HW#3

1 – SOAP vs Restful ?

SOAP is a protocol, REST is an architectural style.

SOAP only permits XML data format, REST permits text,HTML,XML,JSON etc.

SOAP has bigger bandwidth because XML format datas take more memory and need bigger bandwidth.

In SOAP need to generate interface but in REST communication is provided with endpoints directly so we think like that : API is interface.

In SOAP JAX-WS is the Java API, in REST JAX-RS is.

REST is more preferred.

2 - Difference between acceptance test and functional test ?

If we want to check does the program fulfill requests , then we use acceptance test.

If we want to check only one function regardless of environment and side effects, we use functional test.

3 - What is Mocking ?

Mocking is a method that using in unit tests. For example we test a method(add) which takes a class parameter(User user) like below, for this class parameter we use mock object. So this method depend on the class of parameter but in unit test we ignore dependencies and create a fake parameter object this fake object is mock object.

public void add(User user, string name, string surname){}

4 - What is a reasonable code coverage % for unit tests (and why) ?

Code coverage is ratio of checked codes of written tests to written codes. If this percent decrease, this means checked codes also decrease and failure percent increase. But in my research I didn't find a certain percent.

5 – HTTP/POST vs HTTP/PUT ?

POST is used to send data to server, with POST method data is created or updated, if data doesn't exist, will be created, if data exists, will be updated.

PUT is spesific version of POST method. It is used to update data and data doesn't exist, system gives an error. But PUT method has also save or update option, with this option can create data which doesn't exist.

6 - What are the Safe and Unsafe methods of HTTP ?

GET,HEAD,OPTIONS,TRACE methods are safe. PUT,DELETE,POST,PATCH are unsafe.

Unsafe methods are read-only methods so they can't alter server state.

7 - How does HTTP Basic Authentication work ?

1)A client makes a request to a page which use Basic Authentication.

2)The server sends HTTP status code 401, Basic value WWW-Authenticate parameter which tells Basic Authentication should start with HTTP header.

3)A window occurs which takes user id and password from user.

4)The server compare this userid and password with registered userid and password.

5)If they match, the server sends HTTP status code 200 and requested informations.

6)If they don't match , sends HTTP status code 401 and return the step 2.

8 - Define RestTemplate in Spring ?

In Spring, RestTemplate is default class for managing synchronized HTTP requests by client.

9 – What is idempotant and which HTTP methods are idempotant ?

Let's explain this with an example. For example there is a button on web page and we press this button 5 times successively, if method is idempotant, doesn't take 5 times request, checks requests and if requests equal, wait for the response.

GET,HEAD,OPTIONS, PUT,DELETE methods are idempotant.

10 – What is DNS Spoofing ? How to prevent ?

Dns is used to convert a domain name to an IP. DNS Spoofing is a cyber attack and use weaknesses of DNS server. With DNS Spoofing a domain name directs another IP adress that different from the original.

There are many methods and protocols for prevent from DNS Spoofing.

a)DNSSEC protocol has additionals method of verification for security.

b) Encrypting datas of DNS requests and responses.

c)It is also important to use last version of DNS.

d)Adding a security layer on DNS.

e)Using strong perception protocols.

f)Taking cyber security courses.

11 – What is content negotiation ?

Purpose of content negotiation is to present different document types with same URI and in this way users determine the source document type.

12 – What is statelessness in RESTful Web Services ?

Server doesn't keep client informations like session, Client does. Server doesn't know client informations like how many requests or which requests made. When client make a request, gives all informations Server needed.

13 - What is CSRF attack? How to prevent ?

CSRF attack is making requests that using user session without the user's knowledge in web application. CSRF occurs if systems does not checking which sources using and how does send requests.

a)POST method are used for important requests.

b)Giving user a unique randomly generated token.

c)Cookies and websites datas should clean often.

d)Do not open unknown links or mails.

14 - What are the core components of the HTTP request and HTTP response ?

HTTP request has 5 major parts.

1)VERB : shows HTTP methods (POST,GET,PUT etc.)

2)URI : shows the resource of server.

3) HTTP version : shows HTTP version, it is set usually default.

4) Request Header : contains high value datas like client type,format.

5)Request Body : contains request message.

HTTP response has 4 major parts.

1) Status/Response Code : Shows server status for requested resource.

2) HTTP version : shows HTTP version, it is set usually default.

3) Response Header : contains high value datas like content length,type.

4) Response Body : contains response message.