CONFIGURANDO NGINX PARA HTTP/2

Por Sediane Carmem Lunardi Hernandes

AGENDA

Configuração do servidor Web NGINX para utilizar o protocolo HTTP/2

INTRODUÇÃO

- Alguns navegadores (p.e., Google Chrome, Mozilla Firefox) oferecem suporte ao protocolo HTTP/2 somente sobre conexões HTTPS

Logo, para configurar o NGINX com suporte HTTP/2 é necessário habilitar o HTTPS

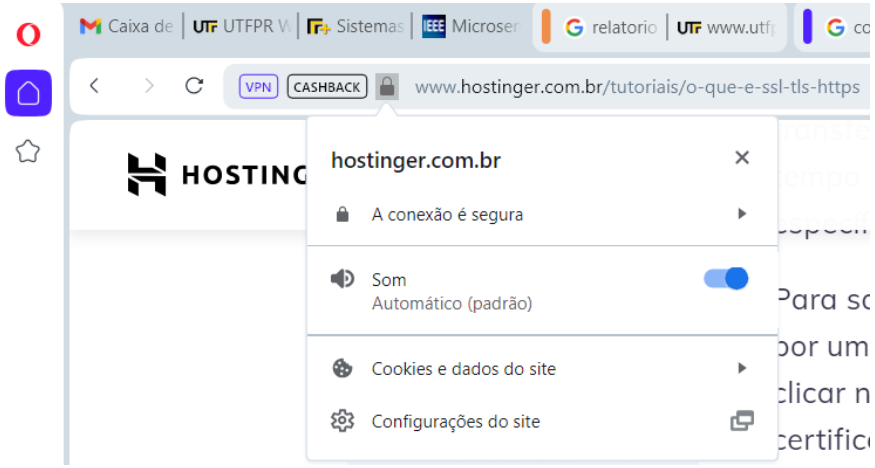
LEMBRANDO QUE...

- O HTTP em si não fornece segurança

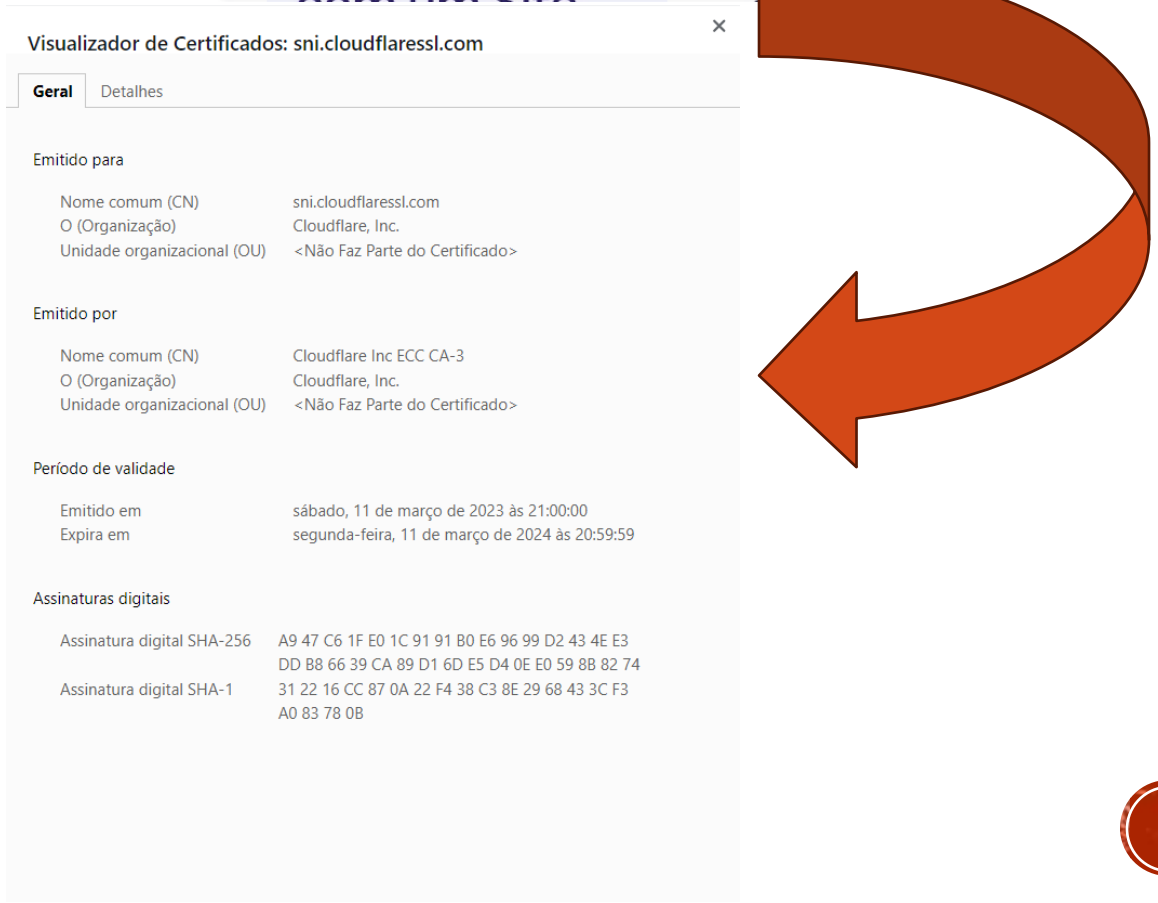
- Contudo...
  - O HTTP pode ser executado sobre a Camada de Sockets Segura (SSL – *Secure Layer*). Nesse caso, o HTTP é denominado HTTPS, que fornece confidencialidade, autenticação do cliente/servidor e integridade dos dados (mudança nos dados somente por entidades autorizadas)

