# Test Case ID

1 TC\_REG\_001

2 TC\_REG\_002

3 TC\_REG\_003

4 TC\_REG\_005

5 TC\_REG\_006

6 TC\_REG\_007

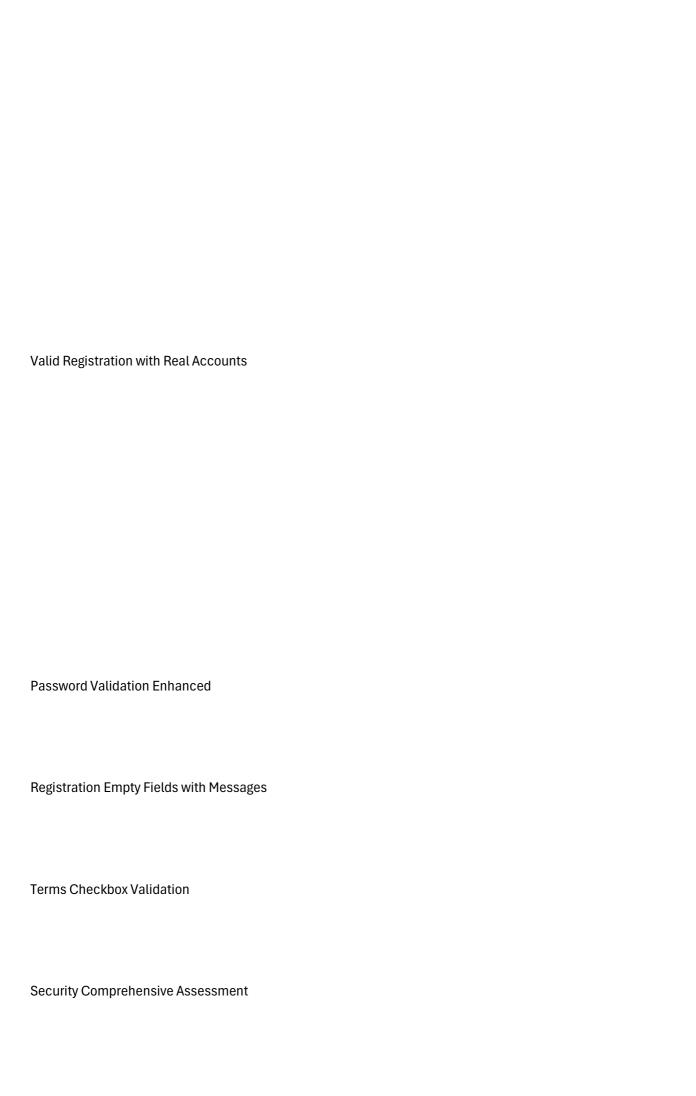
7 TC\_REG\_008

8 TC\_LOGIN\_001

9 TC\_LOGIN\_002

10 TC\_LOGIN\_003





Form Validation UI Elements
Boundary Values Enhanced
Valid Login and Welcome Message
Login-Logout-Welcome Back Flow
Login Page Elements Validation

Project Owner
Address
Application Under Test
Reference Document
Created By
Creation Date
Completion Date
Sprint No

Module

Registration			
Registration			

Registration		
Registration		
Login		
Login		
Login		

<u>Tech von chu</u>
Kolpingstr. 83, 53359, Rheinbach, Germany
https://www.verbatimly.com/
FM12-2023
Theophilus Onolunose
28/7/2025
29/12/2025

Preconditions



User is on Registration Page
User is on Registration Page
User is on Login Page
User is on Login Page
User navigates to Login Page

Test Steps

- 1. Open application in browser
- 2. Navigate to registration page
- 3. Enter valid first name
- 4. Enter valid last name
- 5. Enter valid email
- 6. Enter valid password
- 7. Enter matching confirm password
- 8. Accept terms and conditions
- 9. Click "Create Account"

- 1. Test short password validation
- 2. Test password mismatch validation
- 3. Navigate between tests
- 1. Navigate to signup page
- 2. Enter only first name: "John"
- 3. Leave other fields empty
- 4. Click create account
- 5. Check validation messages
- 1. Navigate to signup page
- 2. Fill all required fields
- 3. Do NOT check terms checkbox
- 4. Click create account5. Verify HTML
- 5 validation
- 1. Test SQL injection in first name
- 2. Test XSS in last name
- 3. Complete other fields
- 4. Submit form
- 5. Verify safe handling

- 1. Navigate to signup page
- 2. Verify presence of all form elements
- 3. Check accessibility
- 1. Test very long first name (256 chars)
- 2. Test very long last name (256 chars)
- 3. Test very long email (300+ chars)
- 4. Test minimum valid inputs
- 1. Get credentials from environment
- 2. Navigate to login page
- 3. Enter valid email
- 4. Enter valid password
- 5. Click login button
- 6. Verify welcome message
- 1. Perform successful login
- 2. Verify login success
- 3. Click user profile menu (TO button)
- 4. Click "Sign out"
- 5. Verify "Welcome back" message
- 1. Navigate to login page
- 2. Verify email input field
- 3. Verify password input field
- 4. Verify login button
- 5. Verify forgot password link



First Name: From pytest.ini
 Last Name: From pytest.ini
 Email: From pytest.ini
 Password: From pytest.ini

