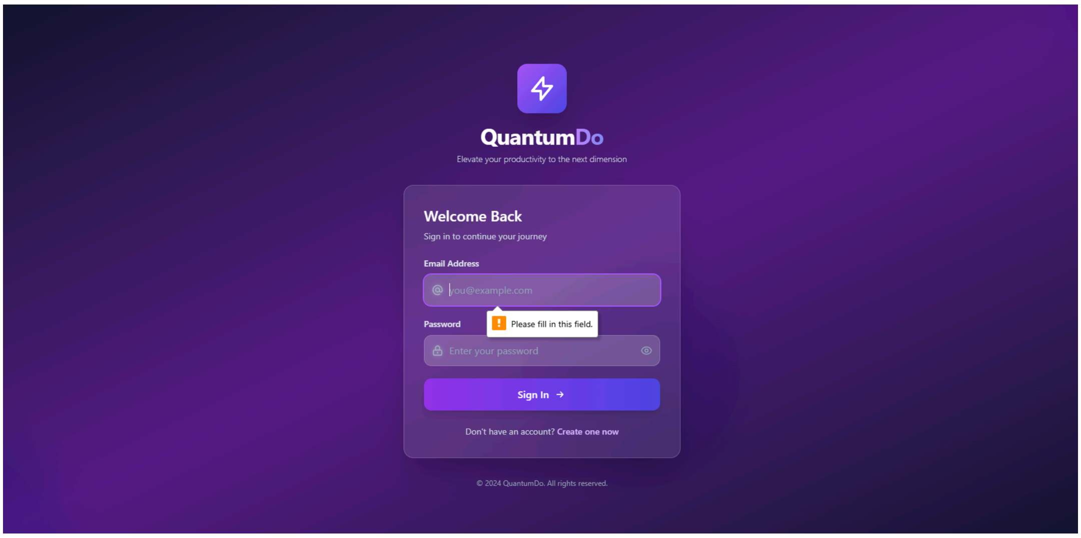
Application Name: Task Management Web Application
Testing Type: Basic Web Security Testing
Tester: Abdur Rahman
Date: 9-2-2026

Vulnerability ID	VULN_01
Test Area	Input Validation (Empty Fields)
Description	Application properly validates required fields such as title, username, and password. Error message is displayed when fields are empty
Severity	Low
Steps to Reproduce	Leave title, username, or password empty and submit form.
Result	Application shows "required" message.
Suggested Fix	No action required. Validation works correctly.



QuantumDo

Elevate your productivity to the next dimension

Welcome Back

Sign in to continue your journey

Email Address: you@example.com

Please fill in this field.

