CLASS-2

Sprint 1 Details

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 'ip23ft.sit.kmutt.ac.th:3306/itbkk_shared' that match the given username. (password was hashed with Argon2 algorithm)

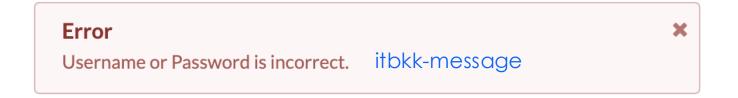
| Scenario | BE Code | FE behavior |
|----------------------|---------|--|
| correct credential | 200 | do nothing |
| incorrect credential | 401 | show message "Username or Password is incorrect" |

Sample UI: Login (/login)

Welcome To ITB-KK

| Username | itbkk-username | |
|----------|----------------|---------------------|
| | | |
| Password | itbkk-password | |
| | | |
| | | |
| | Sign In | itbkk-button-signir |

Sample UI: Login with error (/login)

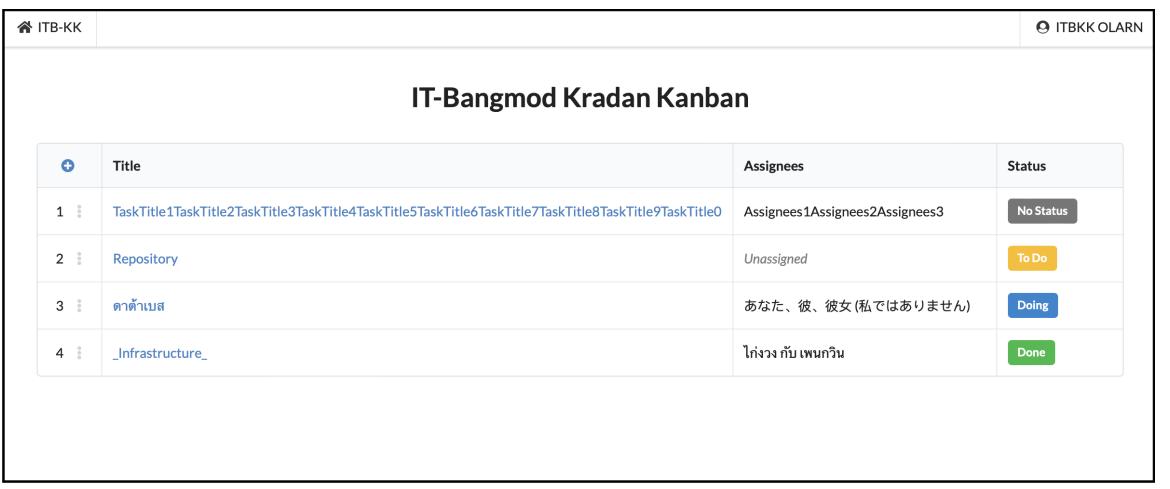


Welcome To ITB-KK

| Username itbkk-username | |
|-------------------------|---------------------|
| Password itbkk-password | |
| Sign In | itbkk-button-signir |

Sample UI: Home with user's fullname

itbkk-fullname



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

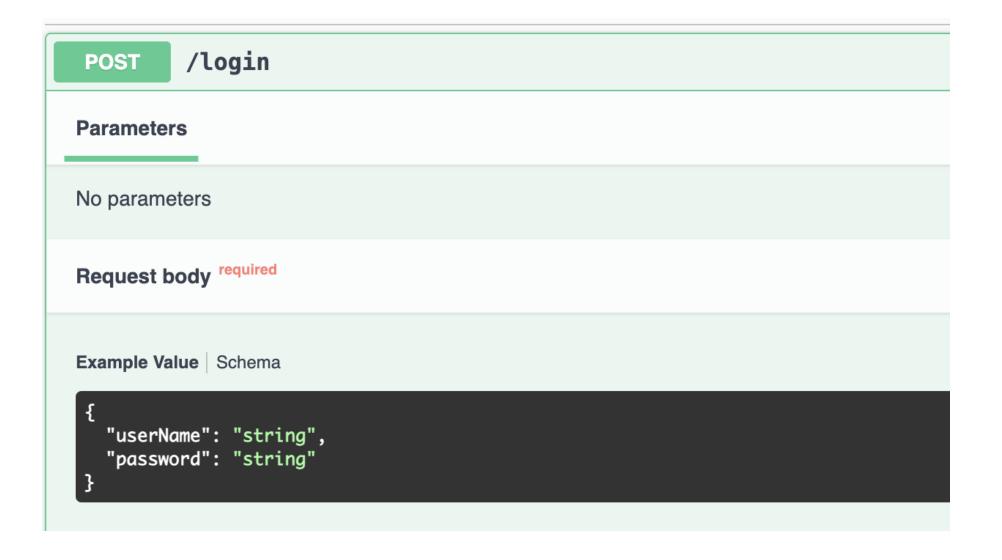
| Scenario | BE behavior | FE behavior |
|--------------------|--------------------------------|-----------------------------------|
| correct credential | code: 200 | redirect to home page and display |
| | access token valid for 30 mins | user's name on the screen. |

| Access | 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 | | |
| ехр | 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 | | |

