HW#5

1 – What are Authentication and Authorization ?

Authentication is the process of proving who a user or program is when accessing a system. Authentication technology provides access control for systems by checking that a user's credentials match those of authorized users in a database or a data validation server.
In today's systems, users generally use the passwords they set while registering to the system for authentication. Many companies use authentication to authenticate users logging into their websites.
Authorization is when an entity proves its access right, its identity. In other words, Authorization proves that you have the right to make requests.

2 - What is Hashing in Spring Security ?

Hashing is the name given to the process of taking an input of any length and converting it into an encrypted output with a set of mathematical algorithms. Hashing solves the problem of immediate access to the system with exposed passwords.

Spring recommends to use ***BCrypt BCryptPasswordEncoder***, a stronger hashing algorithm with randomly generated salt. The passwordEncoder method is the method that hashes the password entered by the user according to the given hash algorithm in order to compare with the password kept in the database in a hash.

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

In this method, before hashing the passwords, a random text called salt (salt) is added to the beginning or the end of the password to ensure that this value is hashed. Below you can see the result of hashing the same text with plain and two different salt values.

hashing("hello") = C39436EE452E641CDE2EB992AB397911

hashing("hello" + "e$7H3$YVYJpeyjAO") = A89A880CF2CB460B689DDF6F2F09EF5C

hashing("hello" + "2!yt*hrBwoK4Avvh") = 82A2A1BA55B1538C22E3D133D4DFB5FC

In this way, the hashes of the passwords of users who have chosen the same password are converted to a completely different text each time.

Since plain text and hash-based encryption can be captured by various methods, encryption methods used by adding prefixes and suffixes to hash passwords called salt together with hash encryption are recommended.

Aleyna ZENGİN

4 - What is “intercept-url” pattern ?

The <intercept-url> element defines a pattern which is matched against the URLs of incoming requests using an ant path style syntax. The access attribute defines the access requirements for requests matching the given pattern. We define the pages we want to manage, restrict and authorize access to.

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

In HTTP Protocol all requests and responses are independent. The server cannot distinguish between new visitors and returning visitors. But sometimes we may need to keep track of client's activity across multiple requests. This can be achieved using Session Management. It is a mechanism used by the Web container to store session information for a particular user. Session management can be achieved in one of the following ways;

- Cookies
- Hidden form field
- URL Rewriting
- HttpSession

6 – Why we need Exception Handling ?

Exceptions are the errors that occur in runtime while the application is running. Some of these errors can be tolerated, while others cause the application to stop completely. As a developer, our aim is to catch these errors and to tolerate them if possible and to ensure that the application continues to work.

Exception Throwing is a feature that facilitates the work of the programmer and also allows us to customize the errors according to our own code. When an error is received in this way, the error logs will become more readable for the software developer.

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. Otherwise, if the principal is not valid, it will throw an AuthenticationException. For the last case, it returns null if it can't decide.

ProviderManager is the default implementation of AuthenticationManager. It delegates the authentication process to a list of AuthenticationProvider instances.

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. FilterChain 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 ?

OAuth2 vs JWT, Both systems have their particular use cases and advantages. While JWT is excellent for API authentication and server-to-server authorization, OAuth 2.0 takes the lead in session management. JWT tokens are stateless; hence the information is not stored on the server site, but a major drawback is that the token expires after a pre-defined duration; hence it is not suitable for applications in which the session should persist.

On the other hand, JWT is not as secure from a security standpoint because changing the password would not expire the previously generated tokens. Hence to figure out which must be better, we must select the one that will benefit our particular use case rather than just looking at the general features of the system.

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

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.

To enable annotation based security, we need to add the @EnableGlobalMethodSecurity annotation on any @Configuration class.

The @Secured annotation is used to specify the list of roles on a method. This allows us to provide access to a specific method in case the user has a role.

```
@Secured("ROLE_CUSTOMER")
  @GetMapping("/user/{id}")
  public String getUserById(@PathVariable String id){
     return "id";
  }
```

Here, the first method is accessible to all users, but the second method is only accessible in case the customer have “ROLE_CUSTOMER” role.

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

Proxy allows you to access the site you want to connect to using another channel. When you are online, your website history is tracked by the website you visit or by your ISP. So it helps to detect your behavior online IP addresses. The IP address can enable your home address to be determined from the location of the website you entered.

You can also use proxy to connect to the Internet from a more free and secure platform. Although it is generally used to access blocked sites, in fact, this application can also be used for fast Internet connection and security by companies with insufficient main Internet servers. It can also be used to protect from advertising fraud, identity fraud, data leaks and similar factors.

If you are on a network with a proxy, such as at work, you can easily find the proxy server's address in your computer's settings. You may need to do this when configuring some programs or applications so that these programs use the proxy's IP address.

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

The Wrapper Class basically gives us different use of primitive types.

Primitive Data Type	Wrapper Class
byte	Byte
short	Short
int	Integer
long	Long
float	Float
double	Double
boolean	Boolean
char	Character

We may need a Wrapper Class for the following reasons:

1. If we want to use Primitive data types as an object
2. In java.util package we can only implement with classes and we can use wrapper classes like this
3. For data structures such as ArrayList and Vector, we can use primitive types through wrapper classes.
4. We can use it to create a necessary object for multithreading synchronization.

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

SSL is a type of digital security technology that allows encrypted communication between a website and a web browser. This technology is now outdated and has been completely replaced by TLS.

TLS (Transport Layer, Security) or Transport Layer Security is the security layer that encrypts data between two communication applications and ensures that it is transmitted securely. TLS is considered a more advanced and secure version of the SSL (Secure Sockets Layer) protocol. **TLS** is used to securely transfer data between applications that communicate with each other. Even if you are not aware of it, you may be using TLS in different ways every day on the internet. TLS is widely used in secure internet site connections, instant messaging software, file transfers, various software, internet applications, VPN connections.

Differences;

Cipher suites
SSL protocol offers support for Fortezza cipher suite. TLS does not offer support. TLS follows a better standardization process that makes defining of new cipher suites easier like RC4, Triple DES, AES, IDEA, etc.
Alert messages
SSL has the “No certificate” alert message. TLS protocol removes the alert message and replaces it with several other alert messages.
Record Protocol
SSL uses Message Authentication Code (MAC) after encrypting each message while TLS on the other hand uses HMAC — a hash-based message authentication code after each message encryption.
Handshake process
In SSL, the hash calculation also comprises the master secret and pad while in TLS, the hashes are calculated over handshake message.
Message Authentication
SSL message authentication adjoins the key details and application data in ad-hoc way while TLS version relies on HMAC Hash-based Message Authentication Code.

In nutshell, SSL is obsolete and TLS is new name of older SSL protocol as modern encryption standard using by everybody. Technically, TLS is more accurate, but everyone knows SSL.

14 - Why do you need the intercept-url ?

With intercept-url we can specify the urls which have to be secured, and also the type of the access (like the role which is necessary).