JWT - JSON Web Token

Process :

Client send request to server and server will ask to client that who are you then server send as response JWT with it to client. Next time when client send request to server then it keeps JWT + request send to server and then server will identify or validated this client.



Debugger : <https://jwt.io/#debugger-io>

Header + payload + signature

Header and payload can be change but signature will not change because it contains secret key.

Disadvantages :

1. If we have JWT token then we can decode as well but it is secure because it doesn’t contain any confidential data .
2. JWT steals and send to server – yes but if we usd with oauth then it should be works self protection or either we have to used machanism to handle this.
3. We can not log off jwt token if some one is steal like when session id stolen by some one if we logoff then session will expired and disable but in jwt it won’t happen.

JWT UTIL :

Generate token – generate token for that username

Create token – use jwt and builder of it . and subject means a person who is authenticated successfully. And set date and expire date then finally sign in with it.

Steps :

1. Create maven project
2. Create controller – Home
3. Create welcome rest api – check on postman
4. Create spring security file – customdetailservice and customdetail
5. Create user repo and user model