HW#3 – Baran AYDIN

1 – SOAP vs Restful ?

- SOAP is a protocol whereas REST is an architectural pattern.
- SOAP uses service interfaces to expose its functionality to client applications while REST uses Uniform Service locators to access to the components on the hardware device.
- SOAP needs more bandwidth for its usage whereas REST doesn't need much bandwidth.
- Comparing SOAP vs REST API, SOAP only works with XML formats whereas REST work with plain text, XML, HTML and JSON.
- SOAP cannot make use of REST whereas REST can make use of SOAP.

---

2 - Difference between acceptance test and functional test ?

Functional Testing: Application of test data derived from the specified functional requirements without regard to the final program structure. Also known as black-box testing.

Acceptance Testing: Formal testing conducted to determine whether or not a system satisfies its acceptance criteria enables an end user to determine whether or not to accept the system.

---

3 - What is Mocking ?

Mocking is a method/object that simulates the behavior of a real method/object in controlled ways. Mock objects are used in unit testing.

Often a method under a test calls other external services or methods within it. These are called dependencies. Once mocked, the dependencies behave the way we defined them.

---

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

100% : Appropriate if you would like to make sure everything is tested.
90% to 99% : Appropriate in cases where you want to convey a level of confidence similar to 100%, but leave yourself some margin to not worry about the occasional hard to test corner of code.
80% : Appropriate is testing is not one of your highest priority.

---

5 – HTTP/POST vs HTTP/PUT ?

POST method is used for creating resource where PUT method is for updating the resource or create resource if it does not exist.

---

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

An HTTP method is safe if it doesn't alter the state of the server. In other words, a method is safe if it leads to a read-only operation. Several common HTTP methods are safe: GET, HEAD, or OPTIONS. All safe methods are also idempotent, but not all idempotent methods are safe. For example, PUT and DELETE are both idempotent but unsafe.

---

7 - How does HTTP Basic Authentication work ?

HTTP basic authentication is a simple challenge and response mechanism with which a server can request authentication information (a user ID and password) from a client. The client passes the authentication information to the server in an Authorization header. The authentication information is in base-64 encoding.

If a client makes a request for which the server expects authentication information, the server sends an HTTP response with a 401 status code, a reason phrase indicating an authentication error, and a WWW-Authenticate header. Most web clients handle this response by requesting a user ID and password from the end user.

---

8 - Define RestTemplate in Spring ?

Rest Template is used to create applications that consume RESTful Web Services. You can use the exchange() method to consume the web services for all HTTP methods.

---

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

An HTTP method is idempotent if an identical request can be made once or several times in a row with the same effect while leaving the server in the same state. In other words, an idempotent method should not have any side-effects. Implemented correctly, the GET, HEAD, PUT, and DELETE methods are idempotent, but not the POST method. All safe methods are also idempotent.

---

10 – What is DNS Spoofing ? How to prevent ?

Domain Name Server (DNS) spoofing (DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.

Prevention: Using transport encryption, Encrypting DNS traffic, Using a virtual private network

---

11 – What is content negotiation ?

In HTTP, content negotiation is the mechanism that is used for serving different representations of a resource to the same URI to help the user agent specify which representation is best suited for the user.

---

12 – What is statelessness in RESTful Web Services ?

RESTful Web Service should not keep a client state on the server. This restriction is called Statelessness. It is the responsibility of the client to pass its context to the server and then the server can store this context to process the client's further request.

---

13 - What is CSRF attack? How to prevent ?

Cross-site request forgery attacks (CSRF or XSRF) are used to send malicious requests from an authenticated user to a web application. The attacker can’t see the responses to the forged requests, so CSRF attacks focus on state changes, not theft of data. Successful CSRF attacks can have serious consequences

Prevention: An attacker can launch a CSRF attack when he knows which parameters and value combination are being used in a form. Therefore, by adding an additional parameter with a value that is unknown to the attacker and can be validated by the server, you can prevent CSRF attacks.

---

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

An HTTP request includes five key elements

HTTP methods : Set of request methods to perform desired action for a given resource (GET, PUT, POST)
Uniform Resource Identifier (URI) : Describes the resource
HTTP Version : describes HTTP version
Request Headers : Content-type : application/json, Content-Length : 511
Payload : It is basically a Request Body which includes message content.

Every HTTP response contains four key elements

Status/Response Code : These are response codes issued by a server to a client's request**.**
HTTP Version : describes HTTP version
Response Header : Includes information for the HTTP response message.
