Autenticação e Autorização

Francisco Rafael - francisco.rafaell.pereira@gmail.com - CPF: 068.778.653-32

Apresentação do Curso

Apresentação do Curso

- Em um mundo cada vez mais conectado e dependente de APIs e sistemas distribuídos, a segurança é um dos pilares fundamentais do desenvolvimento de software.
- A autenticação e autorização eficazes são cruciais para garantir que os usuários certos tenham acesso aos recursos certos, sem comprometer a integridade do sistema.

Apresentação do Curso

- **Neste curso veremos:**
  - O que é Autenticação e Autorização
  - O que é JWT
  - Criando um JWT - Prática
  - Gerando Migrations para Login - Prática
  - Guardando a senha de forma segura
  - Implementando o Login - Prática
  - Validando o Login
  - Configurando e Validando Permissões - Prática
  - Fundamentos de Recuperação de Senha
  - Implementando Recuperação de Senha - Prática
  - Validando a Recuperação de Senha

Sobre o Instrutor

- **Luis Felipe (LuisDev)**
  - Mais de 7 anos de experiência como Desenvolvedor .NET
  - 4x Microsoft MVP
  - 10x Certificações Microsoft
  - 3x Experiências internacionais remotas para Estados Unidos e Irlanda
  - Mais de 1.000 alunos e centenas de mentorandos
  - Produzindo conteúdo a mais de 6 anos

O que é Autenticação

O que é Autenticação

- É o processo de verificar a identidade de um usuário ou sistema, sendo a primeira etapa de qualquer processo de segurança
- É como garantir que uma pessoa ou aplicação é realmente quem afirma ser
- Isso geralmente é feito através de credenciais, como:
    - Senhas.
    - Código para Acesso.
    - App de autenticação (Google Authenticator, Microsoft Authenticator).
    - Biometria.

O que é Autenticação

- É o processo de verificar a identidade de um usuário ou sistema, sendo a primeira etapa de qualquer processo de segurança
- É como garantir que uma pessoa ou aplicação é realmente quem afirma ser
- Isso geralmente é feito através de credenciais, como:
    - Senhas.
    - Código para Acesso.
    - App de autenticação (Google Authenticator, Microsoft Authenticator).
    - Biometria.
- Podem ser utilizadas através da abordagem de autenticação multifator (MFA), que combina dois ou mais métodos de verificação, como senha e códigos enviados por SMS, para aumentar a segurança.

O que é Autenticação

- É o processo de verificar a identidade de um usuário ou sistema, sendo a primeira etapa de qualquer processo de segurança
- É como garantir que uma pessoa ou aplicação é realmente quem afirma ser
- Isso geralmente é feito através de credenciais, como:
    - Senhas.
    - Código para Acesso.
    - App de autenticação (Google Authenticator, Microsoft Authenticator).
    - Biometria.
- Podem ser utilizadas através da abordagem de autenticação multifator (MFA), que combina dois ou mais métodos de verificação, como senha e códigos enviados por SMS, para aumentar a segurança.
- O resultado da autenticação bem-sucedida é uma identidade verificada, muitas vezes representada por um token ou sessão ativa.

O que é Autorização

O que é Autorização

- É o processo de se conceder permissão a um usuário autenticado
- Essa permissão pode envolver dados e/ou funcionalidades, entre outros recursos
- Por exemplo, no nosso projeto prático, usuários freelancers devem ter permissões diferentes de clientes, por exemplo
    - É essencial garantir que usuários não tenham acesso indevido em nossos sistemas

Autenticação x Autorização

Francisco Rafael - francisco.rafaell.pereira@gmail.com - CPF: 068.778.653-32

Autenticação x Autorização

- **Autenticação:** "Você é quem diz ser?"
  - Código de Erro: 401 Unauthorized.
- **Autorização:** "Você tem permissão para fazer isso?"
  - Código de Erro: 403 Forbidden.

O que é JWT

Francisco Rafael - francisco.rafaell.pereira@gmail.com - CPF: 068.778.653-32

O que é JWT

- JSON Web Token (JWT)
- É um padrão aberto que especifica uma maneira de transmitir dados entre partes de forma segura e compacta através de um objeto JSON
- Por exemplo, pode ser utilizado para troca entre uma aplicação front-end e uma back-end, ou mesmo entre duas aplicações back-end
- Amplamente utilizado para autenticação e autorização em aplicações .NET, e mesmo em outras tecnologias

Estrutura do JSON Web Token (JWT)

Francisco Rafael - francisco.rafaell.pereira@gmail.com - CPF: 068.778.653-32

Estrutura do JSON Web Token (JWT)

- **Header:** Define o tipo de token e o algoritmo de assinatura utilizado, e é codificado para Base64Url

