8. Authentication and Authorization Types in Postman - 1

Authentication vs Authorization

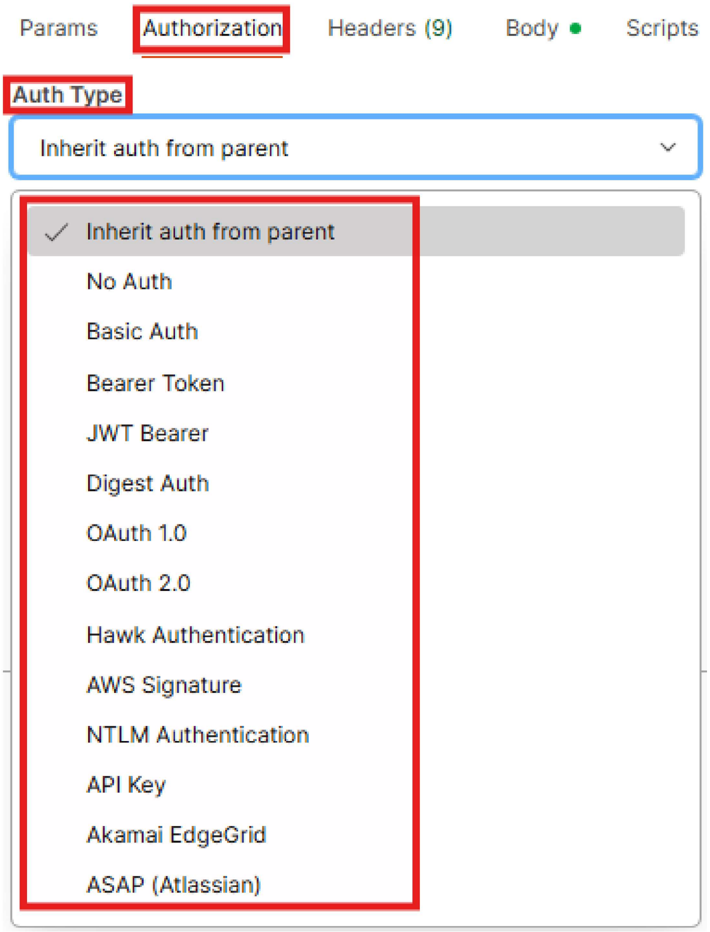
- **Authentication:** Verifies the identity of the user or system trying to access the API, ensuring they are who they claim to be. This step is necessary for securing APIs.

- **Authorization:** Determines what actions or data the authenticated user is permitted to access, controlling their level of access.

- Postman provides various authentication methods through the Authorization tab for secure API access.

Types of Authentications in Postman

- To see types of Authentications in Postman
  - Any Request → Authorization Tab → Auth Type → List of Authorizations



- Some APIs (like JWT, Hawk, Akamai, ASAP, AWS) require special authentication mechanisms specific to that service.

- Application specific Authorizations we cannot simulate in our environment so we will learn about generic ones.

No Auth

- **When to Use:** Public APIs that don't require authentication.

- **Example** → Fetching COVID-19 statistics from a public API.

    - **Request: GET** https://api.rootnet.in/covid19-in/stats/latest
    - **Auth Type:** No Auth

Basic Auth

- **How it works:** Uses a username and password encoded in Base64 into the request header.
- **Use Case:** Accessing a private API on a local server.

Example 1	Example 2
➔ **Request: GET** https://postman-echo.com/basic-auth ➔ **Auth Type:** Basic Auth ◆ Username: postman ◆ Password: password	➔ **Request: GET** http://the-internet.herokuapp.com/basic_auth ➔ **Auth Type:** Basic Auth ◆ Username: admin ◆ Password: admin

Digest Auth

- **How it works:** Similar to Basic Auth, but more secure as it uses encryption.
- **Use Case:** APIs requiring added security over Basic Auth.
- **Example**
    - **Request: GET** https://postman-echo.com/digest-auth
    - **Auth Type:** Digest Auth
        - Username: postman
        - Password: password

