API Session – Chapter 12

- Authentication Types -

# Authorization

Authorization is a process that verifies whether a user or application has the necessary permissions to access a resource. In API testing, it's crucial because it ensures that only authenticated and authorized users can interact with the API. This helps protect sensitive data and functionalities from unauthorized access or misuse. Properly testing authorization verifies that the API correctly enforces security policies and handles access controls as intended.

Postman supports various types of authorization methods for securing API requests. Here’s a rundown of the most common types you can use and how to configure them in Postman:

# Auth Types

## **1. No Auth**

* **Description**: No authentication is used; the request is sent as-is.
* **Usage**: When the API does not require authentication.
* **Configuration**: Select No Auth from the Authorization tab.

## **2. API Key**

* **Description**: A key is sent as a part of the request header or query parameters.
* **Usage**: Common in APIs where the key is used to identify the client.
* **Configuration**:
  + **Type**: API Key
  + **Key**: Enter the key name as specified by the API (e.g., Authorization or x-api-key).
  + **Value**: Enter the API key value.
  + **Add to**: Choose Header or Query Params depending on where the API expects the key.

## **3. Basic Auth**

* **Description**: Authentication using a username and password encoded in Base64.
* **Usage**: Simple and often used for internal or less secure APIs.
* **Configuration**:
  + **Type**: Basic Auth
  + **Username**: Enter your username.
  + **Password**: Enter your password.
  + Postman will automatically encode these details and add them to the Authorization header.

### Example

Here's a quick example configuration for basic auth:

* **URL**: https://postman-echo.com/basic-auth
* **Method**: GET
* **Authorization:** Basic Auth [ Enter username and password]

Another Example - <https://the-internet.herokuapp.com/basic_auth>

## **4. Bearer Token**

* **Description**: A token is used for authentication, usually in OAuth2.0.
* **Usage**: Common in modern APIs and for services using OAuth2.0.
* **Configuration**:
  + **Type**: Bearer Token
  + **Token**: Enter your bearer token value.
  + Postman will automatically add the token to the Authorization header as Bearer <token>.

## **5. Digest Auth**

* **Description**: A more secure method than Basic Auth, where authentication is done via a digest algorithm.
* **Usage**: Often used in APIs requiring additional security over Basic Auth.
* **Configuration**:
  + **Type**: Digest Auth
  + **Username**: Enter your username.
  + **Password**: Enter your password.
  + **Realm**: (Optional) The authentication realm, if required by the server.
  + **Algorithm**: Select the appropriate algorithm (usually MD5).

### Example

Here's a quick example configuration for basic auth:

* **URL**: https://postman-echo.com/digest-auth
* **Method**: GET
* **Authorization:** Digest Auth [ Enter username and password which will be encrypted and sent]

Another Example - <https://the-internet.herokuapp.com/digest_auth>

## **6. OAuth 1.0**

* **Description**: Authentication using OAuth 1.0a protocol with token-based authorization.
* **Usage**: Common in APIs that use OAuth 1.0 for authentication.
* **Configuration**:
  + **Type**: OAuth 1.0
  + **Consumer Key**: Enter your consumer key.
  + **Consumer Secret**: Enter your consumer secret.
  + **Token**: Enter your access token.
  + **Token Secret**: Enter your token secret.
  + **Signature Method**: Choose the signature method (e.g., HMAC-SHA1).

## **7. OAuth 2.0**

* **Description**: A widely used authorization framework that provides a variety of flows (e.g., Authorization Code, Client Credentials).
* **Usage**: Common in modern applications using OAuth2 for user and app authorization.
* **Configuration**:
  + **Type**: OAuth 2.0
  + **Add auth data to**: Choose Request Headers or Request URL.
  + **Grant Type**: Select the appropriate grant type (e.g., Authorization Code, Client Credentials).
  + **Callback URL**: Enter the redirect URI used in the authorization process.
  + **Auth URL**: The authorization URL where users authenticate.
  + **Access Token URL**: The URL to obtain the access token.
  + **Client ID**: Enter your client ID.
  + **Client Secret**: Enter your client secret.
  + **Scope**: Enter the scope of access required.
  + **State**: (Optional) A state parameter for CSRF protection.
  + Click on Get New Access Token to fetch and use the token.