1. Short Password: "short7!"

2. Valid Password: "ValidPass123!"

3. Mismatched Confirm: "DifferentPass123!"

First Name: "John"
 Other fields: Empty
 First Name: "John"
 Last Name: "Doe"

3. Email: "test@example.com"
4. Password: "TallBuildings123!"

5. Terms: Unchecked

1. SQL Injection: '; DROP TABLE users; -- 2. XSS Payload: <script>alert('I AM A

SCAMMER');</script>

3. Email: "security@test.com"

4. Password: "TallBuildings123!"

## N/A

- 1. Long First Name: "A" × 2562.
- 2. Long Last Name: "B" × 2563.
- 3. Long Email: "a" × 300 + "@example.com"
- 4. Min Valid: Single characters
- 1. Email: os.getenv('USERNAME')
- 2. Password: os.getenv('PASSWORD')
- 1. Email: os.getenv('USERNAME')
- 2. Password: os.getenv('PASSWORD')

N/A

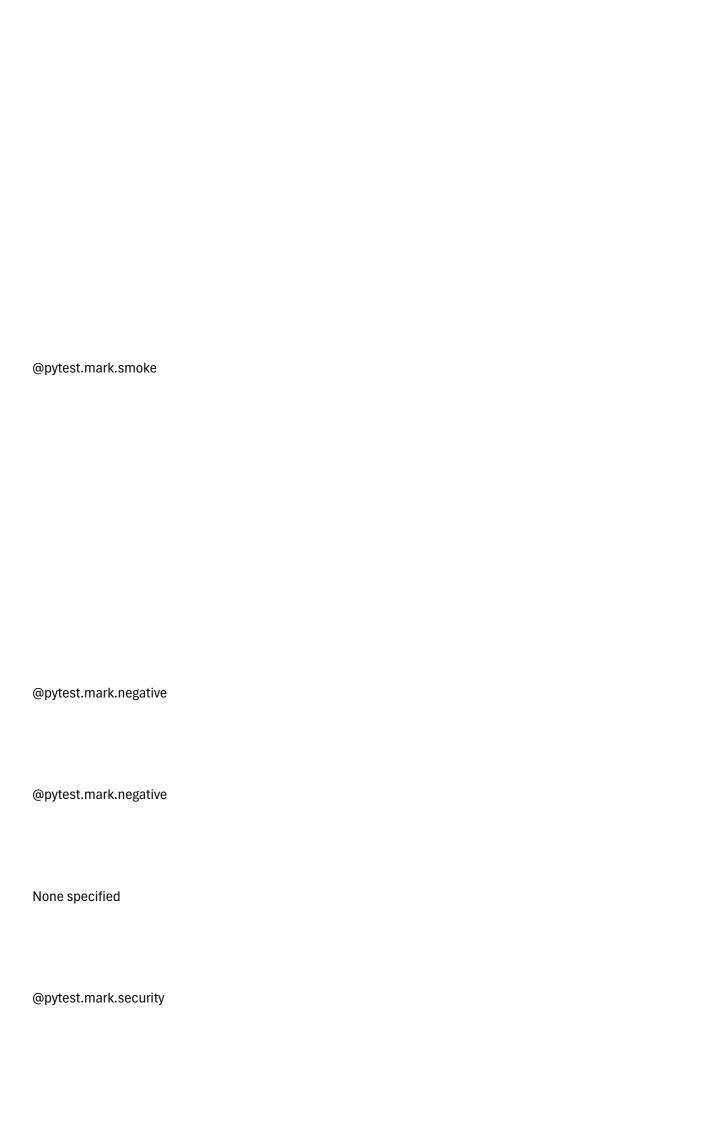
Expected Result Priority Test Type

- 2. Success indicator appears:
- "Check your email" message OR
- "Welcome" message OR
- Success/verify/onboarding URL P1 Smoke

1. Short password rejected		
2. Password mismatch rejected		
3. No success indicators appear	P1	Negative
1. Empty fields rejected		
2. Validation messages appear		
3. No success indicators		
4. Validation message:		
"Please fill out this field."	P2	Negative
1. Registration blocked		
2. HTML5 validation message appears		
3. No success indicators		
4. Expected:		
"Please check this box if you want to proceed."	P2	Negative
1. Payloads sanitized or rejected		
2. No security vulnerabilities		
3. Safe handling		
(either success or rejection acceptable)	P1	Security

1. All elements present:		
- First name field		
- Last name field		
- Email field		
- Password field		
- Confirm password field		
- Terms checkbox		
- Create account button	P2	UI
1. Long inputs rejected		
2. Min valid inputs accepted		
3. Appropriate validation messages		
4. Failed. Not expected	Р3	Boundary
1. Login successful		
2. Welcome message displayed		
3. User redirected to dashboard		
4. Success verification methods triggered	P1	Smoke
1. Login successful	LI	Silloke
-		
2. Logout successful		
3. "Welcome back" message appears		
4. User redirected to login page	D1	Cmaka
5. Complete flow verification	P1	Smoke
1. All essential elements present:		
- Email input field		
- Password input field		
- Login button		
- Forgot password link		
2. 4/4 elements verification	P2	UI





@pytest.mark.ui
@pytest.mark.boundary
@pytest.mark.smoke
@pytest.mark.smoke
None specified