

# Project Details

Task: C  
Done by: Tan Wei Jie (A0202017B)  
Repo Link: [https://github.com/tanweijie123/CS3219\\_Sandbox/tree/main/Task\\_C](https://github.com/tanweijie123/CS3219_Sandbox/tree/main/Task_C)  
Backend Link: <http://tanwj.link:8082/api/general>

Project is based on Task B, but added authorization and authentication.

# Background Information

- Password Manager ( /api/book ) can only be accessed by User with 1 and higher priviledge.
- General Access ( /api/general ) can be accessed by any logged in users.
- Sign up ( /api/signup ) and Log in ( /api/login ) can be accessed by any user.

# Overview

1. When you accessed the restricted links, it will return a **Not authenticated!** reply.

GET

http://tanwj.link:8082/api/general

Send

ParamsAuthorizationHeaders (6)BodyPre-request ScriptTestsSettingsCookies

Headers6 hidden

	KEY	VALUE	DESCRIPTION		Bulk Edit	Presets
	Key	Value	Description			

BodyCookiesHeaders (8)Test Results401 Unauthorized95 ms270 BSave Response

PrettyRawPreviewVisualizeHTML

1Not authenticated!

GET

http://tanwj.link:8082/api/book

Send

ParamsAuthorizationHeaders (7)BodyPre-request ScriptTestsSettingsCookies

Headers6 hidden

BodyCookiesHeaders (8)Test Results401 Unauthorized46 ms270 BSave Response

PrettyRawPreviewVisualizeHTML

1Not authenticated!

2. In this step, I will create a user with 0-level access rights.

The screenshot shows a REST client interface with a POST request to `http://tanwj.link:8082/api/signup`. The request body is `x-www-form-urlencoded` with the following data:

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> user	randomguy	
<input checked="" type="checkbox"/> access	0	

The response status is 200 OK, 457 ms, 276 B. The response body is:

```
{  "message": "User created!"}
```

3. By using this username, I will try to log in to the system. After logging into the system, it will return me with a token.

The screenshot shows a REST client interface with a POST request to `http://tanwj.link:8082/api/login`. The request body is `x-www-form-urlencoded` with the following data:

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> user	randomguy	

The response status is 201 Created, 46 ms, 545 B. The response body is:

```
{  "status": "success",  "message": "Logged in successfully",  "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfcm9udGkiOiJ2MTczZTZjYTRiNGMxODZjYzNkYTU3MTciLCJhY2Nlc3MiOiJAsInVzZXIiOiJyYW5kb21ndXkiLCJfcm9udGkiOiJAsImhhdCI6MTYzNDk5NTI5NCwiZXhwIjozNjM0ODk0fQ.w8pGt4vK0-uunGEPHqJhKbcIks3_iHimw_hW-8u2kqE"}
```

4. By using this token, I will try to access the General Access and Password Manager. Note that this account is unable to access the Password Manager due to insufficient access rights.

GET ▼ http://tanwj.link:8082/api/general Send ▼

Params Authorization Headers (7) Body Pre-request Script Tests Settings Cookies

Headers 6 hidden

	KEY	VALUE	DESCRIPTION	...	Bulk Edit	Presets
<input checked="" type="checkbox"/>	x-access-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.e...				
	Key	Value	Description			

Body Cookies Headers (8) Test Results 200 OK 120 ms 269 B Save Response ▼

Pretty Raw Preview Visualize HTML ▼ ≡

```
1 Welcome all logged in peeps
```

GET ▼ http://tanwj.link:8082/api/book Send ▼

Params Authorization Headers (7) Body Pre-request Script Tests Settings Cookies

Headers 6 hidden

	KEY	VALUE	DESCRIPTION	...	Bulk Edit	Presets
<input checked="" type="checkbox"/>	x-access-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.e...				
	Key	Value	Description			

Body Cookies Headers (8) Test Results 403 Forbidden 36 ms 275 B Save Response ▼

Pretty Raw Preview Visualize HTML ▼ ≡

```
1 Insufficient Access Rights
```

5. In this step, I will create a superuser with 10-level access rights.

POST ▼ http://tanwj.link:8082/api/signup Send ▼

Params Authorization Headers (8) Body Pre-request Script Tests Settings Cookies

☐ none ☐ form-data ☒ x-www-form-urlencoded ☐ raw ☐ binary ☐ GraphQL

	KEY	VALUE	DESCRIPTION	...	Bulk Edit
<input checked="" type="checkbox"/>	user	superuser			
<input checked="" type="checkbox"/>	access	10			
	Key	Value	Description		

Body Cookies Headers (8) Test Results 200 OK 88 ms 276 B Save Response ▼

Pretty Raw Preview Visualize JSON ▼ ≡

```
1 {
2   "message": "User created!"
3 }
```

6. By using this username, I will try to log in to the system. After logging into the system, it will return me with a token.

The screenshot displays a REST client interface with a POST request to `http://tanwj.link:8082/api/login`. The request body is in `x-www-form-urlencoded` format, containing the following data:

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> user	superuser	
Key	Value	Description

The response is shown in the 'Body' tab, indicating a 201 status code, 31 ms duration, and 546 B size. The response body is in JSON format:

```
{
  "status": "success",
  "message": "Logged in successfully",
  "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfawQiOiI2MTczZTg3NmMyNjRlNDRjMTRmMmRlODAiLCJhY2Nlc3MiOiJlLCJ1c2VyIjoic3VwZXJ1c2VyIiwiaXNjaW92IjowLCJpYXQiOiJlMzQ5OTU2MzEsImV4cCI6MTYzNDk5OTIzMX0.F5-kbbc8RJU0H5i8P-6SREc0q_qwNJ01CtCcFwk9HN8"
}
```

7. By using this token, I will try to access the General Access and Password Manager. Note that this account will be able to access the Password Manager and General Access.

GET

http://tanwj.link:8082/api/general

Send

ParamsAuthorizationHeaders (7)BodyPre-request ScriptTestsSettingsCookies

Headers

6 hidden

	KEY	VALUE	DESCRIPTION		Bulk Edit	Presets
<input checked="" type="checkbox"/>	x-access-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.e...				
	Key	Value	Description			

BodyCookiesHeaders (8)Test Results

200 OK55 ms269 BSave Response

PrettyRawPreviewVisualizeHTML

1Welcome all logged in peeps

GET

http://tanwj.link:8082/api/book

Send

ParamsAuthorizationHeaders (7)BodyPre-request ScriptTestsSettingsCookies

Headers

6 hidden

	KEY	VALUE	DESCRIPTION		Bulk Edit	Presets
<input checked="" type="checkbox"/>	x-access-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.e...				
	Key	Value	Description			

BodyCookiesHeaders (8)Test Results

200 OK26 ms873 BSave Response

PrettyRawPreviewVisualizeJSON

1

```
"status": "success",
"message": "Book retrieved successfully",
"data": [
  {
    "_id": "614ea21a1189c357d45b277a",
    "create_date": "2021-09-25T04:14:18.902Z",
    "name": "google.com",
    "id": "tanwj",
    "pw": "GoodPassword",
    "__v": 0
  }
]
```

11