Black Box & White Box Testing

for

Cross Border

Version 1.0 approved

Prepared by Team SimpleOne

Aishwarya Anand

Banerjee Mohor

Chan Jie Ying, Jolene

Chen Guan Zong Aaron

Poonawala Mustafa Jabir

Nanyang Technological University

7th April, 2024

BLACK BOX TESTING DOCUMENTATION

Equivalence Class & Boundary Value Testing

We have used Black Box testing to test the registrationauth controller class which performs the crucial functionality of authenticating new users when they register for a new account.

The evaluatePasswordStrength method of this class has been tested using Boundary Value Testing (Use Case 1). The regauth method of this class has been tested using Equivalence Classes (Use case 2).

Use Case 1: Evaluate Password Strength

Valid Equivalence Class: Strong Passwords

- Score Range for Valid EC: Score > 80

- Boundary Values for Strong Passwords:
  - Lower Boundary (LB): Score = 81 (just crosses into Strong category)
  - Upper Boundary (UB): A high-enough score that well represents strong passwords, e.g. Score = 100

- Final Input Values for Test Cases - Valid:
  - At LB: Score = 81 (80,81,82)
  - At UB: Score = 100 (99, 100, 101)

Invalid Equivalence Classes Based on Score:

- None: Score = 0
- Very Weak: Score > 0 and < 30
- Weak: Score >= 30 and < 60
- Good: Score >= 60 and <= 80

Boundary Values for Invalid ECs:

- Lower Boundary of Very Weak: Score = 1 (0,1,2)

- Very Weak to Weak Transition:
  - Upper Boundary of Very Weak: Score = 29 (28,29,30)
  - Lower Boundary of Weak: Score = 30 (29,30,31)

- Weak to Good Transition:
  - Upper Boundary of Weak: Score = 59 (58,59,60)
  - Lower Boundary of Good: Score = 60 (59,60,61)

- Good to Strong Transition:
  - Upper Boundary of Good: Score = 80 (79,80,81)
  - Lower Boundary of Strong: Score = 81 (80,81,82)

Final Input Values for Test Cases - Invalid:

- Just below Very Weak = 0
- Just into Very Weak = 1
- Just below Weak: Score = 29
- Just into Weak: Score = 30
- Just below Good: Score = 59
- Just into Good: Score = 60
- Just below Strong (Still Good): Score = 80

Test Cases:

Test Case 1	**Valid Strong Password Evaluation**		
Test Scenario	Password Evaluation - Valid scenarios	**Test Case ID**	PasswordEval-01
Test Description	Evaluating password when user enters Strong Password	**Testing Priority**	High
Prerequisite	User is shown field to enter Password	**Post-Requisite**	NA

Test ID	**Description**	**Password Example**	**Expected Score**	**Expected Level**	**Test Steps**	**Expected Outcome**	**Actual Outcome**	**Test Result**

TC1-01	Evaluate low-end strong password	Strong1!	81	Strong	Evaluate password strength using the function	Password classified as "Strong"	Score: 81 Level: Strong	Pass
TC1-02	Evaluate high-end strong password	VeryStrongPassword!2024	100	Strong	Evaluate password strength using the function	Password classified as "Strong"	Score: 100 Level: Strong	Pass

Test Case 2	Invalid Password Strength Evaluation		
Test Scenario	Password Evaluation - Invalid scenarios	**Test Case ID**	PasswordEval-02
Test Description	Evaluating password when user does not enter Strong enough Password	**Testing Priority**	High
Prerequisite	User is shown field to enter Password	**Post-Requisite**	NA

Test ID	Description	Password Example	Expected Score	Expected Level	Test Steps	Expected Outcome	Actual Outcome	Test Result
TC2-00	Empty password	(empty string)	0	None	Evaluate password strength using the function	Password classified as "None"	Score: 0 Level: None	Pass
TC2-01	Very simple password	a	1	Very Weak	Evaluate password strength using the function	Password not classified as "Strong"	Score: 1 Level: Very Weak	Pass
TC2-02	Just below weak	aaa	29	Very Weak	Evaluate password strength using the function	Password not classified as "Strong"	Score: 29 Level: Very Weak	Pass

