3.2 - SSL

prof. Fábio Engel

fabioe@utfpr.edu.br

Conteúdo

SSL

SSL

- Configurando SSL no servidor de desenvolvimento (Apache):
  - Iremos gerar um certificado SSL auto-assinado.
  - Vamos começar gerando um certificado SSL de 2048 bits. A sua chave pública será X.509 (PKI). Utilizaremos o nome utfpr para a chave e certificado, você pode utilizar o nome que desejar.

```
1  openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/
       ssl/utfpr.key -out /etc/apache2/ssl/utfpr.crt
```

SSL

- Configurando o certificado SSL para permitir o tráfego HTTPS na porta 443.
  - Agora precisamos criar um VHost que aceite o tráfego via HTTPS. Para isso, precisaremos do certificado que foi criado.
  - A porta padrão do HTTP é a 80. Já a porta padrão do tráfego HTTPS é 443. O navegador irá automaticamente trafegar por essa porta quando o protocolo for definido para HTTPS. Caso o servidor não esteja escutando nessa porta, o servidor não receberá os dados.

SSL

- É bastante provável que o Apache já esteja configurado para escutar na porta 443 mas, por via das dúvidas, vamos conferir o arquivo de portas.

```
gedit /etc/apache2/ports.conf
```

- Por padrão, o Apache já vem configurado para escutar na porta 443 caso o mod_ssl esteja habilitado. Você deve ver algo semelhante nesse arquivo:

```
<IfModule mod_ssl.c>
Listen 443
</IfModule>
```

SSL

- O próximo passo é configurar o caminho dos arquivos de SSL. Aqui vou usar o gedit, mas você pode utilizar o editor que preferir.

```
1 gedit /etc/apache2/sites-enabled/000-default.conf
```

- Essa é a configuração para porta 80. Precisamos configurar a porta 443. Copie o conteúdo entre <VirtualHost *:80> e </VirtualHost>. Cole este conteúdo logo abaixo, alterando a porta 80 para 443. Antes de </VirtualHost> insira:

```
1 SSLEngine on
2 SSLCertificateFile /etc/apache2/ssl/utfpr.crt
3 SSLCertificateKeyFile /etc/apache2/ssl/utfpr.key
```

SSL

- Agora só resta ativar o módulo SSL no Apache:

```
1 a2enmod ssl
```

- Só falta reiniciar o apache:

```
1 systemctl restart apache2
```

- Para verificar que tudo está OK, você deve tentar acessar https://localhost/.

SSL

- ACME Shell script
  - https://github.com/acmesh-official/acme.sh

Referências

- Material de aula desenvolvido a partir do conteúdo de:
  - http://www.phpit.com.br/artigos/configurando-ssl-servidor-de-desenvolvimento-apache.phpit