Answer:

1. Input validation should be applied on both Syntactical and Semantic level.

2. To prevent cookies from being read by unauthorised parties because they are transmitted in clear text.

3. The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements

4. After a change in privilege inside the related user session, the web application has to regenerate or renew the session ID.

5. 20 bytes of random data from /dev/urandom stored via a hash (e.g. SHA-1)