أكاديمية طويق
Tuwaiq Academy

JWT (JSON Web Token)

Prepared By Ahmed Essam Taj

JWT is a method for **authorization** (making sure the user sending the request to the server is the user that logged in and has the authorities to exchange the information). JWT allows us to transmit information as JSON objects and verify information without needing to store session data on the server.

- **How does JWT work?**

When a user logs-in with his credentials the server will generate a JWT (contains user details). The server will then send the JWT token back to the user. Now when the user sends a request the JWT token must be included in the authorization header.

- A typical encoded JWT consist of the following **three parts** (separated by '. ').

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ
zdWIi0iIxMjM0NTY30DkwIiwibmFtZSI6IkpvaG4
gRG91IiwiaWF0IjoxNTE2MjM5MDIyfQ.Sf1KxwRJ
SMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

1- The Header:
   a. Signing Algorithm
   b. Type of Token (JWT)

2- The Payload (user data) like:
   a. Sub → user id
   b. Name

3- The Signature (verify the authenticity of the token):
   a. Combine and hash both the header and the payload using a secret key

- **HTTP Basic Authintication Vs. JWT:**

  - Both are **stateless** (server does not maintain any session state of the user)
  - In Http basic both username and password must be sent with every request, where in JWT a **token** is sent
  - Http basic relies on Https to secure credentials, where in JWT the **token is signed and encrypted**
  - In Http basic credentials are sent repeatedly (no storage on client), where in JWT tokens are **stored on the client** (cookies, local storage).