CLASS-2

Sprint 1 Details

Olarn Rojanapornpun

SPRINT 1 PBIs

PBI	NAME	BRIEF DESCRIPTION
15	MATCH-PASSWORD	Check whether the *username* : *password* pair matches the stored credential
16	VALIDATE-MATCH-PASSWORD	Extend PBI15. Validate inputs on FE and BE
17	AUTHENTICATE-WITH-JWT-TOKENS	Extend PBI15. BE returns JWT access token when the credential is correct

PBI15 MATCH-PASSWORD

Check whether the *username* : *password* pair matches the stored credential

INPUTS

username: TEXT
password: TEXT, BLIND

FE (/login)

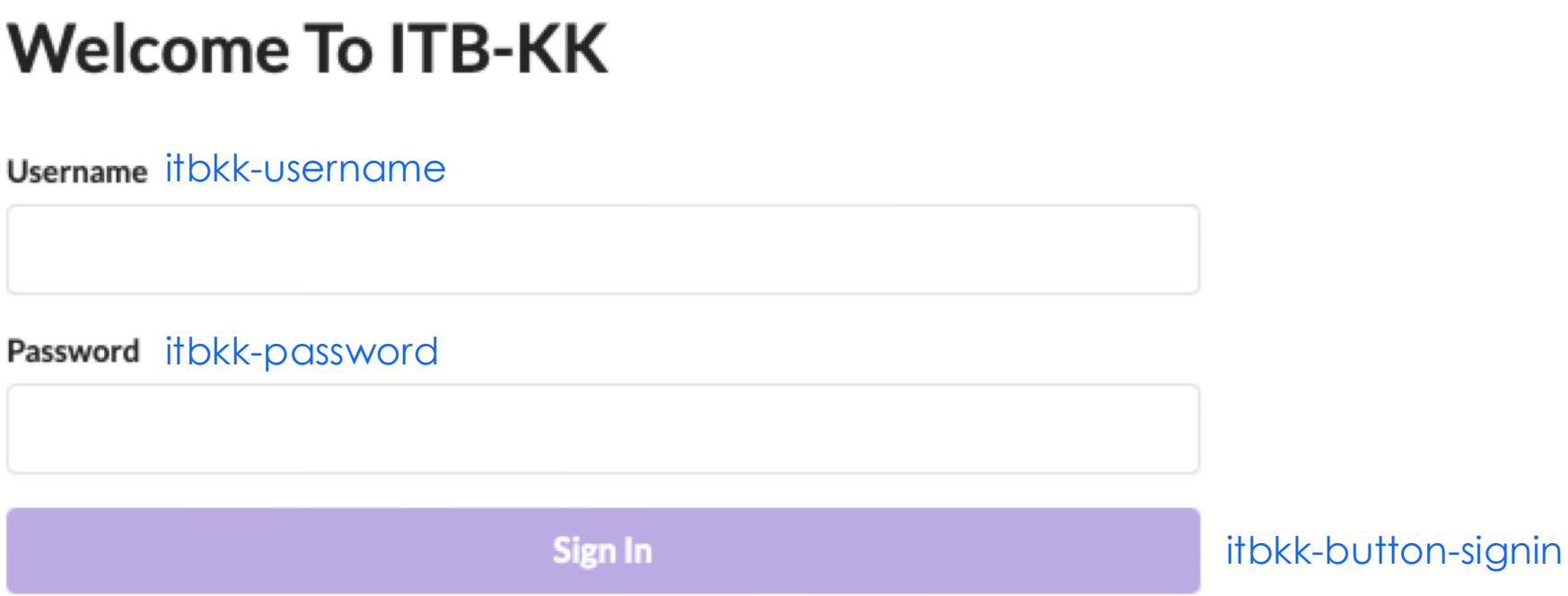
1. sends (raw) inputs to BE

BE (/login)

