**Day 4**

**Node JS security**

**Node JS provided external modules is bcryptjs : This modules help to do hashing password.**

**Password encryption and description using bcrptjs module.**

npm install bcryptjs

crypto modules : This is core modules part of node js which help us to do different type of crypto functionality like security features such encryption, decryption, hashing, digital signature, generate public and private to do encryption and decryption etc.

using crypto module we will check all algorithm support.

let crypto = require("crypto");

//console.log(crypto.getHashes())

//console.log(crypto.getCiphers())

for(let algorithm of crypto.getCiphers()){

    console.log(algorithm)

}

console.log("---------------------")

for(let algorithm of crypto.getHashes()){

    console.log(algorithm)

}

Using above example we can see all supporting algorithms

While using these algorithms we need to give the below format

1. Hex
2. Base64
3. Utf-8/utf-16
4. Base64URL

Etc

While dealing with any format we use one of the pre defined ie Buffer.

SHA-256 (Secure Hash Algorithm) is widely used cryptographic hash function that produce (32 bytes) hash values.

HMAC : (Hash based Message Authentication code). In this algorithms format while generating the code we need to pass secure key which help use to verify algorithms data changed or not.

AES-256-CBC- Advanced Encryption Standard with 256 bit key Cipher Block Chain).

Session Tracking :

Session : Collection of request and response within a particular period of a time is known as session. By default http is state less protocol. Using http server side we can’t keep the track about the client.

Cookies : Cookies is small text file created by server when client send first request to server. This file contains lot of information in key-value format. Which contains session id. This session id pass through cookies file to client. Cookies file stored in client machine.

Url writing technique : this technique we use when cookies option disable on client side.

URL?sessionId=value

It support only Get method.

Rest API is state less communication.

JWT / OAuth

JWT : JSON Web Token

JSON Web Token mainly divided into three

Header : Algorithm

Body : payload (unique information) for that particular user.

Signature

JWT :

mkdir express-jwt-with-postgres-single-page

npm install express pg sequelize bcryptjs jsonwebtoken