HTTPS

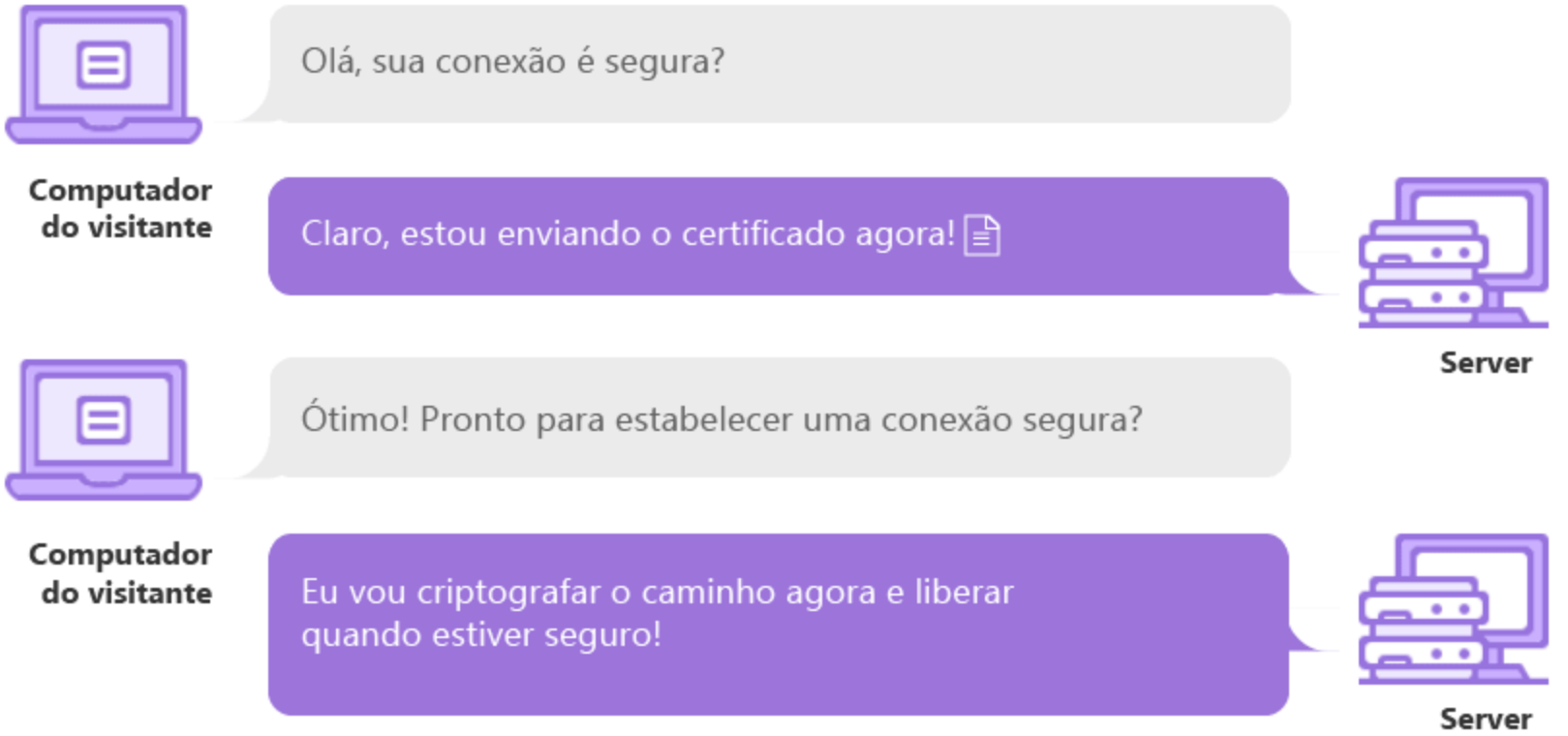
- Os sites que configurarem um **CERTIFICADO** SSL/TLS (*Secure Sockets Layer/Transport Layer Security*) podem utilizar o protocolo HTTPS para estabelecer uma comunicação segura com o servidor
  - É possível identificar que um site possui certificado SSL/TLS quando há um cadeado indicando a conexão segura próximo à URL no navegador


Caixa de
UTFPR W
Sistemas
Microser
relatorio
www.utfp
VPN
CASHBACK
www.hostinger.com.br/tutoriais/o-que-e-ssl-tls-https
HOSTING
hostinger.com.br
A conexão é segura
Som
Automático (padrão)
Cookies e dados do site
Configurações do site

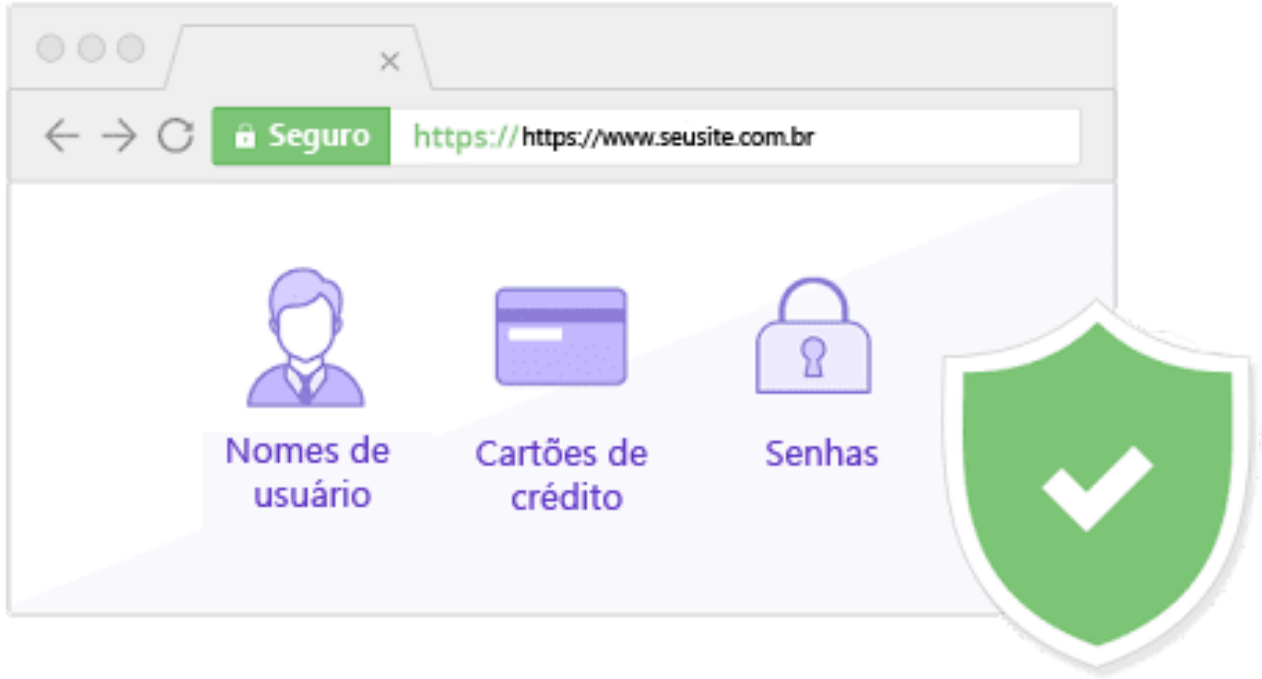

Caixa de
UTFPR W
Sistemas
Microser
relatorio
www.utfp
VPN
CASHBACK
www.hostinger.com.br/tutoriais/o-que-e-ss
HOSTING
Segurança
hostinger.com.br
A conexão é segura
Suas informações (por exemplo, senhas ou números de cartão de crédito) permanecem privadas quando são enviadas para esse site.
Saiba mais
O certificado é válido


Visualizador de Certificados: sni.cloudflaressl.com
Geral
Detalhes
Emitido para
Nome comum (CN) sni.cloudflaressl.com
O (Organização) Cloudflare, Inc.
Unidade organizacional (OU) <Não Faz Parte do Certificado>
Emitido por
Nome comum (CN) Cloudflare Inc ECC CA-3
O (Organização) Cloudflare, Inc.
Unidade organizacional (OU) <Não Faz Parte do Certificado>
Período de validade
Emitido em sábado, 11 de março de 2023 às 21:00:00
Expira em segunda-feira, 11 de março de 2024 às 20:59:59
Assinaturas digitais
Assinatura digital SHA-256 A9 47 C6 1F E0 1C 91 91 B0 E6 96 99 D2 43 4E E3 DD B8 66 39 CA 89 D1 6D E5 D4 0E E0 59 8B 82 74
Assinatura digital SHA-1 31 22 16 CC 87 0A 22 F4 38 C3 8E 29 68 43 3C F3 A0 83 78 0B

CERTIFICADO SSL/TLS



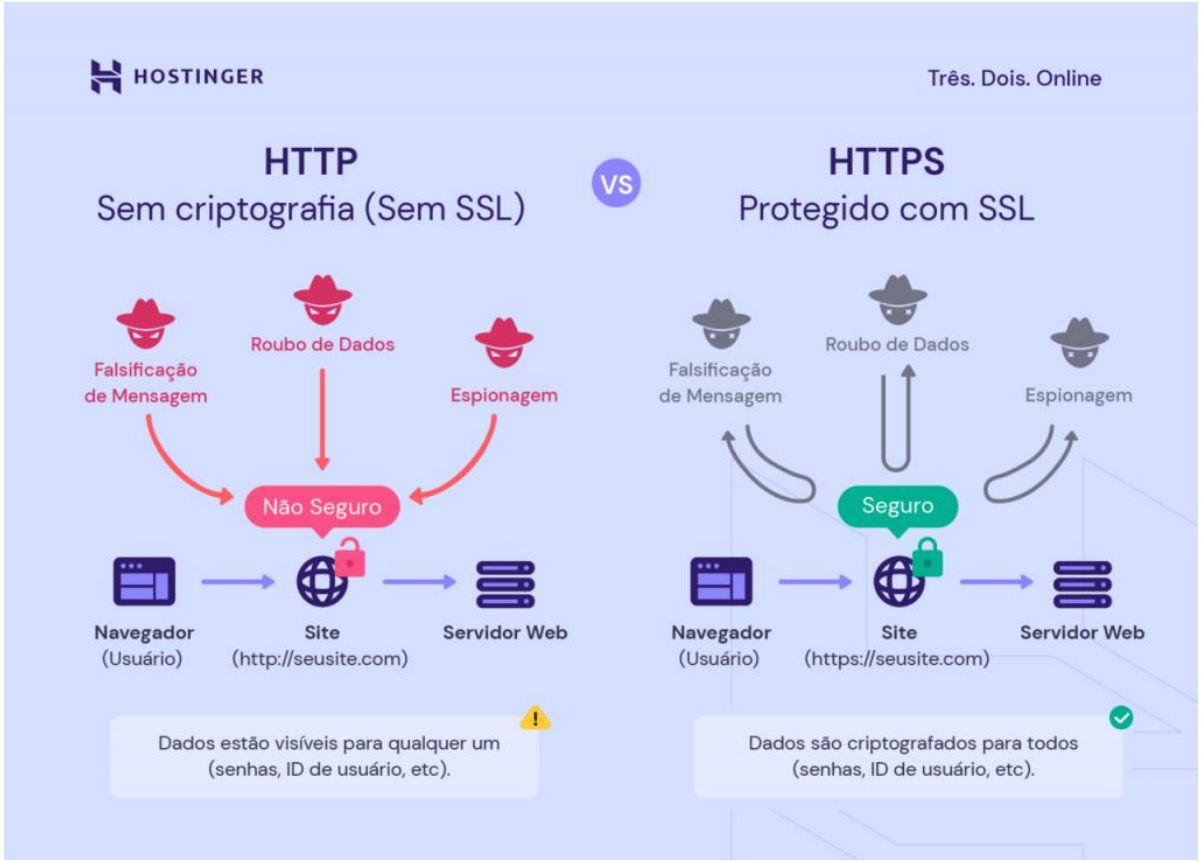
QUANDO O CERTIFICADO SSL/TLS É IMPORTANTE?



Os certificados SSL garantem que os dados enviados são **criptografados**, como no caso de dados bancários, nomes ou mesmo endereços, de forma a impossibilitar que outras pessoas possam utilizá-los indevidamente

POR QUE O CERTIFICADO SSL/TLS É IMPORTANTE?

