HW#5

1) What are Authentication and Authorization?
Authentication is a process of verifying. It is used when a user wants to access any resource. It determines whether users are true. It usually is provided by entering username and password. Authorization defines authorities on resource which authenticated users want to access.

2) What is Hashing in Spring Security?
When we want to store users password in database, we shouldn’t use plain text format to hide. Because this method make it easy to capture passwords when the database be in dangerous. Using hashing method is safer than plain text format. Hash function converts to hash value from plain text. When user entered password, password comparete with hash value in database. If hash value and password matches, it means user enter true password.

3) What is Salting and why do we use the process of Salting?
Salting is usually about password hashing. Before hashing password, we can add unique value to beginning of the password or end of password. This unique value is called salt. Unsalted password and salted password have different hash values. By adding salt, we hide real hash value of password. This provides an extra security for brute force attacks. (Brute force attack means a computer try all character combination until password is found.) Also salting provide that if some of users choose the same password, their passwords hash values take different value by adding salt.

4) What is “intercept-url” pattern?
“intercept-url” pattern defines the Url path. It is used to define the set of URL patterns that the application is interested in and to configure how they should be handled. For example: The configuration belows show that is required authentication for the /nexthome/logout url but not /nexthome/login and /nexthome urls.

```
<security:http auto-config="true">
   <intercept-url pattern="/nexthome" access="IS_AUTHENTICATED_ANONYMOUSLY"/>
   <intercept-url pattern="/nexthome/login"
access="IS_AUTHENTICATED_ANONYMOUSLY"/>
   <intercept-url pattern="/nexthome/logout" access="ROLE_USER,ROLE_ADMIN" />
   <security:form-login/>
</security:http>
```

5) What do you mean by session management in Spring Security?
It is about how many sessions a user opened at the same time and how we manage it. For session management, we should control http sessions. We have two options. First of them: When logging in from a different location with the same user, if the number of allowed sessions is exceeded, giving an error at the last login location. Other is that the last opened session is to terminate.

6) Why we need Exception Handling?
It provides secure code development. Exception handling help us to detect runtime errors and in this way we can control errors.

7) Explain what is AuthenticationManager in Spring security?
AuthenticationManager is an interface and it has only one method: authentication(). This method can do one of three options:
- If user is authenticated, it returns Authentication instance.(authenticated=true)
- If user is invalid, it returns AuthenticationException.
- If it cannot decide, it returns null.

The most commonly used implementation of AuthenticationManager is ProviderManager, which delegates to a chain of AuthenticationProvider instances

8) What is Spring Security Filter Chain?
Spring Security in the web tier is based on Servlet Filters. The client sends a request to the application, and the container decides which filters and which servlet apply to it based on the path of the request URI. At most, one servlet can handle a single request, but filters form a chain, so they are ordered. In fact, a filter can veto the rest of the chain if it wants to handle the request itself. A filter can also modify the request or the response used in the downstream filters and servlet.

9) What are the differences between OAuth2 and JWT ?
Basically, JWT is a token format. OAuth is an authorization protocol that can use JWT as a token. OAuth uses server-side and client-side storage. If you want to do real logout you must go with OAuth2. Authentication with JWT token can not logout actually. Because you don't have an Authentication Server that keeps track of tokens. If you want to provide an API to 3rd party clients, you must use OAuth2 also. OAuth2 is very flexible. JWT implementation is very easy and does not take long to implement

10) What is method security and why do we need it?
Spring method security allows us to add security to individual methods within our service layer. We need to add the spring-security-config dependency in maven for enabling method security.

11) What Proxy means and how and where can be used ?
Proxy is a tool that allows you to access the site you want to connect to using another channel.

12) What is Wrapper Class and where can be used ?
A Wrapper class is a class whose object wraps or contains primitive data types. When we create an object to a wrapper class, it contains a field and in this field, we can store primitive data types. In other words, we can wrap a primitive value into a wrapper class object.

13) What is SSL ? What is TLS ? What is the difference ? How can we use them ?
SSL(Secure Sockets Layer) is a certificate which provide to protect information users enter on your website.
TLS(Transport Layer Security) provide that It encrypts data between two communication applications and provides to transmite securely.
SSL and TSL are both essentially encryption and authentication protocols. But Ssl is more primitive than TLS. TLS emerged as a newer version of SSL.

14) Why do you need the intercept-url?
It help us to specify the urls which have to be secured.