HM#5 **Doğukan Bayrak**

1 – What are Authentication and Authorization ?

Authentication is the process to verify who a person is. Authorization is the process of verifying which applications, files, and data specific users have access to. For example, showing the ID card while entering the match in Turkey is an authentication process. It is used to confirm who we are. Afterwards, the tribune authorization process I will go to is.

2 - What is Hashing in Spring Security ?

Hashing is the process of getting a fixed size output from inputs of different sizes. Regardless of how many letters the input has, the output always contains literal characters. In this way, it is not possible to find out how many characters the input has. The hashing process works one way. Even if the hash value is known, it cannot be restored to its original state. It does not work retroactively. For example, the output of "patikadev" and the word "petikadev" are very different. After the "tikadev" part is not the same.

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

Salting is adding a random word to the beginning or end of the password before the password is hashed. The reason we use this process is to ensure that the hash values of people using the same password are not the same. After salting, the hash values of the same password will give a different output. This increases the length and complexity of the password.

4 - What is “intercept-url” pattern ?

Most web applications using Spring Security only have a couple of intercept-urls because they only have very basic security requirements. You need to have unauthenticated access to the login and login-error screens and usually some aspect of the public site, so that can be a few URL patterns. Then there's often an admin section, and then everything else is ROLE_USER.

5 - What do you mean by session management in Spring Security ?

HTTP session related functonality is handled by a combination of the SessionManagementFilter and the SessionAuthenticationStrategy interface, which the filter delegates to. Typical usage includes session-fixation protection attack prevention, detection of session timeouts and restrictions on how many sessions an authenticated user may have open concurrently.

6 – Why we need Exception Handling ?

Java exception handling is important because it helps maintain the normal, desired flow of the program even when unexpected events occur. If Java exceptions are not handled, programs may crash or requests may fail. Since Java is an error-sensitive programming language, we can use **try-catch** blocks to understand and debug errors.

7 - Explain what is AuthenticationManager in Spring security ?

AuthenticationManager is the interface required for authentication. AuthenticationManager returns an Authentication instance with the authenticated flag set to true. Otherwise, if the principal is not valid, it will throw an AuthenticationException. For the last case, it returns null if it can't decide.

8 - What is Spring Security Filter Chain ?

The filter can enable us to check the request and response or make changes if necessary, before the http request made by the user comes to the application codes we have written. As a general usage, it can be used to direct the request to other pages or to print a log for each incoming request, whether it meets the conditions we have determined. Filter Chain contains the algorithm that allows us to group the filters and run them in order. The applied pattern name is called chain.

9 – What are the differences between OAuth2 and JWT ?

OAuth is a protocol but JWT is a token format. JSON is less verbose, which makes it compact in size. It becomes a better choice to be used in HTML and HTTP environments. The use of JWT at Internet scale increases the ease of client-side processing of tokens on various platforms simultaneously.

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

Spring Security supports method-level authorization semantics.

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

The user can switch to the site he wants to connect using another channel. A proxy server acts as a gateway between you and the internet. This server, which acts as an intermediary between the Internet and the user, tries to change the user's IP address on its own server. It then connects the user to the desired website. To summarize briefly, we are connecting to a server. That server opens the desired site. Our IP address is hidden. Or, if the IP address we want to go to is banned, we can access it through the server.

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

The class structure, called Wrapper Class, enables primitive types to be used in different ways. If we want to use primitive data types as objects or for data structures such as ArrayList, Vector, we can use wrapper class and primitive types.

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

SSL means Secure Sockets Layer. It is the security layer that provides encrypted communication between a website and an internet browser. It makes the data exchange between client-server encrypted. But nowadays it is outdated. TLS is used instead.

TLS means Transport Layer Security. It provides data privacy just like SSL. We can think of TLS as a continuation of SSL. Although there are many bugs in SSL, most bugs have been fixed in the latest versions of TLS. It is more secure against attacks.

14 - Why do you need the intercept-url ?

We can use it to close security holes. Used to distribute access permissions to roles. Authorities can be distributed to roles such as admin, user, customer. Access to places that the role shouldn't have is restricted.