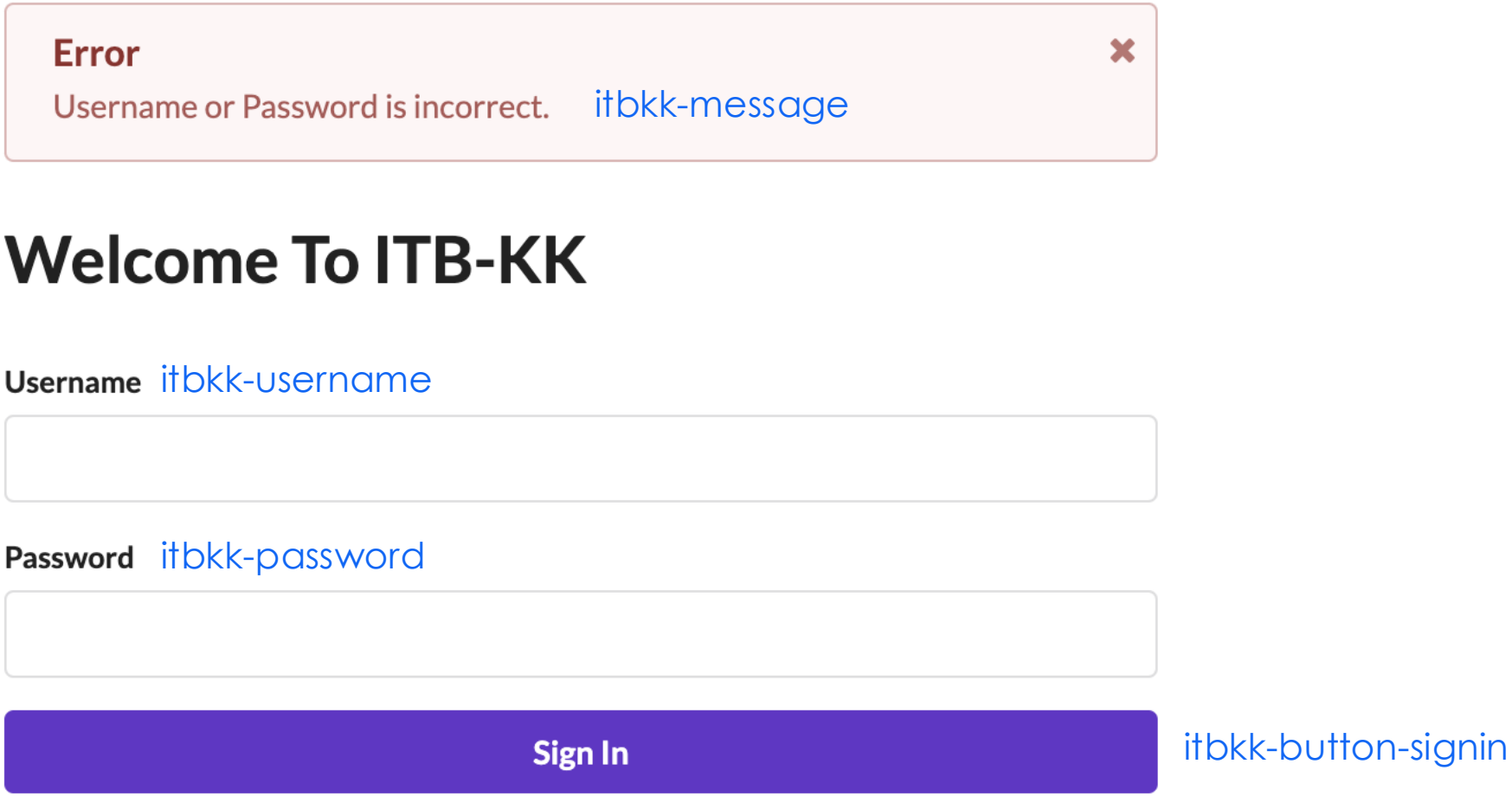
1. BE must not provide any service that return password!
2. BE finds the user record on 'users' table in 'ip32ft.sit.kmutt.ac.th:3306/itbkk_shared' that match the given username. (password was hashed with Argon2 algorithm)

Scenario	BE Code	FE behavior
correct credential	200	do nothing
incorrect credential	401	show message “Username or Password is incorrect”

Sample UI: Login (/login)



Sample UI: Login with error (/login)



PBI16 VALIDATE-MATCH-PASSWORD

Extend PBI15. Validate inputs on FE and BE.

INPUT SPECS

username: TEXT, NOT-EMPTY, MAX-LENGTH(50)
password: TEXT, NOT-EMPTY, MAX-LENGTH(14)

Scenario	BE Code	FE behavior
field is NULL/EMPTY	400	disable 'Sign In' button, otherwise, enable the button
field is over MAX-LENGTH	400	user cannot enter longer than MAX-LENGTH
field contains whitespace	as is	does not trim whitespaces or alert the user
password does not follow required syntax	as is	send the password as is, no alert
BE response = 400	-	show message "Username or Password is incorrect."
BE response != {200, 400, 401}	-	show message "There is a problem. Please try again later."

PBI17 AUTHENTICATE-WITH-JWT-TOKENS

Extend PBI15. BE returns JWT access token when the credential is correct

Scenario	BE behavior	FE behavior
correct credential	code: 200 access token valid for 30 mins	redirect to home page and display user's name on the screen.

