HW Week 5

1 – What are Authentication and Authorization ?

In simple words, authentication is the process of user verification - Checking the information of the users (email, user name, nickname, phone etc) whether they match the password. Authorization is verifying what they have access to. For example a user can only post and get limited functions, while a moderator can additionally delete user posts or prevent users from accessing the content. And admin often has access to every possible function.

2 - What is Hashing in Spring Security ?

Hashing is encoding an input into some form that only authorized parties can read it. It contains no keys, the hashcode can be used directly. It's widely used in security authentication to prevent unauthorized user's access.

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

Password authentication process requires hash code but hash can be generated by an attacker as well. In order to make the hashcode more secure, we can use salting, adding a sequence of randomly generated bytes that gets added into the password. If the salt is long and random enough it helps to secure the password.

4 - What is “intercept-url” pattern ?

It's a concept of authority. There are at least 2 roles of users in any app, in order to limit their access to certain parts of the application, we define path (pattern) and role of the user. For example <intercept-url pattern="/index/*" access="ROLE_USER"> means you need to have privilges of user to access /index/ path. In this example, if we change role to ROLE_ADMIN, then you have to be admin to access the pattern.

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

Session managment is a concept to create secure interactions between a service/app and a user. These interactions include series of requests of user and responses from service which carry valuable information. In order to ease the process, the application needs to keep the connection with user instead of verfying his credentials at every request. And it required an authentication process.

6 – Why we need Exception Handling ?

Exception is basically an error that can occur when defined form of usage is crossed. For example, you can expect an user to give you a numerical value when you ask his age - but the user gives answer in unsupported format, the app cannot use the information and crashes. In order to avoid crashing the app, the developer predicts possible misusage and prohibit the user from this kind of behaviour, lead him to predefined error pages or give him error messages explaining how to use the app.

7 - Explain what is AuthenticationManager in Spring security ?

Authentication manager checks the credentials of the user whether they are valid and verified. If the information is correct, authenticates the session - otherwise throws authentication exception.

8 - What is Spring Security Filter Chain ?

Spring Security works based on servlet filters. This is required for safe authentication. It works as the filters question the authentication process by the order you code them. In short - the information the user entered, faces these filters and must pass all to authenticate the user. Here is detailed information about the filter order:

ChannelProcessingFilter, because it might need to redirect to a different protocol

SecurityContextPersistenceFilter, so a SecurityContext can be set up in the SecurityContextHolder at the beginning of a web request, and any changes to the SecurityContext can be copied to the HttpSession when the web request ends (ready for use with the next web request)

ConcurrentSessionFilter, because it uses the SecurityContextHolder functionality but needs to update the SessionRegistry to reflect ongoing requests from the principal

Authentication processing mechanisms - UsernamePasswordAuthenticationFilter, CasAuthenticationFilter, BasicAuthenticationFilter etc - so that the SecurityContextHolder can be modified to contain a valid Authentication request token

The SecurityContextHolderAwareRequestFilter, if you are using it to install a Spring Security aware HttpServletRequestWrapper into your servlet container

RememberMeAuthenticationFilter, so that if no earlier authentication processing mechanism updated the SecurityContextHolder, and the request presents a cookie that enables remember-me services to take place, a suitable remembered Authentication object will be put there

AnonymousAuthenticationFilter, so that if no earlier authentication processing mechanism updated the SecurityContextHolder, an anonymous Authentication object will be put there

ExceptionTranslationFilter, to catch any Spring Security exceptions so that either an HTTP error response can be returned or an appropriate AuthenticationEntryPoint can be launched

FilterSecurityInterceptor, to protect web URIs and raise exceptions when access is denied

9 – What are the differences between OAuth2 and JWT ?

JWT is just a token format. JWT tokens are JSON encoded data structures contains information about issuer, subject, 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 --- Meanwhile OAuth2 is just for authorization, client software can be authorized to access the resources on behalf of end user using access token. OAuth2 solve a problem that user want to access the data using client software like browse based web apps, native mobile apps or desktop apps.

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

Simply put, Spring Security supports authorization semantics at the method level. Typically, we could secure our service layer by, for example, restricting which roles are able to execute a particular method — and test it using dedicated method-level security test support.

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

Proxy means having authority to act on behalf of another identity. It can be used in many fields - like proxy war is when a country secretly supports a group who is actively fighting on the field against another county - for example in Russia-Ukraine conflict, Russia supports local rebels against Ukraine - but Ukraine and Russia are at peace and not fighting directly.

I guess you wouldn't ask me about world politics so I guess the question is about networks :D 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 provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.

If you’re using a proxy server, internet traffic flows through the proxy server on its way to the address you requested. The request then comes back through that same proxy server, and then the proxy server forwards the data received from the website to you.

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.

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

SSL is "Secure Socket Layer" - TLS is "Transport Layer Security" - These are popular cryptographic protocols that are used to imbue web communications with integrity, security, and resilience against unauthorized tampering. PKI uses the TLS protocol to establish secure connections between clients and servers over the internet, ensuring that the information relayed is encrypted and unable to be read by an external third party.

SSL is the predecessor of TLS but it's name remains in "SSL certificate" although we don't use SSL anymore. We need TLS because without a security protocol, the communication would be open to external access. Nobody would like to share their credentials on a page that doesnt have HTTPS security status. As I said before TLS makes sure your information is encrypted and safe.

We use them by adding the jdk.tls.client.protocols property as a java command-line argument to support TLSv1.2:

java -Djdk.tls.client.protocols=TLSv1.2 <Main class or the Jar file to run>

14 - Why do you need the intercept-url ?

Just as I answered in Question-4, intercept-url checks whether you have the defined role to access the pattern. By limiting access of unwanted requests, you can keep the application secure. As far as I know, you can make this configuration by @RequestMapping.