Cookies and Sessions

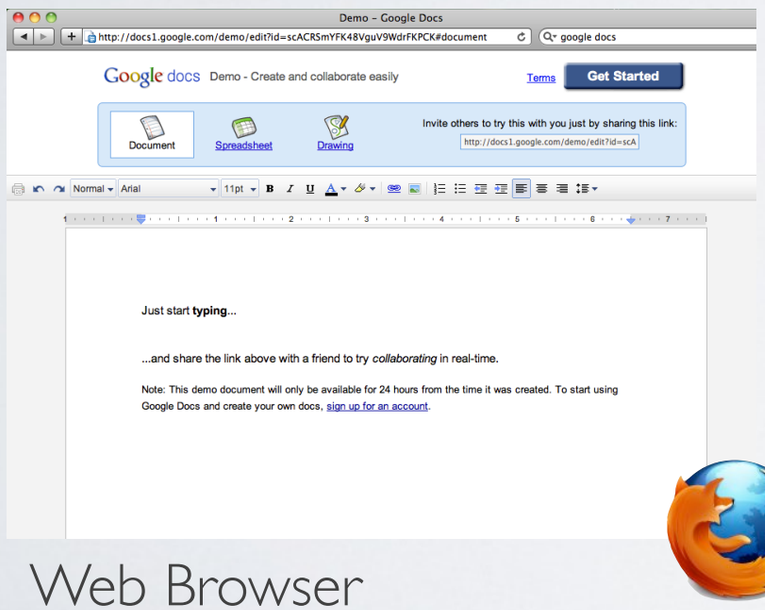
Thierry

Security assumptions

You have **absolutely no control** on the client

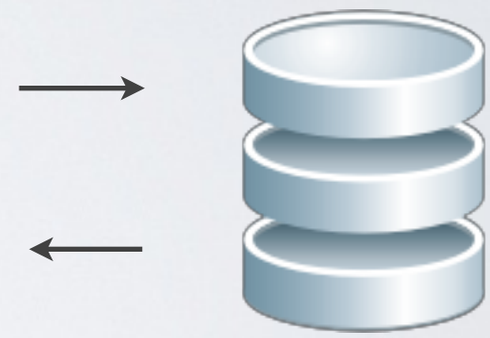
Client Side

Server Side



Web Browser

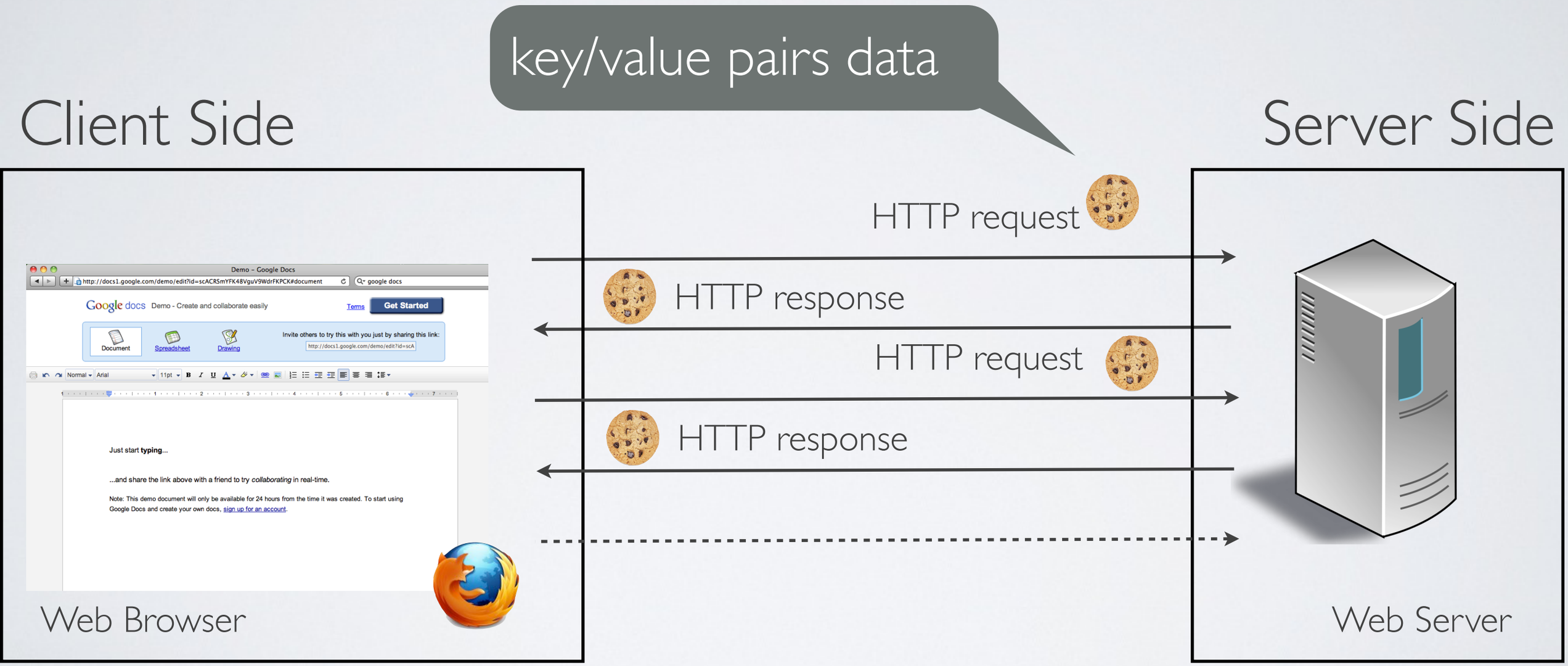
Web Server



Database

Cookies

The big picture



Cookies

Cookies are **key/value pairs** sent back and forth between the browser and the server in HTTP request and response

Anatomy of a Cookie

- Text data (Up to 4kb)
- May (or may not) have an expiration date
- Can be manipulated from the client **and** the server

