Workflow

1. User Login Workflow:

Security Check: Ensure secure transmission of credentials (e.g., using HTTPS).
User inputs credentials (username and password).
Verify input validation for preventing SQL injection.
Check for multi-factor authentication (if applicable).
Ensure password hashing is used in the authentication process.
Enforce login attempt limits to prevent brute force attacks.
Test for proper session management (session timeout, secure and HttpOnly cookies).

2. Add Item to Cart Workflow:

Security Check: Ensure integrity of user session and cart data.
User selects an item to add to the cart.
Verify input validation to prevent XSS attacks.
Ensure the cart is session-specific and cannot be hijacked by another user.
Test for price or discount manipulation via client-side scripts.
Confirm integrity checks on items added to the cart, ensuring no unauthorized modifications.

3. Payment Checkout Workflow:

Security Check: Ensure secure payment processing and protection of sensitive payment details.
User proceeds to checkout and enters payment details.
Ensure encryption of payment details (e.g., credit card information) in transit.
Verify that no sensitive data is stored unnecessarily (e.g., full credit card numbers).
Confirm integration with secure payment gateways.
Test error handling (no sensitive info leaked in error messages) and ensure proper logging.

4. Change Password Workflow:

Security Check: Ensure proper password policy enforcement.
User requests to change the password.
Verify old password confirmation before allowing the change.
Ensure strong password requirements (length, complexity).
Test for secure password storage (bcrypt or equivalent).
Ensure password reset tokens are securely generated and expire after a set time.

5. Add Feedback and Comment Workflow:
Security Check: Prevent injection attacks and data tampering.
User submits feedback or a comment.
Verify input validation and encoding to prevent XSS.
Test for rate limiting to prevent excessive comment submissions.
Ensure the comments are sanitized and displayed securely.
Check that comments cannot be edited or manipulated post-submission by unauthorized users.

6. Access Scoreboard Workflow:
Security Check: Ensure the scoreboard is accessible only to authorized users.
User attempts to access the scoreboard.
Ensure proper authentication and authorization mechanisms.
Check that scoreboard data is securely transmitted over HTTPS.
Test for SQL Injection vulnerabilities when accessing the scoreboard.
Validate input for scoreboard filters or search queries to prevent injection attacks.

7. Edit Comment Workflow:
Security Check: Ensure the integrity of user-submitted data.
User attempts to edit a previously submitted comment.
Verify authentication and authorization for editing.
Check input validation and encoding to prevent XSS.
Test if edited comments are sanitized before being saved/displayed.
Ensure the integrity of the editing process (e.g., timestamps and user tracking).

8. Add to Cart without Authentication Workflow:
Security Check: Ensure unauthorized users cannot manipulate the cart.
User selects an item to add to the cart without logging in.
Check input validation to prevent XSS.
Test for session-specific cart functionality (cart linked to session ID).
Ensure that users cannot manipulate item prices/discounts through scripts.
Confirm that the cart state is preserved or discarded upon login/logout.

9. Browse Products Workflow:
Security Check: Ensure secure browsing of product listings.
User browses the product catalog.
Test for SQL injection vulnerabilities in product search filters.
Validate inputs for sorting, filtering, and searching to prevent injection attacks.
Ensure pagination or infinite scrolling does not expose sensitive data.
Test for secure session handling during browsing.