HOMEWORK-3

Q1) SOAP vs Restful ?

SOAP	REST
SOAP stands for Simple Object Access Protocol	REST stands for Representational State Transfer
SOAP is a protocol .	REST it is just an architectural pattern.
SOAP can only work with XML format	REST permits different data format such as Plain text, HTML, XML, JSON, etc.

Q2) Difference between acceptance test and functional test ?

Functional testing - testing the product, verifying that it has the qualities you've designed or build (functions, speed, errors, consistency, etc.) The functional test confirms the software performs a function within the boundaries of how you've solved the problem.

Acceptance testing - testing the product in its context, this requires (simulation of) human interaction, testing it has the desired effect on the original problem(s). Acceptance tests verify the product actually solves the problem it was made to solve.

Q3) What is Mocking ?

Mock is a type of object. Mock objects is a unit testing technique in which a code chunk is replaced by dummy implementations that emulate real code. This helps one to write unit tests targeting the functionality provided by the class under test.

Q4) What is a reasonable code coverage % for unit tests (and why) ?

Test coverage is a useful tool for finding untested parts of a codebase. Test coverage is of little use as a numeric statement of how good your tests are. Code coverage of 70-80% is a reasonable goal for system test of most projects with most coverage metrics. Use a higher goal for projects specifically organized for high testability or that have high failure costs. Minimum code coverage for unit testing can be 10-20% higher than for system testing.

Q5) HTTP/POST vs HTTP/PUT ?

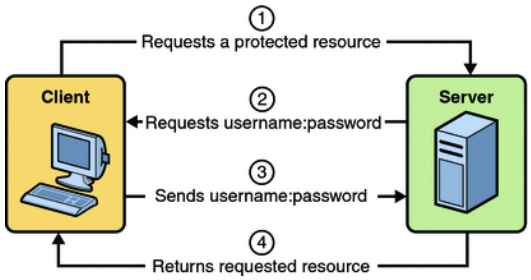
-> PUT method is called when you have to modify a single resource while POST method is called when you have to add a child resource.
-> PUT method response can be cached but you cannot cache POST method responses.
-> You can use UPDATE query in PUT whereas you can use create query in POST.

Q6) What are the Safe and Unsafe methods of HTTP ?

Safe methods are methods that can be cached, prefetched without any repercussions to the resource.

Q7) How does HTTP Basic Authentication work ?

HTTP Basic Authentication requires that the server request a user name and password from the web client and verify that the user name and password are valid by comparing them against a database of authorized users. When basic authentication is declared, the following actions occur:



A client requests access to a protected resource.

The web server returns a dialog box that requests the user name and password.

The client submits the user name and password to the server.

The server authenticates the user in the specified realm and, if successful, returns the requested resource.

Q8) Define RestTemplate in Spring ?

RestTemplate is a synchronous client to perform HTTP requests. It uses a simple, template method API over underlying HTTP client libraries such as the JDK HttpURLConnection, Apache HttpComponents, and others.

Since Spring 5.0, a new client WebClient is available that can be use do create both synchronous and asynchronous requests. In the future releases, RestTemplate will be deprecated in favour of WebClient.

Q9) What is idempotant and which HTTP methods are idempotant ?

Idempotent(unsafe) HTTP method is a HTTP method that can be called many times without different outcomes.

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.

The idempotence of a method is not guaranteed by the server and some applications may incorrectly break the idempotence constraint.

Q10) What is DNS Spoofing ? How to prevent ?

DNS spoofing is a cyber-attack in which fake data is introduced into the DNS resolver's cache, which causes the name server to return an incorrect IP address.

While DNS spoofing attacks are undeniably cunning, they can also be prevented with a few additional security measures, as well as advanced solutions:

-> Set up DNSSEC,

-> Look for the secure connection symbol

-> Regularly apply patches to DNS servers,

-> Perform thorough DNS traffic-filtering

Q11) What is content negotiation ?

Content negotiation allows a user to determine which media types they prefer to receive from the server. It's a mechanism defined in the HTTP protocol (RFC 7231), which is great, because REST APIs work alongside HTTP.

Q12) What is statelessness in RESTful Web Services ?

REST => (REpresentational **"State"** Transfer)

Statelessness : the server does not store any state about the client session on the server-side. This restriction is called Statelessness.

Statelessness means that every HTTP request happens in complete isolation. When the client makes an HTTP request, it includes all information necessary for the server to fulfill the request.

Q13) What is CSRF attack? How to prevent ?

Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform.

CSRF attacks can be prevented:

Being Restful: RESTful design will ensure that your code is clean and can scale. It also has the added benefit of reducing vulnerabilities.

Anti-forgery tokens: To safeguard these endpoints, you can introduce an anti-forgery token in every request that uniquely identifies safe origin sites.

Q14) What are the core components of the HTTP request and HTTP response ?

Verb : Indicate HTTP methods such as GET, POST, DELETE, PUT etc.

URI : Uniform Resource Identifier (URI) to identify the resource on server.

HTTP Version : Indicate HTTP version, for example HTTP v1.1 .

Request Header : Contains metadata for the HTTP Request message as key-value pairs. For example, client (or browser) type, format supported by client, format of message body, cache settings etc.

Request Body : Message content or Resource representation.