Access Token Claims	
iss	issuer of the JWT; your public path, e.g. "https://intproj23.sit.kmutt.ac.th/ft/"
iat	time at which the JWT was issued; can be used to determine age of the JWT
exp	time after which the JWT expires
name	a human-readable value that identifies the subject of the token, e.g. "SOMCHAI JAIDEE"
oid	the immutable identifier for an object; user-id, e.g. "533c0096-a48c-4be1-8e42-769a9f05a725"
email	email address of the user
role	role of the user

users Attributes [SHARED DATABASE]

Attribute	Description / Constraints	Example
oid	Universally unique identifier (UUID) : CHAR(36) UNIQUE, NOT NULL	533c0096-a48c-4be1-8e42-769a9f05a725
name	User full-name : UTF-8 TEXT; Limit to 100 characters; NOT NULL; NOT EMPTY Leading and trailing whitespaces are trimmed;	SOMCHAI JAIDEE
username	User name: TEXT; Limit to 50 characters; NOT NULL; NOT EMPTY Leading and trailing whitespaces are trimmed;	somchai.jai
email	User email Limit to 50 characters; NOT NULL; NOT EMPTY	somchai.jai@kmutt.ac.th
password	User hashed password : VARCHAR(100) NOT NULL	$argon2id$v=19$m=4096,t=3,p=1$fabZIRZZrUuxRrnXoGkMjA$DZ90F9+3/rnHGKY/YmyQoZwOToS4mJbuLYZkpXQt2VY
role	User role: ENUM of {LECTURER, STAFF, STUDENT} NOT NULL; The default value is 'STUDENT';	

API Specifications for SPRINT 1

API Specifications for SPRINT 1

Responses

Code	Description
200	Successful Operation Media type application/hal+json Controls Accept header. **Example Value** | Schema

(PBI17)

```
{
  "access_token" : "string",
}
```

Code	Description
400	Username or Password is invalid
401	Username or Password is incorrect Media type application/hal+json

PBI15 TEST CASES

PBI	username	password	Expect Results
15	abc123	abc123	1. The password must be hidden. 2. BE responses 401, with message "The username or password is incorrect." 3. FE shows message "The username or password is incorrect." and stays on login page
	itbkk.siam	abc123	Same as above
	itbkk.olarn	itbkk/olarn	1. BE responses 200 2. FE stays on login page

PBI16 TEST CASES

PBI	username	password	Expect Results
16			1. The Login button is disabled 2. [postman] status code = 400
	MaxUser001MaxUser002MaxUser003MaxUser004MaxUser005MaxUser006		1. The Login button is disabled 2. MaxUser001MaxUser002MaxUser003MaxUser004MaxUser005 is shown in username field 3. [postman] status code = 400
	MaxUser001MaxUser002MaxUser003MaxUser004MaxUser005MaxUser006	MaxPassword1234567	1. The Login button is enabled 2. MaxUser001MaxUser002MaxUser003MaxUser004MaxUser005 is shown in username field 3. MaxPassword12345 is shown in username field 4. [postman] status code = 400
		MaxPassword12345	1. The Login button is disabled 2. MaxPassword12345 is shown in username field 3. [postman] status code = 400
	MaxUser001MaxUser002MaxUser003MaxUser004MaxUser005Max	MaxPassword12345	1. The Login button is enabled 2. MaxUser001MaxUser002MaxUser003MaxUser004MaxUser005 is shown in username field 3. MaxPassword12345 is shown in username field 4. [postman] status code = 401

PBI17 TEST CASES

PBI	username	password	Expect Results
17	itbkk.olarn	itbkk/olarn	1. BE responses 200 with access_token as follows (use jwt.io) iss: <<public path>> iat: time at which the JWT was issued exp: iat + 30 mins name: OLARN ROJANAPORNPUN oid: <<533c0096-a48c-4be1-8e42-769a9f05a725>> email: itbkk.olarn@ad.sit.kmutt.ac.th role: LECTURER 2. FE redirects to homepage and shows OLARN ROJANAPORNPUN

Sprint 2 Technical Spike

- Vue Router Navigation Guard
- Spring Boot Authorization (WebSecurity)
- Refactor DB to support 1 board/user

RULES

- Team must commit Sprint 1 by Aug 13, 2024!
- Team must NOT create or duplicate the whole users table
- Team must NOT store raw password in DB
- BE must be located in KMUTT network to access shared database
- Team must use 'secret' secret to create JWT token

Team may use https://jwt.io or https://jwt.ms to view token payload/claims