1. JWT is a secure token used to verify user identity.

It is used in backend application and authorization.

2. A Jwt has 3 parts.

Header

Payload

Signature.

3.

Payload - contains user data (like id, email, role)

Signature - verifies that the token is not modified and it created using secret key.

4. jwt.sign is used to create/generate a new Jwt token

5. jwt.verify is used to verify whether the token is valid or not.

6. ~~why should~~ Jwt

To keep the secreat key secure and prevent exposing it in public code.

7. The token will be invalid, and verification will fail

8. It sets the expiration time for the take

9) Send it in

Response body

Or as an HTTP only cookie

10. Authorization : Bearer <token>

11. 401 - Unauthorized

12. 403 - Forbidden

or

401 - Unauthorized (+b)

13. Authentication - Verifying who the user is (login)

Authorization - Checking what the user is allowed to access

15. By creating a middleware that verifies the token

14. Because the server does not store session data

All user information is stored inside the token itself.