Module 5: Assignment 2 User Authentication

Spurthy Mutturaj

Instructor: Dinesh Sthapit

Oct 27,2022

GitHub:

**Project 1**

A screenshot of a computer

Description automatically generated

Inserting user details into the textpassword DB

Graphical user interface, text, application, email

Description automatically generated

Note: Password is saved as plain text

Inserting 5 Users and testing Get MethodGraphical user interface, text, application

Description automatically generated

5 users in DB “textpassword”

Graphical user interface, application, Teams

Description automatically generated

Get User by ID:

Graphical user interface, text, application, email

Description automatically generated

Updating the User(email changed from [spurthy@gmail.com](mailto:spurthy@gmail.com) to spurthy@asu.edu)

Graphical user interface, text, application, email

Description automatically generated

Deleting an User :

Graphical user interface, text, application, email

Description automatically generated

textpassword file in. postman Collection – User Authentication

Graphical user interface, application

Description automatically generated

Project 2:

A screenshot of a computer

Description automatically generated with medium confidence

Signing Up a user:

Graphical user interface, text, application, email

Description automatically generated

Logging In:

Graphical user interface, text, application, email

Description automatically generated

Trying to login without password: error thrown:

Graphical user interface, text, application, email

Description automatically generated

Entering Wrong Password- error

Graphical user interface, text, application, email

Description automatically generated

Getting users stored in the DB:

Graphical user interface, application

Description automatically generated

Deleting a User saved in the DB:

Graphical user interface, text, application, email

Description automatically generated

Updating a User using put:

Graphical user interface, text, application, email

Description automatically generated

Database –“encryptedpassword” Screenshot

Graphical user interface, application, Teams

Description automatically generated

Postman Collection

Graphical user interface, application

Description automatically generated

**Project 3:**

**Text

Description automatically generated**

Signing up a User

Graphical user interface, text, application, email

Description automatically generated

Loging in:

Graphical user interface, text, application, email

Description automatically generated

Verifying the JWT created is functional by adding a task :

Graphical user interface, text, application, email, website

Description automatically generated

Getting all Users (5 users are created)

Graphical user interface, text, email

Description automatically generated

Put (update)– changing email from veronica@asu.com to [veronica@gmail.com](mailto:veronica@gmail.com)

Graphical user interface, text, application, email

Description automatically generated

Deleting the User by ID:

Graphical user interface, text, application, email

Description automatically generated

Database has 5 Users:

Graphical user interface, application, Teams

Description automatically generated

Tasks DB:

Graphical user interface, application, Teams

Description automatically generated

Collection created and exported in Postman:

Graphical user interface, application

Description automatically generated

Text

Description automatically generated

**JSON Web Token**

JSON Web token is a 2-way Protocol in which the client makes a request to the server and a response is generated from the server. It is a stateless protocol in which the token contains all the information needed to identify itself(client) to the server and eliminates the need for session state. The information stored in JWT can be verified and trusted because it is digitally signed.

JSON is usedful for Authentication and information Exchange. A typical JWT consists of 3 parts separated by 3 dots i.e the Header, Payload and the signature which looks like

Text

Description automatically generated

Image Source: <https://auth0.com/learn/json-web-tokens>

**Java Web Token Authentication Flow.**

Diagram

Description automatically generated

* The Client/Browser posts a request to the server using their email.
* Identity hash is checked for in the header,  
  if it exists: Then the stored identity in the header is verified using the signature, universal unique identifier(UUID) with the has of the email.

If it doesn’t exist: The server generates the signed token when the browser or requesting device requests for JWT encoded data, as shown in the diagram above and returns it to the client.

* For every subsequent request that requires authentication on the server, the token can be passed onto the http request. Once the token has been validated, the server returns the secure resource to the client if it is valid.
* If the token is not valid, it regenerates a JWT and returns it the browser as shown in the above diagram

References:

1. Code provided in canvas
2. Module 5: Assignment 1 submitted by “Spurthy Mutturaj” (me) on canvas