Types of Security:

1. OAuth 2.0 Login

This feature provides the facility to the user to login into the application by using their existing account at GitHub or Google. This feature is implemented by using the Authorization Code Grant that is specified in the OAuth 2.0 Authorization Framework.

1. **Single sign-on**

This feature allows a user to access multiple applications with the help of single account(user name and password).

Security in Microservice

Securing a monolith is very different from securing a microservices application .In a monolith, the client can access the application providing the credentials , and it is used in a session and checked with database . If the user data is in session, the user is authorized to access the functionalities exposed by the app .

In a microservice , the client contacts only the API gateway server . Though securing the API gateway is good , it is not good enough against internal threats . The services can not know the source of the request . They can not determine if the request is coming from a user or another service or some malicious code .

Q1. How to secure API gateway (Zull or spring cloud gateway API) ? How to secure individua microservice ? How to secure configServer ? How other microservice will contact secured configServer ?

ANS : Secure API gate way with Oath

Q2. Encrypt Decrypt properties : The sensitive information, including DB credentials are stored in public repository which is not very secure .

How to encrypt property values in Git and how Git itself decrypt the encrypted value :

Q3. Startup order of the microservices ?

Q4. Spring cloud contract ?