Name:Shahzaib khan

Security Features for Social Media Platform

1. Password Hashing

Description: Store user passwords securely using a strong hashing algorithm (e.g., bcrypt) instead of plain text to prevent exposure in case of a data breach. This ensures that even if the database is compromised, attackers cannot easily retrieve passwords.

2. SQL Injection Prevention

Description: Use parameterized queries or prepared statements in SQL queries to prevent attackers from injecting malicious SQL code. This protects the database from unauthorized data access or manipulation.

3. Cross-Site Scripting (XSS) Prevention

Description: Sanitize and encode user inputs (e.g., post content, comments) to prevent malicious scripts from being executed in users' browsers. This protects users from attacks that could steal session cookies or perform unauthorized actions.

4. Cross-Site Request Forgery (CSRF) Protection

Description: Implement CSRF tokens in forms to verify that requests originate from authenticated users, preventing attackers from tricking users into performing unintended actions (e.g., creating posts or deleting users).

5. Session Management

Description: Securely manage user sessions by using secure cookies, setting proper timeouts, and regenerating session IDs upon login to prevent session hijacking or fixation attacks.

6. Role-Based Access Control (RBAC)

Description: Restrict access to sensitive features (e.g., user deletion) based on user roles (Admin vs. Member). This ensures that only authorized users can perform administrative actions.

7. Input Validation and Sanitization

Description: Validate and sanitize all user inputs (e.g., email, username, post content) to ensure they meet expected formats and do not contain malicious data. This reduces the risk of injection attacks and data corruption.