Servidor web seguro HTTPS

Sumario

PROTOCOLO HTTPS.....2
GENERAR CERTIFICADOS.....3
1.Generar la clave privada.....3
2.Genera la solicitud de certificado.....4
3.Crea el certificado digital.....4
ACTIVAR LA SEGURIDAD DE APACHE.....5
4.Mover la clave privada al directorio.....6
5.Mover el certificado al directorio.....6
6.Copia el archivo default-ssl.conf.....6
7.Visualizar el archivo.....6
8.Activar el sitio virtual.....7
9.Comprobación desde el navegador.....8
REDIRECCIONAR HTTP A HTTPS.....8

PROTOCOLO HTTPS

El servidor web decimos que es seguro cuando garantiza la comunicación con el cliente web con autenticación y confidencialidad.

Se basa en dos tipos de criptografía:

- Criptografía simétrica o de clave compartida.
  - – Confidencialidad: cifra la información transmitida.
  - – VENTAJA: Es rápido para el cifrado.

- Criptografía asimétrica de clave pública/privada.
  - – Confidencialidad
  - – Autenticación del servidor con la que se establece la conexión. Certificado del servidor.
  - – INCONVENIENTE: Es lento para el cifrado

GENERAR CERTIFICADOS

1.Generar la clave privada

2.Crea tu Certificate Signing Request (CSR) o solicitud de certificado es la clave pública (garantizan la integridad de los datos.) y algunos datos personales (autenticación) y garantizan la integridad de los datos.

3.Esta solicitud se podría enviar a una autoridad de certificación para generar el certificado (CRT).

1.Generar la clave privada

Meteremos el siguiente comando para crear los ficheros
Crearemos tantos ficheros como sitios virtuales tengamos

```
miadmin@LFFUSED:~$ sudo openssl genrsa 2048 > fichero.key
Generating RSA private key, 2048 bit long modulus
.........................................+++
...................+++
e is 65537 (0x010001)
```

2.Genera la solicitud de certificado

Certificado (CSR-PKCS#10)
Crearemos tantos certificados como sitios virtuales tengamos
ATENCION! En el apartado common Name pondremos el nombre de nuestro sitio web

```
miadmin@LFFUSED:~$ sudo openssl req -new -key fichero.key > fichero.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:SP
State or Province Name (full name) [Some-State]:zamora
Locality Name (eg, city) []:benavente
Organization Name (eg, company) [Internet Widgits Pty Ltd]:casqueros
Organizational Unit Name (eg, section) []:casqueros1
Common Name (e.g. server FQDN or YOUR name) []:empresa1.com
Email Address []:lauraferfer4@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:paso
An optional company name []:casqueros2
```

3.Crea el certificado digital

Crearemos el certificado digital auto firmado ya que no tenemos ninguna certificadora que nos lo firme porque lo haremos nosotros.

```
miadmin@LFFUSED:~$ sudo openssl x509 -req -days 365 -in fichero.csr -signkey fichero.key -out ficher
o.crt
Signature ok
subject=C = SP, ST = zamora, L = benavente, O = casqueros, OU = casqueros1, CN = empresa1.com, email
Address = lauraferfer4@gmail.com
Getting Private key
```

ACTIVAR LA SEGURIDAD DE APACHE

● El método de cifrado SSL/TLS utiliza un método de cifrado de clave pública (cifrado asimétrico) para la autenticación del servidor.

● El módulo ssl es quien permite cifrar la información entre navegador y servidor web.

● Este módulo proporciona SSL v2/v3 y TLS v1 para el Servidor Apache HTTP; y se basa OpenSSL para porporcionar el modo de criptografía.

4.Mover la clave privada al directorio

Moveremos el fichero.key al directorio etc/ssl/private

```
miadmin@LFFUSED:~$ sudo mv fichero.key /etc/ssl/private
```

Propietario de dicho fichero es root:ssl-cert y permisos 640

```
miadmin@LFFUSED:~$ sudo chown -R root:ssl-cert /etc/ssl/private/fichero2.key
miadmin@LFFUSED:~$ sudo chmod -R 640 /etc/ssl/private/fichero2.key
```

5.Mover el certificado al directorio

Mover el certificado (fichero.crt) al directorio /etc/ssl/certs
Propietario de dicho fichero es root

```
miadmin@LFFUSED:~$ sudo mv fichero2.crt /etc/ssl/private/cert
```

6.Copia el archivo default-ssl.conf.

