**Day 11: 04 Oct. 25**

**Security:**

Node JS provided one of the third party module ie **bcryptjs** module. This modules help us to achieve password hashing algorithms concept. This module help use to encrypt as well as descript the password.

Create the folder as bcryptjsmoduleexample

**npm init -y** to create the package.json file

**npm install bcryptjs** install the module

getSalt() : it generate a salt with a cost factor of 10. By default 10 consider.

The cost factor 10 determines how many times the hashing algorithm will run.

More rounds = more secure, but slow in performance.

4 to 14+

4 fast but less secure

14+ secure but slow performance.

**Authentication and authorization**

**Authentication** : it is a process of verify who a user is. Once the person do the logic using their authentication details like id, emailid and password or unique information they only allow to access the resources.

**Authorization :** the process of determining what is user is allowed to do.

To access all rest api for product you need authentication person.

Then base upon role you can access those rest api like

Admin user 🡪 add product, delete product, update product, view product etc

Customer user -🡪 View the all product. Can add the product in cart and place the order.

By default http is state less protocol.

Req

1st request

2nd request + session Id

3rd request + session id

Client Server

1st response + cookies (session id)

2nd response

3rd response

Session id :

Cookies : cookies is small text file created by server when first request send to server. This file contains lot of information with session id. This file store in client machine.

JWT Token : Json Web Token

JWT is a compact secure way to transmit information between client and server. Which mainly help us to do authentication as well as authorization.

JWT divided into 3 parts

1. Header -🡪 algorithms
2. Payload 🡪 data ie unique data as well as role. (but not store password).
3. Signature : which help to generate the token

When client send the request 1st request with login details. Server generate the token. While creating token first we select algorithm by default HS256, in payload we add unique information of that user ie emailid or primary key property and send the token with expiry.

Next time to access any rest api we check token present in your request. If token present we will allow to access that resources else display error.

Node JS provided third party modules **jsonwebtoken** which help to create JWT token

Creating simple example to create and validate json token.

Create the folder with name as **jwttokenexample**

npm init -y

npm install jsonwebtoken