

## HW#5

### 1 – What are Authentication and Authorization ?

Authentication is proof that the person is who it say it is. With password and username, Authentication is provided.

Authorization defines authority of authenticated person that want to access source.

Authorization has 2 steps :

- 1) System administrator defines authorities on resource to be accessed.
- 2) Verifies authorizations when Access to resource.

### 2 - What is Hashing in Spring Security ?

Hashing is a process which with hashing method take inputs and give outputs that same size but unique. But if you give same input, output will be always same. However if you change a letter in input, output changes.

Hash algorithm is unidirectional, so with using output we can not find input.

Hashing has 2 most using algorithms : SHA-256 and MD5.

MD5 produces 128-bit outputs and SHA-256 produces 256-bit outputs.

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

Salting is random text addition to beginning or ending input string before hashing.

We use Salting because if two users create same password, output of passwords will be same with Hashing and in Authentication this causes problem. When we use Salting, even if password strings are same, hash output will be different.

### 4 - What is "intercept-url" pattern ?

With intercept-url tag we define pages which we want manage and restrict access.

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

Session management is used to detect session timeouts, to prevent session attacks, to restrict number of session which one user open concurrent.

### 6 – Why we need Exception Handling ?

When application has errors, we have to fix them for the application to work. At this point exception handling helps us.

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

AuthenticationManager is an interface and has authentication methods. AuthenticationManager directs to Authentication Provider.

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

Filter provides controlling or if it's necessary changing on requests and responses.

FilterChain provides grouping filters and running filters in order.

**9 – What are the differences between OAuth2 and JWT ?**

JWT is web token. OAuth2 is an open standard for authorization. OAuth2 can use JWT for token transfer. For example if you want a mechanism like login with Facebook, you can use OAuth2. But if users work on same server only we can use JWT.

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

Method security provides method-level security, method-level security is provided by @PreAuthorize annotation. If access is not granted for method, method doesn't work and HTTP method returns Unauthorized.

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

Proxy is a tool which using pass through the another channel when try to access a site.

Proxy is used to protect data leak, identity fraud and ad fraud etc. Recently in our country, Proxy is used to access inhibit websites.

Proxy also is used to provide secure and fast connection.

When we use Proxy and send request a site, first Proxy take request and change our IP then send request to site with changed IP.

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

When we work with primitive types we may need objects, at this point Wrapper classes take this primitive types and make them object.

For example, we can use primitive types through Wrapper class for like ArrayList and Vector data structures.

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

SSL (Secure Sockets Layer) is a digital security technology which provides encrypted communication between website and internet browser.

TLS (Transport Layer Security) provides data security like SSL.

Since 2014, SSL has been accepted unsecured for block cipher algorithm because of POODLE Attack.

Only RC4 algorithm are supported but it is not enough. For all these reasons, TLS took place of SSL.

TLS are updated version of SSL.

SSL/TLS are supported by IP Protocols like HTTPS, SMTP, POP3, FTP.

Websites which has uploaded SSL/TLS certification can use HTTPS protocols for provide secure connection.

#### **14 - Why do you need the intercept-url ?**

Intercept-url is used to secure individual URLs. With intercept-url tag we manage given URL authorization.