Review & Final Submission

Great Job!

Everything looks ready to be scored. This is your last opportunity to review your work and leave any final comments.

Once you submit your assessment it will be automatically scored and Decagon will be notified of the results.

Submit My Assessment

✓ Challenge #1

Ready for Scoring

Your Answers | Your Notes (Editable)

1. What do you mean by spring security?

   SPRING SECURITY: is a powerful and customizable authentication and access control framework for Java applications. It provides comprehensive security services for Java EE-based enterprise software applications.

2. What Is Authentication and Authorization? Which Must Come First?

   AUTHENTICATION: is the process of verifying the identity of a user, typically by validating their credentials such as username and password.

   AUTHORIZATION, on the other hand, is the process of determining whether an authenticated user has the necessary permissions to access certain resources or perform specific actions.

   Authentication usually comes before authorization because you need to verify the user's identity before granting access to resources.

0:19:16

3. Does Spring Security Support Password Hashing? What Is Salting?

   Yes, Spring Security supports password hashing. Password hashing is a technique used to securely store passwords by converting them into a scrambled representation using a cryptographic hash function.

   SALTING is the process of adding a random value (salt) to the input data before hashing to increase security.

4. Differentiate between Encryption, Hashing and Salting

   ENCRYPTION: is the process of converting data into a ciphertext that can only be decrypted back to its original form with the right key.

   HASHING: is a one-way process of converting data into a fixed-size string of characters using a hash function, which cannot be reversed to obtain the original data.

   SALTING: is adding a random value to the input data before hashing to increase security.

5. What does the SecurityFilterChain does in spring security?

   The SecurityFilterChain in Spring Security is responsible for processing incoming requests and applying security rules to them. It consists of a series of filters that perform tasks such as authentication, authorization, session management, CSRF protection, and more.

0:19:16

6. Using code create a Java program that simulates a basic login system using username and password authentication

```java
public static void main(String[] args) {
    Scanner input = new Scanner(System.in);

    String username = "user123";
    String password = "password123";

    System.out.println("Welcome to FIRI Login System!");

    System.out.print("Enter username: ");
    String enteredUsername = input.nextLine();

    System.out.print("Enter password: ");
    String enteredPassword = input.nextLine();

    if (enteredUsername.equals(username) && enteredPassword.equals(password)) {
        System.out.println("Login successful! Welcome " + username + "!");
    } else {
        System.out.println("Invalid username or password. Please try again.");
    }

}
```

7. Differentiate between authentication and authorization.

```
AUTHENTICATION: is the process of verifying the identity of a user, typically by validating their credentials such as username and password.

AUTHORIZATION, on the other hand, is the process of determining whether an authenticated user has the necessary permissions to access certain resources or perform specific actions.
```

0:19:16

8. InJWT what is the structure of the Payload?

In JWT, the payload is the second part of the token and it contains claims. These claims are statements about an entity and additional data. The payload is encoded as a JSON object and is used to provide information about the user or token to the application.

9. Describe the structure of a JSON Web Token (JWT).

The structure of a JWT consists of three parts separated by dots: the header, the payload, and the signature. The header consists of the token and the hashing algorithm being used. The payload contains claims about the user or token, while the signature is used to verify that the sender of the request is who it says it is and the message has not been tampered with.

10. what are the advantages of Spring Security

The advantages of Spring Security include robust authentication and authorization mechanisms, support for multiple authentication methods such as form-based, basic, and OAuth, integration with various security standards and protocols, comprehensive protection against common security vulnerabilities, and seamless integration with the Spring Framework.

11. What is OAuth, and how does it work?

OAuth is an open standard for access delegation commonly used as a way for internet users to grant websites or applications access to their information on other websites without sharing their passwords. It works by enabling a user to grant a third-party application limited access to their resources stored on another service, such as Facebook, Google, Microsoft, without revealing their credentials

12. what do you understand by SSO?

SSO (Single Sign-On), is a session/user authentication process that enables a user to access multiple applications and services with one set of login credentials (username and password) eliminating the need for multiple log in attempts.

0:19:16

Comments?

Optional comments about the assessment process, challenges, etc.

0:19:16