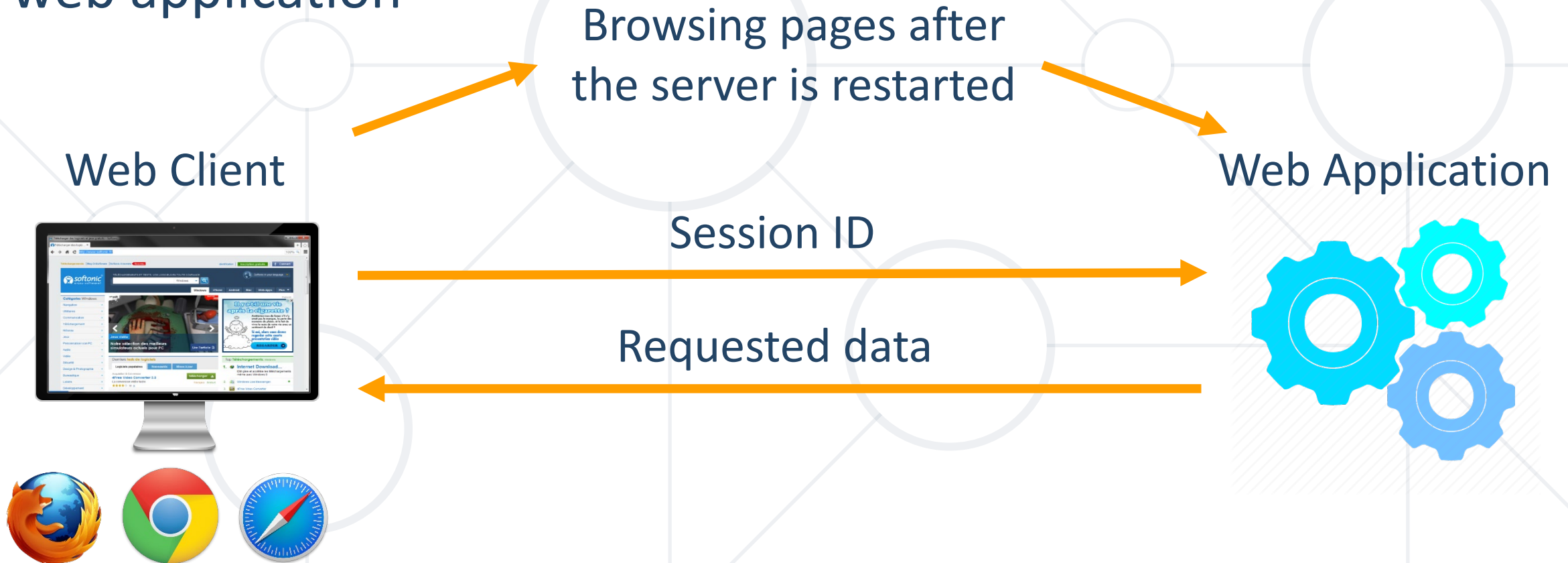
Relation with Cookies

Session Store

```
sid 5 {
  uid: 101
}
sid 7 {
  uid: 102
}
```

Cookie {
  name: sid
  value: 5
}

Req

Resp

Web Application

Validate

Session

Cookie {
  name: sid
  value: 7
}

Req

Resp

Get data

Create personal web page

Database

```
uid  name
101 Teo
102 Bojo
```

Session Structure

Unique Session ID

Key-Value pairs with user data

```
"hje85d3" : {
    user_id: 789
    username: FirstUser
},
"af354dd" : {
    user_id: 456
    username: SecondUser
},
"fg78e5s" : {
    user_id: 654
    username: ThirdUser
}
```
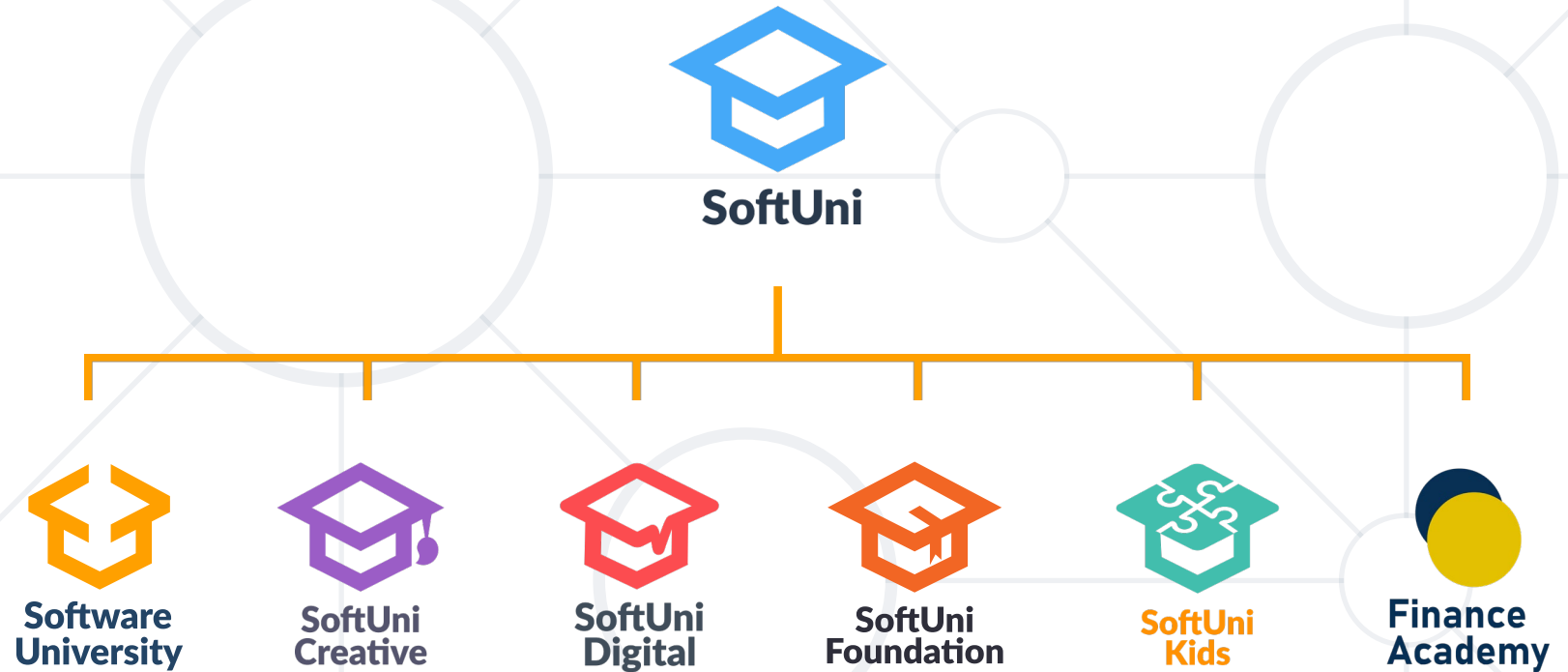
Sessions

Live Demo

Summary

- **Cookies** are client based stored information
  - They are created by web applications
  - Browser sends them back to the application
- **Sessions** are server based information
  - They are used across multiple pages
  - Stores important info about the client

Questions?

SoftUni Diamond Partners

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, about.softuni.bg
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity
- Software University Forums
  - forum.softuni.bg

License

- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**

- Unauthorized copy, reproduction or use is illegal

- © SoftUni – https://about.softuni.bg/

- © Software University – https://softuni.bg