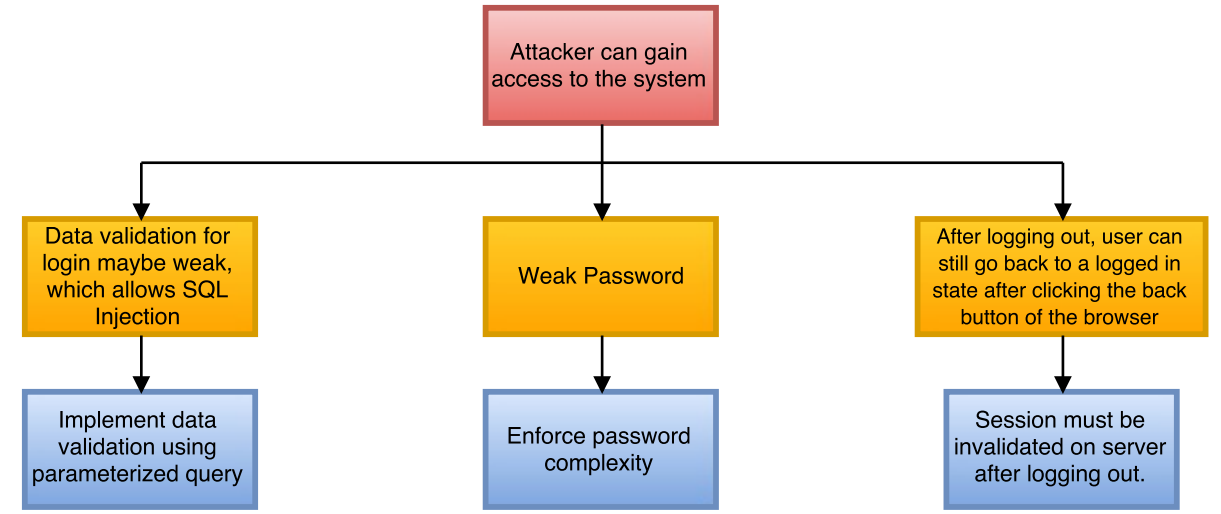
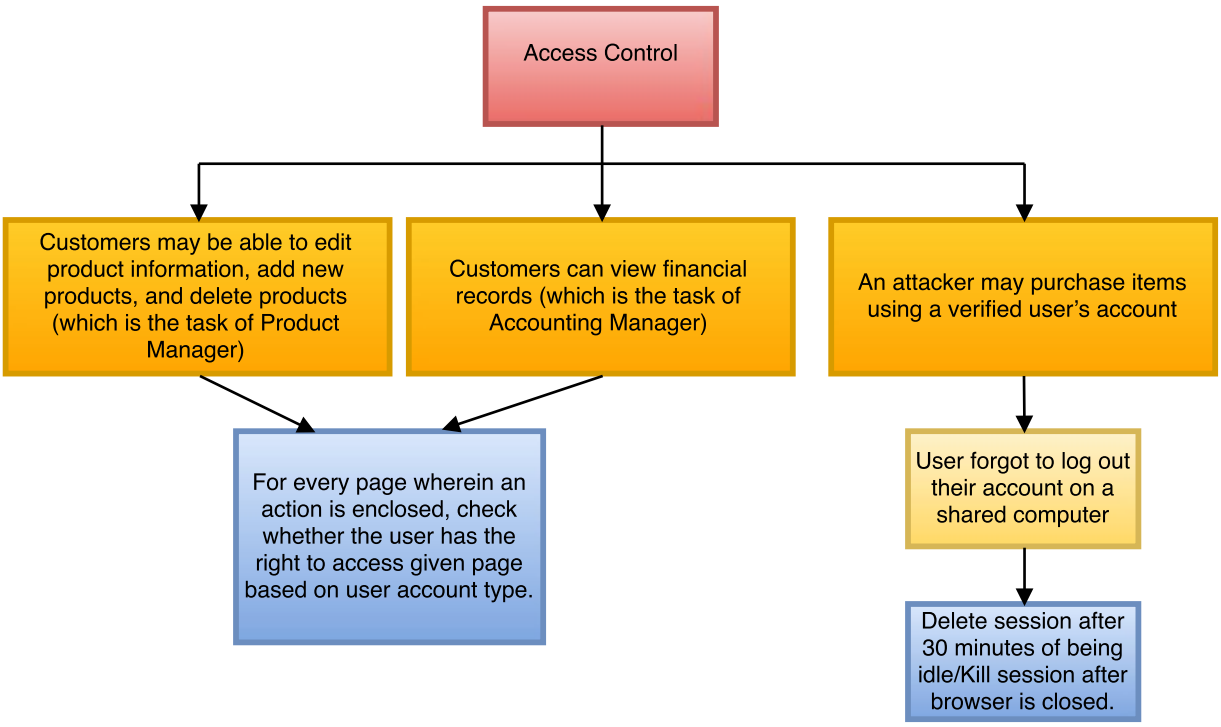
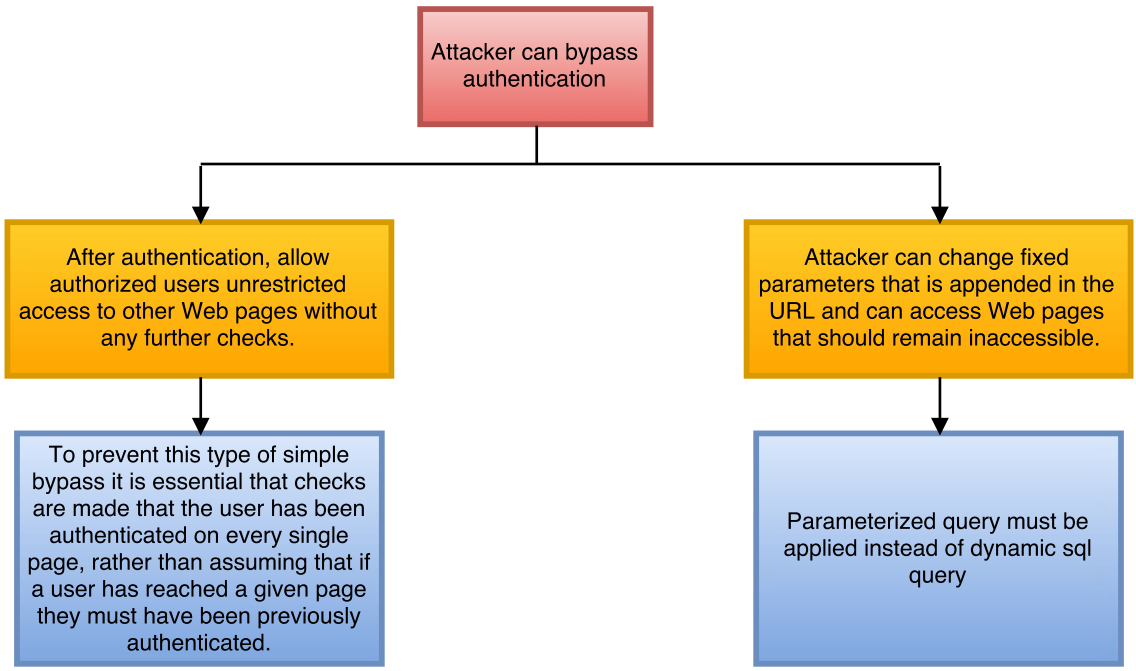
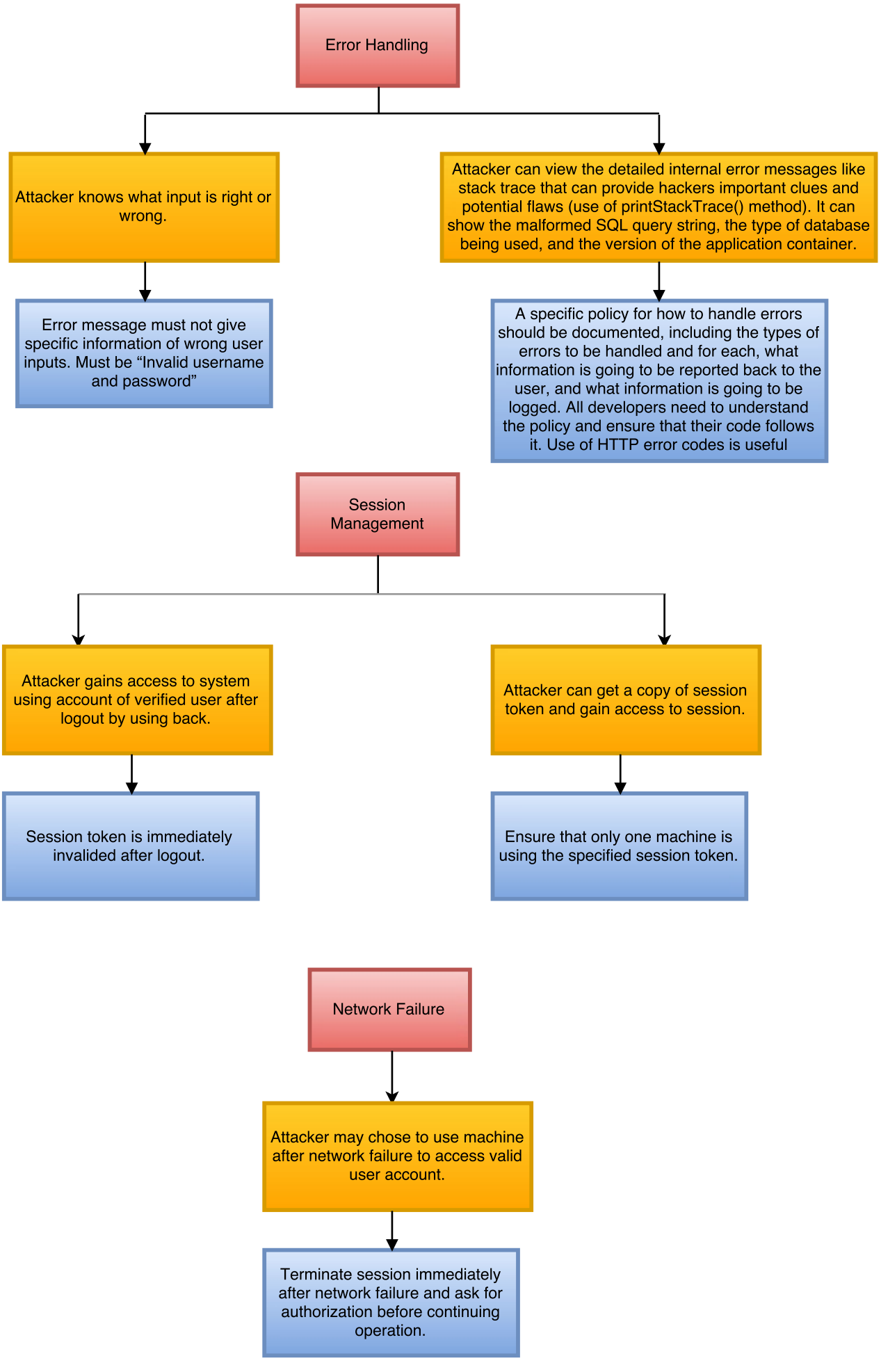

Attacker can gain access to the system
Data validation for login maybe weak, which allows SQL Injection
Weak Password
After logging out, user can still go back to a logged in state after clicking the back button of the browser
Implement data validation using parameterized query
Enforce password complexity
Session must be invalidated on server after logging out.


Access Control
Customers may be able to edit product information, add new products, and delete products (which is the task of Product Manager)
Customers can view financial records (which is the task of Accounting Manager)
An attacker may purchase items using a verified user's account
For every page wherein an action is enclosed, check whether the user has the right to access given page based on user account type.
User forgot to log out their account on a shared computer
