Sessions

Saturday, May 18, 2024 4:38 AM

1. **Definition**
2. **Working**
3. **Types of Sessions**
4. **Security Considerations**
5. **Code Demo**

What is a Web Session ?

Saturday, May 18, 2024 5:36 AM

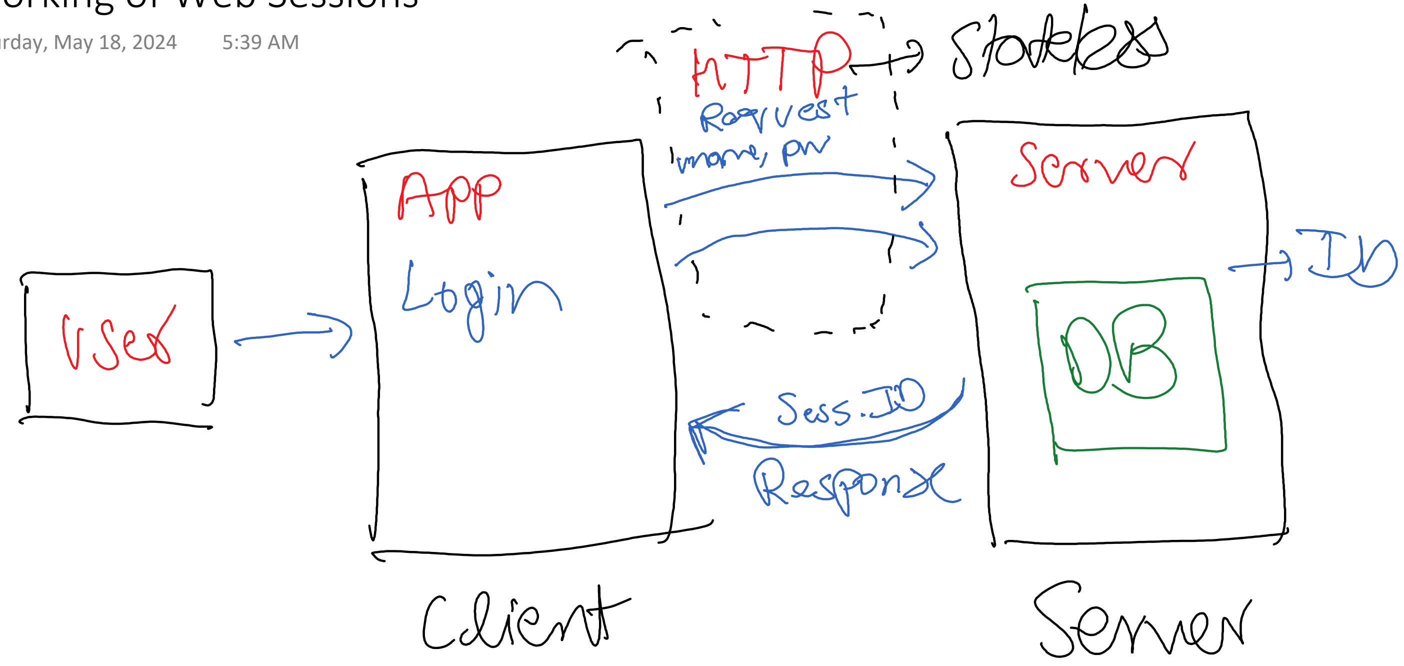
- A web session refers to the period of time an end user is active on a web application during a visit (until they logout or session is timed out)

- Information about the interactions between the user and the application during each visit is usually stored at:
    - Client side - *cookies (small chunks of data sent to application via server)*
    - Server side - *database*

- This helps the server and the browser maintain user preferences throughout the duration of a particular visit to the website
    - *User login status*
    - *Items in online shopping cart*
    - *Website layout/appearance preferences*

Working of Web Sessions

Saturday, May 18, 2024 5:39 AM



1. Client-Server Arch.
2. HTTP is stateless
3. login credentials stored in Server
4. ID generated

↳ "Session ID"

(123)

"123" : { login credentials }

" Session Store "

5. For every interaction, request is generated

   ↳ session ID

6. Client-side session $\xrightarrow{\text{default}}$ Flask

   Server session $\xrightarrow{\text{library}}$

Types of Sessions

Saturday, May 18, 2024 6:31 AM

Based on Duration:

1. **Persistent Sessions** (Permanent)
   - These sessions remain active for a very long period of time
   - Ends only when the user manually terminates the session
   - Ex: social media platforms, OTT platforms
2. **Non-persistent Sessions**
   - These sessions last for a very short period, probably a single application visit
   - Session ends when the application/browser is closed

Based on Security Mechanism:

1. **Authenticated Sessions:**
   - Sessions are created only after the user has been authenticated (via login credentials)
2. **Anonymous Sessions:**
   - Sessions are created even if the user hasn't been authenticated
   - Useful for maintaining state information without authentication (as a 'Guest')
   - Ex: browsing online retail stores

Based on Storage Location:

1. **Client-side:**
   - State information of the sessions is stored within the browser
   - Useful for storing small, insensitive data
   - Ex: browser cookies
2. **Server-side:**
   - State information of the sessions is stored in databases

    - Ideal for large volumes and sensitive data; Offers improved security and integrity

Security Considerations

Saturday, May 18, 2024 6:59 AM

Measures to enhance Security and Integrity of Session data getting stored

1. **Session ID:**

- The session ID should be long and randomly generated
- The session ID should be changed periodically during a session
- The session ID shouldn't be exposed as part of any URL

