1. Para que serve e para o que foi criado o protocolo OAuth ?

- O objetivo original para o desenvolvimento do OAuth seria proteger as credenciais (senhas) dos usuários ao evitar que fosse necessário inserir sua senha em um aplicativo de terceiro. Portanto, antes do uso do OAuth, quando o usuário ia logar em algum sistema como o Gmail ou o Facebook, o mesmo deveria digitar sua senha diretamente na API do aplicativo, então, o OAuth surgiu para mudar isso. Quando há o uso do OAuth, o usuário não mais precisa inserir sua senha na API de terceiros, pois o mesmo é direcionado (de uma maneira imperceptível) para uma página de login com acesso ao servidor OAuth, salvando então sua senha neste servidor e oferecendo mais segurança ao usuário além de facilitar para a equipe de programação o processo de proteger e manutenir o servidor.

2. Descreva o fluxo do protocolo OAuth na versão 2.0

- O protocolo 2.0 do OAuth segue um fluxo um pouco diferente de sua versão anterior. O fluxo segue da seguinte forma:
    - O cliente envia um pedido de autorização ao dono do recurso (que é aquele capaz de permitir acesso a algum recurso protegido ou um servidor hosteando os recursos protegidos e sendo capaz de fornecer tokens de acesso)
    - O cliente receberá uma autorização que contém uma credencial que pode ser de quatro tipos principais diferentes.
    - O cliente deverá enviar a autorização ao servidor de acesso (que é um servidor capaz de entregar tokens desde que a autorização seja válida)
    - O servidor de acesso irá então validar o cliente e seu código de autorização e desde que seja válido o mesmo receberá um token de acesso para acessar o recurso protegido.
    - o cliente irá requisitar acesso ao recurso e será autenticado ao apresentar o token de acesso
    - o servidor de recurso irá validar o token de acesso e desde que seja válido irá atender ao pedido

1. **Quais os agentes envolvidos ?**
    a. Dono do recurso (é referido como end-user): É aquele capaz de permitir acesso ao recurso protegido ao entregar um código de autorização. (Quando há um end-user
    b. Servidor de recurso: É um servidor onde os recursos protegidos estão “online” e o mesmo tem a capacidade de entregar tokens de acesso como resposta a requisições de acesso.
    c. Cliente: é aquele que faz requisições de recursos protegidos em parte do Dono do Recurso possuindo sua própria autorização

d. Servidor de autenticação: o servidor de autenticação é capaz de fornecer tokens ao cliente após o mesmo ter recebido autorização e a autenticação com sucesso pelo Dono do Recurso.

2. **Qual o fluxo de informação entre estes agentes ?**
    a. O cliente envia uma requisição de acesso ao dono do recurso
    b. O dono do recurso responde com uma autorização (composta por algum código fornecido pelo dono do recurso) e é devolvida ao cliente
    c. O cliente envia uma requisição de acesso ao servidor de autenticação enviando a autorização recebida pelo dono do recurso
    d. O servidor de acesso responde a requisição do cliente com um token de acesso
    e. O cliente envia uma requisição de acesso ao servidor de recurso e enviará também seu token de acesso
    f. O servidor de recurso irá autenticar o token e então irá atender a requisição do cliente

3. Descreva como este serviço, se mal utilizado, pode trazer problemas de segurança para uma empresa.

- Quando não é utilizado de forma correta, ele pode ter consequências terríveis, como um ataque de manipulação de URI. Quando o cliente faz uma requisição de acesso o mesmo tem a possibilidade de redirecionar a URI via “redirect_uri”. Se o invasor puder manipular a URI, ele pode fazer com que o servidor de autorização redirecione o dono do recurso para uma URI sob o controle do atacante. Caso isso aconteça, o atacante então inicia um fluxo comum do protocolo OAuth e quando o usuário é enviado ao servidor de autenticação o atacante então repõe a URI original pela URI sob seu controle e após isso o cliente irá enviar uma requisição que supostamente viria de um cliente confiável e portanto a requisição será autorizada. Após isso a vítima é direcionada para uma página final onde terá o código de autorização onde então o invasor poderá concluir o fluxo de informações e terá acesso aos recursos protegidos do servidor.

4. Cite pelo menos 10 serviços, de grandes empresas provedoras de autorização que utilizam este protocolo.

- Amazon
- Apple
- Discord
- DropBox
- Facebook
- GitHub
- LinkedIn
- PayPal
- Spotify
- Yahoo