Manipulating cookies

A cookie can be modified

- on the **server** side
  express middleware : `cookie`

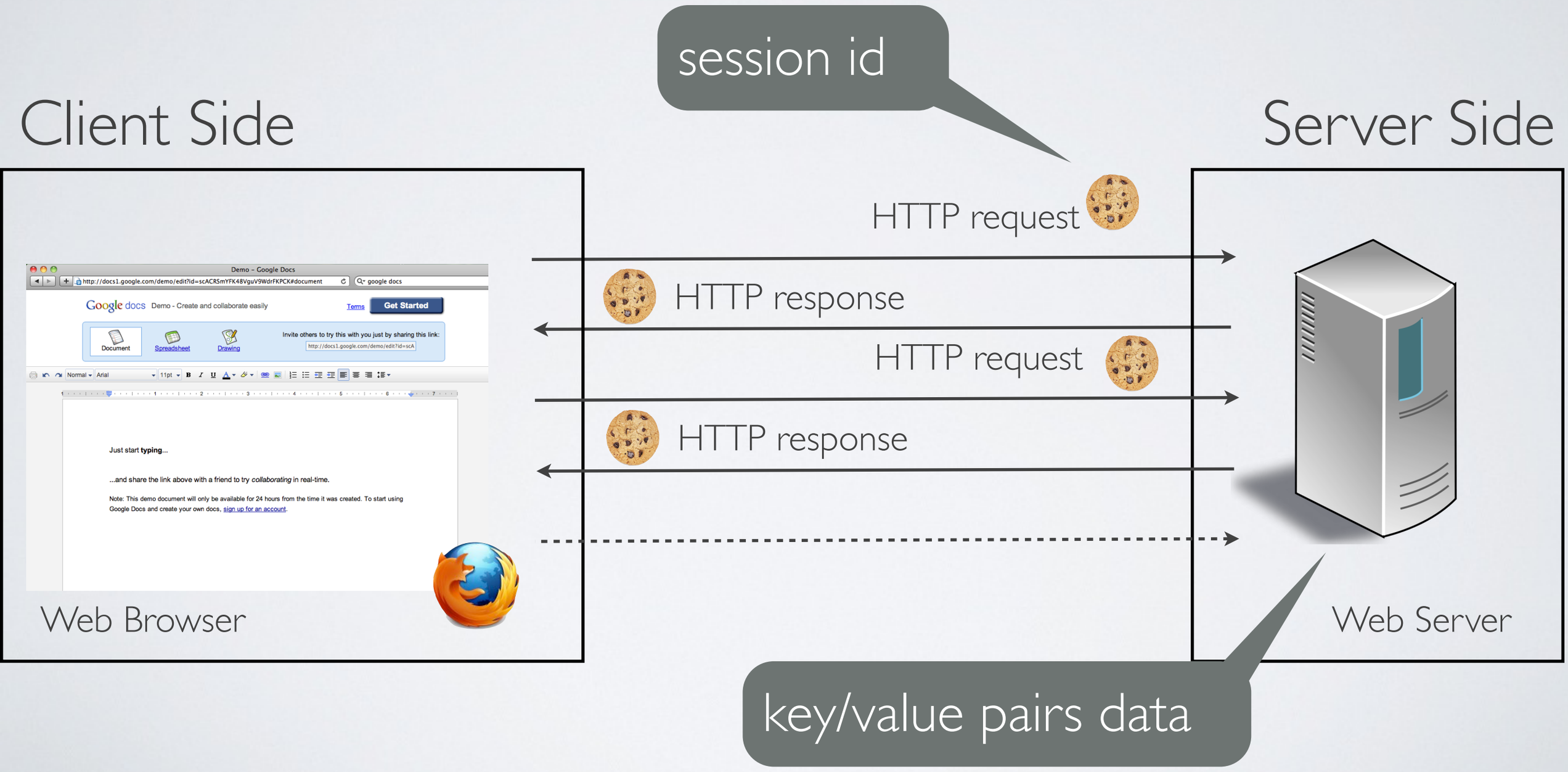
- on the **client** side
  javascript : `Document.cookie`

What cookies are useful for?

- Shopping cart
- Browsing preferences
- User authentication
- Tracking and advertisement

Sessions

The big picture



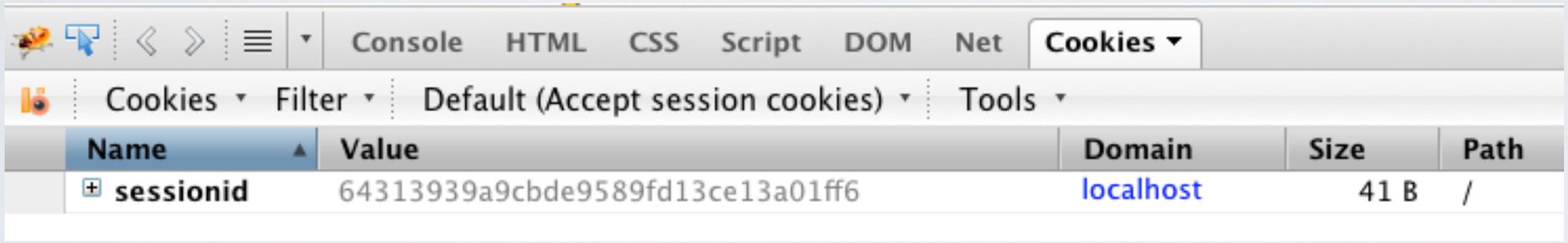
The concept of session

- 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)
- This session id is bind to **key/value pairs data**

Where sessions values are stored

- **Session ID** is stored in a cookie
- **Session key/value pairs** are stored on the server

Hacking sessions



The user can **create, modify, delete** the session ID in the cookie

But **cannot access** the key/value pairs stored on the server