- O objetivo do SSL/TLS é garantir que somente uma pessoa – a pessoa ou organização para quem os dados estão sendo transmitidos – possa ter acesso às informações
  - Importante porque a informação passa por vários dispositivos de comunicação antes de chegar no seu destino


HOSTINGER
Três. Dois. Online
HTTP
Sem criptografia (Sem SSL)
VS
HTTPS
Protegido com SSL
Falsificação de Mensagem
Roubo de Dados
Espionagem
Não Seguro
Navegador (Usuário)
Site (http://seusite.com)
Servidor Web
Dados estão visíveis para qualquer um (senhas, ID de usuário, etc).
Falsificação de Mensagem
Roubo de Dados
Espionagem
Seguro
Navegador (Usuário)
Site (https://seusite.com)
Servidor Web
Dados são criptografados para todos (senhas, ID de usuário, etc).

HTTP X HTTPS

AGORA, VAMOS CONFIGURAR O SERVIDOR NGINX?

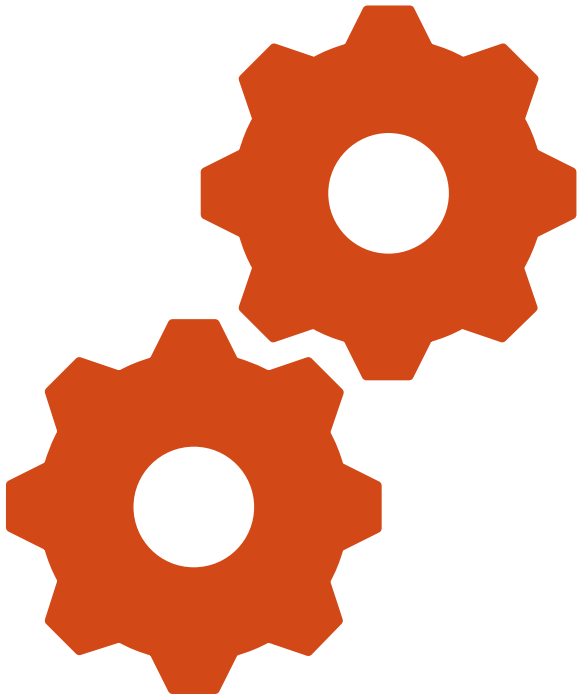
- Para isso, siga o tutorial dos próximos slides...

DEFININDO O DOMÍNIO

- **Definindo o domínio:**
  - sorveteria.com.br

CONFIGURACAO – PARTE I

CONFIGURANDO



- **Passo 1:** Instalar o Certbot e plug-in do NGINX para gerar certificado SSL

```
:~$ sudo apt install certbot python3-certbot-nginx
```

CONFIGURANDO...

OpenSSL é uma implementação de software livre dos protocolos SSL e TLS

- **Passo 2:** Gerar um certificado digital
  - Como não temos um domínio registrado, vamos gerar um certificado autoassinado com openSSL

```
$ cd /etc/ssl/
$ sudo openssl req -x509 -nodes -days 365 -newkey
rsa:2048 -keyout /etc/ssl/private/nginx-selfsigned.key
out /etc/ssl/certs/nginx-selfsigned.crt
```

- **Passo 3:** Configurar o Nginx para usar o SSL

```
$ sudo pico /etc/nginx/snippets/self-signed.conf
```

Com o arquivo aberto digitar:

```
ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
ssl_certificate_key /etc/ssl/private/nginx-
selfsigned.key;
```

- **Passo 4**: agora iremos criar um outro arquivo com configurações de segurança?
  sudo pico /etc/nginx/snippets/ssl-params.conf
  Adicione o conteúdo abaixo nesse arquivo:

```
ssl_protocols TLSv1.3;
ssl_prefer_server_ciphers on;
ssl_dhparam /etc/nginx/dhparam.pem;
ssl_ciphers EECDH+AESGCM:EDH+AESGCM;
ssl_ecdh_curve secp384r1;
ssl_session_timeout  10m;
ssl_session_cache shared:SSL:10m;
ssl_session_tickets off;
ssl_stapling on;
ssl_stapling_verify on;
resolver 8.8.8.8 8.8.4.4 valid=300s;
resolver_timeout 5s;
# Disable strict transport security for now. You can uncomment the following
# line if you understand the implications.
#add_header Strict-Transport-Security "max-age=63072000; includeSubDomains; preload";
add_header X-Frame-Options DENY;
add_header X-Content-Type-Options nosniff;
add_header X-XSS-Protection "1; mode=block";
```

CONFIGURANDO...

- **Passo 5**: Ajustar a configuração do Nginx para usar a camada SSL:
  - sudo cp /etc/nginx/sites-available/your_domain /etc/nginx/sites-available/your_domain.bak
- **Passo 6**: Abrir o arquivo de configuracao do seu domínio e utilizar a porta 443 para conexões seguras:

/etc/nginx/sites-available/your_domain

```
server {
    listen 443 ssl;
    listen [::]:443 ssl;
    include snippets/self-signed.conf;
    include snippets/ssl-params.conf;

root /var/www/your_domain/html;
        index index.html index.htm index.nginx-debian.html;

  server_name your_domain.com www.your_domain.com;

  location / {
                try_files $uri $uri/ =404;
        }
}
```

include snippers/snakeoil.conf;

CONFIGURANDO...

- **Passo 7**: Checar se não existem erros de sintaxe nos arquivos de configuração do NGINX:
  - `$ sudo nginx -t`

  Se tudo estiver correto a saída será:

