Introdução à segurança

Há várias formas de lidar segurança, autenticação e autorização.

E isso normalmente é um tópico "difícil" e complexo.

Em muitos frameworks e sistemas, apenas lidar com segurança e autenticação exige muito esforço e código (em muitos casos isso pode ser 50% ou mais de todo o código escrito).

FastAPI tem muitas ferramentas para ajudar você com a parte de **Segurança** facilmente, rapidamente, de uma forma padrão, sem ter que estudar e aprender tudo sobre especificações de segurança.

Mas primeiro, vamos verificar alguns pequenos conceitos.

Está com pressa?

Se você não se importa com qualquer um desses termos e só precisa adicionar segurança com autenticação baseada em usuário e senha *agora*, pule para os próximos capítulos.

OAuth2

OAuth2 é uma especificação que define várias formas para lidar com autenticação e autorização.

Ela é bastante extensiva na especificação e cobre casos de uso muito complexos.

Ela inclui uma forma para autenticação usando "third party"/aplicações de terceiros.

Isso é o que todos os sistemas com "Login with Facebook, Google, Twitter, GitHub" usam por baixo.

OAuth 1

Havia um OAuth 1, que é bem diferente do OAuth2, e mais complexo, isso incluía diretamente as especificações de como criptografar a comunicação.

Não é muito popular ou usado nos dias atuais.

OAuth2 não especifica como criptografar a comunicação, ele espera que você tenha sua aplicação em um servidor HTTPS.

!!! tip "Dica" Na seção sobre **deployment** você irá ver como configurar HTTPS de modo gratuito, usando Traefik e Let's Encrypt.

OpenID Connect

OpenID Connect é outra especificação, baseada em **OAuth2**.

Ela é apenas uma extensão do OAuth2 especificando algumas coisas que são relativamente ambíguas no OAuth2, para tentar torná-lo mais interoperável.

Por exemplo, o login do Google usa OpenID Connect (que por baixo dos panos usa OAuth2).

Mas o login do Facebook não tem suporte para OpenID Connect. Ele tem a própria implementação do OAuth2.

OpenID (não "OpenID Connect")

Houve também uma especificação "OpenID". Ela tentou resolver a mesma coisa que a **OpenID Connect**, mas não baseada em OAuth2.

Então, ela foi um sistema adicional completo.

Ela não é muito popular ou usada nos dias de hoje.

OpenAPI

OpenAPI (anteriormente conhecido como Swagger) é a especificação aberta para a criação de APIs (agora parte da Linux Foundation).

FastAPI é baseado no **OpenAPI**.

Isso é o que torna possível ter múltiplas automações interativas de interfaces de documentação, geração de código, etc.

OpenAPI tem uma forma para definir múltiplos "esquemas" de segurança.

Por usá-los, você pode ter vantagens de todas essas ferramentas baseadas nos padrões, incluindo os sistemas de documentação interativa.

OpenAPI define os seguintes esquemas de segurança:

- `apiKey`: uma chave específica de aplicação que pode vir de:
  - Um parâmetro query.
  - Um header.
  - Um cookie.
- `http`: padrão HTTP de sistemas autenticação, incluindo:
  - `bearer`: um header de `Authorization` com valor de `Bearer` adicionado de um token. Isso é herança do OAuth2.
  - HTTP Basic authentication.
  - HTTP Digest, etc.
- `oauth2`: todas as formas do OAuth2 para lidar com segurança (chamados "fluxos").
  - Vários desses fluxos são apropriados para construir um provedor de autenticação OAuth2 (como Google, Facebook, Twitter, GitHub, etc):
    * `implicit`
    * `clientCredentials`
    * `authorizationCode`

    - Mas existe um "fluxo" específico que pode ser perfeitamente usado para resolver autenticação diretamente na mesma aplicação:
        * `password`: alguns dos próximos capítulos tratarão disso.
- `openIdConnect`: tem uma forma para definir como descobrir automaticamente o dado da autenticação OAuth2.
    - Essa descoberta automática é o que é definido na especificação OpenID Connect.

!!! tip "Dica" Integração com outros provedores de autenticação/autorização como Google, Facebook, Twitter, GitHub, etc. é bem possível e relativamente fácil.

`O problema mais complexo é criar um provedor de autenticação/autorização como eles, mas o Fa`

FastAPI utilitários

FastAPI fornece várias ferramentas para cada um desses esquemas de segurança no módulo `fastapi.security` que simplesmente usa esses mecanismos de segurança.

Nos próximos capítulos você irá ver como adicionar segurança à sua API usando essas ferramentas disponibilizadas pelo **FastAPI**.

E você irá ver também como isso é automaticamente integrado dentro do sistema de documentação interativo.