Third Homework – Mustafa Selim Gunaydin

1 - SOAP vs Restful ?

➤ SOAP is more secure but REST is faster.

➤ SOAP can only work with XML format, while REST can work with XML, text, JSON and HTML formats.

➤ REST uses cache better and doesn't need development tools.

➤ SOAP cannot make use of REST whereas REST can make use of SOAP.

2 - Difference between acceptance test and functional test ?

➤ Acceptance test is used to check whether the software meets the customer requirements or not. Includes only positive test cases and its located at the top of the test pyramid so done after all tests.

➤ Functional testing is testing the 'Functionality' of a software or an application under test. It exists on the smaller units. Includes positive and negative test cases.

3 - What is Mocking ?

➤ Mock functions allow you to test the links between code by erasing the actual implementation of a function, capturing calls to the function (and the parameters passed in those calls), capturing instances of constructor functions when instantiated with new, and allowing test-time configuration of return values. Mainly used in unit testing.

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

➤ Code coverage of 70-80% is a reasonable goal for system test of most projects with most coverage metrics.

➤ Although we can use a higher goal for projects specifically organized for high testability or that have high failure costs.

➤ %100 test coverage is generally impractical because some test cases are expensive to reproduce but are highly improbable. We need to consider cost to benefit ratio in these cases.

➤ There is no concrete way to measure such coverage, you can of course count features and then measure against number of tests, but that still leaves space for judgement errors.

5 – 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.

➤ Calling the same PUT request multiple times will always produce the same result. But calling a POST request repeatedly have side effects of creating the same resource multiple times.

➤ PUT method response can be cached but you cannot cache POST method responses.

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 short it is safe if it leads to a read-only operation.

➤ All safe methods are also idempotent, but not all idempotent methods are safe. For example, PUT and DELETE are both idempotent but unsafe.

➤ Safe methods doesn't change anything internally(resources).

➤ Idempotent method doesn't change anything externally (response).

HTTP Method	Safe	Idempotent
GET	Yes	Yes
HEAD	Yes	Yes
OPTIONS	Yes	Yes
TRACE	Yes	Yes
PUT	No	Yes
DELETE	No	Yes
POST	No	No
PATCH	No	No

7 - How does HTTP Basic Authentication work ?

➤ HTTP Basic Authentication requires that the server request a username and password from the web client and verify that the username and password are valid by comparing them against a database of authorized users.

➤ A client requests access to a protected resource.

➤ The web server returns a dialog box that requests the username and password.

➤ The client submits the username and password to the server.

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

➤ HTTP basic authentication is not a secure authentication mechanism. Basic authentication sends user names and passwords over the Internet as text that is Base64 encoded, and the target server is not authenticated. This form of authentication can expose user names and passwords. If someone can intercept the transmission, the username and password information can easily be decoded.

8 - Define RestTemplate in Spring ?

➤ Synchronous client to perform HTTP requests, exposing a simple, template method API over underlying HTTP client libraries such as the JDK HttpURLConnection, Apache HttpComponents, and others.

➤ The RestTemplate offers templates for common scenarios by HTTP method, in addition to the generalized exchange and execute methods that support of less frequent cases.

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

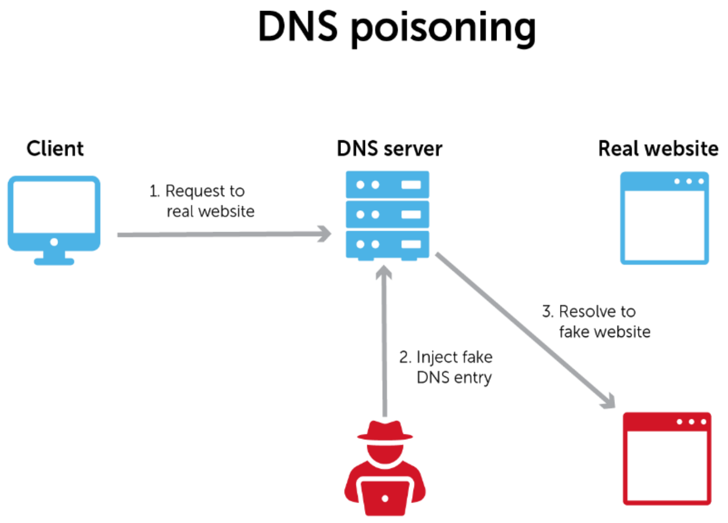
➤ Idempotency is a property of HTTP methods. Idempotent method should not have any side-effects (except for keeping statistics).

➤ As I shown in the previous page GET, HEAD, OPTIONS, TRACE, PUT and DELETE methods are idempotent.

➤ To be idempotent, only the actual back-end state of the server is considered, the status code returned by each request may differ.

10 – What is DNS Spoofing ? How to prevent ?

➤ DNS spoofing, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record.



➤ DNS Security Protocol (DNSSEC) protocol was developed specifically to counter DNS poisoning.

