# DAW Práctica 2.4: Certificados Apache

Para ver qué módulos están habilitados en Apache, utilizamos el siguiente comando en la terminal: apachectl -MCaptura de pantalla de computadora

Descripción generada automáticamente

Si queremos filtrar específicamente los módulos relacionados con SSL, podemos usar el comando grep para obtener una lista más específica: apachectl -M | grep ssl

Si el módulo SSL no está activo debemos habilitarlo con el siguiente comando: sudo a2enmod ssl

Apache viene con una configuración predeterminada para SSL llamada default-ssl.conf. Para habilitar esta configuración, utilizamos: sudo a2ensite default-ssl.conf

Captura de pantalla de computadora

Descripción generada automáticamente

Después reiniciamos el servidor apache y creamos la carpeta ssl en el directorio /etc/apache2

Generamos la clave privada que será utilizada para crear el certificado SSL. Utilizamos el comando sudo openssl genrsa -des3 -out /etc/apache2/ssl/server.key 2048

Captura de pantalla de computadora

Descripción generada automáticamente

* Genrsa: permite generar claves de forma manual o automática
* -des3: es un tipo de cifrado
* -out: Este parámetro indica el nombre del archivo en el que se guardará la solicitud de firma de certificado generada.
* Numbits (2048): indica una longitud de 2048 bits

A continuación, necesitamos generar una solicitud de firma de certificado (CSR). Usamos el siguiente comando para generar el CSR, que pedirá algunos detalles de la organización: sudo openssl req -new -key /etc/apache2/ssl/server.key -out /etc/apache2/ssl/server.csr

Texto

Descripción generada automáticamente

* Req: Este comando indica que queremos trabajar con el módulo req de OpenSSL, que se utiliza para generar solicitudes de firma de certificado (CSR) o certificados auto-firmados.
* -new: Este parámetro le indica a OpenSSL que queremos generar una nueva solicitud de firma de certificado (CSR).
* -key: Este parámetro especifica el archivo de clave privada que se usará para firmar la solicitud de certificado (CSR).
* -out: Este parámetro indica el nombre del archivo en el que se guardará la solicitud de firma de certificado generada.

Para crear el certificado auto-firmado, utilizamos el siguiente comando. Este comando firma la solicitud de certificado (server.csr) con la clave privada (server.key) y genera un archivo de certificado que será válido por 365 días: sudo openssl x509 -req -days 365 -in /etc/apache2/ssl/server.csr -signkey /etc/apache2/ssl/server.key -out /etc/apache2/ssl/server.crt

Texto

Descripción generada automáticamente

* X509: indica que queremos trabajar con el formato X.509
* -req: indica que estamos procesando una solicitud de certificado
* -days: define la duración de validez del certificado generado
* -in: especifica el archivo de entrada que contiene la solicitud de firma de certificado (CSR)
* -signkey: especifica el archivo de clave privada que se usará para firmar el certificado
* -out: indica el archivo de salida en el que se guardará el certificado digital firmado

Ahora debemos incluir la ruta de nuestro certificado y clave en la configuración SSL de Apache. Editamos el archivo de configuración de Apache /etc/apache2/sites-available/default-ssl.conf para que apunte a los archivos recién creados (server.crt y server.key):

SSLCertificateFile /etc/apache2/ssl/server.crt

SSLCertificateKeyFile /etc/apache2/ssl/server.key

Captura de pantalla de computadora

Descripción generada automáticamente

Para aplicar los cambios necesitamos reiniciar el servicio de Apache. Al reiniciar el servicio nos pedirá la clave que hemos introducido anteriormente

Una captura de pantalla de una computadora

Descripción generada automáticamente

Cuando intentamos acceder al servidor a través de HTTPS (por ejemplo, https://localhost), el navegador mostrará una advertencia indicando que el certificado no es válido. Esto ocurre porque el certificado es auto-firmado, lo que significa que no ha sido emitido por una autoridad de certificación confiable. Esto es normal para un entorno de prueba o desarrollo.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente