Disclaimer : If DO NOT claim or guarantee whether the answer written here is 100% accurate. If you feel something is not accurate or out-of-order, it will be a great help, you let me know. You know how to find me. Those question which are crossed (i.e strikethrough) refer to repeated question which has been solved/answered already.

Web Technology II (Q&A)

2019 Fall

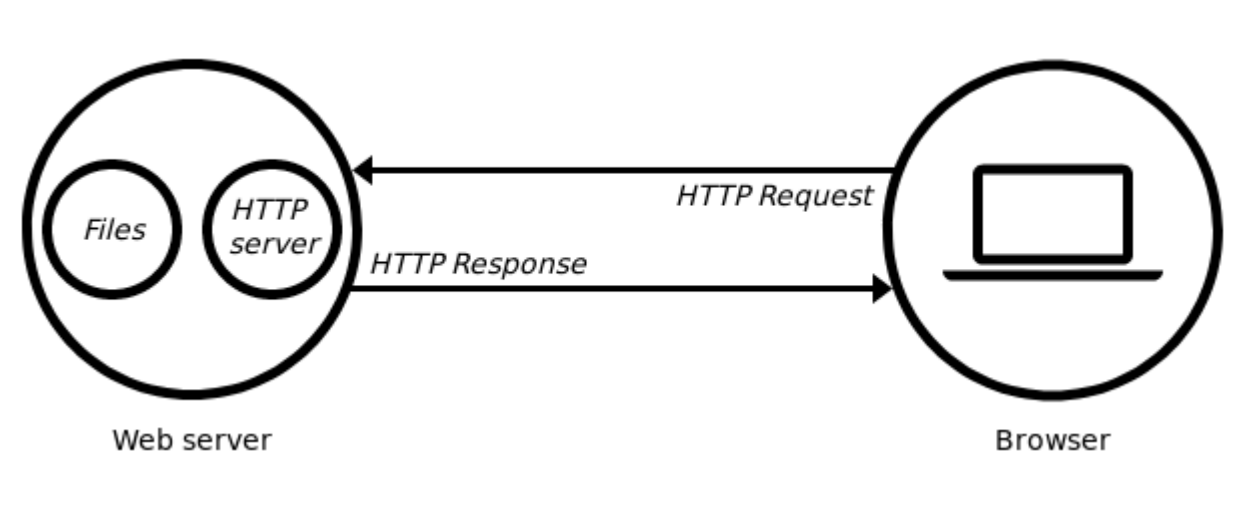
1 a) Differentiate between server side and client side scripting language with suitable example?
For Web pages they are instructions either to the Web server(server-side scripting) or to the Web Browser (client-side scripting). Let's have a look how they differ from each other :

Server Side Scripting Language	Client Side Scripting Language
Server side scripting language are used to to create a program that runs on server dealing with generation of content of web page.	
It is relatively secure.	It is not secure in-comparison with Server side scripting.
It can be used to connect to the database that reside on the web server.	It can't be used to connect to database that are on web server.
Server side scripting is done on the server-side.	Client side scripting is done on client's machine,
PHP, C++, Java & JSP, Python, Ruby on Rails, etc are some popular chosen language for server-side scripting language.	JavaScript, VBScript, HTML, CSS, AJAX, etc are some example of client-side scripting language.

1 b) What are web servers? Mention importance of web server in web application.
"Web server" can refer to hardware or software, or both of them working together.

- *On the hardware side*, a web server is a computer that stores web server software and a website's component files (e.g. HTML documents, images, CSS stylesheets, and JavaScript files). It is connected to the Internet and supports physical data interchange with other devices connected to the web.
- *On the software side*, a web server includes several parts that control how web users access hosted files, at minimum an HTTP server. An HTTP server is a piece of software that understands URLs (web addresses) and HTTP (the protocol your browser uses to view webpages). It can be accessed through the domain names (like *google.com*) of websites it stores, and delivers their content to the end-user's device.

At the most basic level, whenever a browser needs a file which is hosted on a web server, the browser requests the file via HTTP. When the request reaches the correct web server (hardware), the HTTP server (software) accepts request, finds the requested document (if it doesn't then a 404 response is returned), and sends it back to the browser, also through HTTP.



In computing, a **web application** or **web app** is a client–server computer program that the client (including the user interface and client-side logic) runs in a web browser. Common web applications include webmail, online retail sales, online banking, and online auction. As we know, the primary function of a web server is to store, process and deliver web pages to clients. This means without the help of web server, the whole concept of web application can't exits. Web application heavily relies on web server to send data, or any sort of request the client made.