Delete session after 30 minutes of being idle/Kill session after browser is closed.


Attacker can bypass authentication
After authentication, allow authorized users unrestricted access to other Web pages without any further checks.
Attacker can change fixed parameters that is appended in the URL and can access Web pages that should remain inaccessible.
To prevent this type of simple bypass it is essential that checks are made that the user has been authenticated on every single page, rather than assuming that if a user has reached a given page they must have been previously authenticated.
Parameterized query must be applied instead of dynamic sql query


Error Handling
Attacker knows what input is right or wrong.
Attacker can view the detailed internal error messages like stack trace that can provide hackers important clues and potential flaws (use of printStackTrace() method). It can show the malformed SQL query string, the type of database being used, and the version of the application container.
Error message must not give specific information of wrong user inputs. Must be “Invalid username and password”
A specific policy for how to handle errors should be documented, including the types of errors to be handled and for each, what information is going to be reported back to the user, and what information is going to be logged. All developers need to understand the policy and ensure that their code follows it. Use of HTTP error codes is useful
Session Management
Attacker gains access to system using account of verified user after logout by using back.
Attacker can get a copy of session token and gain access to session.
Session token is immediately invalided after logout.
Ensure that only one machine is using the specified session token.
Network Failure
Attacker may chose to use machine after network failure to access valid user account.
Terminate session immediately after network failure and ask for authorization before continuing operation.