2. **Secure Cookies:**

- Set the flags *HttpOnly* and *Secure* and the attribute *SameSite* while setting cookies over HTTP
- *HttpOnly* prevents client-side scripts (Java Script) from accessing browser cookies, thus preventing XSS (cross-site scripting) attacks
- *Secure* ensures that cookies are sent over the HTTPS domain, preventing interception over unsecured connections
- *SameSite* helps prevent chances of CSRF attacks

```
Set-Cookie: sessionId=abc123; HttpOnly; Secure; SameSite=Strict
```

3. **Session Timeout:**

- Can end sessions after a predefined period of inactivity
- Can terminate sessions after a fixed duration, regardless of activity
- Helps reduce the time window available for attackers

4. **Logging & Monitoring:**

- Maintain logs of session creation, access, termination & various events to detect any unusual activity
- Implement real-time monitoring systems to analyse logs and detect anomalies as they occur
- Use automated tools to generate alerts for suspicious activities, enabling prompt investigation and response

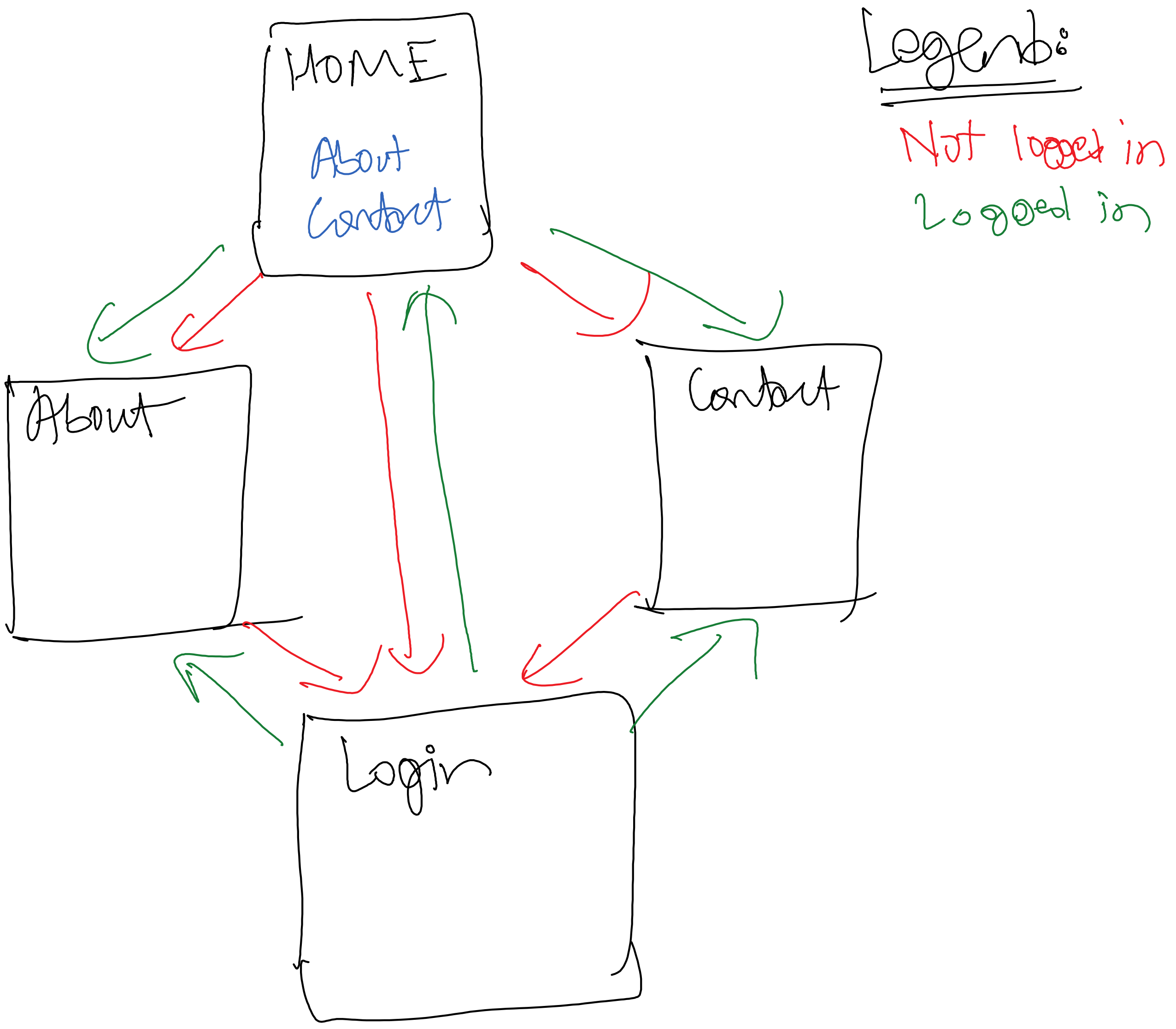
5. **<u>Additional Measures:</u>**

   - Implement MFA (multi-factor authentication) for security of sessions
   - Prompt users to confirm any and all critical actions within a session
   - Notify users before session timeout due to inactivity, if they want to extend a session. This can improve user experience while maintaining security.

Code Demo

Saturday, May 18, 2024 6:59 AM

Application Flow:



HOME
About
Contact
About
Contact
Login
Legend:
Not logged in
Logged in