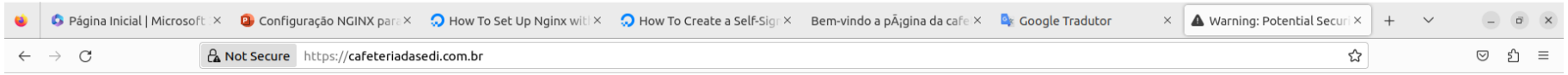
```
nginx: [warn] "ssl_stapling" ignored, issuer certificate not found for certificate "/etc/ssl/certs/nginx-selfsigned.crt"
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

- **Passo 8**: Restartar o NGINX para assumir as novas configurações:
  - `$ sudo systemctl restart nginx`

TESTANDO

Navegador Firefox

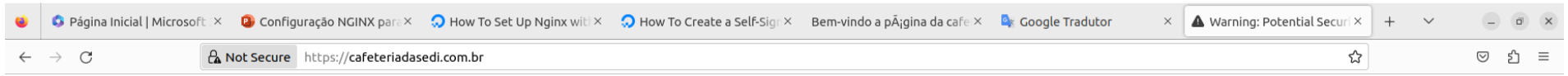
Agora está tudo pronto para testar seu servidor SSL.
Para isso, digite: **http://your_domain**

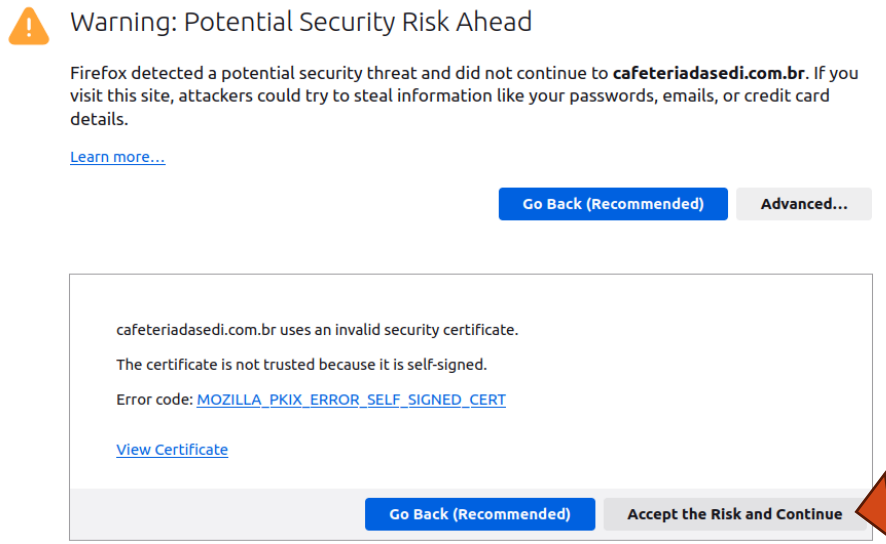


