Illustrate the different phases of Waterfall model.	The sequential phases in Waterfall model are: 1) Requirement Gathering and analysis All possible requirements of the system to be developed are captured in this phase and documented in a requirement specification doc. 2) System Design: The requirement specifications from first phase are studied in this phase and system design is prepared. System Design helps in specifying hardware and system requirements and also helps in defining overall system architecture. 3) Implementation: With inputs from system design, the system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality which is referred to as Unit Testing. 4) Integration and Testing: All the units developed in the implementation phase are integrated into a system after testing of each unit. Post integration the entire system is tested for any faults and failures. 5) Deployment of system: Once the functional and non functional testing is done, the product is deployed in the customer environment or released into the market. 6) Maintenance: There are some issues which come up in the client environment. To fix those issues patches are released. Also to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment.
Summarize risk management throughout the lifetime of the project.	✓ Project Communication ✓ Steering Team ✓ Project Core Team ✓ Scope Management ✓ Risk Management ✓ Meetings, Reviews and Control Issues ✓ Project Leadership

Outline the different models implented by software requirement.	1) Waterfall Model 2) Iterative Model 3) Spiral Model 4) V-Model 5) Big Bang Model 6) Agile Model
Outline various testing approaches of software development.	The following are some of the most common testing approaches: 1) Unit testing - Individual component is in a controlled environment where programmers validate data structure, logic, and boundary conditions. 2) Integration testing - Verifying that components work together as outlined in design specifications. 3) Acceptance testing - Ensuring that the code meets customer requirements. 4) Regression testing - After a change to a system takes place, retesting to ensure functionality, performance, and protection.
Illustrate the components of client-server model.	There are three components to client-server environments: the client, the server (there may be multiple servers), and the network. • The network bridges the physical and functional separation between the client and the server. • The multiple connections possible between clients and multiple servers really provides the visual of a web or network. • Networks provide a flexible environment where clients can mix and match hardware, software, and operating systems. • The characteristics that make client-servers popular also makes it the most vulnerable to breach in security. • It is precisely the distribution of services between client and server that open them up to damage, fraud, and misuse.

Outline the different categories of security concerns associated with cloud computing.	Security concerns associated with cloud computing fall into two broad categories: 1. Security issues faced by cloud providers. 2. Security issues faced by their customers
Outline the different characteristics of good project management.	✓ Moving in the right direction. ✓ Allocates the necessary resources. ✓ Provides the necessary information. ✓ Plans for the worst yet hopes for the best.
Summarize Agile model.	Agile SDLC model is a combination of iterative and incremental process models with focus on process adaptability and customer satisfaction by rapid delivery of working software product. Agile model believes that every project needs to be handled differently and the existing methods need to be tailored to best suit the project requirements. In agile the tasks are divided to time boxes (small time frames) to deliver specific features for a release. Iterative approach is taken and working software build is delivered after each iteration. Each build is incremental in terms of features; the final build holds all the features required by the customer.

Outline the ways to prevent Cross Site scripting?	Different ways to prevent cross site scripting are - 1) User input escaping (escaping special symbols like <, >, % etc and use other text instead of these symbols) 2) Consider all input as threat (Sanitize all inputs) 3) Data validation (as per specific format like email etc) 4) Sanitize data (eliminate script – tag or using regular expression) 5) Encode output (encoding url for input and output) 6) Use right response headers (decide what data can be sent or received) 7) Use content security policy (standard to avoid XSS)
Summarize SQL injection.	SQL Injection is a code injection technique used to execute malicious SQL statements. SQL injection (SQLi) is a cyberattack that injects malicious SQL code into an application, allowing the attacker to view or modify a database. According to the Open Web Application Security Project, injection attacks, which include SQL injections, were the third most serious web application security risk in 2021. In the applications they tested, there were 274,000 occurrences of injection. To protect against SQL injection attacks, it is essential to understand what their impact is and how they happen so you can follow best practices, test for vulnerabilities, and consider investing in software that actively prevents attacks.

Illustrate active and passive attacks.	Active attacks: An Active attack attempts to alter system resources or affect their operations. Active attacks involve some modification of the data stream or the creation of false statements. Types of active attacks are as follows: • Masquerade • Modification of messages • Repudiation • Replay • Denial of Service Passive attacks: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission. The goal of the opponent is to obtain information that is being transmitted. Types of Passive attacks are as follows: • The release of message content • Traffic analysis

Illustrate a session id using PHP on a web page.	In order to create a session, you must first call the PHP session_start function and then store your values in the $_SESSION array variable.
	Let's suppose we want to know the number of times that a page has been loaded, we can use a session to do that.
	The code below shows how to create and retrieve values from sessions
	<?php
	
	session_start(); //start the PHP_session function
	
	if(isset($_SESSION['page_count']))
	{
	$_SESSION['page_count'] += 1;
	}
	else
	{
	$_SESSION['page_count'] = 1;
	}
	echo 'You are visitor number ' . $_SESSION['page_count'];
	