2 a) What is CRUD operation? Write a full code to illustrate the mailing using PHP from client to server.
CRUD stands for create, read, update and delete. These are the four basic functions of persistent storage. Also, each letter in the acronym can refer to all functions executed in relational database applications and mapped to a standard HTTP method, SQL statement or DDS operation.

- **C**REATE procedures: Performs the INSERT statement to create a new record.
- **R**EAD procedures: Reads the table records based on the primary keynoted within the input parameter.
- **U**PDATE procedures: Executes an UPDATE statement on the table based on the specified primary key for a record within the WHERE clause of the statement.
- **D**ELETE procedures: Deletes a specified row in the WHERE clause.

PHP mail is the built in PHP function that is used to send emails from PHP scripts.
The PHP mail function has the following basic syntax :

```
<?php
mail($to_email_address,$subject,$message,[$headers],[$parameters]);
?>
```

PHP mailer uses Simple Mail Transmission Protocol (SMTP) to send mail.

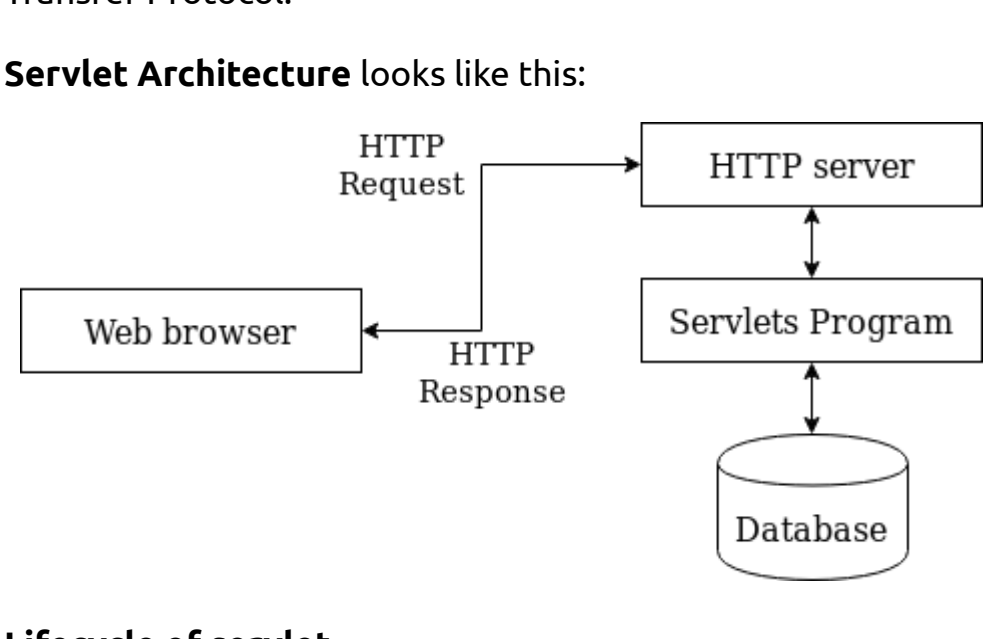
#code to illustrate the mailing using PHP from client to server

2 b) Write a PHP code to validate a form having controls Email, Password and Retype Password. Also insert data into a table in a database. (HTML form in must).

PHP code to validate a form having controls Email, Password and Retype Password

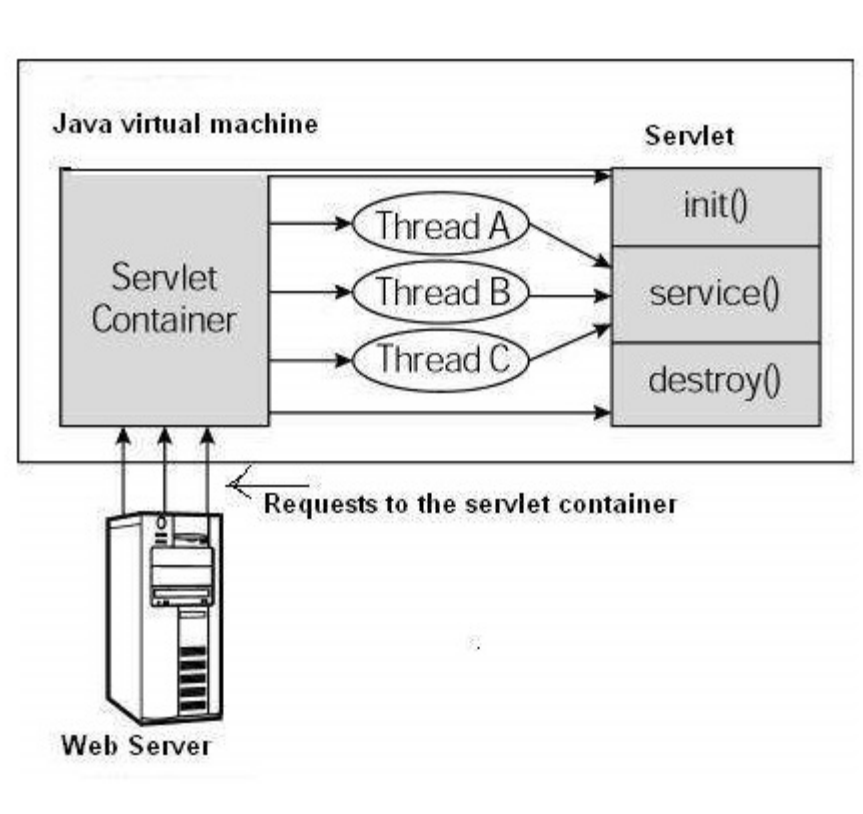
3 a) What are Servlets? Explain servlet architecture and lifecycle with help of suitable diagram.
A servlet is a small Java program that runs within a Web server. Servlets receive and respond to requests from Web clients, usually across HTTP, the HyperText Transfer Protocol.

Servlet Architecture looks like this:



<u>**Lifecycle of servlet**</u>
A servlet life cycle can be defined as the entire process from its creation till the destruction. The following are the paths followed by a servlet.

- The servlet is initialized by calling the **init()** method.
- The servlet calls **service()** method to process a client's request.
- The servlet is terminated by calling the **destroy()** method.
- Finally, servlet is garbage collected by the garbage collector of the JVM.



The figure at the side shows a typical servlet life-cycle scenario. What happens in that figure is explained below:

- First the HTTP requests coming to the server are delegated to the servlet container.
- The servlet container loads the servlet before invoking the service() method.
- Then the servlet container handles multiple requests by spawning multiple threads, each thread executing the service() method of a single instance of the servlet.

3 b) What are cookies? How cookies differ from sessions? Write a code to implement sessions using servlet.
Cookies are the small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing. The main purpose of a cookie is to identify users and possibly prepare customized web pages for them.

Cookies and sessions can differ from in following ways:

Cookies	Sessions
• They are stored in client's side.	• They are stored in server side.
• They are not secure since they are in text format.	• They are secure in comparison to cookies because they resides at server-side in encrypted format.
• They can be disabled.	• They can't be disabled because they can be used without cookies.

#Code to implement sessions using servlet.

4 a) What is web services description language (WSDL)? Describe some uses of WSDL in web technology.
The Web Services Description Language an XML-based interface description language that is used for describing the functionality offered by a web service. It was developed by *World Wide Web Consortium*. The current version of WSDL is WSDL 2.0. The meaning of the acronym has changed from version 1.1 where the "D" stood for "Definition".

Some uses of WSDL in web technology are enlisted down below:
- WSDL is often used in combination with SOAP and an XML Schema to provide Web services over the Internet.

4 b) Explain any two Java frameworks in details.
Any two Java framework are explained in details below:

i. <u>**Spring framework**</u>
Spring Framework is a powerful lightweight application development framework used for Enterprise Java (JEE).

The core features of the Spring Framework can be used in developing any Java application. It is described as a complete modular framework. This framework can be used for all layer implementations of a real-time application. It can also be used for the development of a particular layer of a real-time application unlike the other frameworks, but with Spring we can develop all layers.

Spring and all the modules including Spring MVC, Spring Core, Spring Security, Spring ORM, etc are used in enterprise applications. The Spring Framework is open source. The latest version of this framework is **Version 5** which was released on 2017.

<u>Uses</u>:
- Web application development.
- Its features can be used to create any Java application.
- Its also used in Enterprise Java (JEE)

<u>Advantages</u>
- It provides a lightweight container that can be triggered without using a web server or application server software.
- Spring supports JDBC that improves productivity and reduces the error.
- It targets to make J2EE development easier to use.
- Spring supports both XML and annotation based configuration.
- It provides backward compatibility and test-ability of the code

Companies like Amazon, eBay, etc uses this framework for application development. Netflix uses Spring Boot and Yatra uses Spring MVC.

ii. <u>**Hibernate framework**</u>
Hibernate ORM is a stable object-relational mapping framework for Java. It makes better communication possible between the Java programming language and relational database management systems (RDBMS).

When we work with an object-oriented language like Java, you'll encounter a problem called Object-Relational Impedance Mismatch also called Paradigm Mismatch. This is because OO languages and RDBMS handle the data differently, which can lead to severe mismatch problems. So, this Hibernate provides you with a framework that overcomes the mismatch problems of Java.

<u>Uses</u>
- It allows you to develop persistent classes following the object-oriented idiom
- It allows you to communicate with any database using very tiny alterations in the code, bridging the gap between objects and relational words
- It is an advanced ORM framework that lets you perform the database operation on Java entities

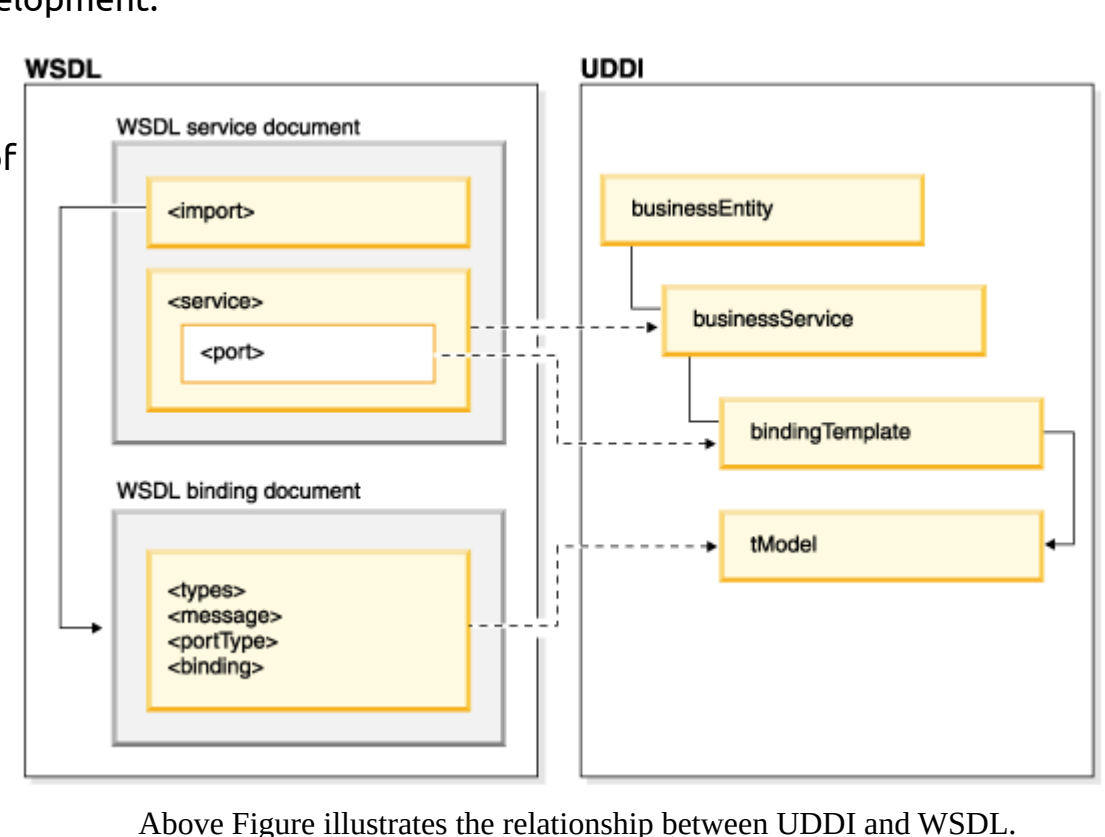
<u>Advantages</u>
- Portability, productivity, maintainability
- Free and open source framework
- It removes a lot of repetitive code from the JDBC API

Companies like Dell, Oracle, IBM, Accenture, etc use Spring framework for application development.

5 a) Explain WSDL and UDDI in details.
Web Services Description Language (WSDL) is an XML-based standard specification for describing Web services. WSDL defines an XML format for describing network services as a set of endpoints that operate on messages that contain either document-oriented or procedure-oriented information.

The Universal Description, Discovery, and Integration (UDDI) specification defines a way to publish and discover information about Web services. UDDI has two functions:

i) It is a SOAP-based protocol that defines how UDDI clients communicate with registries.
ii) It is a particular set of globally replicated registries.



Above Figure illustrates the relationship between UDDI and WSDL.

5 b) What are different protocols used in internet? Explain in details about URL encoding and HTML encoding with reference to PHP.
There are many internet protocols used in the internet. The most common Internet protocols include TCP/IP (Transmission Control Protocol/Internet Protocol), UDP/IP (User Datagram Protocol/Internet Protocol), HTTP (HyperText Transfer Protocol) and FTP (File Transfer Protocol).

i. <u>TCP/IP</u>
TCP/IP is a stream protocol. This means that a connection is negotiated between a client and a server. Any data transmitted between these two endpoints is guaranteed to arrive, thus it is a so-called lossless protocol. Since the TCP protocol (as it is also referred to in short form) can only connect two endpoints, it is also called a peer-to-peer protocol.

ii. <u>HTTP</u>
HTTP is the protocol used to transmit all data present on the World Wide Web. This includes text, multimedia and graphics. It is the protocol used to transmit HTML, the language that makes all the fancy decorations in our browser. It works upon TCP/IP.

iii. <u>FTP</u>
FTP is the protocol used to transmit files between computers connected to each other by a TCP/IP network, such as the Internet.

<u>**URL encoding**</u>
URL encoding, also known as Percent-encoding, is a mechanism for encoding information in a Uniform Resource Identifier (URI) under certain circumstances.

In PHP, the **urlencode()** function is an inbuilt function which is used to encode the url. This function returns a string which consist all non-alphanumeric characters except -_. and replace by the percent (%) sign followed by two hex digits and spaces encoded as plus (+) signs.

Syntax:
```
string urldecode( $input )
```

<u>**HTML Encoding**</u>

6 a) Why security is more important for web application? What is the security foundation in web application?
Security is more important for web application because of following points:
i) Hacker could steal client data using various attacks and can held for ransomware.
ii) A company profile is built on its products and services. If its easy to break, then it can damage company's image too. Can also bring down share market value of that company.
iii) For ISO certification, web application security is also reviewed. If security standards don't meet, then that company might loose its ISO certification.
iv) Web application can crash or on some cases can even damage host computer where it is installed if security is not tightly maintained.

In short, organizations failing to secure their web applications run the risk of being attacked. Among other consequences, this can result in information theft, damaged client relationships, revoked licenses and legal proceedings.

The security foundation in web application refers to standard protocols followed to protect web application, upon which tight security is built. These foundation upon which web application security based on are enlisted below:

6 b) Explain Network threats and host threats. Also write down some countermeasures for both of them.

7. Write short notes on **any two**:
a) <u>**SOAP elements**</u>
SOAP (abbreviation for Simple Object Access Protocol) is a messaging protocol specification for exchanging structured information in the implementation of web services in computer networks. Its purpose is to provide extensibility, neutrality and independence. It uses XML Information Set for its message format, and relies on application layer protocols, most often Hypertext Transfer Protocol (HTTP), although some legacy systems communicate over Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission.

A SOAP message is an ordinary XML document containing the following elements:

An **Envelope element** that identifies the XML document as a SOAP message
A **Header element** that contains header information
A **Body element** that contains call and response information
A **Fault element** containing errors and status information

b) <u>**Content Management Systems**</u>
A content management system (CMS) is a software application that can be used to manage the creation and modification of digital content.

A content management system (CMS) typically has two major components: a content management application (CMA), as the front-end user interface that allows a user, even with limited expertise, to add, modify, and remove content from a website without the intervention of a webmaster; and a content delivery application (CDA), that compiles the content and updates the website.

c) <u>**GET and POST**</u>

GET is used to request data from a specified resource. It is one of the most common HTTP methods. In short:
Some other notes on GET requests:
- GET requests can be cached
- GET requests remain in the browser history
- GET requests can be bookmarked
- GET requests should never be used when dealing with sensitive data
- GET requests have length restrictions
- GET requests are only used to request data (not modify)

POST is used to send data to a server to create/update a resource. It is also one of the most common HTTP methods.
- POST request are never cached
- POST requests don't remain in the browser history
- POST requests have no restrictions on data length

2018 Spring

1 a) ~~Differentiate between client side scripting and server side scripting with example.~~
1 b) Explain about web application architecture with a diagram.
2 a) ~~What is URL encoding~~? Write the syntax and example of for loop.
2 b) What is array? Mention different types of array in PHP. Write a code snippet to illustrate use of array.
An array is a special variable, which can hold more than one value at a time.

An array in PHP is actually an ordered map. Arrays in PHP is a type of data structure that allows us to store multiple elements of similar data type under a single variable thereby saving us the effort of creating a different variable for every data. In PHP, there are three different types of arrays:

i. <u>Indexed Arrays</u>
An array with a numeric index where values are stored linearly. These type of arrays can be used to store any type of elements, but an index is always a number. By default, the index starts at zero.

ii. <u>Associated Arrays</u>
An array with a string index where instead of linear storage, each value can be assigned a specific key. These type of arrays are similar to the indexed arrays but instead of linear storage, every value can be assigned with a user-defined key of string type.

iii. <u>Multidimensional Arrays</u>
An array which contains single or multiple array within it and can be accessed via multiple indices. Multi-dimensional arrays are such arrays which stores an another array at each index instead of single element. In other words, we can define multi-dimensional arrays as array of arrays.

3 a) What is java servlet? Explain its lifecycle.
3 b) ~~What is Servlet Life Cycle~~? Explain all the methods.
4 a) What is framework? Explain any MVC framework in details.
4 b) What is sessions? Write a PHP sessions to illustrate the use of sessions?
5 a) What is SOAP? Mention different element of SOAP and explain them. Also mention the general structure of a SOAP message.
5 b) What is WSDL? Explain its uses in web technology.
6 a) Explain Threats, Vulnerabilities and Attacks.

- **Threats**
- **Vulnerabilities**
- **Attacks**

6 b) How can you build secure web application? Explain.
We can develop secure web application by applying security checkpoints and techniques at early stages of development as well as throughout the software development lifecycle. Special emphasis should be applied to the coding phase of development. Security mechanisms that should be used include, threat modeling, risk analysis, static analysis, digital signature, among others.

While security is fundamentally based on people and processes, there are a number of technical solutions to consider when designing, building and testing secure web applications. At a high level, these solutions include:

- Black box testing tools such as Web application security scanners, vulnerability scanners and penetration testing software
- White box testing tools such as static source code analyzers
- Fuzzing, tools used for input testing
- Web application security scanner (vulnerability scanner)
- Web application firewalls (WAF),[13] used to provide firewall-type protection at the web application layer
- Password cracking tools for testing password strength and implementation

7. Write shorts notes on **any two**:
a) <u>**JDBC**</u>
Java Database Connectivity (JDBC) is an application programming interface (APT) for the programming language java, which defines how a client may access a database. It is a java-based data access technology used for java database connectivity. It is a part of the Java Standard Edition platform, from Oracle Corporation. It provides methods to query and update data in database, and is oriented towards relational databases. A JDBC-to-ODBC bridge enables connections to any ODBC-accessible data sources in the java virtual machine (JVM) host environment.

The latest stable release in JDBC **4.3** which was released on September 21, 2017. It a cross platform.

b) <u>**CMS**</u>
A content management system (CMS) is a software application that can be used to manage the creation and modification of digital content. CMSs are typically used for enterprise content management (ECM) and web content management (WCM). **WordPress** which is powered by PHP is a perfect example of CMS. WordPress is popular all around the globe due to how it makes easier for people to design their website.

c) <u>**HTML Encoding**</u>

Fall 2018

1 a) Explain HTTP request message and HTTP response message in details.
1 b) Explain uses of methods with suitable for methods with return type and method with parameters.
2 a) Explain file handling in PHP with suitable example for reading, writing and appending data.
2 b) Write a PHP code to validate a form having controls Email, Password and Retype Password. Also insert these data into a table in a database. (HTML form is must),
3 a) ~~What are servlets? Explain servlet architecture and lifecycle with help of suitable diagram.~~
3 b) ~~What are cookies? How cookies differ from sessions?~~ Write a code to implement sessions using servlet.
4 a) Write a JSP code to make database connectivity, select all columns from a table and display them in HTML table format (make your own assumption for table and database).
4 b) ~~Explain any two Java framework in details.~~
5 a) ~~Explain WSDL and UDDI in details.~~
5 b) ~~What are different protocol used in internet? Explain in details about URL encoding and HTML encoding with reference to PHP.~~

6 a) Explain network and host. Also make a highlight on countermeasure for both of them. //Network & Host in itself is not a threat to countermeasure. So basically the question is a typo.
A host is a computer or any form device (e.g Mobile, laptop, server computer, tablet, etc) which do certain task.
A networks is component through with data flows between two or more devices, host.

Hosts on a network include clients and servers -- that send or receive data, services or applications.

<u>**Network Threats and Countermeasures**</u>
The primary components that make up our network infrastructure are routers, firewalls, and switches. They act as the gatekeepers guarding our servers and applications from attacks and intrusions. An attacker may exploit poorly configured network devices. Common vulnerabilities include weak default installation settings, wide open access controls, and devices lacking the latest security patches. Top network level threats include:
- Information gathering
- Sniffing
- Spoofing
- Session hijacking
- Denial of service

Countermeasures to prevent information gathering include:
i. Configure routers to restrict their responses to footprinting requests.
ii. Configure operating systems that host network software (for example, software firewalls) to prevent footprinting by disabling unused protocols and unnecessary ports.

Countermeasures to help prevent sniffing include:
i. Use strong physical security and proper segmenting of the network. This is the first step in preventing traffic from being collected locally.
ii. Encrypt communication fully, including authentication credentials. This prevents sniffed packets from being usable to an attacker. SSL and IPSec (Internet Protocol Security) are examples of encryption solutions.

Countermeasures to prevent spoofing include:
i. Filter incoming packets that appear to come from an internal IP address at your perimeter.
ii. Filter outgoing packets that appear to originate from an invalid local IP address.

Countermeasures to help prevent session hijacking include:
i. Use encrypted session negotiation.
ii. Use encrypted communication channels.
iii. Stay informed of platform patches to fix TCP/IP vulnerabilities, such as predictable packet sequences.

Countermeasures to prevent denial of service include:
i. Apply the latest service packs.
ii. Harden the TCP/IP stack by applying the appropriate registry settings to increase the size of the TCP connection queue, decrease the connection establishment period, and employ dynamic backlog mechanisms to ensure that the connection queue is never exhausted.
iii. Use a network Intrusion Detection System (IDS) because these can automatically detect and respond to SYN attacks.

<u>**Host Threats and Countermeasures**</u>
Host threats are directed at the system software upon which your applications are built. This includes Windows 2000, Internet Information Services (IIS), the .NET Framework, and SQL Server 2000, depending upon the specific server role. Top host level threats include:

- Viruses, Trojan horses, and worms
- Footprinting
- Profiling
- Password cracking
- Denial of service
- Arbitrary code execution
- Unauthorized access

Countermeasures that you can use against viruses, Trojan horses, and worms include:
i. Stay current with the latest operating system service packs and software patches.
ii. Block all unnecessary ports at the firewall and host.
iii. Disable unused functionality including protocols and services.
iv. Harden weak, default configuration settings.

Countermeasures to help prevent footprinting include:
i. Disable unnecessary protocols.
ii. Lock down ports with the appropriate firewall configuration.
iii. Use TCP/IP and IPSec filters for defense in depth.
iv. Configure IIS to prevent information disclosure through banner grabbing.
v. Use an IDS that can be configured to pick up footprinting patterns and reject suspicious traffic.

Countermeasures to help prevent password cracking include:
i. Use strong passwords for all account types.
ii. Apply lockout policies to end-user accounts to limit the number of retry attempts that can be used to guess the password.
iii. Don't use default account names, and rename standard accounts such as the administrator's account and the anonymous Internet user account used by many Web applications.
iv. Audit failed logins for patterns of password hacking attempts.

Countermeasures to help prevent denial of service include:
i. Configure your applications, services, and operating system with denial of service in mind.
ii. Stay current with patches and security updates.
iii. Harden the TCP/IP stack against denial of service.
iv. Make sure your account lockout policies cannot be exploited to lock out well known service accounts.
v. Make sure your application is capable of handling high volumes of traffic and that thresholds are in place to handle abnormally high loads.
vi. Review your application's failover functionality.
vii. Use an IDS that can detect potential denial of service attacks.

Countermeasures to help prevent arbitrary code execution include:
i. Configure IIS to reject URLs with "../" to prevent path traversal.
ii. Lock down system commands and utilities with restricted ACLs.
iii. Stay current with patches and updates to ensure that newly discovered buffer overflows are speedily patched.

Countermeasures to help prevent unauthorized access include:
i. Configure secure Web permissions.
ii. Lock down files and folders with restricted NTFS permissions.
iii. Use .NET Framework access control mechanisms within your ASP.NET applications, including URL authorization and principal permission demands.

6 b) Explain in details the design guidelines for secure web applications.
Web application security is the process of protecting websites and online services against different security threats that exploit vulnerabilities in an application's code. Common targets for web application attacks are content management systems (e.g., WordPress), database administration tools (e.g., phpMyAdmin) and SaaS applications.

7. Write short notes on **any two**:
a) <u>**STRIDE**</u>
STRIDE is a model of threats developed by **Praerit Garg** and **Loren Kohnfelder** at **Microsoft** for identifying computer security threats. It provides a mnemonic for security threats in six categories.

The threats are:

- <u>Spoofing</u>
  Spoofing refers to the act of posing as someone else (i.e. spoofing a user) or claiming a false identity (i.e. spoofing a process).
  This category is concerned with authenticity.
- <u>Tampering</u>
  Tampering refers to malicious modification of data or processes. Tampering may occur on data in transit, on data at rest, or on processes.
  This category is concerned with integrity.
- <u>Reputation</u>
  Repudiation refers to the ability of denying that an action or an event has occurred.
  This category is concerned with non-repudiation.
- <u>Information Disclosure</u>
  Information Disclosure refers to data leaks or data breaches. This could occur on data in transit, data at rest, or even to a process.
  This category is concerned with confidentiality.
- <u>Denial of Service</u>
  Denial of Service refers to causing a service or a network resource to be unavailable to its intended users.
  This category is concerned with availability.
- <u>Elevation of Privilege</u>
  Elevation of Privileges refers to gaining access that one should not have.
  This category is concerned with authorization.

In short, STRIDE is a threat model methodology that should help us systematically examine and address gaps in the security posture of our applications.

b) ~~Content Management Systems~~
c) ~~SOAP elements~~

2017 Spring

1 a) Differentiate between HTTP and HTTPS with some examples.

HTTP	HTTPS
It is hypertext transfer protocol.	It is hypertext transfer protocol with secure.
It is less secure as the data can be vulnerable to hackers.	It is designed to prevent hackers.
It uses port 80 by default.	It was use port 443 by default.
HTTP users begin with http://	HTTPS URLs begin with https://
It operates at TCP/IP level.	It doesn't have any separate protocol. It operates using HTTP but uses encrypted TLS/SSL certificate.
It don't use encryption.	It uses encryption.
It is fast.	It is slower than HTTP.
It doesn't improve search rankings.	It helps to improve search rankings.

1 b) What is user defined function in PHP? Write a program to calculate factorial of given number using recursion.
2 a) Why file handling is needed in PHP? Write a code to illustrate the mailing using PHP from client to server.
2 b) ~~Differentiate between the sessions and cookies?~~ Write a simple program to illustrate the cookie using PHP.
3 a) ~~Define JSP and Servlet lifecycle~~

7.Write short notes on **any two**:
a) ~~Spring and Hibernate~~

b) <u>**RESTful**</u>
REST (Representational State Transfer) is an architectural style for developing web services. REST is popular due to its simplicity and the fact that it builds upon existing systems and features of HTTP in order to achieve its objectives, as opposed to creating new standards, frameworks and technologies.

A primary benefit of using REST, both from a client and server's perspective, is REST-based interactions happen using constructs that are familiar to anyone who is accustomed to using the HTTP.

An example of this arrangement is REST-based interactions all communicate their status using standard HTTP status codes. So, a 404 means a requested resource wasn't found; a 200 code means everything is OK, etc.

Similarly, details such as encryption and data transport integrity are solved not by adding new frameworks or technologies, but instead by relying on well-known Secure Sockets Layer (SSL) encryption and Transport Layer Security (TLS). So, the entire REST architecture is built upon concepts with which most developers are already familiar.

REST is also a language-independent architectural style. REST-based applications can be written using any language, be it Java, Kotlin, .NET, AngularJS or JavaScript. As long as a programming language can make web-based requests using HTTP, it is possible for that language to be used to invoke a RESTful API or web service. Similarly, RESTful web services can be written using any language, so developers tasked with implementing such services can choose technologies that work best for their situation.

c) <u>**JSP Implicit Object**</u>
JSP implicit objects are created during the translation phase of JSP to the servlet. These objects can be directly used in scriplets that goes in the service method. They are created by the container automatically, and they can be accessed using objects.

There are **nine** JSP implicit objects. These objects are created by the web container that are available to all the JSP pages.
i. out
ii. request
iii. response
iv. config
v. application
vi. sessions
vii. pageContext
viii. page
ix. exception