OAuth - Open Authorization

==========================

primary reason it is built for authorization but later it is also used fo authentication

Terminologies:

==============

1)Resource Owner:- End user

2)Client :- The website/3rd party app which is making request behalf of resource owner

3)Authorization server:- Server which knows about resource owner.

4)Resource Server:- Server where resources that the client want to consumed are hosted

5)Scopes:- granular data that the client wants to access data. Auth server can issue token to clinet with scope of email etc.

OpenId Connect: it is a protocol built on top of Oauth2 Framework which supports Authentication.

==============

\*While OAuth2 provides authorization via access tokens containing scopes.

\*OpenId provides authentication by new token Id which contains new set of information.

Keyclock

========

alternatives amazon cognito/Okta/Forgerock/Spring Authorization Server

First setup auth server at keyclock

Since we have docker installed in our local system we can go with docker

Run the command. use -d to run in detached mode.

now goto that port and login as admin

Realm is like environment.(dev,test,qa)default master realm will be there

\* Clients need to register with auth server

goto->clients->create client-> Select client type as OpenId Connect-> Client Id ending with cc-> enable client authentication-> enable account role and deselect others-> give root url and home url as empty

then, under credentials of client we can find clinet secret which has to be entered by client

How client can connect to auth server

=====================================

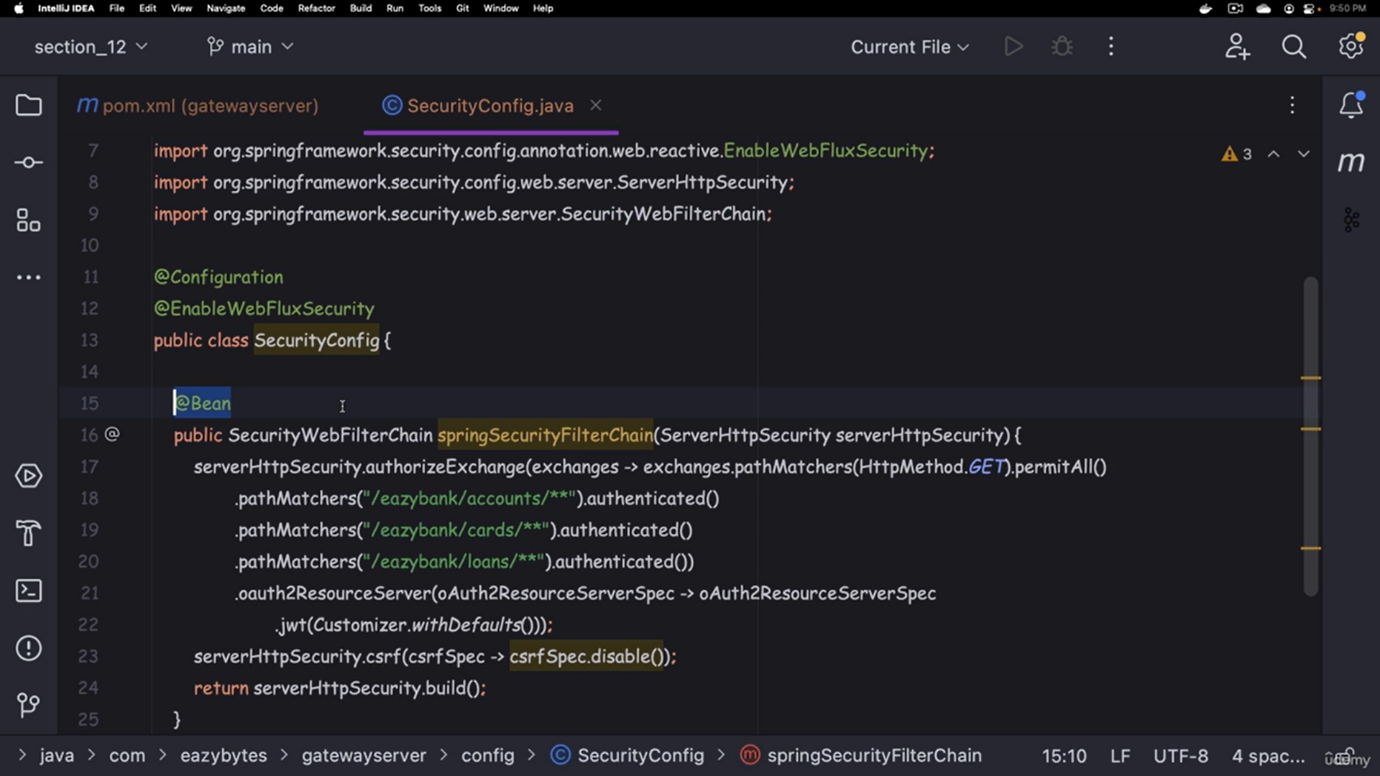
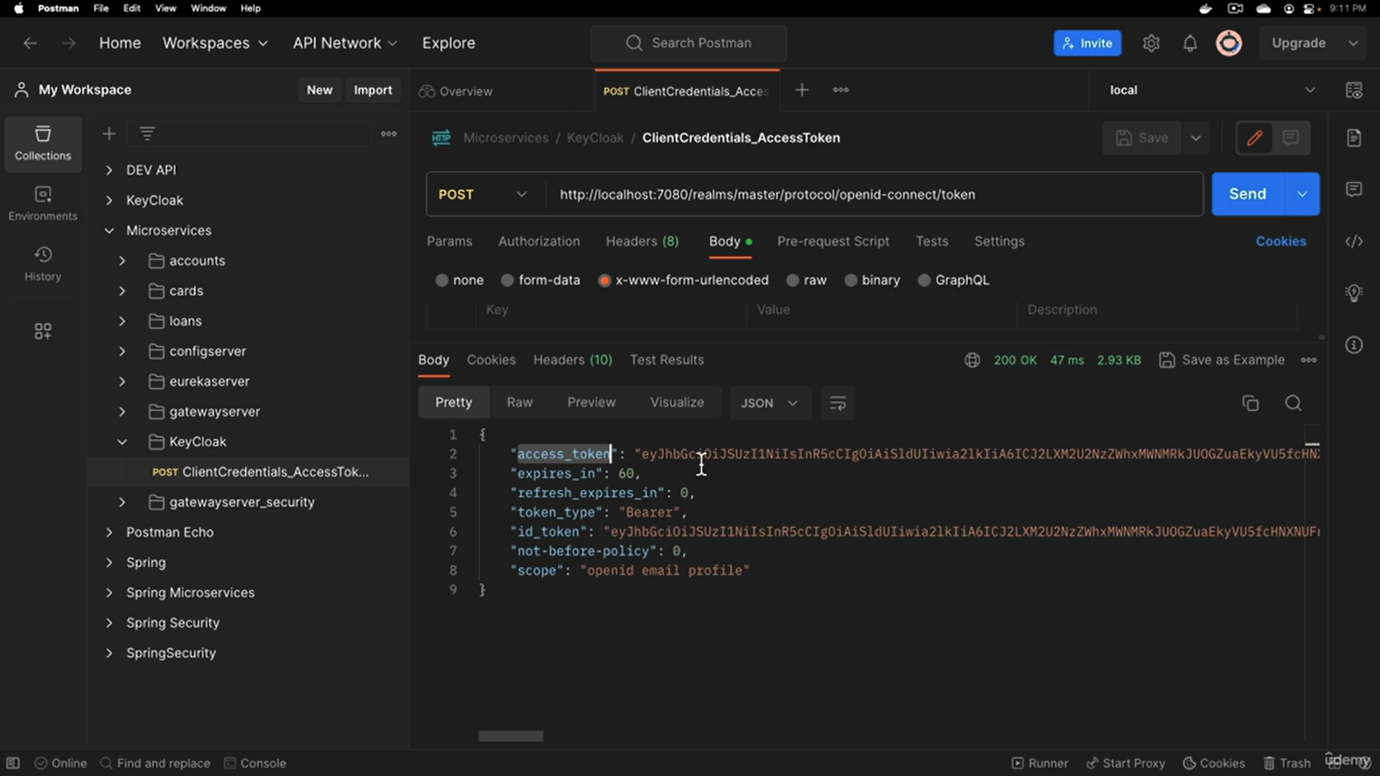
Client need to know url

to get access token clinet needs to invoke endpoint which can be found under realm settings and endpoint settings in admin dashboard

and In postman and needs to send certain details. by default openid scope is present after sending request in response clinet gets access token

in real time app they invoke using java code.A screenshot of a computer

Description automatically generated.



and after it in under resouces application.yaml file configuration should be add with the jwtcert path present in the endpoint settings to check whether this authtoken is valid