TC2-03	Transition from very weak to weak	abcde1	30	Weak	Evaluate password strength using the function	Password not classified as "Strong"	Score: 30 Level: Weak	Pass
TC2-04	Just below good	Abc123	59	Weak	Evaluate password strength using the function	Password not classified as "Strong"	Score: 59 Level: Weak	Pass
TC2-05	Transition from weak to good	GoodPass1	60	Good	Evaluate password strength using the function	Password not classified as "Strong"	Score: 60 Level: Good	Pass
TC2-06	Just below strong	BetterPass#12	80	Good	Evaluate password strength using the function	Password not classified as "Strong"	Score: 80 Level: Good	Pass

Use Case 2: Register for a New Account

Valid Equivalence Classes (EC):

- EC1: Username does not exist, and passwords are valid and match.
- EC3: Passwords match and meet minimum strength requirements.

Invalid Equivalence Classes (EC):

- EC2: Username already exists.
- EC4: Passwords do not match.
- EC5: Password does not meet strength requirements.

Test Cases:

Test Case 1	Valid Registration Attempts

Test Scenario	User Registration - Valid scenarios	**Test Case ID**	RegAuth-01
Test Description	Registering a user with valid conditions	**Testing Priority**	High
Prerequisite	User navigated to Registration Page	**Post-Requisite**	NA

No.	Equivalence Class ID	Username	Password	Confirm Password	Existing User in DB	Expected HTTP Status	Expected Response Message	Actual Result	Test Result
1	EC1	newUser1	Pass123!	Pass123!	No	200	"" (Empty message signifies success)	HTTP Status: 200 Response Message: "" (Empty message signifies success)	Pass
2	EC3	newUser2	StrongPass1!	StrongPass1!	No	200	"" (Empty message signifies success)	HTTP Status: 200 Response Message: "" (Empty message signifies success)	Pass

Test Case 2	**Invalid Registration Attempts**		
Test Scenario	User Registration - Invalid scenarios	**Test Case ID**	RegAuth-02
Test Description	Registering a user with invalid conditions	**Testing Priority**	Medium

Prerequisite	User navigated to Registration Page	**Post-Requisite**	NA

No.	Equivalence Class ID	Username	Password	Confirm Password	Existing User in DB	Expected HTTP Status	Expected Response Message	Actual Result	Test Result
1	EC2	existing user	Pass123!	Pass123!	Yes	409	"Username already in use. Please choose a different one"	HTTP Status: 409 Response Message: "Username already in use. Please choose a different one"	Pass
2	EC4	newUser3	StrongPass2!	StrongPass2?	No	400	"Password and confirm password do not match."	HTTP Status: 400 Response Message: "Password and confirm password do not match."	Pass
3	EC5	newUser4	pw	pw	No	422	"Password does not meet the strength requirements."	HTTP Status: 422 Response Message: "Password does not meet the strength requirements."	Pass

Notes:

- "Username" and "Password/ConfirmPassword" columns contain sample inputs to simulate different registration scenarios.

