(1) Mention what are the categories of defects?

~ **Data Quality/Database Defects:** Deals with improper handling of data in the database.
Examples:
  ~ Values not deleted/inserted into the database properly
  ~ Improper/wrong/null values inserted in place of the actual values

~ **Critical Functionality Defects:** The occurrence of these bugs hampers the crucial functionality of the application. Examples: - Exceptions

~ **Functionality Defects:** These defects affect the functionality of the application.
Examples:
  ~ All JavaScript errors
  ~ Buttons like Save, Delete, Cancel not performing their intended functions

~ **Security Defects:** Application security defects generally involve improper handling of data sent from the user to the application. These defects are the most severe and given highest priority for a fix.
Examples:
  ~ Authentication: Accepting an invalid username/password
  ~ Authorization: Accessibility to pages though permission not given

~ **User Interface Defects:** As the name suggests, the bugs deal with problems related to UI are usually considered less severe.
Examples:
  ~ Improper error/warning/UI messages
  ~ Spelling mistakes
  ~ Alignment problems

(2) Difference between Priority and Severity?

S.N.	Priority	Severity
1.	Defect Priority has defined the order in which the developer should resolve a defect.	Defect Severity is defined as the degree of impact that a defect has on the operation of the product.
2.	Priority is associated with scheduling.	Severity is associated with functionality or standards.
3.	Priority indicates how soon the bug should be fixed.	Severity indicates the seriousness of the defect on the product functionality.
4.	Priority of defects is decided in consultation with the manager/client.	QA engineer determines the severity level of the defect.
5.	Priority is driven by business value.	Severity is driven by functionality.
6.	Its value is subjective and can change over a period of time depending on the change in the project situation.	Its value is objective and less likely to change.
7.	High priority and low severity status indicates defects have to be fixed on immediate basis but does not affect the application.	High severity and low priority status indicates defects have to be fixed but not on immediate basis.

8.	Priority status is based on customer requirements.	Severity status is based on the technical aspect of the product.
9.	During UAT the development team fixes defects based on priority.	During SIT, the development team will fix defects based on the severity and then priority.
10.	Priority is categorised into three types ● Low ● Medium ● High	Severity is categorised into five types ● Critical ● Major ● Moderate ● Minor ● Cosmetic

(3) What is the Bug Life Cycle?

~ Bug life cycle is nothing but the various phases a bug undergoes after it is raised or reported.

~ The different phases of Bug life cycle are,

- ~ New or Opened
- ~ Assigned
- ~ Fixed
- ~ Tested
- ~ Closed

(4) What is priority?

~ Priority is Relative and Business-Focused.

~ Priority defines the order in which we should resolve a defect.

~ This priority status is set by the tester to the developer mentioning the

~ time frame to fix the defect.

~ If high priority is mentioned then the developer has to fix it at the earliest.

~ The priority status is set based on the customer requirements.

~ 3 types of categories:

- ~ Low
- ~ Medium
- ~ High

(5) What is the severity?

~ Severity is absolute and Customer-Focused.

~ It is the extent to which the defect can affect the software.

~ In other words it defines the impact that a given defect has on the system.

~ 4 type of categories:

- ~ Critical
- ~ Major
- ~ Medium
- ~ Low

(6) Bug categories are…

~ Software bugs can be classified into multiple categories based on their nature and impact. Broadly speaking, these categories include Functional Bugs, Logical Bugs, Workflow Bugs, Unit Level Bugs, System-Level Integration Bugs, Out of Bound Bugs, and Security Bugs.

(7) Advantage of Bugzilla?

~ It is an open source widely used bug tracker.
~ It is easy to use and its user interface is understandable for people without technical knowledge.
~ It easily integrates with test management instruments.
~ Advanced search capabilities.
~ E-mail Notifications.
~ Modify/file Bugs by email.
~ Time tracking.
~ It automates documentation.

(8) Explain the difference between Authorization and Authentication in Web testing.What are the common problems faced in Web testing?

S.N.	Authorization	Authentication
1.	In the authorization process, the person's or user's authorities are checked for accessing the resources.	In the authentication process, the identity of users are checked for providing access to the system.
2.	In this process, users or persons are validated.	In the authentication process, users or persons are verified.
3.	This process is done after the authentication process.	It is done before the authorization process.
4.	It needs the user's privilege or security levels.	It usually needs the user's login details.
5.	It determines What permission does the user have?	Authentication determines whether the person is a user or not.
6.	Generally, transmit information through an Access Token.	Generally, transmit information through an ID Token.
7.	The user authorization is not visible at the user end.	The user authentication is visible at the user end.
8.	The authorization permissions cannot be changed by the user as these are granted by the owner of the system and only he/she has the access to change it.	The authentication credentials can be changed in part as and when required by the user.
9.	The user authorization is carried out through the access rights to resources by using roles that have been pre-defined.	The user authentication is identified with username, password, face recognition, retina scan, fingerprints, etc.
10.	Ex: After an employee successfully authenticates, the system determines what information the employees are allowed to access.	Example: Employees in a company are required to authenticate through the network before accessing their company email.