Sobre HTTPS

É fácil assumir que HTTPS é algo que é apenas "habilitado" ou não.

Mas é bem mais complexo do que isso.

!!! tip "Dica" Se você está com pressa ou não se importa, continue com as seções seguintes para instruções passo a passo para configurar tudo com diferentes técnicas.

Para aprender o básico de HTTPS de uma perspectiva do usuário, verifique https://howhttps.works/pt-br/.

Agora, a partir de uma perspectiva do desenvolvedor, aqui estão algumas coisas para ter em mente ao pensar em HTTPS:

- Para HTTPS, o servidor precisa ter certificados gerados por um terceiro.
    - Esses certificados são adquiridos de um terceiro, eles não são simplesmente "gerados".
- Certificados têm um tempo de vida.
    - Eles expiram.
    - E então eles precisam ser renovados, adquirindo-os novamente de um terceiro.
- A criptografia da conexão acontece no nível TCP.
    - Essa é uma camada abaixo do HTTP.
    - Portanto, o manuseio do certificado e da criptografia é feito antes do HTTP.
- O TCP não sabe sobre "domínios". Apenas sobre endereços IP.
    - As informações sobre o domínio solicitado vão nos dados HTTP.
- Os certificados HTTPS “certificam” um determinado domínio, mas o protocolo e a encriptação acontecem ao nível do TCP, antes de sabermos de que domínio se trata.
- Por padrão, isso significa que você só pode ter um certificado HTTPS por endereço IP.
    - Não importa o tamanho do seu servidor ou quão pequeno cada aplicativo que você tem nele possa ser.
    - No entanto, existe uma solução para isso.
- Há uma extensão para o protocolo TLS (aquele que lida com a criptografia no nível TCP, antes do HTTP) chamado SNI.
    - Esta extensão SNI permite que um único servidor (com um único endereço IP) tenha vários certificados HTTPS e atenda a vários domínios / aplicativos HTTPS.
    - Para que isso funcione, um único componente (programa) em execução no servidor, ouvindo no endereço IP público, deve ter todos os certificados HTTPS no servidor.
- Depois de obter uma conexão segura, o protocolo de comunicação ainda é HTTP.
    - Os conteúdos são criptografados, embora sejam enviados com o protocolo HTTP.

É uma prática comum ter um programa/servidor HTTP em execução no servidor (máquina, host, etc.) e gerenciar todas as partes HTTPS: enviando as solicitações HTTP descriptografadas para o aplicativo HTTP real em execução no mesmo servidor (a aplicação **FastAPI**, neste caso), pegue a resposta HTTP do aplicativo, criptografe-a usando o certificado apropriado e envie-a de volta ao cliente usando HTTPS. Este servidor é frequentemente chamado de TLS Termination Proxy.

Let's Encrypt

Antes de Let's Encrypt, esses certificados HTTPS eram vendidos por terceiros confiáveis.

O processo de aquisição de um desses certificados costumava ser complicado, exigia bastante papelada e os certificados eram bastante caros.

Mas então Let's Encrypt foi criado.

Ele é um projeto da Linux Foundation que fornece certificados HTTPS gratuitamente. De forma automatizada. Esses certificados usam toda a segurança criptográfica padrão e têm vida curta (cerca de 3 meses), então a segurança é realmente melhor por causa de sua vida útil reduzida.

Os domínios são verificados com segurança e os certificados são gerados automaticamente. Isso também permite automatizar a renovação desses certificados.

A ideia é automatizar a aquisição e renovação desses certificados, para que você tenha HTTPS seguro, de graça e para sempre.