



Autenticação com NodeJs



Quem sou eu?

Henrique Serra

Graduando de Ciência da Computação - UESC.

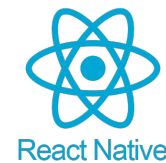
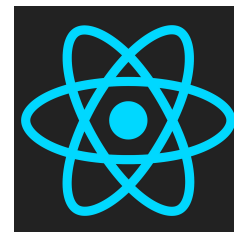
Pesquisador e desenvolvedor blockchain e de criptomoedas.

Desenvolvedor Fullstack com Node, ReactJs e React-Native.

Desenvolveu plataformas de delivery, chatbots, criptomoedas, gestor pecuário, gestor jurídico, plataforma de design integrada com IA e várias outras

Freelancer web e mobile

Atualmente trabalhando com robôs na área jurídica e plataformas cripto





Antes de começarmos





O que veremos?

- O que é autenticação?
- Tipos de autenticação
- Autenticação com JWT
- Permissões



O que é Autenticação?

Autenticação de aplicação é quando a **API exige** que a **aplicação cliente se identifique** para poder acessar os recursos, mesmo que não haja um usuário logado.



Tipos de autenticação

Autenticação	Ambiente ideal	Segurança	Complexidade
Basic Auth	Testes rápidos, APIs internas, protótipos	● Baixa	● Muito baixa
API Key	Identificar aplicações que consomem a API	● Média	● Baixa
Cabeçalho personalizado	APIs simples ou privadas onde você define seu próprio esquema	● Média	● Baixa
Sessão + Cookie	Sites com login tradicional, apps com renderização no servidor	● Média	● Média



Tipos de autenticação

Autenticação	Ambiente ideal	Segurança	Complexidade
JWT (JSON Web Token)	Login de usuários em APIs, mobile e SPA (Single Page Apps)	● Alta	● Média
OAuth 2.0 - Client Credentials	Integrações entre servidores e autenticação de aplicações	● Alta	● Média
OTP via SMS/E-mail	Verificação em dois fatores, login sem senha	● Alta	● Média
TOTP (Authenticator App)	2FA com app como Google Authenticator ou Authy	● Alta	● Média



Tipos de autenticação

Autenticação	Ambiente ideal	Segurança	Complexidade
Magic Link	Login sem senha via link temporário por e-mail	● Alta	● Média
Login Social (OAuth2)	Login com Google, Facebook, GitHub, etc.	● Alta	● Alta
OAuth 2.0 - Authorization Code	Login com provedores (Google, Facebook), apps com frontend + backend	● Alta	● Alta
SAML	Login corporativo (ex: AD, Google Workspace), Single Sign-On	● Alta	● Alta



Tipos de autenticação

Autenticação	Ambiente ideal	Segurança	Complexidade
Mutual TLS (mTLS)	APIs privadas, comunicação entre sistemas internos	● Muito alta	● Alta
Biometria (via terceiros)	Apps mobile com autenticação local ou integração com provedores externos	● Muito alta	● Alta



Autenticação JWT

JWT (JSON Web Token) é um padrão aberto (RFC 7519) para transmitir informações de forma segura entre partes como um objeto JSON compactado e assinado.

Criado em 2015



Autenticação JWT

Um JWT é composto por 3 partes separadas por ponto (.):

HEADER.PAYLOAD.SIGNATURE



Autenticação JWT

Header

```
{  
  "alg": "HS256",  
  "typ": "JWT"  
}
```



Autenticação JWT

Payload (Não é criptografado)

```
{  
  "userId": 1,  
  "role": "admin",  
  "exp": 1715649600  
}
```



Autenticação JWT

Signature

HMACSHA256(

base64UrlEncode(header) + "." + base64UrlEncode(payload),

chave_secreta

)



Vamos codar!



Fim?