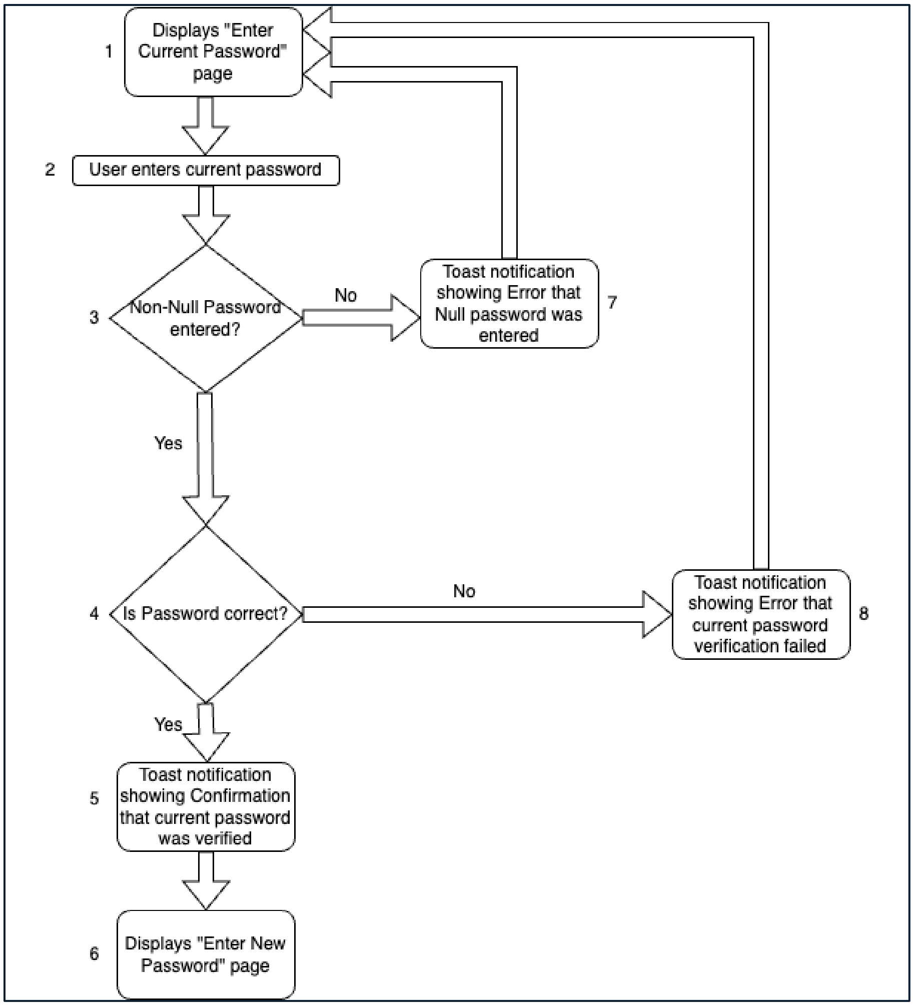
- "Existing User in DB" indicates whether the test setup should simulate the presence of a user record in the database.

WHITE BOX TESTING DOCUMENTATION

We have tested the ChangePassword page component, particularly its two methods-: verifyCurrentPassword (Use Case 1) and handlePasswordChangeSubmit (Use case 2). They perform the crucial functions of verifying the current password (before letting user change their password) and changing the user’s password respectively.

*Basis Path Testing Techniques for **ChangePassword** Component Functions*

Use Case 1: Verification of Current Password before allowing user to change password



1
Displays "Enter Current Password" page
2
User enters current password
3
Non-Null Password entered?
No
Toast notification showing Error that Null password was entered
7
Yes
4
Is Password correct?
No
Toast notification showing Error that current password verification failed
8
Yes
5
Toast notification showing Confirmation that current password was verified
6
Displays "Enter New Password" page

Control Flow Graph

*Table of Basis Paths for **verifyCurrentPassword** method*

No.	Set of Basis Paths	Path Description
1	1, 2, 3, 4, 5, 6	Current password entered and verified
2	1, 2, 3, 7, 1	No current password entered
3	1, 2, 3, 8, 1	Current password verification failed

Test Case 1	**VerifyCurrentPassword method**		
Test Scenario	Verifying Current Password	**Test Case ID**	VerifyPass-01
Test Path	1, 2, 3, 4, 5, 6	**Testing Priority**	High
Prerequisite	User has an account, is on the Change Password Page and is prompted to enter the current password.	**Post-Requisite**	User can proceed to enter a new password

No.	Action	Inputs	Expected Output	Actual Output	Test Result
1	Input current password	Correct password	Backend verifies the password	Backend verifies the password	Pass
2	Submit password for verification	-	Notification of successful verification and prompts to enter new password appear	Notification of successful verification and prompts to enter new password appear	Pass