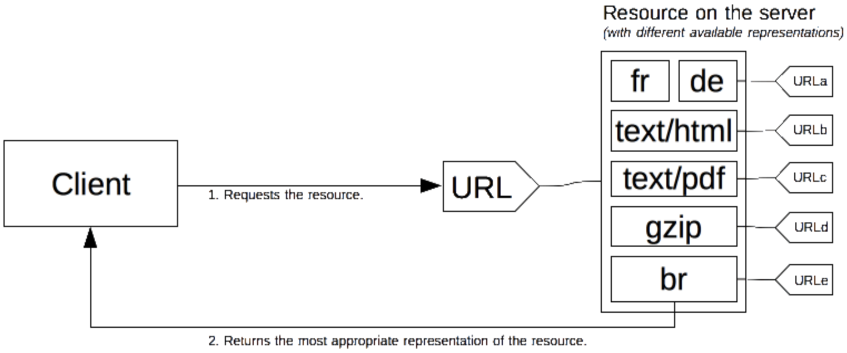
➤ DNSSEC uses public-key cryptography to verify that an authoritative nameserver is providing the correct information back to the requesting device.

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.

➤ A resource may be available in several different representations; for example, it might be available in different languages or different media types. One way of selecting the most appropriate choice is to give the user an index page and let them select the most appropriate choice; however it is often possible to automate the choice based on some selection criteria.

➤ HTTP provides for several different content negotiation mechanisms including: server-driven (or proactive), agent-driven (or reactive), transparent, and/or hybrid combinations thereof.


Resource on the server
(with different available representations)
fr
de
text/html
text/pdf
gzip
br
URLa
URLb
URLc
URLd
URLe
Client
1. Requests the resource.
URL
2. Returns the most appropriate representation of the resource.

12 – What is statelessness in RESTful Web Services ?

➤ 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.

➤ 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 (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.

➤ An attacker may trick the users of a web application into executing actions of the attacker's choosing (transferring funds, changing their email address, etc.).

➤ Synchronizer token pattern, Cookie-to-header token, Double Submit Cookie, SameSite cookie attribute, Client-side safeguards are widely used prevention techniques.

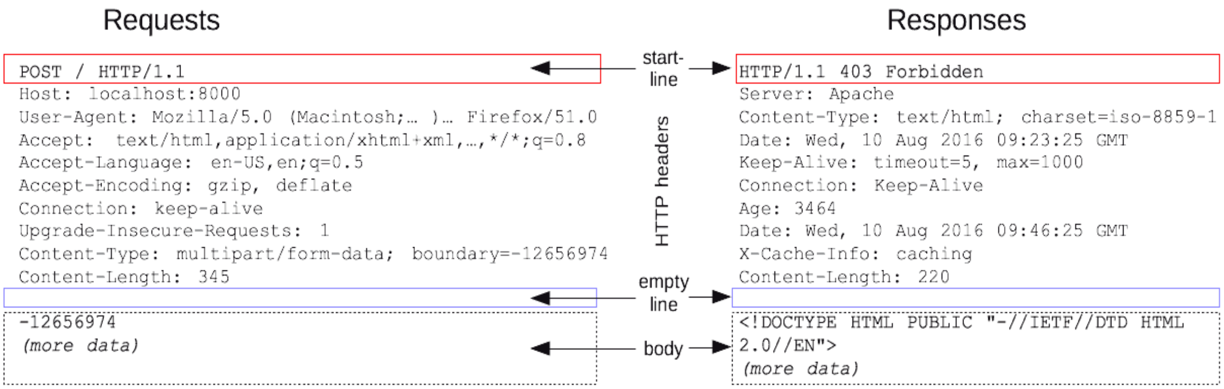
14 - What are the core components of the HTTP request and HTTP response ?

➤ HTTP Response and Requests have a special structure that is followed so that the client can easily understand it.

➤ Core components of HTTP requests are: HTTP Version, Request Body, Request Header, URI, and Verb.

➤ Core components of HTTP responses are: HTTP Version, Response Body, Response Header and Status/Response Code.

➤ HTTP Response and Request has 3 common main components: HTTP version, Headers and Body.



```
POST / HTTP/1.1
Host: localhost:8000
User-Agent: Mozilla/5.0 (Macintosh;… )… Firefox/51.0
Accept: text/html,application/xhtml+xml,…,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-12656974
Content-Length: 345

-12656974
(more data)
```

```
HTTP/1.1 403 Forbidden
Server: Apache
Content-Type: text/html; charset=iso-8859-1
Date: Wed, 10 Aug 2016 09:23:25 GMT
Keep-Alive: timeout=5, max=1000
Connection: Keep-Alive
Age: 3464
Date: Wed, 10 Aug 2016 09:46:25 GMT
X-Cache-Info: caching
Content-Length: 220

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML
2.0//EN">
(more data)
```