Week-3 Homework Questions

1 - SOAP vs Restful ?

Both SOAP and REST rely on well-established rules that everyone has agreed to abide by in the interest of exchanging information. But REST is easier and more flexible as REST uses simple URL instead of requiring XML for every step.

2 - Difference between acceptance test and functional test ?

Functional testing is basically the test of functions in the app. You would test functions, speed, errors, consistency etc.

Acceptance testing is a bit more about validation of the product. Like does the app help what the customer needs, does it suit the requirements of the project etc.

3 - What is Mocking ?

Mocking is a process used in unit testing when the unit being tested has external dependencies. It's done by creating a fake version of an external or internal service that can stand in for the real one, helping your tests run more quickly.

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

Code coverage for unit tests depend on your app, your needs and expectations. The point is testing the key points of the code, whether the functions give desired responses or handle occasional errors. But if you are asking a simple answer, reasonable code coverage should be over 70-80% and not lesser.

5 - HTTP/POST vs HTTP/PUT ?

HTTP POST is used to create or add resource to the server. And PUT changes values of already created resource.

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

Read-only methods like GET, OPTIONS are safe methods as they don't make changes in the server. On the other hand, PUT or DELETE are considered as unsafe methods because they make changes.

7 - How does HTTP Basic Authentication work ?

The web page asks for id and password from the client. Client passes the information and the information, in base-64 encoding form, gets checked at the server. If credentials are not correct, server gives response 401 authentication error.

8 - Define RestTemplate in Spring ?

RestTemplate is a widely used class in the Spring framework, and it's responsible for synchronized HTTP requests on the client side.

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

Idempotent is, in short, no matter how many times you do something, the action is done only once. Like adding 0 to 1 again and again, still equals to 0 + 1. In HTTP methods, when you send the same method multiple times, but it gets executed just once.

Idempotent methods are : DELETE, GET, HEAD, OPTIONS, PUT, TRACE

10 - What is DNS Spoofing ? How to prevent ?

DNS Spoofing is a malicious attack done by altering the DNS records and redirect the victim to a fake website.

How to prevent it :

Implement DNS spoofing detection software. (Such as XArp help product against ARP cache poisoning)

Use encrypted data transfer protocols - (Example: Using end-to-end encryption)

Use DNSSEC - DNSSEC, or Domain Name System Security Extensions

11 - What is content negotiation ?

Content negotiation may be defined as the process of inspecting the structure of an incoming HTTP request to determine the best representation of a resource from amongst multiple available representations of the same resource. In essence, content negotiation is a concept that allows the same Url to serve the same content in various formats. You can take advantage of content negotiation to select the preferred media type.

12 - What is statelessness in RESTful Web Services ?

The Web Service should not keep the client information. So, client can use his info to use the service, but it’s limited with the session. They shouldn’t be stored in the server without the clients will.

13 - What is CSRF attack? How to prevent ?

When a malicious web site, email, blog, instant message, or program causes a user's web browser to perform an unwanted action on a trusted site when the user is authenticated. A CSRF attack works because browser requests automatically include all cookies including session cookies. The site can’t know whether it’s the real client or a bot because the request comes from the same source. Such an attack can end up changing account credentials, make online purchases, sending emails to other contacts etc.

How to prevent it :

Use built in CSRF protection while coding.

Use synchronizer token pattern.

Use double submit cookies.

Don’t use GET requests for state changing operations.

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

Core components of the HTTP request :

Verb – GET, POST, DELETE etc.

URI - address

HTTP Version – version number

Request Header – metadata, like browser type, format etc.

Request Body – the content of the request

Core components of the HTTP response :

Status Response Code – 200 for ok, 40x for errors etc.

HTTP Version – version number

Response Header – content type, length etc.

Response Body – The actual message response from the server.