HOMEWORK #5

1 – What are Authentication and Authorization?

Authentication is the act of validating that users are whom they claim to be. This is the first step in any security process. **Authentication**, in the form of a key. The lock on the door only grants access to someone with the correct key in much the same way that a system only grants access to users who have the correct credentials.

Authorization in system security is the process of giving the user permission to access a specific resource or function.**Authorization,** in the form of permissions. Once inside, the person has the authorization to access the kitchen and open the cupboard that holds the pet food. The person may not have permission to go into the bedroom for a quick nap.

2 - What is Hashing in Spring Security?

Hashing is the process of generating a string, or *hash*, from a given *message* using a mathematical function known as a *cryptographic hash function*. Hashing is a one-way function that converts the input to a line of symbols. Normally the length of this line is fixed. Spring Security ships with support for all these recommended algorithms via the *PasswordEncoder* interface:

- *Pbkdf2PasswordEncoder* gives us PBKDF2
- *BCryptPasswordEncoder* gives us BCrypt, and
- *SCryptPasswordEncoder* gives us SCrypt

3 - What is Salting and why do we use the process of Salting?

Salting hashes is like a salt is added to the hashing process to force their uniqueness, increase their complexity without increasing user requirements, and to mitigate password attacks like hash tables.

4 - What is “intercept-url” pattern?

intercept-url is being used to access to all links starting with */auth/* restricted to users that are logged in with role *USER* or role *ADMIN.* Moreover, to access links starting with */auth/admin/* we need to have *ADMIN* role in the system.

5- What does it mean by session management in Spring Security?

Spring security use the following options to control the HTTP session functionalities SessionManagementFilter, SessionAuthenticationStrategy. These 2 helps spring security to manage the following options in the security session: Session Timeout detection and handling, Concurrent sessions (how many sessions an authenticated user may have open concurrently), Session-fixation – handle the session.

6 – Why we need Exception Handling?

Exception Handling is a mechanism to handle runtime errors such as ClassNotFoundException, IOException, SQLException, RemoteException. advantage of exception handling is to maintain the normal flow of the application**.** An exception normally disrupts the normal flow of the application; that is why we need to handle exceptions.

7 - Explain what is AuthenticationManager in Spring security?

AuthenticationManager is the main strategy interface for authentication.

If the principal of the input authentication is valid and verified, AuthenticationManager#authenticate returns an Authentication instance with the authenticated flag set to true.

8 - What is Spring Security Filter Chain?

Spring Security maintains a filter chain internally where each of the filters has a particular responsibility and filters are added or removed from the configuration depending on which services are required. The ordering of the filters is important as there are dependencies between them.

9 – What are the differences between OAuth2 and JWT?

OAuth as it name suggests is simply a standard for Authorization. JWT is a JSON based format of a security token which is basically a base64 url-encoded string which is used as a means of transferring secure content between two applications. The real difference is that JWT is just a token format, OAuth 2.0 is a protocol (that may use a JWT as a token format or access token which is a bearer token.).

10 - What is method security and why do we need it?

Method Security is the method level Spring security allows us to add security to individual methods within our service layer. Spring method security allows us to support / add authorization supports at the method level. On a high level, we can configure which roles are allowed to access what method within the same service class.

11 – What Proxy means and how and where can be used?

A proxy server is a system or router that provides a gateway between users and the internet. Therefore, it helps prevent cyber attackers from entering a private network. Proxies come with several benefits that can give your business an advantage:

1. Enhanced security
2. Private browsing, watching, listening, and shopping
3. Access to location-specific
4. Prevent employees from browsing inappropriate or distracting sites

12 – What is Wrapper Class and where can be used?

Wrapper classes are objects encapsulating primitive Java types. Generic classes only work with objects and don't support primitives. As a result, if we want to work with them, we have to convert primitive values into wrapper objects.

13 – What is SSL? What is TLS? What is the difference? How can we use them?

SSL refers to Secure Sockets Layer whereas TLS refers to Transport Layer Security. Basically, they are one and the same, but, entirely different. SSL and TLS are cryptographic protocols that authenticate data transfer between servers, systems, applications and users. For example, a cryptographic protocol encrypts the data that is exchanged between a web server and a user.

There is a need for secure system that encrypt data flow from either side. An SSL/TLS certificate helps with that. It acts as an endpoint encryption system that encrypt data preventing unauthorized access by hackers.