1) what are the predefined functions in collection in java?

Ans : In Java, predefined methods are the method that is already defined in the Java class libraries is known as predefined methods. It is also known as the standard library method or built-in method. We can directly use these methods just by calling them in the program at any point. Some pre-defined methods are length(), equals(), compareTo(), sqrt(), etc. When we call any of the predefined methods in our program, a series of codes related to the corresponding method runs in the background that is already stored in the library.

2) what are the underlying ds for linked list and arraylist in java?

Ans : It is similar to an ArrayList, in that an array is used as the underlying data structure. A linked list is composed of a series of nodes, with each node linked to the next. The linked list is traversed by calling something like node.next() on the current node until the target or the end of the list is reached

3) what are the advantages and disadvatages of array list?

Ans : ADVANTAGES : An ArrayList shrinks and grows as needed in a program, whereas an array has a fixed length that is set when the array is created.

In an ArrayList list, the last slot is always list.size()-1, whereas in a partially filled array, you, the programmer,must keep track of the last slot currently in use.

For an ArrayList, you can do insertion or deletion with just a single statement. Any shifting of elements is handled automatically. In an array, however, insertion or deletion requires you to write the code that shifts the elements.

DISADVANTAGES : Time Complexity — If a new data is added or removed from an ArrayList data in entire list has to be shifted to update it which will result into a time complexity of o(n).

ArrayList have a sequential memory representation , so larger the list more complex it is to get allocated in the memory

ArrayList is loosely typed so boxing and unboxing takes place which hits its performance.

ArrayLists cannot hold primitive data types such as int, double, char, and long (they can hold String since String is an object, and wrapper class objects (Double, Integer).

ArrayList is unsynchronised, making them, therefore, not thread safe. With that difference in mind, using synchronisation will incur a performance hit. So if you don't need a thread-safe collection, use the ArrayList .

4) What are iterators and cursors?

Ans : We use cursors when we want to get objects from a Collection one by one. There are 3 cursors in JAVA :

1. Enumeration

We can use Enumeration to get objects one by one from legacy collection object. To create Enumeration object we have to use 'elements()' method of Vector Class (i.e. public enumeration elements()).

2. Iterator

Unlike Enumeration, Iterator is applicable to all Collection (Interface), that means Iterator is a Universal Cursor.

In Enumeration, we get only read access over objects, we couldn't remove objects. But in case of Iterator, we can both read and remove objects.

3. List Iterator

List Iterator is the child interface of Iterator.

List Iterator is a bidirectional cursor, which means we can move both in forward and reverse (backward) direction.

By using List Iterator we can perform addition, removal, and replacement operations on elements in a Collection.

5)what are the 10 OWASP?

Ans : The Open Web Application Security Project (OWASP) is a non profit organization dedicated to improving software security.

The OWASP operates on a core principle that makes all of its material freely available and accessible on its website. This open community approach ensures that anyone and any organization can improve their web application security.

Injection

Injection attacks occur when untrusted data is injected through a form input or other types of data submission to web applications. A common type of injection attack is a Structured Query Language injection, which occurs when cyber criminals inject SQL database code into an online form used for plaintext.

Broken Authentication

Authentication vulnerabilities can enable attackers to gain access to user accounts, including admin accounts that they could use to compromise and take full control of corporate systems.

Sensitive Data Exposure

Sensitive data exposure or data leakage is one of the most common forms of cyberattack. Sensitive data, like credit card information, medical details, Social Security numbers, and user passwords, can be exposed if a web application does not protect it effectively. Attackers who are able to access and steal this information can use it as part of wider attacks or sell it to third parties.

XML External Entities (XXE)

XXE attacks target web applications that parse the Extensible Markup Language (XML). They occur when an XML input that contains a reference to an external entity, such as a hard drive, is processed by an XML parser with weak configuration. XML parsers are often vulnerable to an XXE by default, which means developers must remove the vulnerability manually.

Broken Access Control

Access control refers to the specific data, websites, databases, networks, or resources that users are allowed to visit or have access to. Broken access controls result in users having access to resources beyond what they require. This enables attackers to bypass access restrictions, gain unauthorized access to systems and sensitive data, and potentially gain access to admin and privileged user accounts.

Security Misconfigurations

Security misconfigurations are considered the most common vulnerability in the OWASP Top 10. They are most frequently caused by organizations using default website or content management system (CMS) configurations, which can inadvertently reveal application vulnerabilities. Common misconfigurations also include failing to patch software flaws, unused web pages, unprotected directories and files, default sharing permissions on cloud storage services, and unused or unnecessary services.

Cross-site Scripting (XSS)

It occurs when web applications enable users to submit custom code into URL paths or public websites. XSS attacks take place when cyber criminals inject malicious scripts into a website, which enables them to modify the website’s display. The attacker then relies on victims visiting the page from a browser to execute their code, which they typically achieve through social engineering or embedding malicious links into phishing emails. Exploiting an XSS vulnerability can give an attacker full control of browsers and enable them to inject malicious JavaScript code into websites.

Insecure Deserialization

In data storage and computer science terms, serialization means converting objects, or data structures, into byte strings. Deserialization means converting those byte strings into objects. Insecure deserialization involves attackers tampering with data before it has been deserialized.

OWASP protection advice regarding insecure deserialization revolves around super cookies that contain serialized information about users. If attackers can successfully deserialize an object, they may be able to give themselves an admin role, serialize the data, and compromise entire web applications.

Using Components with Known Vulnerabilities

Software components like frameworks and libraries are often used in web applications to provide specific functionalities, such as sharing icons and A/B testing. However, these components can often result in vulnerabilities that, unknown to the developers, provide a security hole for an attacker to launch a cyberattack.

Insufficient Logging and Monitoring

Many web applications do not do enough to detect data breaches, which sees attackers not only gain unauthorized access to their systems but also enable them to linger for months and years. Organizations need to log and monitor their applications for unusual or malicious behavior to prevent their websites from being compromised.

6)can catch be return without try in java?

Ans : No, catch cannot be returned without try.

7)can try be return catch in java?

Ans : Yes, we can have try without catch block by using finally block. You can use try with finally.

8)can finally be return without try catch in java?

Ans : The finally block always executes when the try block exits. So you can use finally without catch but you must use try.

9)diffarence b/w comparable and comparator in java?

Ans :

1) Comparable provides a single sorting sequence. In other words, we can sort the collection on the basis of a single element such as id, name, and price.	The Comparator provides multiple sorting sequences. In other words, we can sort the collection on the basis of multiple elements such as id, name, and price etc.
2) Comparable affects the original class, i.e., the actual class is modified.	Comparator doesn't affect the original class, i.e., the actual class is not modified.

3) Comparable provides compareTo() method to sort elements.	Comparator provides compare() method to sort elements.
4) Comparable is present in java.lang package.	A Comparator is present in the java.util package.
5) We can sort the list elements of Comparable type by Collections.sort(List) method.	We can sort the list elements of Comparator type by Collections.sort(List, Comparator) method.