- Protecting specific endpoint means that those endpoints should only be accessible / work, only if the user is logged in.
If not logged-in, user will be forced to login first, and then perform any operation.

7:28:00

- We already know, to force a user to login before accessing a path operation, we just need to add an extra parameter to the function:-

3rd parameter

```
[ ...user_id: int = Depends(oauth2.get_current_user)
```

This function now becomes a dependency for the path operation. [means this function must ~~run~~ run successfully, for the path operation to run]

- Upon successful execution of the oauth2.get_current_user function, it will return the extracted user id from the token, that we are storing into the user_id parameter variable.

- Now, if the user now tries to acess the path oper. without logging in, in response he/she will get the following error msg:-

```
{
  "detail": "Not authenticated"
}
```

⇒ Suppose, we added this above authentication parameter to the create_post path operation. Then, create_post can only be accessed, if the request header contains the token of specified type.

What we can do is that we can login, take the returned token, and in the request header for creation of post, pass it as follow:-

in postman

| Key | Value |
|---|---|
| Authorization | Bearer eyZH4$321 ... -- |

space in between

We must mention the token-type first, in the value.

the valid access token

Without this header, no one can create post.