END TERM EXAMINATION [MAY 2016]
SIXTH SEMESTER [B.TECH]
WEB ENGINEERING [ETCS–308]

Time : 3 Hrs. **M.M. : 75**

Note: *Attempt any five questions including Q.No.1 which is compulsory.*

Q.1. Attempt All

Q.1. (*a*) How does XHTML differ from HTML? **(5)**

Ans.

HTML	XHTML
HTML or HyperText Markup Language the main markup language for creating web pages and other information that can be displayed in a web browser.	XHTML (Extensible HyperText Language) is a family of XML markup languages that mirror or extend versions of the widely used Hypertext Markup Language (HTML), the language in which web pages are written.
Filename extension	**Filename extension**
.html, .htm	xhtml, .xht, .xml, .html, .htm
Internet media type	
text/html	application/xhtml+xml
Developed by	
W3C &WHATWG	World Wide Web Consortium
Type of format	
Document file format	Markup language
Function	
Web pages are written in HTML.	Extended version of HTML that is stricter and XML-based.
Origin	
Proposed by Tim Berners-Lee in 1987.	World Wide Web Consortium Recommendation in 2000.
Nature	
Flexible framework requiring lenient HTML specific parser.	Restrictive subset of XML and needs to be parsed with standard XML parsers.
Application	
Application of Standard Generalized Markup Language (SGML).	Application of XML

Q.1. (*b*) Differentiate between server side scripting and client side scripting. **(5)**

Ans. There are two main ways to customise Web pages and make them more interactive. The two are often used together because they do very different things.

Scripts: A script is a set of instructions. For Web pages they are instructions either to the Web browser (client-side scripting) or to the server (server-side scripting). These are explained more below.

Scripts provide change to a Web page. Think of some Web pages you have visit
Any page which changes each time you visit it (or during a visit) probably u
scripting.

Client-side: *The client is the system on which the Web browser is running. JavaScr*
is the main client-side scripting language for the Web. Client-side scripts are interpret
by the browser. The process with client-side scripting is:

- *The user requests a Web page from the server*
- *The server finds the page and sends it to the user*
- *The page is displayed on the browser with any scripts running during or aft*

display

So client-side scripting is used to make Web pages change after they arrive at th browser. It is useful for making pages a bit more interesting and user-friendly. It ca also provide useful gadgets such as calculators, clocks etc. but on the whole is used fo appearance and interaction.

Server-side: The server is where the Web page and other content lives. The server sends pages to the user/client on request. The process is:

- The user requests a Web page from the server
- The script in the page is interpreted by the server creating or changing the page content to suit the user and the occasion and/or passing data around
- The page in its final form is sent to the user and then cannot be changed using server-side scripting

Server-side scripting tends to be used for allowing users to have individual accounts and providing data from databases. It allows a level of privacy, personalisation and provision of information that is very powerful. E-commerce, MMORPGs and social networking sites all rely heavily on server-side scripting. PHP and ASP.net are the two main technologies for server-side scripting.

Q.1. (c) Explain the usage of plugins, extensions, and web apps. **(5)**

Ans. PLUG-INS: In computing, a plug-in (or plugin, add-in, addin, add-on, addon, or extension) is a software component that adds a specific feature to an existing computer program. When a program supports plug-ins, it enables customization. The common examples are the plug-ins used in web browsers to add new features such as search-engines, virus scanners, or the ability to use a new file type such as a new video format. Well-known browser plug-ins include the Adobe Flash Player, the QuickTime Player, and the Java plug-in, which can launch a user-activated Java applet on a web page to its execution on a local Java virtual machine.

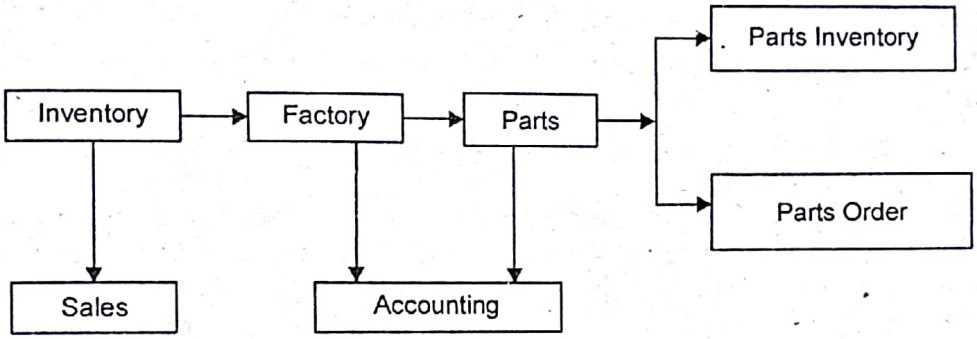
EXTENSIONS: A browser extension is a plug-in that extends the functionality of a web browser in some way. Some extensions are authored using web technologies such as HTML, JavaScript, and CSS.Browser extensions can change the user interface of the web browser without directly affecting viewable content of a web page; for example, by adding a "toolbar."Browser extensions are most commonly used for improving security, accessibility, blocking advertisements, and generally improving a browser's user interface and adding various other features to make browsing the internet more easy and pleasant.

WEB APPS: In computing, a web application or web app is a client–server software application in which the client (or user interface) runs in a web browser.Common web applications include webmail, online retail sales, online auctions, wikis, instant messaging services and many other functions.

Web sites most likely to be referred to as "web applications" are those which have similar functionality to a desktop software application, or to a mobile app. HTML5 introduced explicit language support for making applications that are loaded as web pages, but can store data locally and continue to function while offline.

Q.1. (*d*) How does the JMS API Work with the JAVA EE Platform? (5)

Ans. The Message Service is a Java API that allows applications to create, send, receive, and read messages. Designed by Sun and several partner companies, the JMS API defines a common set of interfaces and associated semantics that allow programs written in the Java programming language to communicate with other messaging implementations.



When the JMS API was introduced in 1998, its most important purpose was to allow Java applications to access existing messaging-oriented middleware (MOM) systems, such as MQSeries from IBM. Since that time, many vendors have adopted and implemented the JMS API, so a JMS product can now provide a complete messaging capability for an enterprise.

Beginning with the 1.3 release of the Java EE platform, the JMS API has been an integral part of the platform, and application developers have been able to use messaging with Java EE components.

The JMS API in the Java EE platform has the following features:Application clients, Enterprise JavaBeans (EJB) components, and web components can send or synchronously receive a JMS message. Application clients can in addition receive JMS messages asynchronously. (Applets, however, are not required to support the JMS API.) Message-driven beans, which are a kind of enterprise bean, enable the asynchronous consumption of messages. A JMS provider can optionally implement concurrent processing of messages by message-driven beans.

The JMS API enhances the Java EE platform by simplifying enterprise development, allowing loosely coupled, reliable, asynchronous interactions among Java EE components and legacy systems capable of messaging. A developer can easily add new behavior to a Java EE application that has existing business events by adding a new message-driven bean to operate on specific business events.

Q.1. (*e*) List two advantages and two disadvantages of dynamic script loading (5)

Ans. Some of the benefits include :

- It reduces the load on the user's computer, as it does not require plugins or browser scripting technology (such as Javascript).
- You can use it to dynamically create pages on the fly. New pages can even be instantly created based on certain user interaction.

Some disadvantages are:

- It requires the scripting software to be installed on the server
- Many scripts and CMS tools require databases in order to store dynamic data

The nature of dynamic scripts creates new security concerns, in some cases making it easier for hackers to gain access to servers exploiting code flaws.

Q.2. (*a*) Discuss the application of Web Engineering Technologies in distributed systems. (6)

Ans. Distributed system is a a system in which hardware or software components located at networked computers communicate and coordinate their actions only by message passing defines it and it can also be defined by a collection of independent computers that appear to the users of the system as a single computer.

There are various types of distributed systems, such as Clusters , Grids , P2P (Peer-to-Peer) networks , distributed storage systems and so on.

Over the years, technologies such as CORBA and DCOM have provided the means to build distributed component-based systems. Such technologies allow systems to interoperate at the component level, by providing a software layer and protocols that offer the interoperability needed for components developed in different programming languages to exchange messages. However, such technologies present scalability issues when applied to, for instance, the Internetand some restrict the developer to aspecific programming language. Hence, a pproaches based on Web protocols and XML(eXtensible Markup Language) have been proposed toallow interoperable distributed systems irrespective the programming language in which they are developed.Web Services are based on XML and provide a means to develop distributed systems that follow a Service Oriented Architecture (SOA).

Services are described in an XML-based dialect (WSDL). In a similar fashion, the request and reply messages exchanged in such systems are formatted according to the Simple Object Access Protocol (SOAP).SOAP messages can be encoded and transmitted by using Web protocols such as the Hypertext Transfer Protocol (HTTP). Various industrial technologies and application platforms such as .NET from Microsoft, J2EE from Sun, WehSphere from IBM are targeted at supporting the development of applications based on Web Services.

Q.2. (*b*) Explain and discuss the various issues in WEB Security. (6.5)

Ans. Web security is very complex – with a lot of unknowns. As an executive running a business with a lot of moving parts, I'm sure you can relate. There are numerous areas – both operational and technical – where web security is lacking in practically every organization regardless of skills and budget.

1. Untested systems: The web security focus is typically on the latest applications essential to running the business or increasing sales. The thing is, there are other (likely dozens) of other websites and applications running in your environment that are creating as much, if not more, business risk simply because they have not been tested for vulnerabilities.

2. Production data being used in development and QA: Developers and QA professionals often use a copy of production databases when writing and testing their code. It's typically an honest oversight but it can have serious ramifications. The thing is, the systems they're running are often under-secured.

3. Exposed source code: Developers are some of the smartest and most reasonable people I work with. Yet they're still human and make mistakes like everyone else.

4.Weak passwords: It's the bane of web security. You can have the most secure code, strongest encryption, and the fanciest web application firewall, yet all it takes to expose your entire application (and data) to the world is one weak password. Often times, developers will build in strong password enforcement features.

5. Input validation flaws: On the more technical side of web security are websites and applications that do not "cleanse" or validate what's entered into the URL or form fields. When these flaws exist, things like cross-site scripting and SQL injection can occur which allow an attacker or malware to manipulate the vulnerable web pages and gain access to things like local web browser information, user login sessions, or even the entire database.

Q.3. Create a HTML form that has the following controls. **(12.5)**

- **A TEXT control called firstName to collect the first name.**
- **A TEXT control called lastName to collect the last name.**
- **A TEXT control called email to collect the email address.**
- **A TEXT control called phone to collect the phone number.**
- **A SELECT control called software for displaying a combo box with software list.**
- **A SELECT control called os for displaying a combo box with operating systems.**
- **A TEXTAREA control called txtArea for displaying problem description.**
- **A SUBMIT control called submit for submitting the information.**

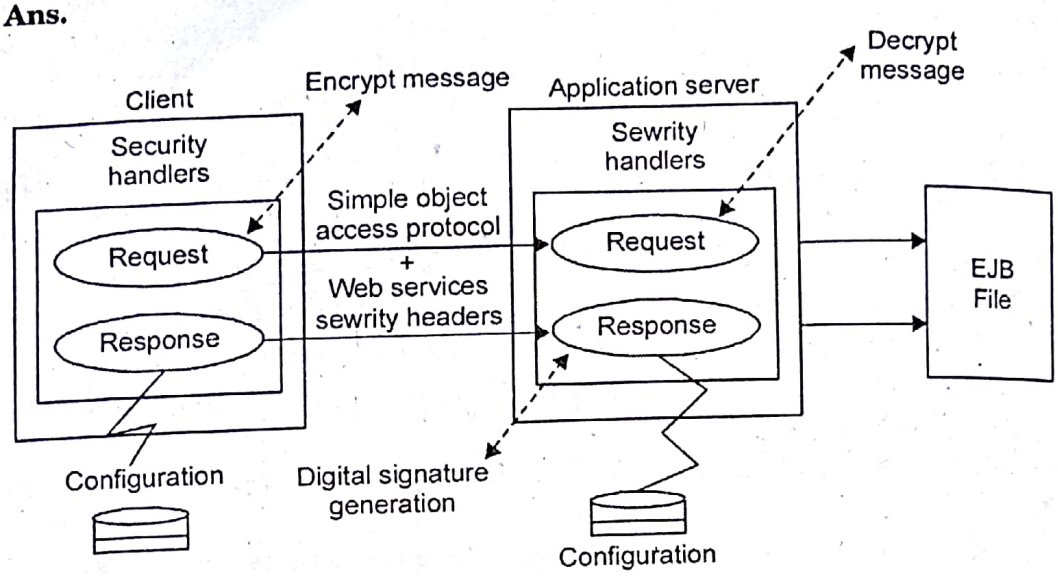
Ans.

```
<html>
<body>
<form action="action_page.php">
First name:<br>
<input type="text" name="firstname"><br>
Last name:<br>
<input type="text" name="lastname">
Email:<br>
<input type="text" name="email"><br>
Phone:<br>
<input type="text" name="phone"><br>
<select>
 <option value="software">MS WORD</option>
 <option value="software">MS EXCEL</option>
 <option value="software">ORACLE</option>
 <option value="software">MYSQL</option>
</select>
<select>
 <option value="os">windows</option>
 <option value="os">linux</option>
 <option value="os">mac</option>
 </select>
<input type="submit" value="Submit">
```

```
</form>
</body>
</html>
```

Q.4. (*a*) Discuss and explain Web Secuirty model in detail. **(6.5)**

Ans.



Web security has two sides:

- Web Browser (client side): Attacks target browser security weakness uninstallation which results in malware uninstallation and loss of private data.
- Web Application code (server side): Writtern in PHP, ASP, ----- Attacks lead to defaced sites.

So a browser is used as a security interface. HTTP protocol is simple, stateless and unencrypted which provides HTTP request and HTTP response as a security mechanism. Various components of browser security are:

1. FRAMCE to FRAME RELATIONSHIPS: can script (A, B)
2. FRAME to COOKIE RELATIONSHIPS: Read cookie (A, B) write cookie (A, S)
3. Security Indicator (W): (SSl lock icon)

(6)

Q.4. (*b*) Explain the following:

(*i*) HTTPS and certificates

(*ii*) HTTP security extensions

Ans. HTTPS and Certificates: Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted. HTTPS is often used to protect highly confidential online transactions like online banking and online shopping order forms. Web browsers such as Internet Explorer, Firefox and Chrome also display a padlock icon. When you request a HTTPS connection to a webpage, the website will initially send its SSL certificate to your browser. This certificate contains the public key needed to begin the secure session. Based on this initial exchange, your browser and the website then initiate the 'SSL handshake'. The SSL handshake involves the generation of shared secrets to establish a uniquely secure connection between yourself and the website. When a trusted SSL(Secure Socket Layer) Digital Certificate

is used during a HTTPS connection, users will see a padlock icon in the browser address bar. All communications sent over regular HTTP connections are in 'plain text' and can be read by any hacker that manages to break into the connection between your browser and the website. This presents a clear danger if the 'communication' is on an order form and includes your credit card details or social security number. With a HTTPS connection, all communications are securely encrypted. This means that even if somebody managed to break into the connection, they would not be able decrypt any of the data which passes between you and the website.

HTTPS security exteusious: A Reporting Services security extension enables the authentication and authorization of users or groups; that is, it enables different users to log on to a report server and, based on their identities, perform different tasks or operations. By default, Reporting Services uses a Windows-based authentication extension, which uses Windows account protocols to verify the identities of users who claim to have accounts on the system. Reporting Services uses a role-based security system to authorize users. The Reporting Services role-based security model is similar to the role-based security models of other technologies.

Because security extensions are based on an open and extensible API, you can create new authentication and authorization extensions in Reporting Services. The following is an example of a typical security extension implementation that uses Forms-based authentication and authorization:

It is recommended that you use Windows Authentication if at all possible. However, custom authentication and authorization for Reporting Services may be appropriate in the following two cases:

- You have an Internet or extranet application that cannot use Windows accounts.
- You have custom-defined users and roles and need to provide a matching authorization scheme in Reporting Services.

Q.5. (*a*) Explain the following in respect to JAVA **(12.5)**

Ans. Java servelets: A **Java servlet** is a Java program that extends the capabilities of a server. Although servlets can respond to any types of requests, they most commonly implement applications hosted onWeb servers. Such Web servlets are the Java counterpart to other dynamic Web content technologies such as PHP and ASP.NET. To deploy and run a servlet, a web container must be used. A web container (also known as a servlet container) is essentially the component of a web server that interacts with the servlets. The web container is responsible for managing the lifecycle of servlets, mapping a URL to a particular servlet and ensuring that the URL requester has the correct access rights.The Servlet API, contained in the Java package hierarchy javax.servlet, defines the expected interactions of the web container and a servlet. A Servlet is an object that receives a request and generates a response based on that request. The basic Servlet package defines Java objects to represent servlet requests and responses, as well as objects to reflect the servlet's configuration parameters and execution environment. The packagejavax.servlet.http defines HTTP-specific subclasses of the generic servlet elements, including session management objects that track multiple requests and responses between the web server and a client. Servlets may be packaged in a WAR file as a web application.

Q.5. (*b*) Intrinsic event handling

Ans. Intrinsic event handlers are ways to attach specific scripts to your documents that are executed only when something happens to an element. Not all event handlers apply to all elements, but here's the lot:

Intrinsic event handlers:

• ONLOAD (Script)

This event occurs when the browser finishes loading a document or a all frames in a frameset. It applies to BODY and FRAMESET elements.

• ONUNLOAD (Script)

This event occurs when the browser stops displaying a document or a frame. It applies to BODY and FRAMESET elements.

•ONCLICK (Script)

This event occurs when a mouse button is clicked over an element.

• ONDBLCLICK (Script)

This event occurs when a mouse button is double-clicked over an element.

• ONMOUSEDOWN (Script)

In order to use intrinsic event handlers, you *must* define the default scripting language using the Content-Style-Type header. Most scripting languages, including JavaScript, offer a way to define event handlers in scripts instead of using HTML attributes, and this is a better approach from a design point of view.

Q.5. (c) JSP

Ans. JSP technology is used to create web application just like Servlet technology. It can be thought of as an extension to servlet because it provides more functionality than servlet such as expression language, jstl etc.A JSP page consists of HTML tags and JSP tags. The jsp pages are easier to maintain than servlet because we can separate designing and development. It provides some additional features such as Expression Language, Custom Tag etc.

There are many advantages of JSP over servlet. They are as follows:

(1) Extension to Servlet: JSP technology is the extension to servlet technology. We can use all the features of servlet in JSP. In addition to, we can use implicit objects, predefined tags, expression language and Custom tags in JSP, that makes JSP development easy.

(2) Easy to maintain: JSP can be easily managed because we can easily separate our business logic with presentation logic. In servlet technology, we mix our business logic with the presentation logic.

(3) Fast Development: No need to recompile and redeploy: If JSP page is modified, we don't need to recompile and redeploy the project. The servlet code needs to be updated and recompiled if we have to change the look and feel of the application.

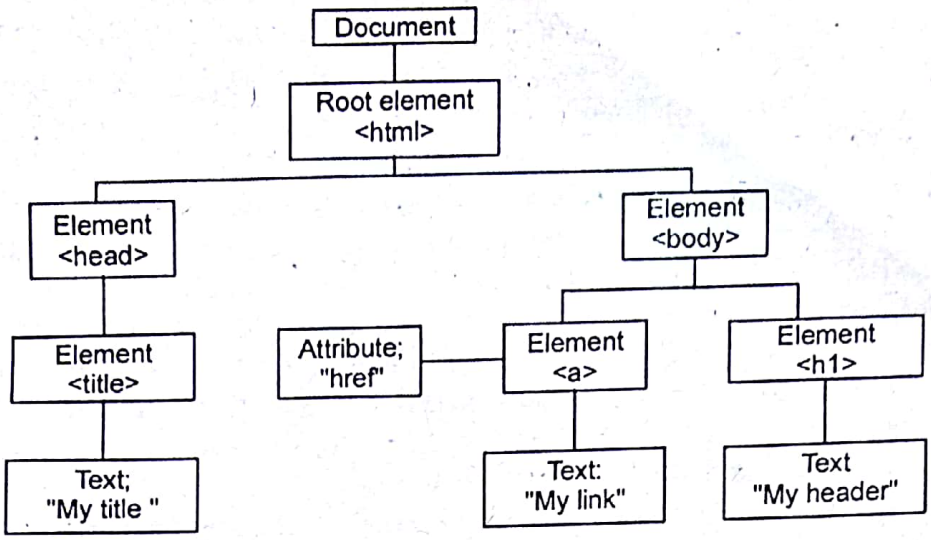
(4) Less code than Servlet: In JSP, we can use a lot of tags such as action tags, jstl, custom tags etc. that reduces the code. Moreover, we can use EL, implicit objects etc.

Q.6. Define the following terminology.

Q.6. (a) Document tress **(12.5)**

Ans. When a web page is loaded, the browser creates a Document Object Model of the page.

HTML DOM model is constructed as a tree of Objects:



With the object model, JavaScript gets all the power it needs to create dynamic TML:

- JavaScript can change all the HTML elements in the page
- JavaScript can change all the HTML attributes in the page
- JavaScript can change all the CSS styles in the page
- JavaScript can remove existing HTML elements and attributes

Q.6. (*b*) CSS style sheets

Ans. CSS stands for Cascading Style Sheets.CSS describes how HTML elements e to be displayed on screen, paper, or in other media. It is a style sheet language used describing the presentation of a document written in a markup language. Although st often used to set the visual style of web pages and user interfaces written HTML and XHTML, the language can be applied to any XML document, luding plain XML, SVG and XUL, and is applicable to rendering in speech, or on other dia. Along with HTML and JavaScript, CSS is a cornerstone technology used by most bsites to create visually engaging webpages , user interfaces for web applications, d user interfaces for many mobile applications.

CSS saves a lot of work. It can control the layout of multiple web pages all at ce.CSS can be added to HTML elements in 3 ways:

- **Inline -** by using the style attribute in HTML elements
- **Internal -** by using a <style> element in the <head> section
- **External -** by using an external CSS file

The most common way to add CSS, is to keep the styles in separate CSS files.

Q.6. (*c*) DNS and URL

Ans. The **Domain Name System** (DNS) is a hierarchical decentralized naming em for computers, services, or any resource connected to the Internet or a private work. It associates various information with domain names assigned to each of the ticipating entities. Most prominently, it translates more readily memorized domain mes to the numerical IP addresses needed for the purpose of locating and identifying puter services and devices with the underlying network protocols. By providing a rldwide, distributed directory service, the Domain Name System is an essential

component of the functionality of the Internet.The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain. Network administrators may delegate authority over sub-domains of their allocated name space to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid a single large central database.

URL is the abbreviation of Uniform Resource Locator. It is the global address of documents and other resources on the World Wide Web. For example, www.webopedia.com is a URL. A URL is one type of Uniform Resource Identifier (URI); the generic term for all types of names and addresses that refer to objects on the World Wide Web. The first part of the URL is called a protocol identifier and it indicates what protocol to use, and the second part is called a resource name and it specifies the IP address or the domain name where the resource is located. The protocol identifier and the resource name are separated by a colon and two forward slashes.

Q.7. (a) Discuss the procedure to maintain the concurrency issues in a Website?

Ans. A concurrency conflict occurs when one user displays an entity's data in order to edit it, and then another user updates the same entity's data before the first user's change is written to the database. If you don't enable the detection of such conflicts, whoever updates the database last overwrites the other user's changes. In many applications, this risk is acceptable: if there are few users, or few updates, or if isn't really critical if some changes are overwritten, the cost of programming for concurrency might outweigh the benefit. In that case, you don't have to configure the application to handle concurrency conflicts. **(6.5)**

Pessimistic Concurrency (Locking): If your application does need to prevent accidental data loss in concurrency scenarios, one way to do that is to use database locks. This is called pessimistic concurrency. For example, before you read a row from a database, you request a lock for read-only or for update access. If you lock a row for update access, no other users are allowed to lock the row either for read-only or update access, because they would get a copy of data that's in the process of being changed. If you lock a row for read-only access, others can also lock it for read-only access but not for update.

Optimistic Concurrency: The alternative to pessimistic concurrency is optimistic concurrency. Optimistic concurrency means allowing concurrency conflicts to happen, and then reacting appropriately if they do.

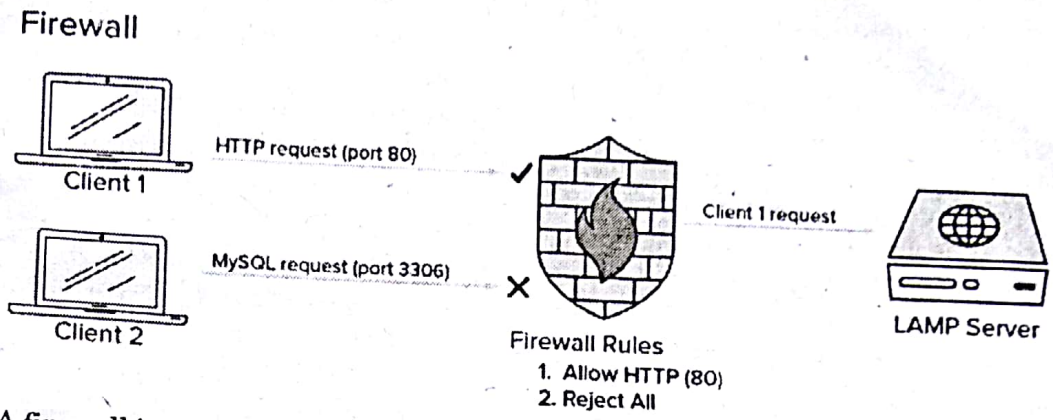
You can resolve conflicts by handling Optimistic ConcurrencyException exceptions that the Entity Framework throws. In order to know when to throw these exceptions, the Entity Framework must be able to detect conflicts. Therefore, you must configure the database and the data model appropriately. Some options for enabling conflict detection include the following:

Managing Concurrency: The data type of the tracking column is typically rowversion. The rowversion value is a sequential number that's incremented each time the row is updated. In an Update or Delete command, the Where clause includes the original value of the tracking column (the original row version) . If the row being updated has been changed by another user, the value in the rowversion column is different than the original value, so the Update or Delete statement can't find the row to update because of the Where clause. When the Entity Framework finds that no rows have

been updated by the Update or Delete command (that is, when the number of affected rows is zero), it interprets that as a concurrency conflict. Configure the Entity Framework to include the original values of every column in the table in the Where clause of Update and Delete commands.

Q.7. (*b*) Explain any tool for maintaining Server-side security and client side security.

Ans. **(6)**



A firewall is a piece of software (or hardware) that controls what services are exposed to the network. This means blocking or restricting access to every port except for those that should be publicly available.

On a typical server, a number services may be running by default. These can be categorized into the following groups:

- Public services that can be accesses by anyone on the internet, often anonymously. A good example of this is a web server that might allow access to your site.
- Private services that should only be accessed by a select group of authorized accounts or from certain locations. An example of this may be a database control panel.
- Internal services that should be accessible only from within the server itself, without exposing the service to the outside world. For example, this may be a database that only accepts local connections.

Firewalls are an essential part of any server configuration. Even if your services themselves implement security features or are restricted to the interfaces you'd like them to run on, a firewall serves as an extra layer of protection.

A properly configured firewall will restrict access to everything except the specific services you need to remain open. Exposing only a few pieces of software reduces the attack surface of your server, limiting the components that are vulnerable to exploitation.

Q.8. Write short notes on any-two of the following: **(6.25×2=12.5)**

Q.8. (*a*) Web application Firewalls (WAFs) and Fuzzers

Ans. A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

Fuzz testing or fuzzing is a software testing technique used to discover coding errors and security loopholes in software, operating systems or networks by inputting massive amounts of random data, called fuzz, to the system in an attempt to make

it crash. If a vulnerability is found, a tool called a fuzz tester (or fuzzer), indicates potential causes. Fuzz testing was originally developed by Barton Miller at the University of Wisconsin in 1989.Fuzzers work best for problems that can cause a program to crash, such as buffer overflow, cross-site scripting, denial of service attacks, format bugs and SQL injection.

Q.8. (b) Latest Trends in Web Technologies

Ans. Internet of Things (IoT) will have a huge impact: The Internet of Things has taken app development to a new level. According to Technavio, IoT will grow by 31.72% (CAGR) between 2015 and 2019. By linking smart objects to the internet, IoT enables the exchange of data that was never possible before.

As more and more devices are being connected and accessible to the network, we'll find web developers coming up with upgraded solutions to help users control and communicate with their everyday gadgets and equipment.

Browser based IDEs: Odds are that you have your own favorite development environment. Maybe you fell in love with VIM years ago or you're an IntelliJ fanatic. That's going to change soon as more and more people are starting to use cloud-based versions of IDEs.

They're fast and they're accessible, and some of them have a huge community behind them. Flexibility is key here, and while you may not use these tools full time, it's definitely good to know that they're available if you want to do a quick test of a bootstrap code of Jade without having to download a single file.

Full-screen navigation design: Full-screen navigation design is a feature that improves the user experience on mobile devices. Let's say a user is navigating a website on his mobile phone and he comes across a registration form. As he taps on the registration form, the form jumps to a full-screen size enabling the user to fill out the form in a more natural way. More and more web developers and designers are developing sites for full-screen navigation designs and this trend is going to continue.

Q.8. (c) Web attacks and their prevention.

Ans. The most common web application threats include:

• **Cross site scripting (XSS):** XSS (Cross-Site Scripting) is regarded as the most common type of computer security vulnerability, with a huge number of web applications that are online today being vulnerable to this type of malicious script.

TOP PREVENTION TIP: An intelligent Web Application Firewall (WAF) can shield these vulnerabilities, working in conjunction with the behavioural firewall, blocking sophisticated and dangerous attacks.

• **SQL injection:** SQL Injections are one of the most serious type of attack on the internet. These attacks take advantage of web application vulnerabilities to gain control of databases and all of the information contained within them.

TOP PREVENTION TIP: In order to keep your databases secure you should practice regular auditing and remediation of your application to ensure that any vulnerability are discovered and dealt with as quickly as possible.

•**DDoS attacks:** DDoS stands for a denial-of-service or as it's more commonly known, a distributed denial-of-service (DDoS). This type of attack is an attempt to make a machine or network resource unavailable to its intended users.

TOP PREVENTION TIP: A reliable and well-reviewed DDoS protection tool is the best defence against DDos Attacks; there are plenty of tools to choose from.