Universidade Evangélica de Goiás – UniEVANGÉLICA

CURSO DE ENGENHARIA DE SOFTWARE

Atividade pré-aula (semana 16)

Antônio Claudio Ferreira Filho

Matrícula: 2110854

Anápolis - GO

2023

Antônio Claudio Ferreira Filho

Atividade pré-aula (semana 16)

Trabalho apresentado à disciplina de Programação Web como requisito parcial para aprovação.

Anápolis – GO

2023

Explique como funciona o processo de autenticação entre duas aplicações:

O processo de autenticação entre duas aplicações geralmente segue um fluxo básico que envolve a verificação da identidade de um usuário ou serviço para permitir o acesso a recursos ou funcionalidades protegidas. Vou explicar o processo geral de autenticação entre duas aplicações:

1. Solicitação de Autenticação: a aplicação que deseja acessar recursos protegidos envia uma solicitação de autenticação para a aplicação responsável pela autenticação, geralmente por meio de uma API ou comunicação direta;
2. Envio de Credenciais: a aplicação solicitante envia as credenciais de autenticação, que podem ser um nome de usuário e senha, um token de acesso ou outras informações necessárias para verificar a identidade do usuário;
3. Validação de Credenciais: a aplicação responsável pela autenticação recebe as credenciais e realiza a validação. Isso pode envolver consultar um banco de dados de usuários, verificar a assinatura de um token ou realizar autenticação em um provedor externo;
4. Geração de Token de Autenticação: se as credenciais forem válidas, a aplicação responsável pela autenticação gera um token de autenticação. Esse token é um identificador único que é enviado de volta para a aplicação solicitante;
5. Armazenamento do Token: a aplicação solicitante armazena o token de autenticação para uso futuro. Isso pode ser feito em um cookie, armazenamento local ou cabeçalho de autorização;
6. Requisição de Recursos: a aplicação solicitante envia requisições para recursos protegidos, incluindo o token de autenticação no cabeçalho da requisição ou em outra forma especificada pela API;
7. Validação do Token: a aplicação que recebe as requisições verifica a validade do token de autenticação. Isso pode envolver a verificação da assinatura do token, a consulta de um banco de dados ou a validação em um provedor externo;
8. Autorização e Acesso aos Recursos: se o token for válido, a aplicação concede acesso aos recursos solicitados, considerando também as permissões associadas ao usuário autenticado;

É importante ressaltar que esse é apenas um fluxo básico de autenticação entre duas aplicações e que podem existir variações dependendo do sistema, das tecnologias utilizadas e dos requisitos de segurança. Além disso, medidas adicionais de segurança, como criptografia de dados, podem ser aplicadas para proteger a transmissão das credenciais e dos tokens de autenticação.