E.E. Irene Branco da Silva PEI

São Paulo,8 de outubro, 2024.

OAuth

OAuth é um protocolo de autorização que permite que aplicativos acessem recursos de usuários em outros serviços sem precisar compartilhar suas credenciais. Ele é amplamente utilizado para permitir que aplicativos de terceiros acessem APIs em nome do usuário.

Fluxo de Funcionamento:

1. O usuário se autentica no Authorization Server.
2. O usuário consente em dar acesso ao Client.
3. O Authorization Server emite um token de acesso para o Client.
4. O Client usa o token para acessar os recursos protegidos no Resource Server.

JWT (JSON Web Token)

JWT é um padrão aberto (RFC 7519) que define um formato compacto e independente de transmitir informações entre partes como um objeto JSON. Essa informação pode ser verificada e confiável porque é assinada digitalmente.

Uso do JWT em Autenticação:

1. O usuário se autentica com suas credenciais.
2. O servidor gera um JWT e o envia de volta ao cliente.
3. O cliente armazena o JWT (normalmente em localStorage ou cookies).
4. Em requisições subsequentes, o cliente envia o JWT no cabeçalho de autorização.
5. O servidor verifica a assinatura do JWT e permite o acesso se for válido.

Comparação entre OAuth e JWT:

OAuth é um protocolo de autorização, enquanto **JWT** é um formato de token. OAuth pode usar JWT como formato de token, mas não está limitado a isso. OAuth é útil para acesso a recursos de terceiros, enquanto JWT é frequentemente usado para autenticação em aplicações.

Essas tecnologias são frequentemente usadas juntas em aplicações modernas para garantir segurança e facilitar a interação entre diferentes serviços.