Umut Yıldız

1) Authentication is that verifying the user identity. Authorization is related to the resources that the user can access and the permissions given to user.

2) As a security requirement, we must hash user password when we save data to database. Because priority data such as user password cannot be accessible directly. So, Spring security provides some solution by default implementation. It encourages the developers to hash important data. In short, Hashing is a process that converting different size inputs to constant size output.

3) Before the password is hashed, a random word is added to the beginning or end of the password. This procedure is used to verify that the hash values of users who use the same password are not identical. The hash values of the same password will provide various results after salting. This raises the password's length and complexity. Salting values are stored in database with hashed password because Salting value is necessary when user password is validating.

4) The Intercept-URL pattern is used to restrict access to specific endpoints and methods for users. Accessibility may also be specified through roles, with some roles being able to access particular endpoints while others are unable to.

5) The establishment and deletion of sessions is handled by Spring security. It may be set up to time out sessions in the manner we like. Spring security may also be used to configure continuous session management. We can control sessions by SessionCreationPolicy.

6) Exception handling in Java is vital because it helps keep the program's usual, desired flow even when unexpected occurrences occur. Programs may crash or requests may fail if Java exceptions are not handled properly. Unhandled exceptions are Java exceptions that are difficult to foresee ahead of time.

7) Simply described, the AuthenticationManager is the primary authentication strategy interface. AuthenticationManager#authenticate returns an authentication instance with the authenticated flag set to true if the input authentication's principal is legitimate and confirmed. Otherwise, an AuthenticationException will be thrown if the principal is invalid. If it can't determine in the last instance, it returns null. The default implementation of AuthenticationManager is ProviderManager. The authentication procedure is delegated to a list of AuthenticationProvider objects. If we extend WebSecurityConfigurerAdapter, we may set either a global or local AuthenticationManager. We may override configure for a local AuthenticationManager (AuthenticationManagerBuilder).

8) During authentication and authorization, the filter chain is a method in spring security that applies different filters to accepted requests. The filter chain can be customized with custom filters.

9) OAuth2 is an authorization protocol that explains how to approve a client and a request. The method of producing a token using an encryption key is known as JWT. When a user logs in, JWT sends a token to the client, which the client must process. Clients, on the other hand, are handled through OAuth2.

10) Backend and frontend are separated in a well-designed application. Because the backend security system cannot trust that any particular frontend would handle security appropriately, it must manage it itself.

11) A proxy is a system or router that acts as a connection point between users and the internet. As a result, it aids in the prevention of cyber-attacks on a private network. It's a server that acts as a "intermediary" between end-users and the web pages they browse on the internet.

An IP address is used when a computer connects to the internet. This is comparable to your home's street address in that it directs incoming data where it should go and provides a return address for other devices to authenticate. A proxy server is a machine connected to the internet that has its own IP address.

12) Wrapper classes provides primitive data types as objects. When we use wrapper class, it provides to developers some extra functionality. For example, Wrapper classes are required collections.

13) SSL is a cryptographic protocol that uses explicit connections to establish secure communication between web server and client. TLS is also a cryptographic protocol that provides secure communication between web server and client via implicit connections. It’s the successor of SSL protocol. SSL stands for “Secure Socket Layer.” TLS stands for “Transport Layer Security.”

14) An application can have multiple roles. Therefore, the endpoints and data that these users can access may vary. We can easily manage them with intercept-url.