Cookies

Sunday, May 19, 2024 10:40 AM

1. **About Cookies**
2. **Working**
3. **Types**
4. **Security Considerations**
5. **Code Demo**

About Cookies

Sunday, May 19, 2024 12:35 PM

1. Definition:

- A cookie, technically known as HTTP cookie, is a small piece of data that's stored within the browser where the end user is interacting with the web application.
- Main purpose of a cookie is to 'remember' the preferences of the user over a session. This helps provide the users a more *personalized experience*.
- Each browser has a specific database it uses to store cookies.
  - *Chrome and Firefox use SQLite database*

2. Why Cookies ?

Helps improve overall user browsing experience:

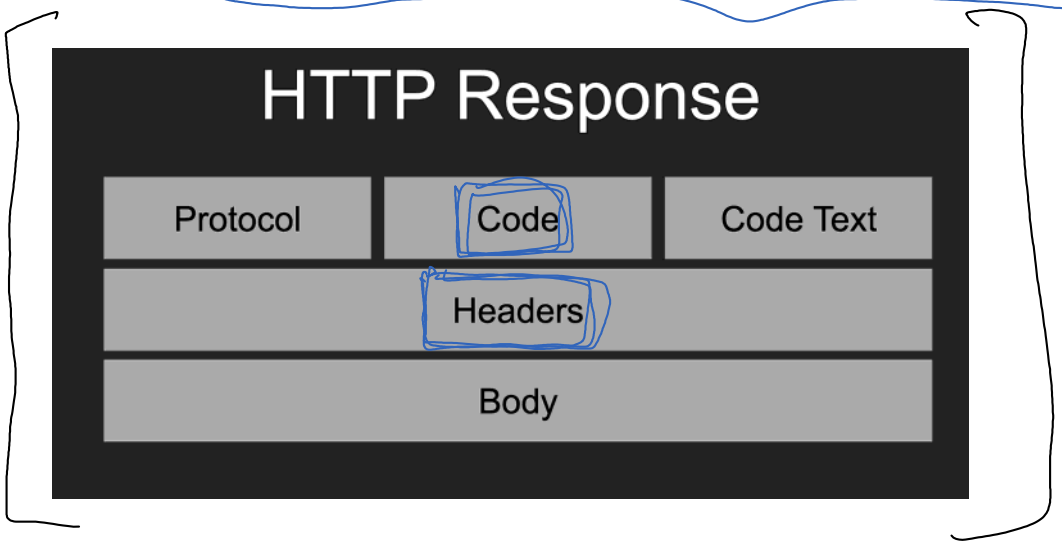
- Maintaining login status
- Shopping carts in online retail stores
- Store user language, theme, appearance, custom settings and preferences
- Save website traffic for analytics
- Reduce CSRF/XSS attacks

Working of Cookies

Sunday, May 19, 2024 12:48 PM

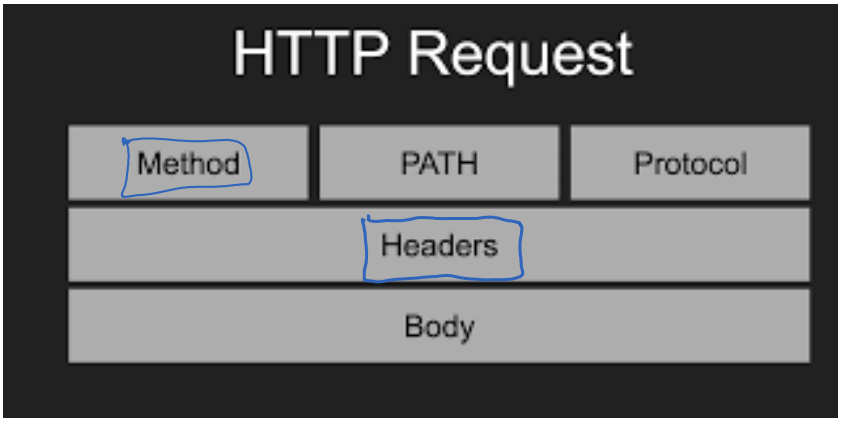
1. When user visits a web application and interacts with it, a HTTP request is sent to the server.
2. The server generates an appropriate response message and sends it back to the application (browser), along with the session ID generated as well as a cookie header. This is done by the *Set-Cookie* header in the 'headers' part of the response message:

```
Set-Cookie: sessionId=abc123; Expires=Wed, 21 Oct 2023 07:28:00 GMT; Secure; HttpOnly
```