API Key

- **How it works:** Uses a unique key provided by the API provider to authenticate.
- **Use Case:** Public APIs like weather, stock market, or basic data access services.
- Postman appends the relevant information to your request Headers or the URL query string.
- **Example** → OpenWeatherMap API
    - **Request: GET** https://api.openweathermap.org/data/2.5/weather?q=Delhi&appid={API key}
    - **Auth Type:** API Key
        - **Key:** appid
        - **Value:** fe9c5cddb7e01d747b4611c3fc9eaf2c
        - **Add to:** Query Params

Bearer Token

- **How it works:** Uses a token as a secure, self-contained identifier for a user or app, containing all necessary validation information for the server.
- **Use Case:** Secure API access without repeated authentication, like accessing user profiles or transaction history.
- The token is a cryptic string, included in the request header.
- **Example** → GitHub API
  - **Request: GET** https://api.github.com/user/repos
  - **Auth Type:** Bearer Token
    - **Token:** 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
  - We need to generate this token from your GitHub account.

Hawk Authentication

- Hawk authentication **verifies (Partial cryptographic verification)** a request(is from a trusted source by creating a special code (signature) from important parts of the request (like the method, URL, timestamp, and payload hash).
- Partial cryptographic verification means it only checks some parts of the request to make sure they haven't been changed, not the whole message.
- The Hawk Authentication parameters are as follows
  - **Hawk Auth ID** - Your API authentication ID value.
  - **Hawk Auth Key** - Your API authentication key value.
  - **Algorithm** - The hash algorithm used to create the message authentication code (MAC).
  - **Advanced parameters (optional, can be left blank)**
    - **User** - The username.
    - **Nonce** - A random string generated by the client.
    - **ext** - Any application-specific information to be sent with the request.
    - **app** - The binding between credentials and the application to prevent an attacker using credentials issued to someone else.
    - **dlg** - The ID of the application the credentials were issued to.
    - **Timestamp** - Timestamp the server uses to prevent replay attacks outside the time window.
- **Example**
  - **Request: GET** https://postman-echo.com/auth/hawk
  - **Auth Type:** Hawk Authentication

        - **Hawk Auth ID:** dh37fgj492je
        - **Hawk Auth Key:** werxhqb98rpaxn39848xrunpaw3489ruxnpa98w4rxn
        - **Algorithm:** sha256
    - Hitting send should give you a response with a status code of 200 OK.

JWT bearer (JSON Web Token)

- An open standard for securely sharing JSON data between parties. The data is encoded and digitally signed, which ensures its authenticity.
- JWT is widely used for data transfer between clients and servers.
- The Hawk Authentication parameters are as follows
    - **Add JWT token to -** Select Request Header or Query Param to specify how the JWT token will be added to your request.
    - **Algorithm -** Select a signing algorithm to use for the JWT token.
    - **Secret -** The secret that's used with the HMAC-SHA algorithm.
    - **Payload -** payload data for your JWT token, in JSON format.
    - **Advanced Configuration (Optional / Auto-generated)**
        - **Request header prefix -** An optional prefix for request headers, not part of the JWT itself.
        - **JWT headers -** Custom headers for the JWT, with algorithm-specific headers added automatically.
- **Example**
    - **Request: GET** https://postman-echo.com/auth/hawk
    - **Auth Type:** JWT bearer
        - **Algorithm:** HS256
        - **Secret:** Mysecret123
        - **Payload:**

```
{
  "iss": "doodle",
  "fruit": "mango"
}
```

    - Hitting send should give you a response with a status code of 200 OK.
- https://jwt.io/introduction
- https://jwt.io/
- https://www.postman.com/postman/postman-team-collections/request/nrrsx27/using-jwt-helper

NTLM Auth

- ➔ **When to Use:** Windows-based enterprise systems.
- ➔ **Example:** Internal company APIs using Active Directory.

AWS Signature

- ➔ **When to Use:** Connecting to Amazon Web Services.
- ➔ **Example:** Uploading files to an S3 bucket.

Akamai EdgeGrid

- ➔ **When to Use:** Secure APIs served through Akamai's CDN, where a URL signature is required for authentication.
- ➔ **Example:** Streaming video content securely over Akamai's CDN.

ASAP (Atlassian Security Architecture and Platform)

- ➔ **When to Use:** Secure communication between Atlassian cloud apps and third-party services using JWT.
- ➔ **Example:** Building a secure integration for Jira or Confluence.