# Ödev - 5

**Q1 - What are Authentication and Authorization?**

**A:** Authentication is the process of validating the identity of a user. Authorization is permitting a user to perform an action.

**Q2 - What is Hashing in Spring Security?**

**A:** Hashing is one-way encryption that is, depending on the key, practically impossible to decrypt the hashed string to find original input. Hashing is used to store sensitive information, including user passwords. Later, the validity of an input can be verified with hashing with the same key as hashing is efficiently one to one function (Mathematically hashing can map multiple strings to a single one but that is statistically very unlikely to occur.)

**Q3 - What is Salting and why do we use the process of Salting?**

**A:** Salting is a method to increase the security of hashing. It is used to increase uniqueness among password hashes. Hashing is done via one-to-one and dedicated functions which means having different people use the same password will result in the same hash. This can cause security issues as repetitive hashes can be compared to common words used in passwords and then reverse engineered to expose the encryption key. To reduce the chance of this happening, salting is used. Salting is to modify the existing password in such a way that the noise in hashes is increased. Salting is done mostly by adding a random string at the end of the passwords. To make this useful, the string applied to the same passwords needs to be random and not repetitive otherwise the same string will produce the same hash.

**Q4 - What is the “intercept-URL” pattern?**

**A:** Intercept-URL pattern is used to limit users’ access to certain endpoints and methods. Accessibility can also be defined for roles as some roles can access a certain endpoint while others cannot.

**Q5 - What do you mean by session management in Spring Security?**

**A:** Spring security manages the creation and dropping of sessions. It can be configured to time out sessions in a way we want. Management of ongoing sessions also can be configured through spring security.

**Q6 - Why do we need Exception Handling?**

**A:** Exception handling is necessary to maintain the flow of the program. It is also handy to log errors or exceptional scenarios and debug.

**Q7 - Explain what is AuthenticationManager in Spring security?**

**A:** AuthenticationManager is an interface with only one method, authenticate. It takes an Authentication object. Depending on the input, the function can behave in one of the following ways; returning an Authentication object with authenticated=true, throwing an AuthenticationException, returning null.

**Q8 - What is Spring Security Filter Chain?**

**A:** Filter chain is a mechanism in spring security where different filters are applied to received requests during authentication and authorization. Custom filters can be added to the filter chain.

**Q9 - What are the differences between OAuth2 and JWT?**

**A:** OAuth2 is an authorization protocol that describes steps and logic to authorize a client and request. JWT is the process standard of creating a token using an encryption key. When a user logs in, JWT returns a token and the client needs to handle it themselves. On the other hand, OAuth2 handles them for clients.

**Q10 - What is method security and why do we need it?**

**A:** Method security is a way of authorizing users on a method level. This is done with @Secured annotation. If a user is not authorized, it throws an AccessDeniedException. This adds another chain to the filter chain.

**Q11 - What Proxy means and how and where can be used?**

**A:** Proxy pattern is using a surrogate object in place of another one. The proxy pattern should be used; when we need to reduce the complexity of a complicated object, when an object needs a local representation, or when we do not want to provide direct access to the object for security reasons and want to add another security layer.

**Q12 - What is Wrapper Class and where can it be used?**

**A:** A wrapper class is a class that encapsulates another class. This helps to hide the functionality of the wrapped class. Design patterns that use wrappers; Adapter, Proxy, Decorator.

**Q13 - What is SSL? What is TLS? What is the difference? How can we use them?**

**A:** SSL, Secure Socket Layer, is an Internet security protocol done by encrypting links between networked computers. It is deprecated and replaced by TLS in 1999. Like SSL, TLS, also known as Transport Layer Security, is an Internet security protocol. TLS is the industry standard at encryption protocol. TLS protocol process begins with a handshake where both sides message each other with a public asymmetric key. Then session keys are shared with asymmetric encryption. After that, the origin server gets authenticated.

**Q14 - Why do you need the intercept-URL?**

**A:** It is smarter to do distribute access permissions to do different roles to reduce the vulnerability of our API. It also helps with declining users to access methods they are supposed not to.

**Emin Yılmaz**