Clicar aqui

TESTANDO...

Navegador Firefox

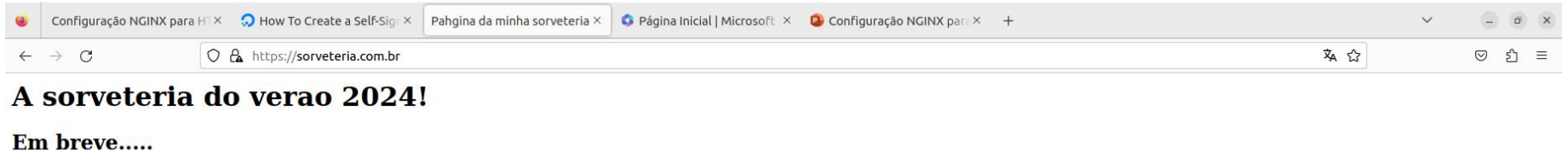




Clicar aqui

POR FIM...

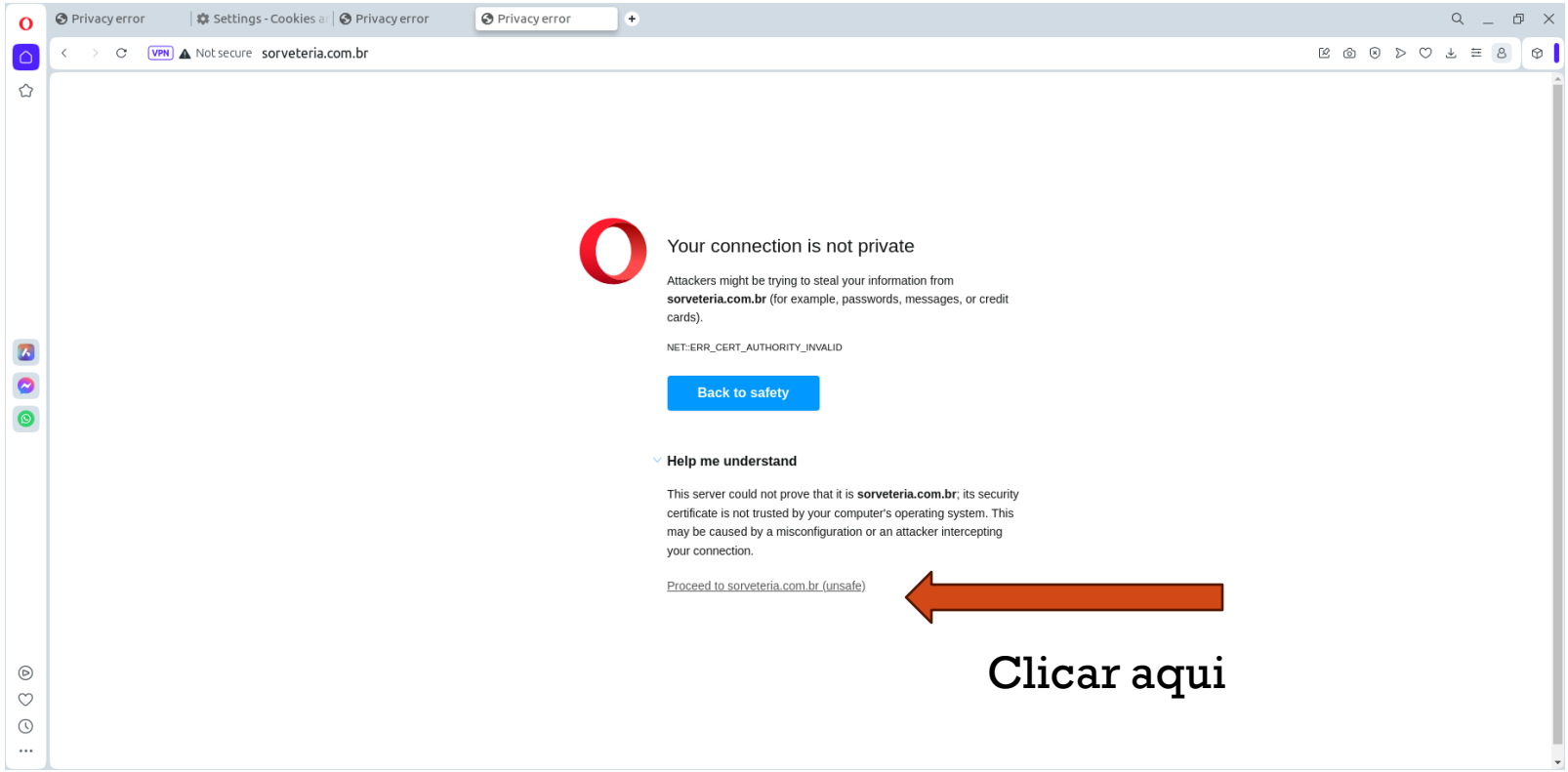
Navegador Firefox



TESTANDO

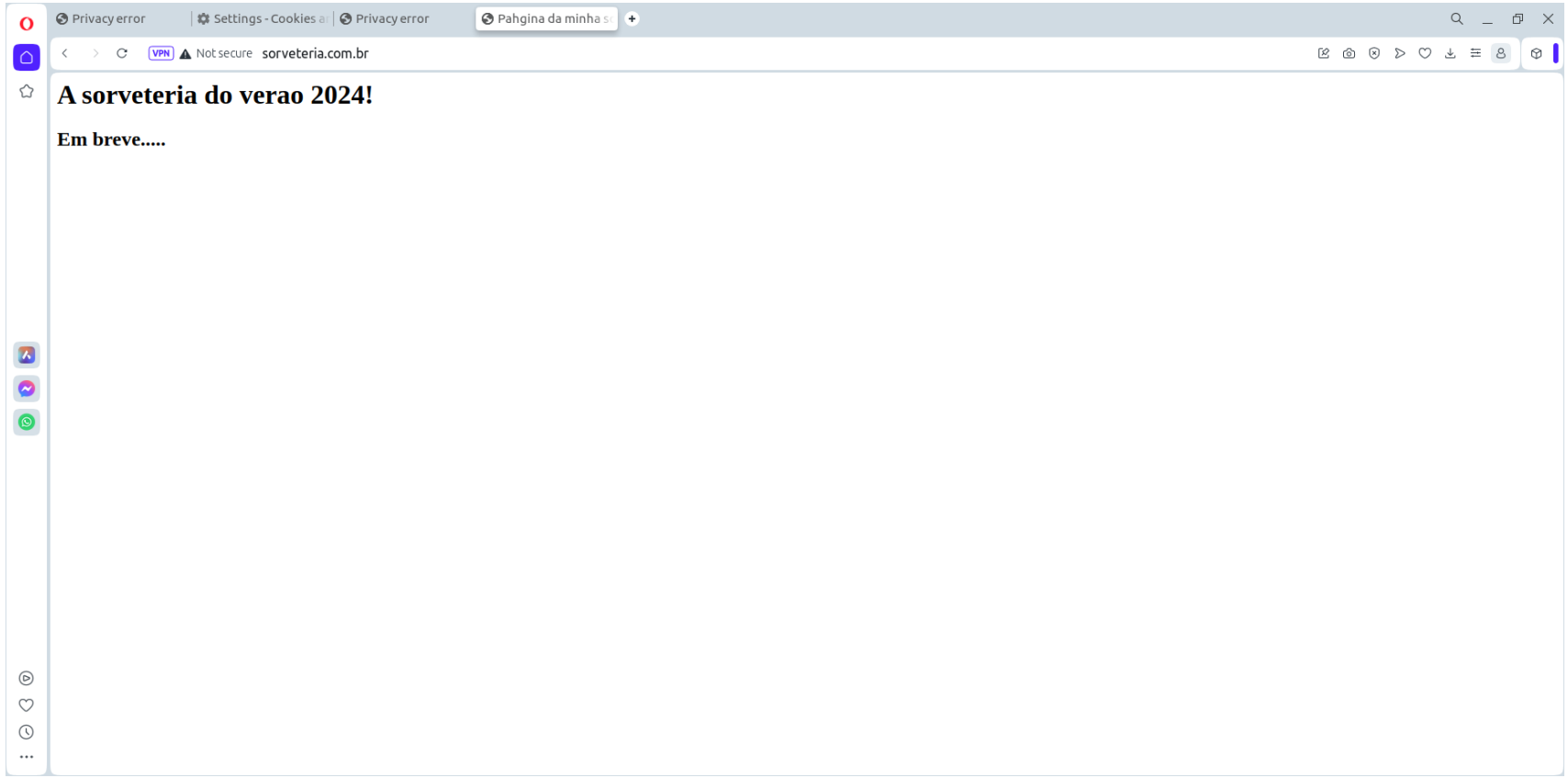
Navegador Opera

Agora está tudo pronto para testar seu servidor SSL.
Para isso, digite: **http://your_domain**



POR FIM...

Navegador Opera



REDIRECIONAMENTO

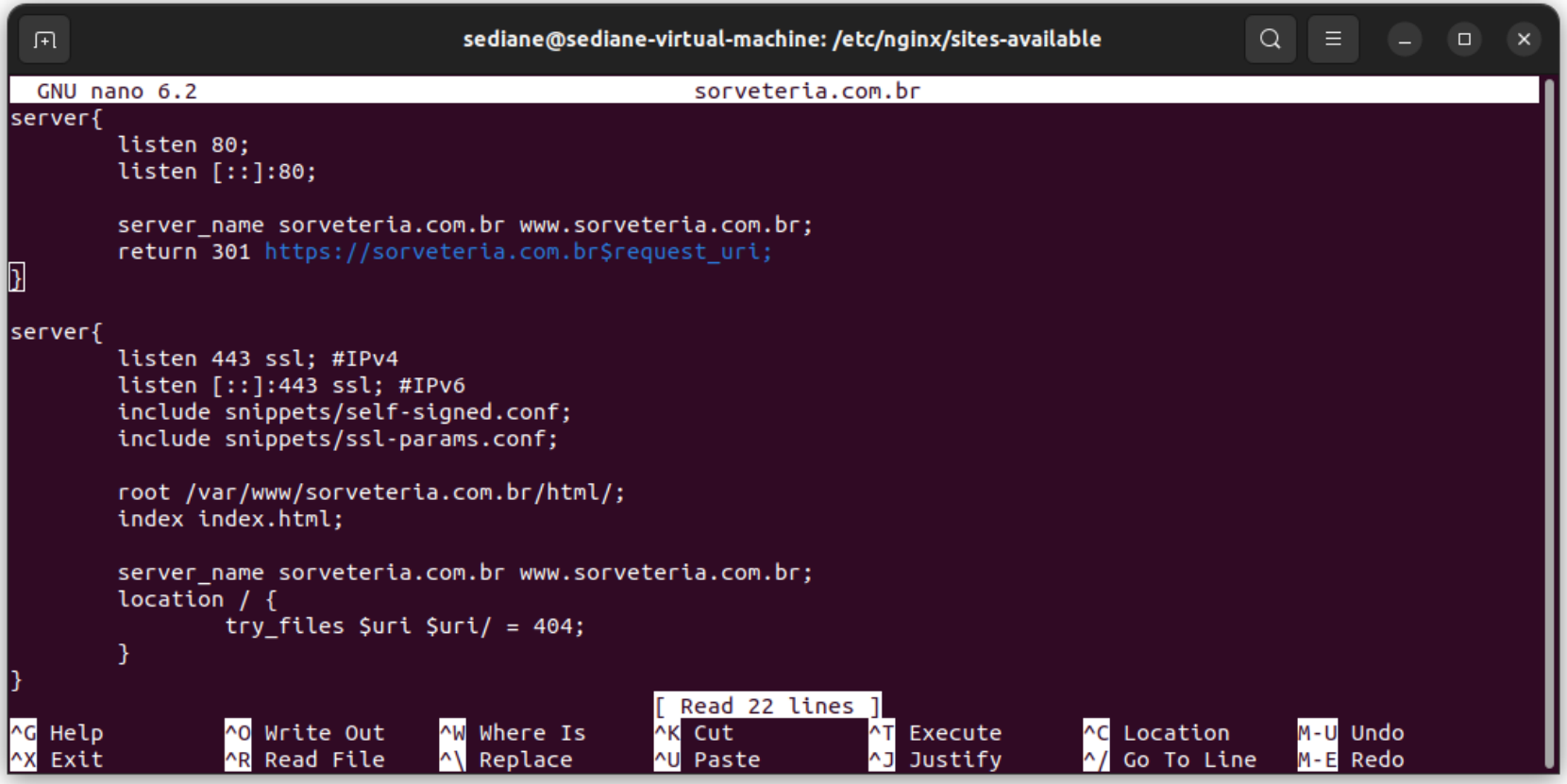
E se o usuário digitar

http://sorveteria.com.br

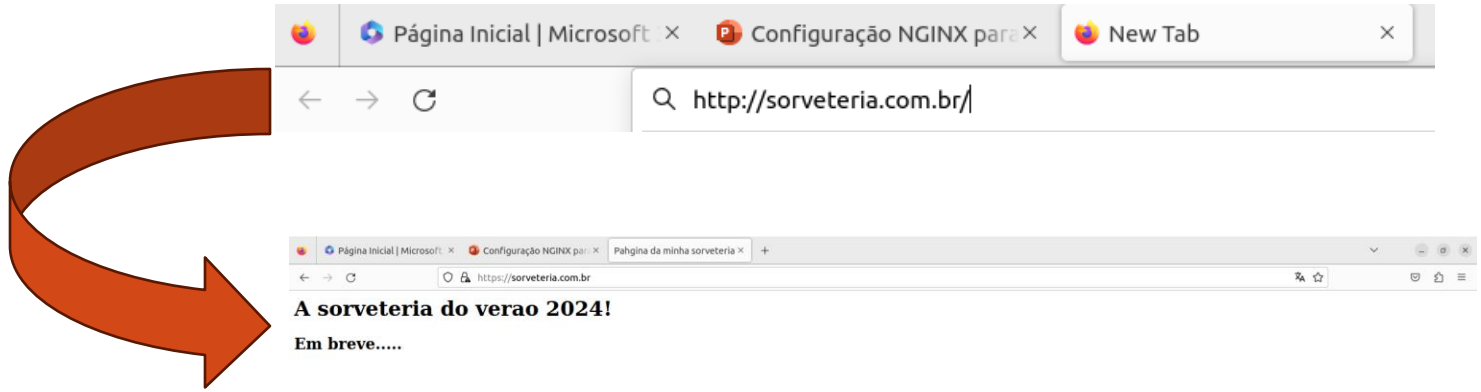