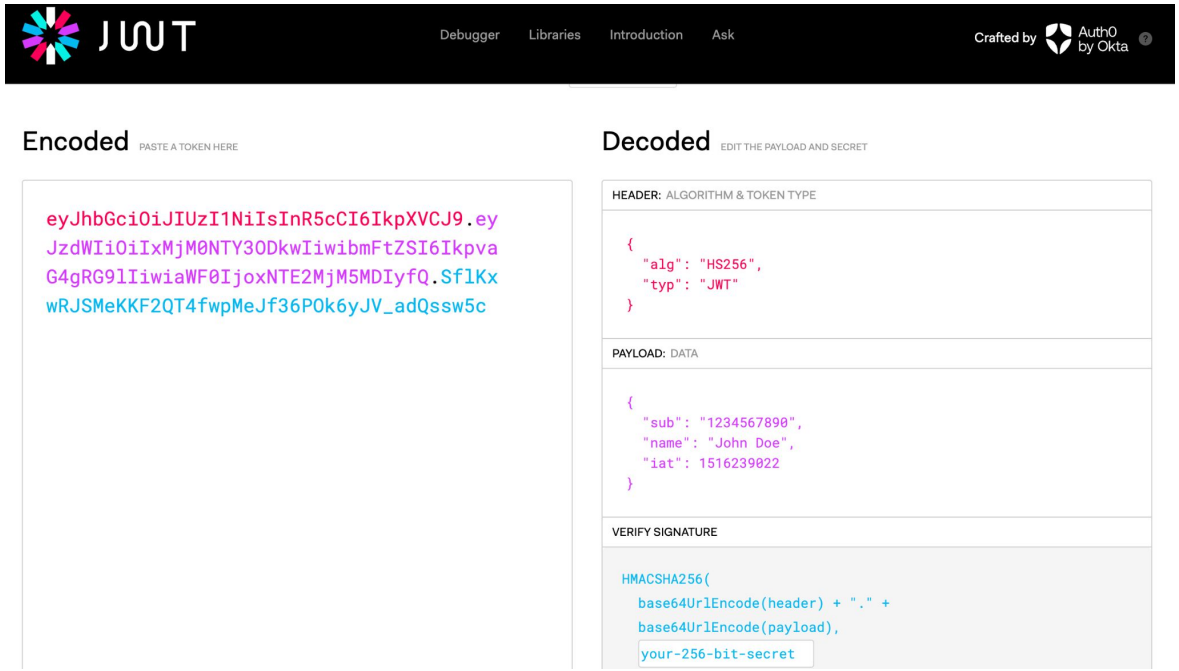
Estrutura do JSON Web Token (JWT)

- **Header:** Define o tipo de token e o algoritmo de assinatura utilizado, e é codificado para Base64Url
- **Payload:** Define as Claims, que são basicamente dados sobre o usuário e dados adicionais, e é convertido para Base64Url

Estrutura do JSON Web Token (JWT)

- **Header:** Define o tipo de token e o algoritmo de assinatura utilizado, e é codificado para Base64Url
- **Payload:** Define as Claims, que são basicamente dados sobre o usuário e dados adicionais, e é convertido para Base64Url
- **Signature:** É obtido através do cabeçalho e payload codificados, um código secreto, o algoritmo especificado no cabeçalho, e então assinado com um algoritmo como HMAC SHA256

Estrutura do JSON Web Token (JWT)



Fundamentos de Recuperação de Senha

Francisco Rafael - francisco.rafaell.pereira@gmail.com - CPF: 068.778.653-32

Fundamentos de Recuperação de Senha

- A recuperação de senhas é uma funcionalidade essencial para ajudar usuários que esqueceram suas credenciais.
- **Elementos da Recuperação de Senhas**
  -

Fundamentos de Recuperação de Senha

- A recuperação de senhas é uma funcionalidade essencial para ajudar usuários que esqueceram suas credenciais.
- **Elementos da Recuperação de Senhas**
  - **Solicitação de redefinição:**
    - O usuário fornece um identificador, como email ou nome de usuário.
    - Um mecanismo de validação, como um token ou link, é enviado ao usuário por um canal seguro.

Fundamentos de Recuperação de Senha

- A recuperação de senhas é uma funcionalidade essencial para ajudar usuários que esqueceram suas credenciais.
- **Elementos da Recuperação de Senhas**
  - **Solicitação de redefinição:**
    - O usuário fornece um identificador, como email ou nome de usuário.
    - Um mecanismo de validação, como um token ou link, é enviado ao usuário por um canal seguro.
  - **Validação:**
    - O sistema verifica a validade do token ou link, sua não expiração e se ele pertence ao usuário correto.

Fundamentos de Recuperação de Senha

- A recuperação de senhas é uma funcionalidade essencial para ajudar usuários que esqueceram suas credenciais.
- **Elementos da Recuperação de Senhas**
  - **Solicitação de redefinição:**
    - O usuário fornece um identificador, como email ou nome de usuário.
    - Um mecanismo de validação, como um token ou link, é enviado ao usuário por um canal seguro.
  - **Validação:**
    - O sistema verifica a validade do token ou link, sua não expiração e se ele pertence ao usuário correto.
  - **Redefinição da senha:**
    - O usuário define uma nova senha que atende aos critérios de segurança.

Considerações de Segurança

Considerações de Segurança

- **Tokens Expirados:** Configure tokens para expirarem após um período razoável (ex.: 24 horas).

Considerações de Segurança

- **Tokens Expirados:** Configure tokens para expirarem após um período razoável (ex.: 24 horas).
- **Senha Forte:** Exija que as novas senhas sigam boas práticas de segurança (comprimento mínimo, caracteres especiais, etc.).

Considerações de Segurança

- **Tokens Expirados:** Configure tokens para expirarem após um período razoável (ex.: 24 horas).
- **Senha Forte:** Exija que as novas senhas sigam boas práticas de segurança (comprimento mínimo, caracteres especiais, etc.).
- **Hashing de Senhas:** Sempre armazene senhas usando algoritmos de hash seguros.

Considerações de Segurança

- **Tokens Expirados:** Configure tokens para expirarem após um período razoável (ex.: 24 horas).
- **Senha Forte:** Exija que as novas senhas sigam boas práticas de segurança (comprimento mínimo, caracteres especiais, etc.).
- **Hashing de Senhas:** Sempre armazene senhas usando algoritmos de hash seguros.
- **Auditoria:** Registre tentativas de redefinição para monitorar possíveis abusos.