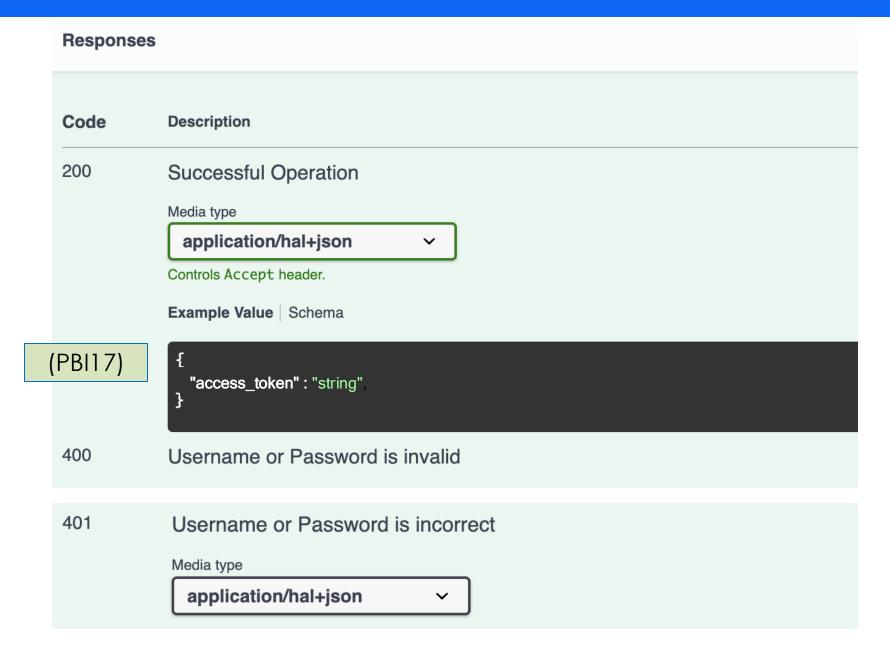
users Attributes [SHARED DATABASE]

| 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\$f abZIRZZrUuxRrnXoGkMjA\$DZ90F9+3 /rnHGKY/YmyQoZwOToS4mJbuLYZ kpXQt2VY |
| 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



PBI15 TEST CASES

| PBI | username | password | Expect Results |
|-----|------------|------------|--|
| 15 | itbkk.siam | ip23/SIA | password is not shown BE responses 200 FE stays on the same page |
| | itbkk.siam | itbkk.siam | BE responses 401 FE shows message "Username or Password is incorrect." and stays on the same page |
| | itbkk.sia | itbkk.siam | Same as above |

PBI16 TEST CASES

| PBI | username | password | Expect Results |
|-----|---|-----------------|--|
| 16 | MaxUser001MaxUser 002MaxUser003Max User004MaxUser005 | MaxPassword123 | The Login button is enabled BE returns 401 and FE shows "Username or Password is incorrect." [postman] status code = 401 |
| | | | The Login button is disabled [postman] status code = 400 |
| | MaxUser001MaxUser 002MaxUser003Max User004MaxUser005 M | | The Login button is disabled MaxUser001MaxUser002MaxUser003MaxUser004MaxUser005 is shown in username field [postman] status code = 400 |
| | MaxUser001MaxUser 002MaxUser003Max User004MaxUser005 M | MaxPassword1234 | The Login button is enabled MaxUser001MaxUser002MaxUser003MaxUser004MaxUser005 is shown in username field MaxPassword123 is shown in password field BE returns 401 and FE shows "Username or Password is incorrect." [postman] status code = 400 |
| | | MaxPassword1234 | The Login button is disabled MaxPassword 123 is shown in password field [postman] status code = 400 |

PBI17 TEST CASES

| PBI | username | password | Expect Results |
|-----|-------------|----------|---|
| 17 | itbkk.olarn | ip23/OLA | BE responses 200 with access_token as follows (use jwt.io or jwt.ms) iss: https://intproj23.sit.kmutt.ac.th/<<team-code>>/ iat: time at which the JWT was issued exp: iat + 30 mins name:ITBKK OLARN oid: 2b2f94fd-68be-4ff2-8c67-cb35e139f6fb email: itbkk.olarn@ad.sit.kmutt.ac.th role: LECTURER</team-code> FE redirects to homepage and shows ITBKK OLARN |

Sprint 2 Technical Spike

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

RULES

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