Application Name: Task Management Web Application
Testing Type: Basic Web Security Testing
Tester: Abdur Rahman
Date: 9-2-2026

1. Introduction

This report presents the results of basic security testing conducted on the Task Management Web Application. The objective of the test was to identify common web application vulnerabilities such as input validation weaknesses, SQL injection, Cross-Site Scripting (XSS), authentication issues, and session management flaws.

Testing was performed manually using standard browser-based testing techniques.

2. Scope of Testing

The following areas were tested:

- Input Validation
- SQL Injection
- Cross-Site Scripting (XSS)
- Login/Logout Authentication
- Session Timeout Management

3. Testing Methodology

The testing was performed manually by interacting with the application forms and authentication system. The following techniques were used:

- Submitting empty and long input values
- Injecting special characters
- Attempting basic SQL injection payloads
- Testing XSS using script injection
- Verifying login/logout behavior
- Checking session timeout functionality

4. Summary of Findings

Vulnerability ID	Test Area	Severity	Status
VULN_01	Input Validation (Empty Fields)	Low	Passed
VULN_02	Input Validation (Long Input)	Low	Minor Weakness
VULN_03	SQL Injection Test	Low	Passed
VULN_04	Cross-Site Scripting (XSS)	Low	Passed
VULN_05	Authentication Error Handling	Low	Passed
VULN_06	Session Timeout Management	Medium	Vulnerability Found

5. Detailed Findings

VULN_01 – Input Validation (Empty Fields)

Severity: Low
Description:
The application properly validates required fields such as title, username, and password. When submitted empty, an appropriate error message is displayed.

Result:
Validation works correctly.

Recommendation:
No action required.

VULN_02 – Input Validation (Long Input)

Severity: Low

Description:
The application does not restrict the length of input fields. Very long text inputs are accepted and stored without validation.

Risk:
May lead to database performance issues or potential buffer-related problems.

Recommendation:
Implement maximum character limits for input fields.

VULN_03 – SQL Injection Test

Severity: Low

Description:
Basic SQL injection attempts during login were unsuccessful. The application rejected invalid credentials properly.

Result:
No SQL injection vulnerability detected.

Recommendation:
Continue using parameterized queries and input sanitization.

VULN_04 – Cross-Site Scripting (XSS)

Severity: Low

Description:
A script payload `<script>alert('XSS')</script>` was inserted into the task title field. The application stored it as plain text and did not execute the script.

Result:
No XSS vulnerability detected.

Recommendation:
Continue proper output encoding and sanitization.

VULN_05 – Authentication Error Handling

Severity: Low

Description:
The application correctly rejects invalid login attempts and displays an “Invalid credentials” message.

Result:
Authentication validation works correctly.

Recommendation:
No action required.

VULN_06 – Session Timeout Management

Severity: Medium

Description:
The application does not automatically log out users after a period of inactivity. The session remains active unless the user manually logs out.

Risk:
If a user leaves their session open on a shared or public device, unauthorized users may gain access.

Recommendation:
Implement automatic session expiration after a defined period of inactivity (e.g., 10–15 minutes).

6. Conclusion

The basic security testing revealed that the application has proper input validation, authentication controls, and protection against basic SQL injection and XSS attacks.

However, a session management weakness was identified due to the absence of automatic session timeout. Implementing session expiration would significantly improve overall security.

Overall Risk Level: Low to Medium