De La Salle University
College of Computer Studies

Secure Web Development Machine Project Checklist

Members:	Carl Ko, Brianna Salvador, Harmony Dy	Date:	November 24, 2025
Section:	S11	Grade:	

Requirement	Complete (2)	Incomplete (1)	Missing (0)
1.0 Pre-demo Requirements (must be created before the actual demo)			
1.1. Accounts (at least 1 per type of user)			
1.1.1. Website Administrator	✓		
1.1.2. Role A (example: Product Manager)	✓		
1.1.3. Role B: Customer/Resto Owner	✓		
2.0 Demo Requirements			
2.1. Authentication			
2.1.1. Require authentication for all pages and resources, except those specifically intended to be public	✓		
2.1.2. Only cryptographically strong one-way salted hashes of passwords are stored	✓		
2.1.3. Authentication failure responses should not indicate which part of the authentication data was incorrect. For example, instead of "Invalid username" or "Invalid password", just use "Invalid username and/or password" for both	✓		
2.1.4. Enforce password complexity requirements established by policy or regulation	✓		
2.1.5. Enforce password length requirements established by policy or regulation	✓		
2.1.6. Password entry should be obscured on the user's screen (use of dots or asterisks on the display)	✓		
2.1.7. Enforce account disabling after an established number of invalid login attempts (e.g., five attempts is common). The account must be disabled for a period of time sufficient to discourage brute force guessing of credentials, but not so long as to allow for a denial-of-service attack to be performed	✓		
2.1.8. Password reset questions should support sufficiently random answers. (e.g., "favorite book" is a bad question because "The Bible" is a very common answer)	✓		
2.1.9. Prevent password re-use to be checked against the user's history of passwords	✓		
2.1.10. Passwords should be at least one day old before they can be changed, to prevent attacks on password re-use	✓		
2.1.11. The last use (successful or unsuccessful) of a user account should be reported to the user at their next successful login	✓		
2.1.12. Re-authenticate users prior to performing critical operations such as password change	✓		
2.2. Authorization/Access Control			
2.2.1. Use a single site-wide component to check access authorization	✓		
2.2.2. Access controls should fail securely with error messages	✓		
2.2.3. Enforce application logic flows to comply with business rules using role-based access control	✓		
2.3. Data Validation			
2.3.1. All validation failures should result in input rejection. Sanitizing should not be used.	✓		
2.3.2. Validate data range for numeric input OR set of allowed characters for other types of input	✓		

Requirement	Complete (2)	Incomplete (1)	Missing (0)
2.3.3. Validate data length on text field/text boxes	✓		
2.4. Error Handling and Logging			
2.4.1. Use error handlers that do not display debugging or stack trace information	✓		
2.4.2. Implement generic error messages and use custom error pages	✓		
2.4.3. Restrict access to logs to only website administrators	✓		
2.4.4. Log all input validation failures (example: out of range, incorrect character/s)	✓		
2.4.5. Log all authentication attempts, both successful and failed, including lockout	✓		
2.4.6. Log all access control failures	✓		
TOTAL			