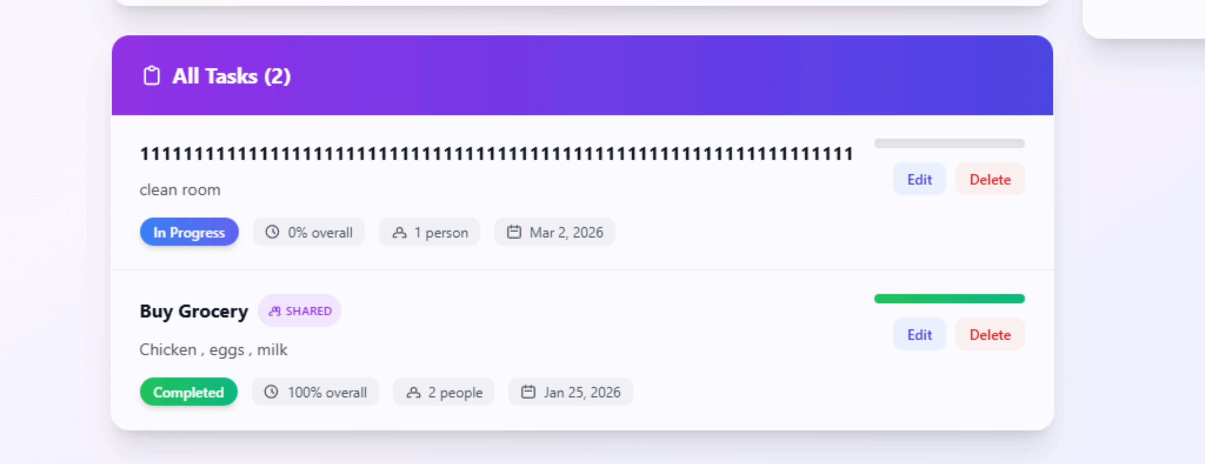
Password: Enter your password

Don't have an account? Create one now

© 2024 QuantumDo. All rights reserved.

Figure 1: Login page showing required field validation message

Vulnerability ID	VULN_02
Test Area	Input Validation (Long Input)
Description	Application does not limit long input length. Extremely long text is accepted without validation. This may lead to storage issues or UI problems.
Severity	Low
Steps to Reproduce	Enter 300+ characters in Task Title and submit.
Result	Task is added successfully without restriction.
Suggested Fix	Implement server side and client side input length validation (e.g., max 100 characters).



All Tasks (2)

111111111111111111111111111111111111111111111111111111111111111111

clean room

In Progress · 0% overall · 1 person · Mar 2, 2026

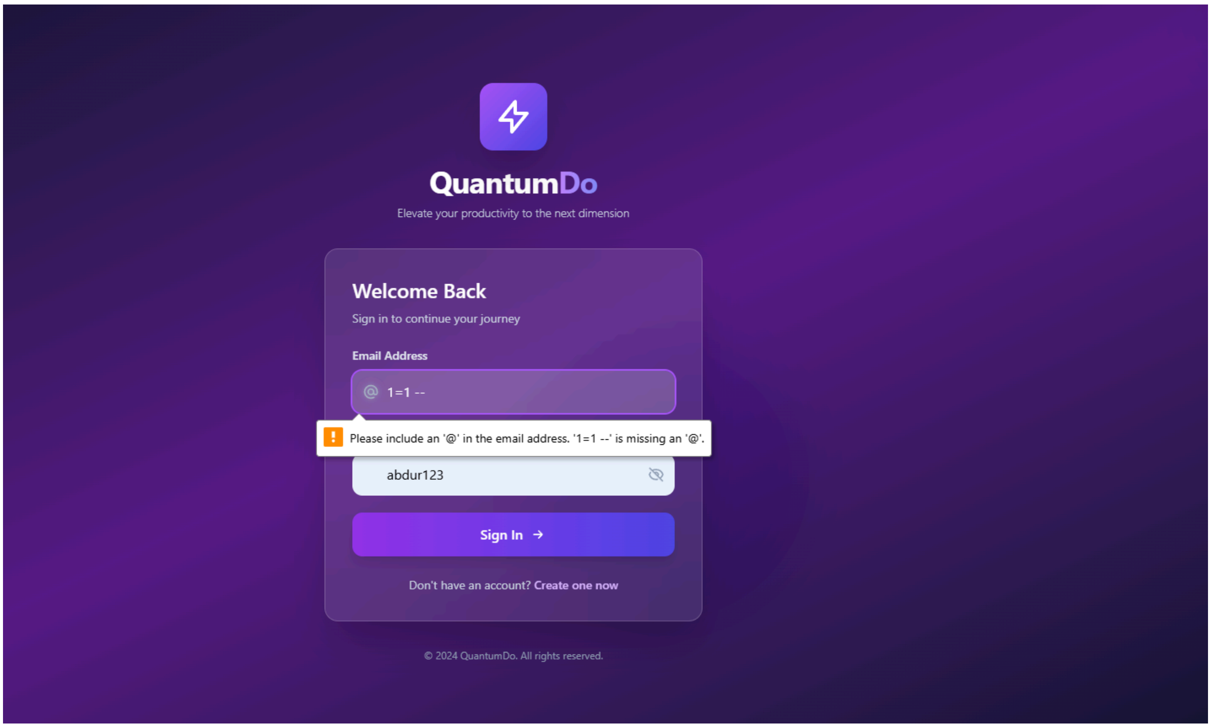
Buy Grocery · SHARED

Chicken , eggs , milk

Completed · 100% overall · 2 people · Jan 25, 2026

Figure 2: Task shows with long input validations

Vulnerability ID	VULN_03
Test Area	SQL Injection Test
Description	Login form is not vulnerable to basic SQL injection attempt
Severity	Low
Steps to Reproduce	Enter 1=1 as username and any password.
Result	Login fails normally.
Suggested Fix	Continue using parameterized