sem o s?

PROSSEGUINDO...

Bloco de redirecionamento



TESTANDO...


Página Inicial | Microsoft
Configuração NGINX para
New Tab
http://sorveteria.com.br/
Página Inicial | Microsoft
Configuração NGINX par
Pahgina da minha sorveteria
https://sorveteria.com.br
A sorveteria do verao 2024!
Em breve.....

CONFIGURACAO — PARTE II

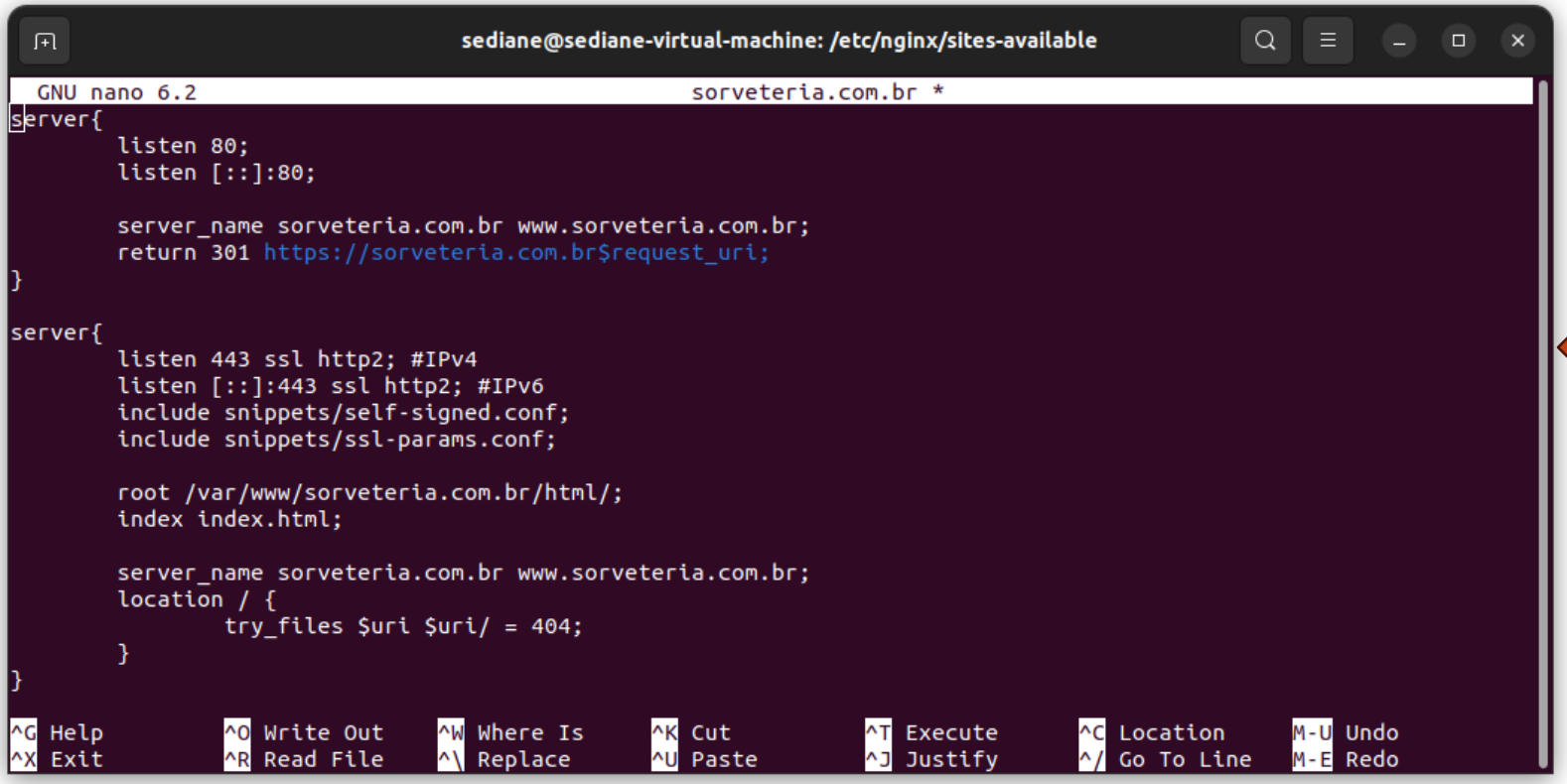
INICIANDO...

- **Passo 1:** Habilitar as conexões IP para suportar o HTTP/2 adicionando a primitiva http2 na primitiva `listen`

/etc/nginx/sites-enabled/your_domain

