**Checklist for Api Testing:**

1.Authentication and Authorization Testing:

Test authentication mechanisms (ex: API keys, tokens, OAuth) to ensure they work correctly.

Verify that users can only access resources they are authorized to access.

Verify that the API enforces proper authentications for all endpoints.

2.Input Validation and Injection Testing:

Test for common injection vulnerabilities, such as SQL injection, XML injection, and JSON injection.

Ensure that all input is properly validated and sanitized to prevent malicious input. (In your API, proper validation means checking the data you receive to make sure it's in the right format and doesn't contain any harmful commands or code. Sanitization means cleaning the data to remove any potentially dangerous parts.)

3. Data Protection Testing:

Check if sensitive data is encrypted in transit (HTTPS) and at rest.

Verify that data exposure is limited to authorized users.

Verify that sensitive data, such as passwords or API keys, are not exposed in responses.

4. Session Management Testing:

Test for session-related vulnerabilities, such as session fixation and session hijacking.

Verify that session management is secure, and sessions expire properly.

5. Error Handling and Information Disclosure Testing:

Check how errors and exceptions are handled to ensure sensitive information is not disclosed.

Test for predictable error messages that could reveal system information.

6. API Rate Limiting and Throttling:

Verify if the API has rate limiting and throttling mechanisms to prevent abuse.

Test the effectiveness of these mechanisms.

7. Security Headers Testing:

Check for the presence and correctness of security headers like Content Security Policy (CSP), X-Content-Type-Options, X-Frame-Options, and X-XSS-Protection.

8.File Upload Testing:

If the API allows file uploads, test for proper validation and handling to prevent file-based attacks.

9 types of API testing 👇👇👇   
   
📌 Smoke Testing   
➡️ Purpose: To quickly check if the API is functional.   
➡️ Focus: Basic functionality validation.   
➡️ Scope: Testing critical paths to ensure that the API is operational without major issues.   
   
📌 Functional Testing   
➡️ Purpose: To validate if the API functions as per its documented specifications.   
➡️ Focus: Testing specific functionality, input parameters, output results, and business logic.   
➡️ Scope: Evaluating the API for various use cases to ensure it meets the defined requirements and expectations.   
   
📌 Integration Testing   
➡️ Purpose: To test interactions between multiple APIs or services.   
➡️ Focus: Validation of data flow and communication between APIs.   
➡️ Scope: Ensuring that APIs can work seamlessly together in an end-to-end scenario, checking if they can exchange data and function collectively.   
   
📌 Regression Testing   
➡️ Purpose: To prevent new changes from breaking existing API functionality.   
➡️ Focus: Re-running previous test cases to check for any regression or unintended side effects.   
➡️ Scope: Verifying that the existing features and behaviors of the API remain intact after making changes or updates.   
   
📌 Load Testing   
➡️ Purpose: To assess API performance under expected loads.   
➡️ Focus: Measuring response times, throughput, and resource utilization during various load conditions.   
➡️ Scope: Testing the scalability of the API and identifying performance bottlenecks or resource limitations.   
   
📌 Stress Testing   
➡️ Purpose: To evaluate how the API performs under extreme loads beyond normal usage.   
➡️ Focus: Pushing the system to its limits to identify its breaking points.   
➡️ Scope: Assessing the robustness and error-handling capabilities of the API under severe stress, helping uncover potential issues.   
   
📌 Security Testing   
➡️ Purpose: To identify vulnerabilities and weaknesses in API security.   
➡️ Focus: Checking authentication, authorization, data protection, encryption, and other security measures.   
➡️ Scope: Protect the API against external threats, such as SQL injection, cross-site scripting (XSS), and unauthorized access.

   
📌 UI Testing   
➡️ Purpose: To validate the interaction between the user interface and APIs.   
➡️ Focus: Ensuring that data is displayed correctly in the user interface when accessed through the API.   
➡️ Scope: Testing the integration of the API with the front-end components to guarantee a smooth user experience.   
   
📌 Fuzz Testing   
➡️ Purpose: To identify vulnerabilities and security issues in the API.   
➡️ Focus: Injecting unexpected, invalid, or malicious data to provoke unexpected behavior.   
➡️ Scope: Revealing potential vulnerabilities that could be exploited by attackers, such as buffer overflows, injection attacks, and data validation weaknesses. 