**Day 6 :17 Aug 24**

React JS Security : React security refer to the practise and strategies use to protect react application from various threats.

Req(http/https)----🡪

Client Server

🡨---Res(http/https)

1. Cross site scripting (XSS) protection

This technique generally hacker use while client server communication happing. Whenever client send some request to server when server give response with that they pass some scripting file. That file when client send request it execute in client machine to get secure data.

To avoid we need use in frontend side technologies as a technique Sanitizer user input.

DOM any html tag provide some attribute ie dangerouslySetInnerHTML

create-react-app react-xss-app

react js use one of the third party library ie dompurify

npm install dompurify

http is stales protocol.

Whenever client send first request to client. Server generate one text file which is known as cookies. Cookies is small text file created by server when client send first request. This file pass with response + cookies( which contains lot of information as sessionId). This file store in client machine.

Cookies :

CSRF token

Cross Site Request Forgery

CSRF token is unique, random value generated by server when client send first request to server. In second request server checking token present in your request or not. This token help us to identity authenticate user and using this token we can avoid or intended to make the request.

Cookies cc=new Cookies(name,value)

response.addCookies(cc);

authentication and authorization

When we create n number rest api

Authentication is use to access the resource like access rest api.

Base upon role, we can restrict the user to access limited or all resources.

JWT : JSON Web Token

This generate by backend technologies like node js, we

We generate unique token.

JWT token contains mainly three parts

Header : we can use different type of algorithms to generate high secure token.

Payload : actual data like unique information for specific user accno, emaild, employee\_id, and role

Signature : this part is responsible to combine header and palylaod with public and private key pairs.

This token we can set expiry

<form>

<input type=”hidden” name=”csrf\_token” value={{csrf\_token}}/>

</form>

Generally in react js we call backend technologies using

fetch or axios

axios(“”)

please refer the folder as csrf token server

open the command prompt inside this folder.

Run the command as

npm install this command read all dependencies details from package.json file and download all dependencies in local machine.

Then run node server.js file

This file provider two url

First one for generate token

<http://localhost:3001/api/csrf-token>

Second one for submit form with csrf token

<http://localhost:3001//api/submit-form>

Now we will create react application to communicate backend app which is responsible to generate and validate the token

**create-react-app react-csrf-token-app**

**cd react-csrf-token-app**

**npm install axios**

<http://www.gmail.com> -----🡪 req

client server

res with gmail.com

**JWT token**

Please refer express-jwt folder which contains server.js file and package.json file. Open the terminal and run the command as

npm install

Please test all end point using rest client plugin like post man

Now we will create the create application that interact with backend technology to get jwt token.