QuantumDo

Elevate your productivity to the next dimension

Welcome Back

Sign in to continue your journey

Email Address

1=1 --

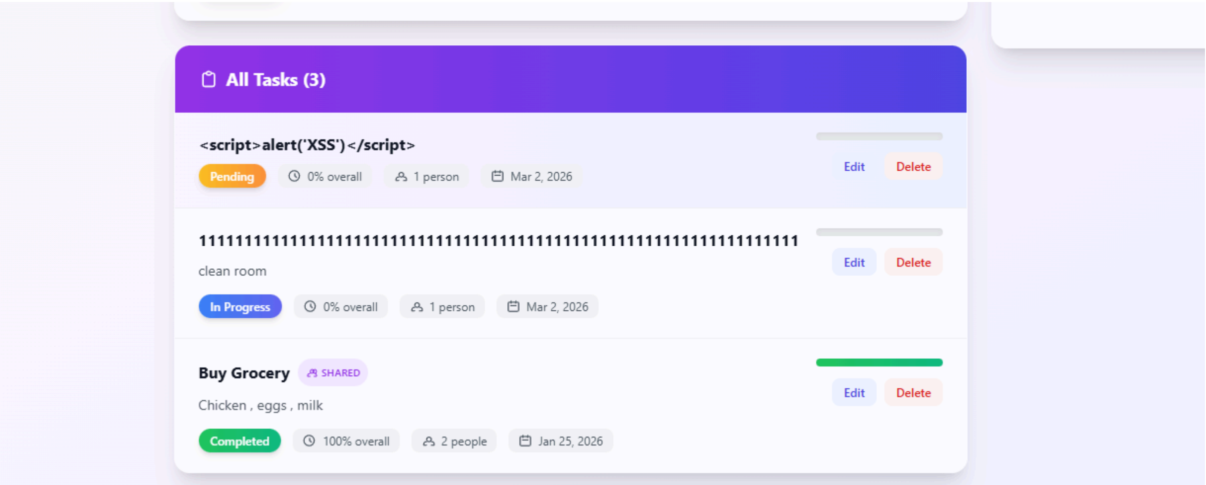
Please include an '@' in the email address. '1=1 --' is missing an '@'.

abdur123

© 2024 QuantumDo. All rights reserved.

Figure 3: Login page showing SQL injection attempt

Vulnerability ID	VULN_04
Test Area	Cross-Site Scripting (XSS)
Description	Application stores `<script>alert('XSS')</script>` as plain text and does not execute it. No JavaScript execution observed.
Severity	Low
Steps to Reproduce	Enter `<script>alert('XSS')</script>` in task title and save.
Result	Script is saved as text. No alert popup appears.
Suggested Fix	Continue implementing output encoding and input sanitization.



All Tasks (3)