	?>
	Output:
	You are visitor number 1

Compare session and cookie with an example.	Difference Between Session and Cookies : Cookie Session Cookies are client-side files on a local computer that hold user information. Sessions are server-side files that contain user data. Cookies end on the lifetime set by the user. When the user quits the browser or logs out of the programmed, the session is over. It can only store a certain amount of info. It can hold an indefinite quantity of data. Because cookies are kept on the local computer, we don't need to run a function to start them. To begin the session, we must use the session start() method. Cookies are not secured. Session are more secured compare than cookies. Cookies stored data in text file. Session save data in encrypted form. Cookies stored on a limited data. Session stored a unlimited data. In PHP, to get the data from Cookies, $_COOKIES the global variable is used In PHP , to set the data from Session, $_SESSION the global variable is used.
Summarize attack surface.	The Attack Surface describes all of the different points where an attacker could get into a system, and where they could get data out. • The Attack Surface of an application is: • The sum of all paths for data/commands into and out of the application. • The code that protects these paths (including resource connection and authentication, authorisation, activity logging, data validation and encoding), and all valuable data used in the application, including secrets and keys, intellectual property, critical business data, personal data and PII. • The code that protects these data (including encryption and checksums, access auditing, and data integrity and operational security controls).

Outline the significant characteristics of distributed systems.	Three significant characteristics of distributed systems are: 1. Concurrency of components 2. Lack of a global clock 3. Independent failure of components.
Illustrate mobile environment security issues.	Concern is the security of personal and business information now stored on smartphones - as more and more users and businesses use smartphones to communicate, but also to plan and organise their users' work and also private life. • Smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company. • Attacks exploit weaknesses inherent in smartphones that can come from the communication mode—like Short Message Service, MMS, emails, social networking sites, Wi-Fi, Bluetooth and the cellular network itself.

Compare ActiveX to Applets.	• The main security difference between Java applets and ActiveX controls is that Java sets up a sandbox for the applet code to execute in, and this restricts the code's access to resources within the user's computer. • ActiveX uses Authenticode technology, which relies on digital certificates and trusting certificate authorities. • Although both are extremely important and highly used technologies, they have inherent flaws. • Java has not been able to ensure that all code stays within the sandbox, which has caused several types of security compromises. • Authenticode does not necessarily provide security in fact, it often presents annoying dialogue boxes to users. • Since most users do not understand this technology, they continually click OK because they do not understand the risks involved.
Summarize Signature-based detection in detail.	• Signature-based detection (also called as fingerprint detection) is an effective way to detect malicious software, but there is a delayed response time to new threats. • Once a virus is detected, the antivirus vendor must study it, develop and test a new signature, release the signature, and all customers must download it. • Since new malware is released daily, it is hard for antivirus software to keep up. • The technique of using signatures means, this software can only detect viruses that have been identified and where a signature is created.

Illustrate code injection vulnerabilities.	The injection method sends invalid data/request by the attacker to the web application having intention to do something that the application was not designed to perform. In this way, the attacker may be able to insert code that the application will then execute. The intension is to enter the database commands as input, and the application converts it into a query that includes the attacker's command and sends it to the database. When it gets executed, it provides an attacker with the desired information.
Illustrate URL Interpretation Attack.	• URL Interpretation attack is also termed as URL poisoning in which an attacker manipulates the URL by changing the semantics of URL while keeping the syntax unchanged. • The parameters of URL are adjusted so that information beyond what is intended can be retrieved from the web server.
Analyze authentication attack.	This is a type of attack in which the attacker targets and attempts to exploit the process of authentication over a web site by verifying the identity of the user, service or application.
Outline the different ways to implement Two-factor Authentication (2FA).	There are a number of ways to implement 2FA technology, including: • RSA tokens • Code generators such as Google Authenticator • Duo and SMS text messaging of one-time codes

Analyze the term authorization.	Authorization is a way to enforce policies and determine the types or qualities of activities, resources, and services for a user.
Analyze Buffer overflow.	• This is performed by exploiting the buffer overflow issue and by overwriting the memory of an application. • This changes the program's execution path, triggering a response that damages files or exposes private information. Eg. An attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.
Outline some examples of input validation attack.	Examples of input validation attacks include: • Buffer overflow, • Directory traversal / Canonicalization Attack • Cross-site scripting and • SQL injection.
Analyze Clickjacking attack.	An attacker may perform Clickjacking attack by exploiting HTML Iframe web application vulnerability and protection methods.

Illustrate the role of a System Analyst in SDLC.	The system analyst is a person who is thoroughly aware of the system and guides the system development project by giving proper directions. He is an expert having technical and interpersonal skills to carry out development tasks required at each phase.
Illustrate the concept of Economic feasibility.	An evaluation of economic feasibility must include reliable estimates of the economic benefits and costs of the project. If the benefits generated by a project exceed project costs, then the project is considered to be economically feasible.
Predict the best SDLC model.	SDLC – is a continuous process, which starts from planning the project, and it ends at the moment of its launch. The reason for having many SDLC models is that they have specific features and weaknesses that can't be tailored to all projects. Where the Agile model works well, Waterfall can decrease the project workflow and create many problems. The suitable SDLC model should meet the specific requirements and concerns of the project to drive success. Otherwise, it may have a negative impact on the project and the team itself.
Analyze the term DNS rebinding.	DNS rebinding is a type of attack in which the victim's web browser turns into a proxy and let the attacker to run client-side script (JavaScript) for attacking private networks.