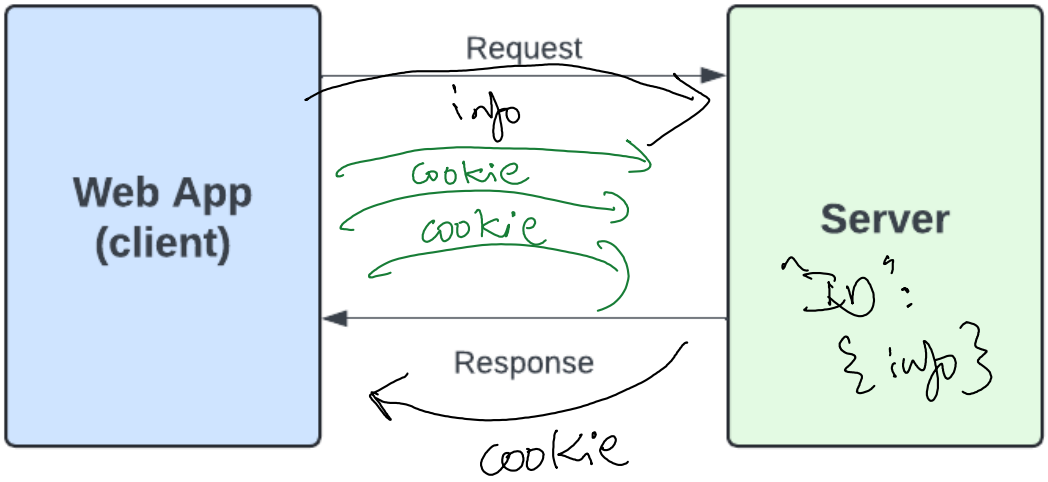


3. Attributes to set a Cookie:
   - *Name/Value*: Contains the main data of the cookie
   - *Expires/Max-Age*: This determines the lifespan of the cookie
   - *Path*: Determines the URL for the cookie to be sent
   - *Secure*: A flag used to ensure cookies are sent over HTTPS
   - *HttpOnly*: Prevents XSS attacks
   - *SameSite*: Prevents CSRF attacks
4. The storage location of cookies at client-side varies depending on the browser and operating system. Typically, cookies are stored in databases.
5. For subsequent requests from the client side, the relevant cookies will be included in the *Cookie* header in the 'headers' section of the request message.

```
Cookie: sessionId=abc123; userId=78910; theme=dark
```



6. Now, the server can identify the Session ID and retrieve the corresponding session data. This way, the server 'remembers' the user's preferences and is able to provide a personalized browsing experience.
7. Cookies with the *Expires* or *Max-Age* attribute will be deleted automatically when the time comes. Else, they'll be deleted when the browser is closed.



Types of Cookies

Sunday, May 19, 2024 1:28 PM

First-party Cookies:

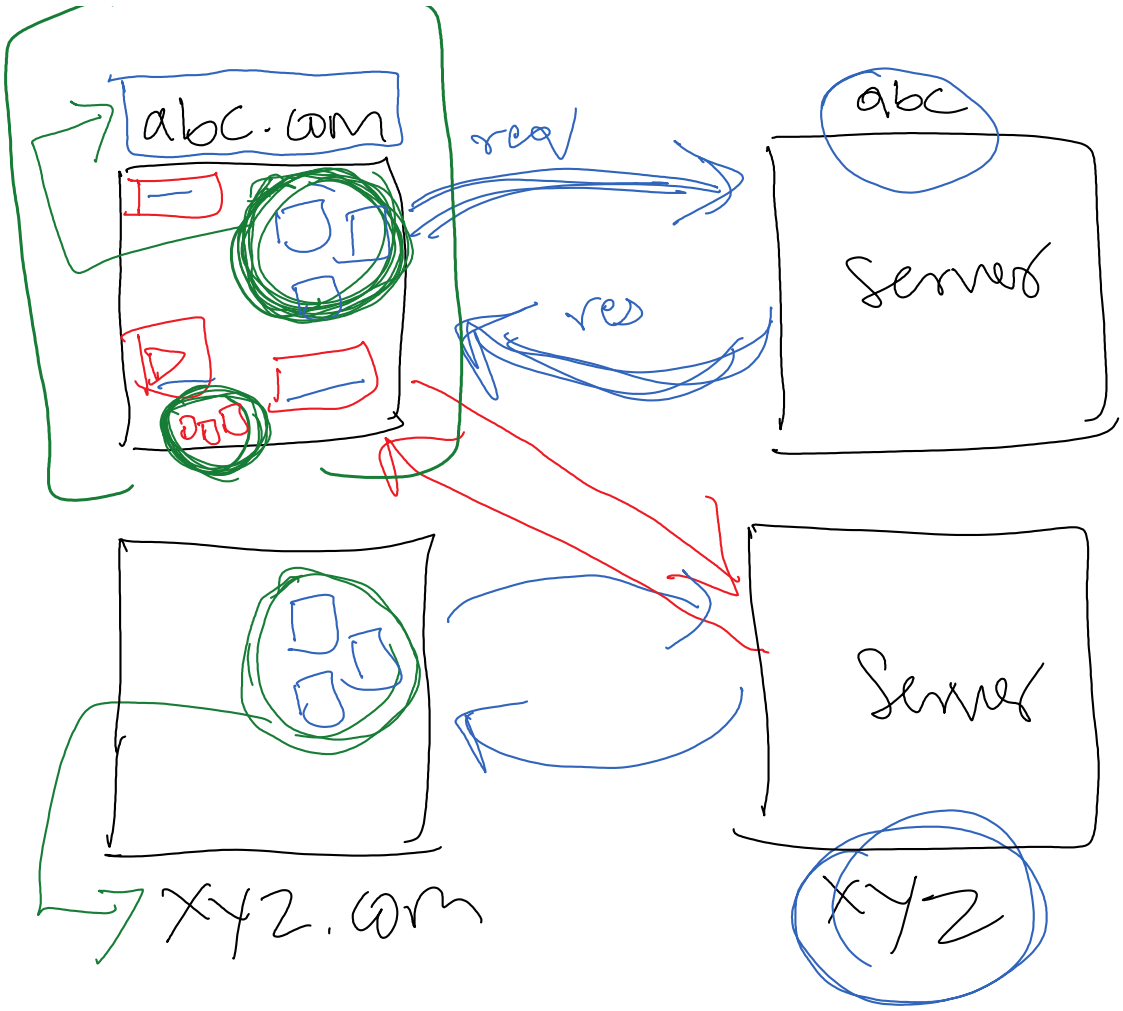
- These cookies are used by the same application/website that the user is currently interacting with.
- These are considered to be more secure and protected, as they can only be accessed by the website the user is currently visiting.
- First Party cookies help with:
  - Maintaining login status in application
  - Keeping track of and storing user's preferences (language, theme, custom settings)
  - Duration of visits on application
  - Providing a personalized experience

Third-party Cookies:

- Cookies that get stored in the browser but actually created by some other website which the user isn't currently visiting, are third-party cookies.
- Associated with greater security concerns as it exposes users' browsing data to external parties (sometimes without consent)
- These cookies are mainly used for:
  - Tracking a user's activities across different websites, to generate targeted ads
  - Analysing website traffic and performance for analytics
  - Tailoring social media feeds by tracking user activity
  - Generating user profiles based on data collected about a user's activities across different websites

What happens when we select 'Accept All Cookies' ?

- Equivalent of a user giving consent to store and use first-party and third-party cookies.
- Allows third-party companies to collect browsing data and activity across multiple websites. This helps with targeted ad generation, building user profiles, etc.
- Higher risk of data leakage if the third-party companies are compromised.


abc.com
req
res
abc
Server
Server
xyz
xyz.com

Security Considerations

Monday, May 20, 2024 7:26 AM

Measures to take, to protect data stored in Cookies:

1. **Cookie Attributes:**
    - Use attributes and flags like *HttpOnly* and *SameSite*
    - Helps avoid CSRF and XSS attacks
2. **Cookie Poisoning:**
    - An attacker can modify the contents of cookies to gain unauthorized access to data
    - Encrypt cookie data using hashes
    - Avoid storing critical and sensitive information in cookies
3. **Man-in-the-Middle Attacks:**
    - Attackers can intercept cookies and manipulate the communication between client & server
    - Ensure to use *Secure* attribute and HTTPS channels for communication
4. **Consent:**
    - Read all terms and conditions before accepting all cookies
    - Minimize use of third-party cookies unless absolutely necessary
5. **Similar to Sessions:**
    - Cookies are a part of sessions
    - Cookies are generated within a session
    - Similar security considerations will apply

Code Demo

Monday, May 20, 2024 8:23 AM