Copia el archivo default-ssl.conf en un archivo nuevo. Ejemplo: empresa1-ssl.conf
También por cada uno de los sitios virtuales que tengamos.

```
empresa1-ssl.conf
empresa2.conf
empresa2-ssl.conf
```

7.Visualizar el archivo.

En el archivo que hemos creado antes tendrá que tener una apariencia como esta:

* Significa que es para todas las ips

```
 GNU nano 2.9.3                          empresa1-ssl.conf

<IfModule mod_ssl.c>
        <VirtualHost *:443>
                ServerName empresa1.com
                ServerAlias www.empresa1.com
                ServerAdmin webmaster@localhost
                DocumentRoot /var/www/empresa1.com/public_html
                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined
                SSLEngine on
                SSLCertificateFile      /etc/ssl/certs/ficherol.crt
                SSLCertificateKeyFile /etc/ssl/private/ficherol.key
                <FilesMatch "\.(cgi|shtml|phtml|php)$">
                                SSLOptions +StdEnvVars
                </FilesMatch>
                <Directory /usr/lib/cgi-bin>
                                SSLOptions +StdEnvVars
                </Directory>
        </VirtualHost>
</IfModule>
```

8.Activar el sitio virtual.

sudo a2ensite fichero.conf

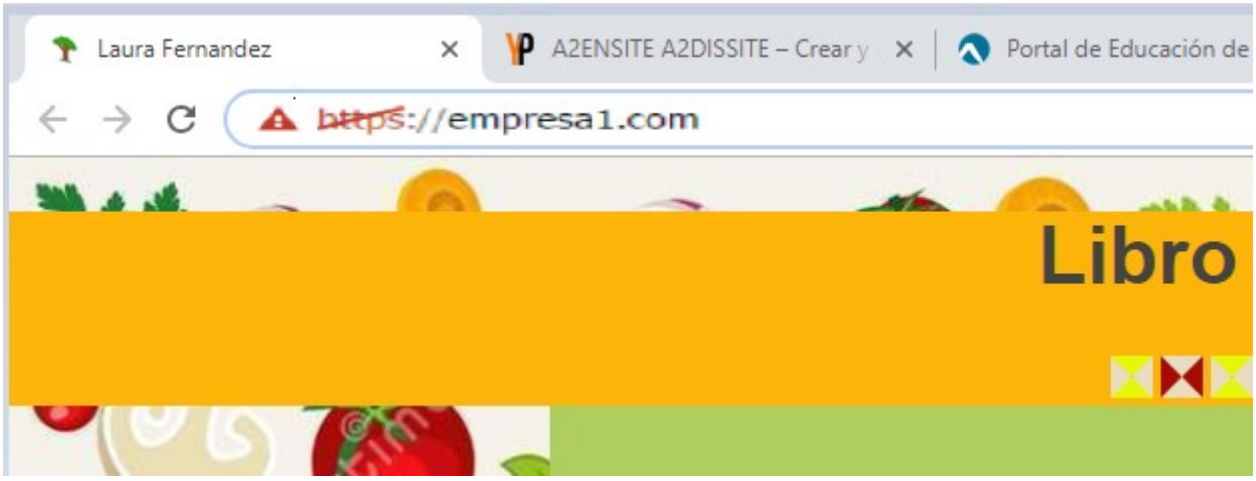
```
miadmin@LFFUSED:/etc/apache2/sites-available$ sudo a2ensite empresa-ssl.conf
Enabling site empresa-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

Y reiniciamos el sistema:

```
miadmin@LFFUSED:/etc/apache2/sites-available$ sudo systemctl reload apache2
```

9.Comprobación desde el navegador

Comprobamos que al poner el sitio virtual nos sale esta pagina:



REDIRECCIONAR HTTP A HTTPS

Para redireccionar tendremos que ir al archivo .htaccess y escribir las siguientes lineas: