QUESTION 1

We can use a cookie-less session.

Example:

The variables necessary to link users to their sessions in cookie-less sessions are **added to the browser's URL.**

The example is referring to ASP.NET C# cookie-less session. We need to modify some configuration in the Web.Config file by adding a <sessionState> tag under the <system.web> tag.

It should look like this:

<sessionState cookieless=”AutoDetect” regenerateExpiredSessionId=”true”/>

For “AutoDetect”, If cookies are allowed, the session makes use of a background cookie. In the absence of cookies, session data is stored in the URL.

If a cookieless url expires, "regenerateExpiredSessionId" is used to make sure that a new url is produced with a new session. Additionally, each user receives a fresh session url if they utilise the same cookieless url at the same time.

QUESTION 2

Advantages of using .NET WCF:

1. WCF **offers more security and dependability** than ASMX Web services.
2. To leverage the security model and adjust the binding in WCF, very little coding is required.
3. Your needs may be met with **minor configuration file adjustments.**
4. **Interoperability** between services is offered via WCF.

Disadvantages of using NET WCF:

1. The learning curve for developers to understand how it works when they just getting started.

Advantages of using RMI:

1. Applications are more resilient, maintainable, and adaptable when they are implemented simply and cleanly.
2. It is possible to create distributed systems while concurrently decoupling the client and server components.
3. Users might design their own zero-install clients.
4. The only clients that require installation are browsers that support Java.
5. Only the server objects must be recompiled when the database is changed; the server interface and client stay unchanged.

Disadvantages of using RMI:

1. ineffective compared to Socket objects.
2. Assuming that the servers are thread-safe and resilient, disregarding the code will be possible.
3. Code that is outside of Java's purview cannot be used.
4. Security concerns require closer monitoring.

Advantages of using COBRA:

1. Both platform and language independence apply to the services.
2. Encourages diverse implementations based on the same interface.
3. Provides support for basic data types and data structures as arguments.
4. Easily connects systems and things by offering means to do so.

Disadvantages of using COBRA:

1. Definition of the interface Writing for one language may not support the other in language mapping.
2. New additions to the current code or system might not work with the IDL language tools.
3. CORBA doesn't support object or data transport.
4. CORBA specs become a legacy system if the industry fails to implement them.

QUESTION 3

You will have slow performance issues and malicious code issues by using the eval() method.

Firstly, for example, the script compiler executes the compiler even though the code is built at run-time since eval() cannot be pre-compiled. Even while it doesn't affect performance significantly, it still does.

Lastly, for example, Because eval() treats strings like code, it makes it much simpler for hackers to access confidential data. When software runs client-side and accepts user input, there is a significant security risk. The original software itself may then be altered as a result of this.

QUESTION 4

XSS attack is a Cross-Site Scripting Attack. It is when the user input code in the input fields of a website.

Sending and inserting malicious code or script is known as a cross-site scripting attack. Client-side programming languages like Javascript, HTML, VBScript, Flash, etc. are frequently used to create malicious malware. However, this assault mostly employs HTML and Javascript. There are several methods for carrying out this assault. The malicious script may be shown on the victim's browser or stored in the database and run each time the user calls the relevant function, depending on the kind of XSS attack.

The major cause of this attack is improper user input validation, which allows output to contain malicious data. A script entered by a malicious user can be injected into the website's source code. The browser is then unable to determine whether the code that was executed was malicious or not. Because of this, the malicious script is running on the victim's browser or users are seeing bogus forms.

This attack happens when a malicious user locates the website's weak points and submits the information as appropriate harmful input. The output is delivered to the user after a malicious script has been inserted into the source code.

QUESTION 5

WSDL:

A web service is described in a WSDL file. Using these key components, it describes the service's location and its procedures <message>, <binding>, <portType>, <types>. It is an XML document.

SOAP:

It is XML-based protocol that enables data transmission between programs through a certain protocol (like HTTP or SMTP, for example). Its name is Simple Object Access Protocol, and it communicates information using XML as its message format.

REST:

Representational State Transfer is an architecture for networked systems. Although it does employ standards like HTTP, URL, XML, etc., it is not a standard in and of itself.