experts club

Spring Security : autenticação via JWT com refresh token

24-04-2022

Agenda

experts club

- Quem sou eu
- Objetivo
- O que é JWT?
- Quando usar JWT?
- Como ver o conteúdo de um token jwt?
- O que é refresh token e pra que ele serve?
- Apresentação do projeto base
- Desenvolvimento do projeto

Sobre mim e a minha relação com o código

experts club

- Dev backend na Ame Digital
- Microsoft mvp em developer technologies
- Community Organizer
- Book co-author
- speaker
- content creator @kamila_code
- 4 anos de xp
- https://app.rocketseat.com.br/me/kamila-de-fatima-santos-oliveira-1566497781

O que vamos desenvolver hoje?

experts club

Um projeto que realiza autenticação via JWT com a funcionalidade de refresh token

Ferramentas utilizadas

experts club

Java 11+

Maven

Spring (Web, Security e Data)

JsonWebToken

O que é JWT?

JsonWebToken é um padrão aberto (RFC 7519) que define uma forma compacta e autocontida para o tráfego de informações de forma segura entre as partes como um objeto json.

O que é JWT?

Essas informações são assinadas digitalmente , logo são confiáveis e podem ser verificadas.

O que é JWT?

Essa assinatura dos token jwts pode ser feita usando um segredo ou um par de chaves pública/privada.

Quando usar JWT?

Autorização - cenário mais comum do JWT , após o login da pessoa usuária todas as solicitações serão feitas usando um token JWT (será o que iremos fazer nessa aula).

Quando usar JWT?

Troca de informações: os Tokens JWTs são uma alternativa bem segura para troca de informações pois eles podem ser assinados e essa assinatura usa seu cabeçalho e seu conteúdo , se algo foi adulterado será possível saber.

Como ver o conteúdo de um token jwt?

experts club

Vá na seção debugger desse site:

https://jwt.io/

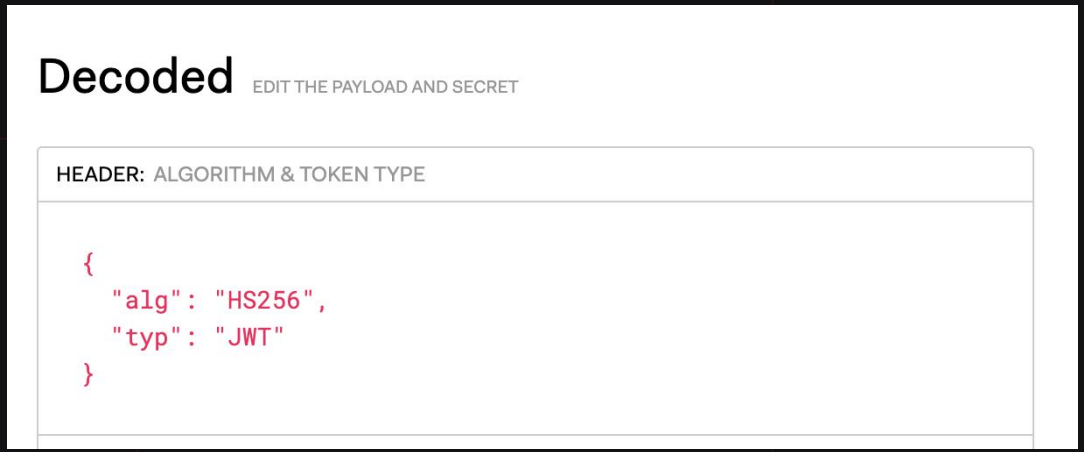
Como ver o conteúdo de um token jwt?

Entendendo cada parte do token JWT (usando o exemplo default do site nesse momento):

Como ver o conteúdo de um token jwt?

experts club

Header: geralmente contém a informação do titpo e Token (JWT) e o algoritmo de assinatura, que nesse caso é o HS256 (mesmo que vamos usar na nossa aplicação)



Como ver o conteúdo de um token jwt?

experts club

Payload: Contém as claims que são declarações sobre a entidade (pessoa usuária) e mais alguns dados adicionais, por ex:

PAYLOAD: DATA


```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

Como ver o conteúdo de um token jwt?

sub (subject): a quem o token se refere

iat (Issued at): Timestamp de quando o token foi criado

name: nome da pessoa usuária que esse token pertence

Como ver o conteúdo de um token jwt?

Signature: A assinatura é composta por: cabeçalho codificado em base 64 + payload codificado em base 64 + o segredo que definimos na geração do token + e o algorirmo de hash que escolhemos no cabeçalho

Como ver o conteúdo de um token jwt?

experts club

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

O que é refresh token e pra que ele serve?

experts club

Por motivos de segurança os tokens JWTs que são gerados ao realizar login possuem um determinado prazo de "validade". Quando eles expiram podemos (o app que usa o token) atualizar esse token de acesso prolongando sua validade.

O que é refresh token e pra que ele serve?

Ou seja, refreshs tokens servem para que o app cliente que usa esse token renove o token sem precisar que a pessoa usuária faça login novamente.

Projeto base

experts club

Iremos partir do projeto desenvolvido na aula anterior dessa série de Spring Security:

https://github.com/rocketseat-experts-club/spring-security-password-encoder-bcrypt-2022-02-07

Projeto base

experts club

Se quiser assistir a aula sobre bcrypt que originou esse código:

https://app.rocketseat.com.br/experts-club/lesson/spring-security-vantagens-e-aplicacao-de-password-encoding-usando-bcrypt-e-pontos-fracos-do-md-5-hash

Desenvolvimento do projeto

Vamos evoluir esse projeto para que:

- Tenha um endpoint de login
- Receba um Bearer Token JWT como autenticação
- Retorne um token e um refresh token na resposta

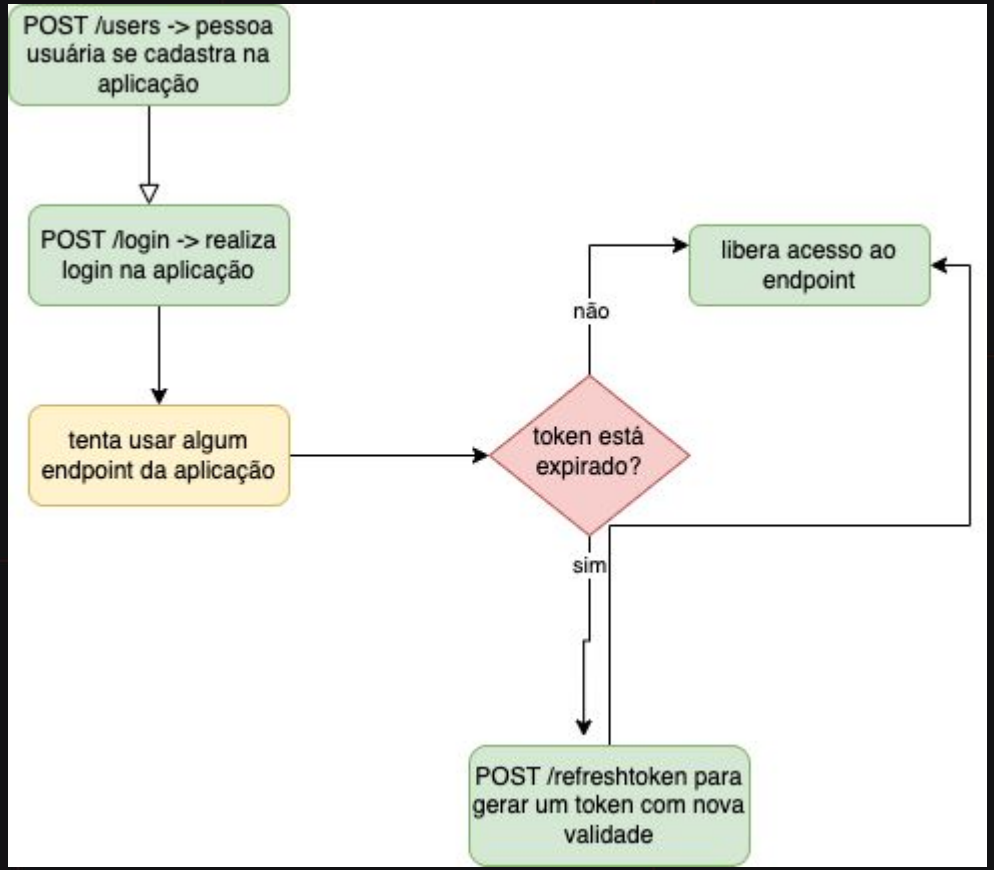
Desenvolvimento do projeto

Vamos evoluir esse projeto para que:

- Valide se o token está expirado
- Tenha a funcionalidade de gerar um refresh token e permita que a pessoa usuária continue usando a aplicação com ele

Fluxo do projeto

experts club



Referências e onde saber mais

experts club

https://jwt.io/introduction

https://jwt.io/

https://auth0.com/blog/refresh-tokens-what-are-they-and-when-to-use-them/

experts club

Obrigada !

Kamila Santos
https://youtube.com/Kamilacode
https://github.com/Kamilahsantos
https://www.linkedin.com/in/kamila-santos-oliveira/
https://www.instagram.com/kamila_code/