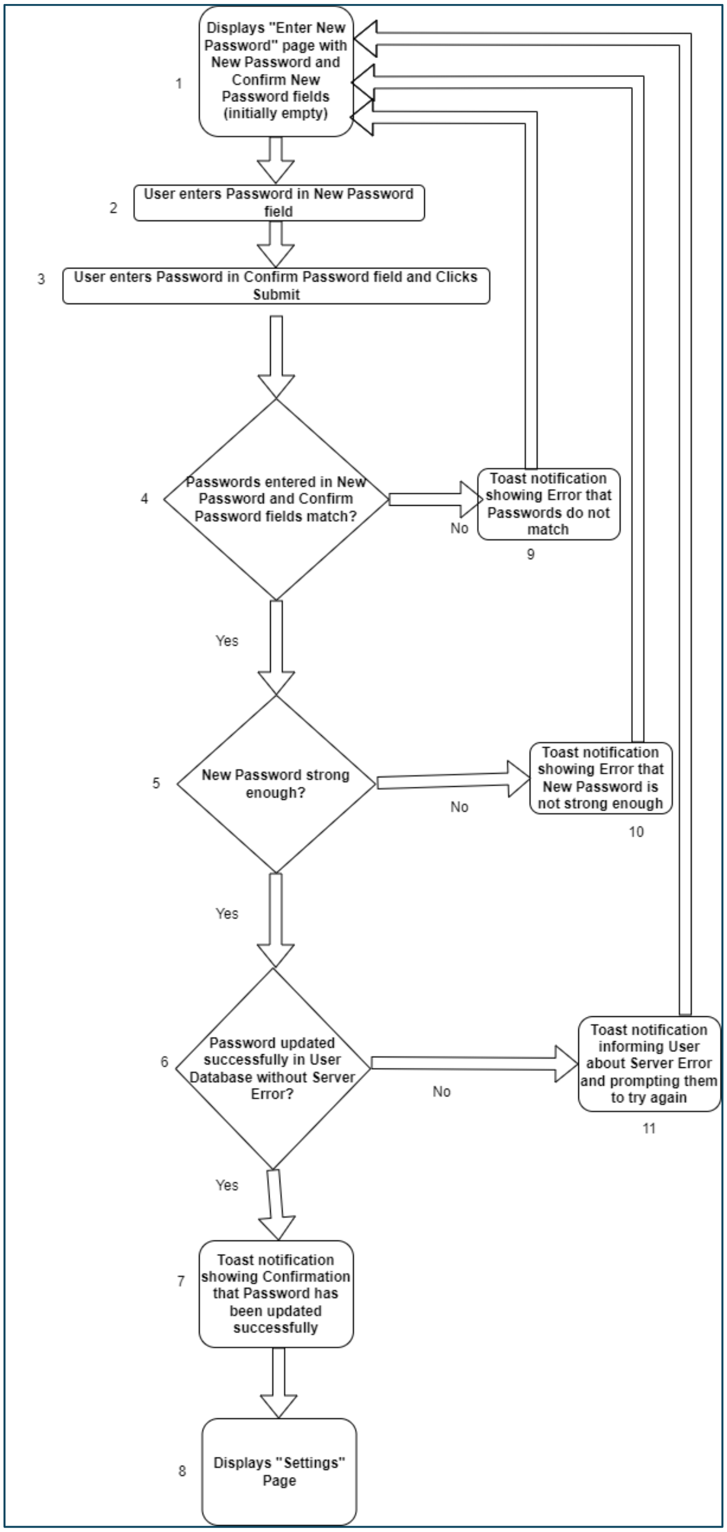
Test Case 2	Current Password Field Empty		
Test Scenario	Current Password Field Empty	**Test Case ID**	VerifyPass-02
Test Path	1, 2, 3, 7, 1	**Testing Priority**	Medium
Prerequisite	User is prompted to enter the current password	**Post-Requisite**	User is prompted again to enter the current password

No.	Action	Inputs	Expected Output	Actual Output	Test Result
1	Attempt verification without inputting anything in password field	-	Toast notification informing to enter password appears	Toast notification informing to enter password appears	Pass

Test Case 3	Current Password Verification Failure		
Test Scenario	Current Password Verification Failure	**Test Case ID**	VerifyPass-03
Test Path	1, 2, 3, 8, 1	**Testing Priority**	High
Prerequisite	User enters the current password	**Post-Requisite**	User remains on the current screen with an error notification and is prompted to re-enter password