```
...
    listen [::]:443 ssl http2 ipv6only=on;
    listen 443 ssl http2;
...
```

CONFIGURANDO...



IPv4
IPv6

para https porta 443

Foi habilitado o http2 para endereçamento IPv4 e IPv6

CONFIGURANDO...

- **Passo 2**: Testar as configurações do NGINX

```
nginx: [warn] "ssl_stapling" ignored, issuer certificate not found for certificate "/etc/ssl/certs/nginx-selfsigne
d.crt"
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

- **Passo 3**: Restartar o o servidor

```
$ sudo systemctl restart nginx.service
```

TESTANDO...

```
sediane@sediane-virtual-machine:/etc/nginx/sites-available$ curl --insecure -I -L --http2 https://sorveteria.com.br
HTTP/2 200
server: nginx/1.18.0 (Ubuntu)
date: Tue, 24 Oct 2023 15:06:55 GMT
content-type: text/html
content-length: 184
last-modified: Mon, 23 Oct 2023 22:04:15 GMT
etag: "6536eddf-b8"
x-frame-options: DENY
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
accept-ranges: bytes
```

TESTANDO

- Configuração HTTP/2 ok!

AGORA É A SUA VEZ...

- Para o domínio **sorveteria.com.br**, pede-se:
  - Acessar o material **Mais sobre o NGINX** no Moodle e:
    1. Configurar Página não encontrada - 404
    2. Configurar Página em manutenção - 503
    3. Configurar autenticação para acesso ao seu website

- **Atenção:** Manter as duas linhas relacionadas a logs ao *server-block* do domínio cafeteria

```
access_log /var/www/your_domain/logs/nginx_access.log;
error_log /var/www/your_domain/logs/nginx_error.log;
```

AGORA É A SUA VEZ (CONT.)

- Todos os alunos deverão ter para esse domínio cafeteria as páginas solicitadas (página não encontrada, site em manutenção, logs e autenticação)
- Por que?
  - Análise de arquivos de log
  - Análise do tráfego http pela ferramenta Wireshark

PRÓXIMOS PASSOS...

- Configurar NGINX para páginas dinâmicas
- Análise de tráfego HTTP com o uso da ferramenta Wireshark verificando o código de status da mensagem de resposta

REFERÊNCIAS

- https://www.nginx.com/blog/http2-module-nginx/#overview
- https://www.digitalocean.com/community/tutorials/how-to-secure-nginx-with-let-s-encrypt-on-ubuntu-20-04
- https://www.ibm.com/docs/pt-br/api-connect/5.0.x?topic=profiles-generating-self-signed-certificate-using-openssl
- https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-nginx-in-ubuntu-22-04
- https://www.digitalocean.com/community/tutorials/how-to-set-up-nginx-with-http-2-support-on-ubuntu-22-04
- https://medium.com/programandus/como-redirecionar-http-para-https-ssl-no-servidor-apache-ou-nginx-156fdb421f97#:~:text=Forçar%20redirecionamento%20no%20servidor%20Nginx&text=Em%20seu%20arquivo%20de%20configuração,www%20para%20https%20não-www%20.&text=Depois%2C%20você%20precisará%20recarregar%20a,o%20servidor%20da%20web%20Nginx.