<script>alert('XSS')</script>

Pending · 0% overall · 1 person · Mar 2, 2026 · Edit · Delete

11111111111111111111111111111111111111111111111111111111111111111111111111111

clean room

In Progress · 0% overall · 1 person · Mar 2, 2026 · Edit · Delete

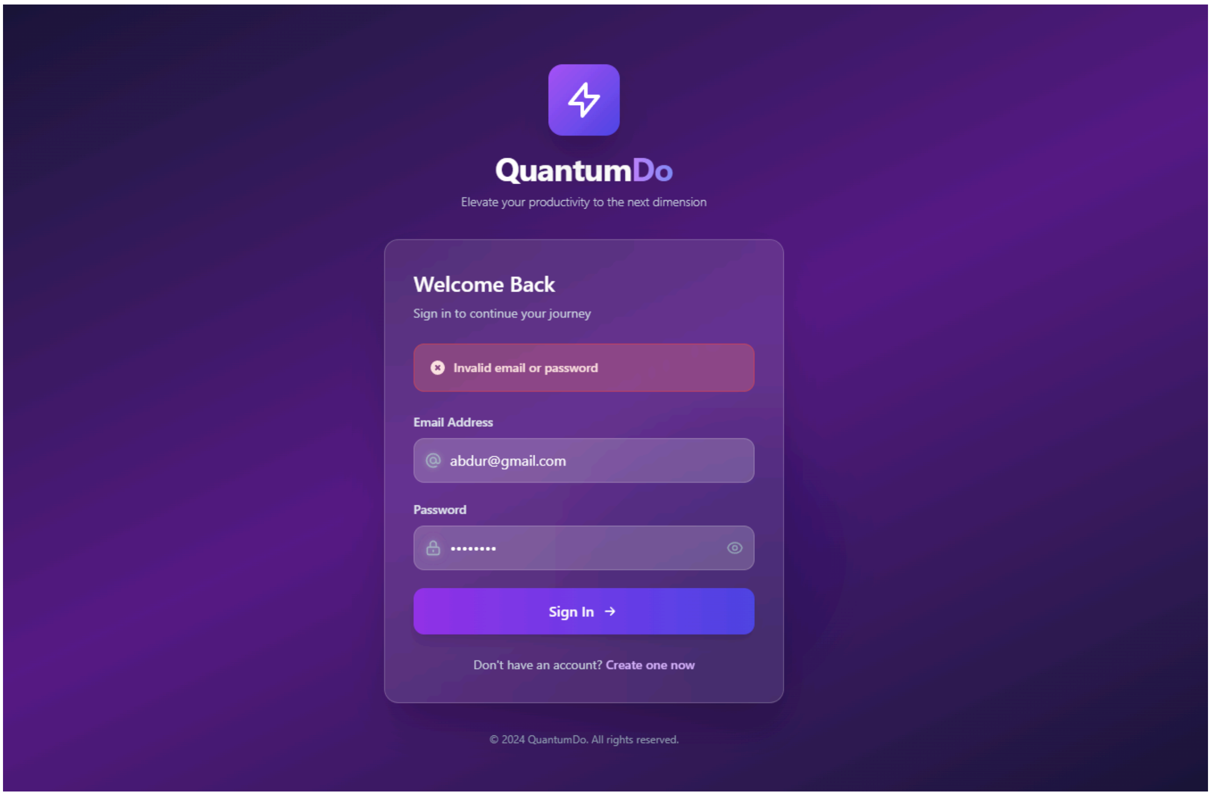
Buy Grocery · SHARED

Chicken , eggs , milk

Completed · 100% overall · 2 people · Jan 25, 2026 · Edit · Delete

Figure 4: Task showing java script saving as text .

Vulnerability ID	VULN_05
Test Area	Authentication Error Handling
Description	Application displays generic error message "Invalid credentials" for wrong email or password.
Severity	low
Steps to Reproduce	Enter incorrect login credentials.
Result	Displays "Invalid credentials".
Suggested Fix	No action required.



QuantumDo

Elevate your productivity to the next dimension

Welcome Back

Sign in to continue your journey

Invalid email or password

Email Address

abdur@gmail.com

Password

••••••••

Don't have an account? Create one now

© 2024 QuantumDo. All rights reserved.

Figure 5: Login fails with wrong credentials

Vulnerability ID	VULN_06
Test Area	Session Timeout Management
Description	Application does not automatically expire user session after inactivity. User remains logged in until manual logout.
Severity	Medium
Steps to Reproduce	Login and remain idle for 10+ minutes. Refresh page.
Result	Session remains active.
Suggested Fix	Implement session timeout (e.g., 10–15 minutes inactivity expiration).