No.	Action	Inputs	Expected Output	Actual Output	Test Result
1	Input current password	Incorrect password	Backend verifies the password with the User database	Backend verifies the password with the User database	Pass
2	Submit password for verification	-	Toast notification informing verification failed	Toast notification informing verification failed	Pass

Use Case 2: Submit New Password


1
Displays "Enter New Password" page with New Password and Confirm New Password fields (initially empty)
2
User enters Password in New Password field
3
User enters Password in Confirm Password field and Clicks Submit
4
Passwords entered in New Password and Confirm Password fields match?
No
Toast notification showing Error that Passwords do not match
9
Yes
5
New Password strong enough?
No
Toast notification showing Error that New Password is not strong enough
10
Yes
6
Password updated successfully in User Database without Server Error?
No
Toast notification informing User about Server Error and prompting them to try again
11
Yes
7
Toast notification showing Confirmation that Password has been updated successfully
8
Displays "Settings" Page

Control Flow Graph

*Table of Basis Paths for **handlePasswordChangeSubmit** Function*

No.	Set of Basis Paths	Path Description
1	1, 2, 3, 4, 5, 6, 7 ,8	Password changed successfully
2	1, 2, 3, 9, 1	New passwords mismatch
3	1, 2, 3, 10, 1	New password strength insufficient
4	1, 2, 3, 11, 1	Password update failed due to server error

*Test Cases for **handlePasswordChangeSubmit** Function*

Test Case 1	Changing Password Successfully		
Test Scenario	Current Password Verification Failure	**Test Case ID**	ChangePass-01
Test Path	1, 2, 3, 4, 5, 6, 7, 8	**Testing Priority**	High
Prerequisite	User has been authenticated and has verified the current password.	**Post-Requisite**	User's password is updated, and they are redirected to settings

No.	Action	Inputs	Expected Output	Actual Output	Test Result
1	Input new password in Password field	New Password	New Password reflects in Password field	New Password reflects in Password field	Pass
2	Input new password again in Confirm Password field	Matching New Password	New Password reflects in Confirm Password field	New Password reflects in Confirm Password field	Pass
3	Submit new passwords	-	The backend verifies that both passwords match, that the New Password is strong enough and updates the password.	The backend verifies that both passwords match, that the New Password is strong enough	Pass

			Successful change notification is shown and User is redirected to Settings page	and updates the password. Successful change notification is shown and User is redirected to Settings page	

Test Case 1	New Passwords Mismatch		
Test Scenario	Current Password Verification Failure	**Test Case ID**	ChangePass-02
Test Path	1, 2, 3, 9, 1	**Testing Priority**	High
Prerequisite	User has been authenticated and has verified the current password.	**Post-Requisite**	User is prompted to correct the passwords.

No.	Action	Inputs	Expected Output	Actual Output	Test Result
1	Input new and confirm passwords	Non-matching passwords	Does Nothing	Does Nothing	Pass
2	Click Submit	-	Toast showing Error that passwords don’t match	Toast showing Error that password s don’t match	Pass

Test Case 2	New Password Strength Insufficient		
Test Scenario	New Password Strength Insufficient	**Test Case ID**	ChangePass-03
Test Path	1, 2, 3, 10, 1	**Testing Priority**	Medium
Prerequisite	User has been authenticated and has	**Post-Requisite**	User is informed to use a stronger password

verified the current password.

No.	Action	Inputs	Expected Output	Actual Output	Test Result
1	Input new and confirm passwords	Weak new password	Does Nothing	Does Nothing	Pass
2	Click Submit	-	Toast warning to use a stronger password	Toast warning to use a stronger password	Pass

Test Case 3	Server Error on Password Update		
Test Scenario	Server Error on Password Update	**Test Case ID**	ChangePass-04
Test Path	1, 2, 3, 11, 1	**Testing Priority**	Low
Prerequisite	User is authenticated, has verified the current password, and entered a strong new password	**Post-Requisite**	Error is communicated to the user

No.	Action	Inputs	Expected Output	Actual Output	Test Result
1	Input new and confirm passwords	Strong new password	Does Nothing	Does Nothing	Pass
2	Click Submit	-	Server error notification	Server error notificatio n	Pass