HW#5 – Baran AYDIN

1 – What are Authentication and Authorization ?

Authentication is the process of verifying who someone is, whereas authorization is the process of verifying what specific applications, files, and data a user has access to.

---

2 - What is Hashing in Spring Security ?

Hashing in Spring Security is Password Encoding and it is recommended to use for following cases;
- When the user registers in the application we hash the password and save it to the database.

- When the user wants to authenticate, we hash the provided password and compare it with the password hash from the database.

One of the most used password encoder in Spring Boot is BCryptPasswordEncoder.

---

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

To prevent an attack with rainbow tables we can use salted passwords. A salt is a sequence of randomly generated bytes that is hashed along with the password. The salt is stored in the storage and doesn't need to be protected.

---

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.

---

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 ?

Exception handling is important because it helps maintain the normal, desired flow of the program even when unexpected events occur. If exceptions are not handled, programs may crash or requests may fail

---

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 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 ?

Spring Security's web infrastructure is based entirely on standard servlet filters. It doesn't use servlets or any other servlet-based frameworks (such as Spring MVC) internally, so it has no strong links to any particular web technology. It deals in HttpServletRequests and HttpServletResponses and doesn't care whether the requests come from a browser, a web service client, an HttpInvoker or an AJAX application.

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.

---

9 – What are the differences between OAuth2 and JWT ?

JWT tokens are JSON encoded data structures contains information about issuer, subject (claims), expiration time etc. It is signed for tamper proof and authenticity and it can be encrypted to protect the token information using symmetric or asymmetric approach. JWT is simpler than SAML 1.1/2.0 and supported by all devices and it is more powerful than SWT(Simple Web Token).

OAuth2 — OAuth2 solve a problem that user wants to access the data using client software like browse based web apps, native mobile apps or desktop apps. OAuth2 is just for authorization, client software can be authorized to access the resources on-behalf of end user using access token.

---

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

Method-level security is implemented by placing the @PreAuthorize annotation on controller methods (actually one of a set of annotations available, but the most commonly used). This annotation contains a Spring Expression Language (SpEL) snippet that is assessed to determine if the request should be authenticated.

---

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

A proxy server acts as a gateway between you and the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests

---

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.

They convert primitive data types into objects. Objects are needed if we wish to modify the arguments passed into a method (because primitive types are passed by value).

Data structures in the Collection framework, such as ArrayList and Vector, store only objects (reference types) and not primitive types.

An object is needed to support synchronization in multithreading.

---

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

TLS, short for Transport Layer Security, and SSL, short for Secure Socket Layers, are both cryptographic protocols that encrypt data and authenticate a connection when moving data on the Internet.
TLS is actually just a more recent version of SSL. It fixes some security vulnerabilities in the earlier SSL protocols.
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.
SSL has the “No certificate” alert message. TLS protocol removes the alert message and replaces it with several other alert messages.
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.
In SSL, the hash calculation also comprises the master secret and pad while in TLS, the hashes are calculated over handshake message.
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.

---

14 - Why do you need the intercept-url ?

Spring Security is generally good for Role based access. and that's about it. You could create your own ProcessingFilter to do some additional things. However, i find that this is a lot of work for little benifit.
The alternative, is to use Request Interceptors. On several projects for RESTful services using Spring MVC, I utilize Request Interceptors to finalize some authentication beyond the basic Role access. This works, and in my opinion makes the chain of events much easier to follow, but if you're dealing with thousands of transactions per minute, it could bog down the requests.