Most Commonly Asked API Interview Questions

What is API Testing?

API (Application Programming Interface) testing focuses on verifying the functionality, reliability, performance, and security of APIs. An API is a set of rules that allows one software application to interact with another.

How API Testing Works?

API testing involves sending requests to an API endpoint and analyzing the responses to ensure the API behaves as expected. The process is

- Understand the API Requirements with available endpoints, request/response formats, authentication requirements
- Set Up the Testing Environment by getting necessary credentials or API keys for authentication
- Choose Testing Tools like Postman and Rest Assured
- Design and Execute Test Cases by sending requests to the API endpoints with proper input parameters, headers, and body data.
- Validate the Responses that the returned data matches expected results by ensuring the correct HTTP status codes are returned

Advantages of API Testing

- API testing helps in finding critical bugs early in development before they reach the user interface.
- APIs work independently of the technology or platform being used for the front-end or back-end.
- API tests are quicker to execute compared to UI testing because they bypass rendering processes.
- Fixing bugs at the API level is less costly than addressing them after UI development.

Different HTTP methods

- GET - Retrieve data from the server.
- POST - Create a new resource on the server.
- PUT - Update or replace an existing resource.
- PATCH - Partially update an existing resource.
- DELETE - Remove a resource from the server.

Difference Between URI and URL

- URI - Identifies a resource by its name or location or both and can include URL's.
  Example: https://reqres.in/api/users?page=2
- URL – It includes the location of the resource.
  Example: https://reqres.in

Difference Between Path Parameter and Query Parameter

- Path parameter is part of the URL path itself, typically used to specify a specific resource or resource identifier. It is used in identifying a specific resource or a hierarchical relationship.
  Example: https://api.example.com/users/123
- Query parameter is a key-value pair appended to the end of a URL, often used to filter or refine the results of a request. It is used in applying filters, sorting, or pagination
  Example: https://api.example.com/users?role=admin&status=active

Different types of authorization used in API

- API Key - A unique key is issued to the client, which is sent with each request to authenticate and authorize access.
  Example: GET /api/resource HTTP/1.1 **Authorization:** ApiKey abc123xyz
- Basic Authentication - Clients provide a username and password, typically encoded in Base64, with each request.
  Example: **Authorization:** Basic dXNlcm5hbWU6cGFzc3dvcmQ=
- Bearer Token - Clients use an access token issued by the server to authenticate requests
  Example: **Authorization:** Bearer eyJhbGciOiJIUzI1NiIsIn...
- OAuth - A standard protocol for third-party access delegation without sharing user credentials

HTTP status codes:

- 200 - OK - Indicates a successful operation
- 201 - Created - Used after creating a resource
- 204 - No Content - Indicates a successful operation with no returned data
- 400 - Bad Request - Used when the client sends invalid input or data
- 401 - Unauthorized - Indicates that authentication is required or failed
- 403 - Forbidden - The client is authenticated but not authorized to access the resource
- 404 - Not Found - Used when a resource cannot be located
- 500 - Internal Server Error - Server-side error
- 502 - Bad Gateway - Server received an invalid response
- 503 - Service Unavailable - Server is currently unavailable
- 504 - Gateway Timeout - Server did not receive a timely response

What are the prerequisites of sending an API request?

- Understanding the API with its endpoints, required parameters, HTTP methods, and expected responses and confirm the version of the API interacting with.
- Get Access by obtaining an API key, token, or credentials required for authentication.
- Setup the request with appropriate HTTP method for the operation (e.g., GET, POST, PUT, DELETE) and identify the exact API endpoint to be called, including any required path parameters and include required headers such as Authorization and Content-Type.
- Ensure all required path parameters are included in the endpoint and prepare the payload for methods like POST or PUT in the format expected by the API.
- Prepare test data to verify the API's behavior and responses.

What is JSON, JSONPath, JSONObject and JSONArray?

- JSON (JavaScript Object Notation) is used for representing structured data in API responses for transmitting data between the client and server in RESTful APIs.
- JSONPath is a query language used for navigating and extracting specific elements or data from JSON document
- JSONObject is an object representation of JSON data, where data is stored as key-value pairs.
- JSONArray is a data structure used to represent an **array** (or list) of values in JSON. It can hold multiple elements, which can be of any data type, including other JSON objects or arrays.

Difference Between Serialization and Deserialization

- Serialization is the process of converting an object into a data format (byte stream, JSON, XML).
- Deserialization is the process of converting serialized data back into an object.

What is Webservices and API Testing?

- Web Services Testing focuses on testing services that communicate over a network, such as SOAP or REST. It focuses on testing communication between client and server using web protocols.
- API Testing focuses on testing any kind of API (including web services, database APIs, etc.). It focuses on testing any system-level API, including non-web-based APIs.