Apache2 Práctica 4

FRANCISCO JAVIER LÓPEZ CALDERÓN

2021

# Práctica 4: HTTPS

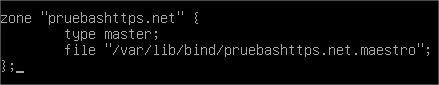
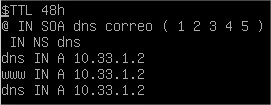
## Práctica 1

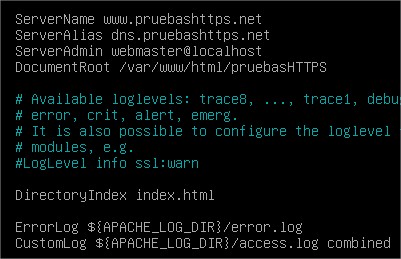
Dado un servidor web Apache Linux en Debian02, poner en marcha el sitio de defecto bajo un doble funcionamiento, teniendo en cuenta que se mostrará una página inicial distinta según se acceda con el protocolo HTTP o HTTPS.

* El nombre de dominio será [www.pruebas.net](http://www.pruebas.net/).
* Las carpetas de páginas serán**: /var/www/pruebasHTTP** para HTTP y

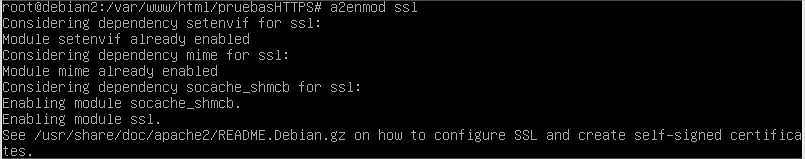
**/var/www/pruebasHTTPS** para HTTPS

****

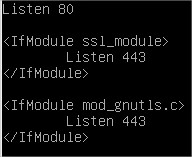




**Activaremos el módulo que activa el HTTPS “a2enmod ssl” y reiniciamos apache**

****

**Comprobamos que el puerto del SSL está activo, en /etc/apache2/ports.conf.**

****

**Ahora modificamos el archivo SSL por defecto para configurar el HTTPS**

******

* **Añadimos la ruta en “DocumentRoot”**
* **Creamos la directiva Directory, seleccionamos el documento fijado, permisos**

****

**Activamos el sitio por defecto HTTPS y reiniciamos Apache**

****

* Características de las páginas con **protocolo HTTPS** a mostrar:
* Nombre por defecto ***index\_https.html***

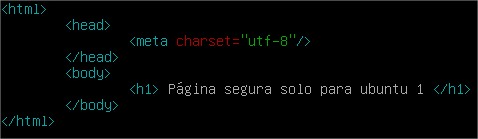
**Aparece el aviso de seguridad por el certificado default.**

****

* El index contendrá un acceso a una segunda página segura, contenida en un subdirectorio al que se permitirá el acceso sólo desde Ubuntu 1

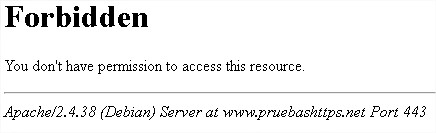
**Creamos el directorio y el archivo html, en este caso segubuntu.html**

****

****

**Modificamos el archivo index\_https.html**

**Intentamos acceder sin éxito desde Windows 7 y con Ubuntu 1 es posible.**

****

**Es importante aclarar que dicho bloqueo solo se aplica en “https” ya que hemos modificado el .SSL y no el archivo original.conf, desde HTTP sí podría acceder.**

* En esta segunda página deberemos incluir un enlace para volver a la página anterior.

**Modificamos el archivo**

****

****

****

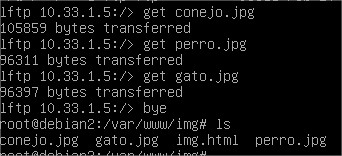
*Desde ambos sitios se podrá acceder a la carpeta /var/www/img para mostrar varias imágenes. Se usará el alias img.*

*Incluir en la página index.html del sitio HTTP una de las imágenes de la carpeta anterior.*

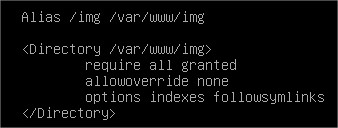
Realizar las comprobaciones oportunas para verificar su funcionamiento.

****

**Se ha creado el directorio img en www**

****

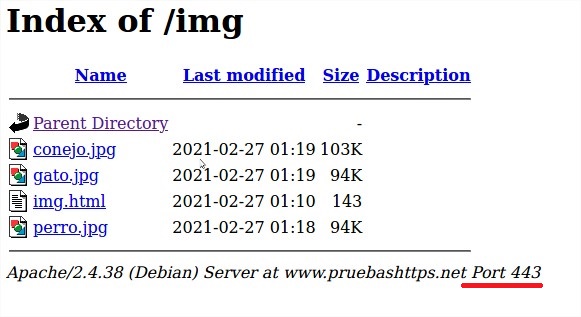
**Descargamos las imágenes con lftp**

****

**Creamos el alias “/img”**

****

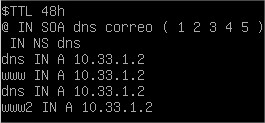
**Accedemos a la página**

****

**Comprobamos que ha funcionado correctamente y el puerto es el correcto**

## Práctica 2

Sobre el ejercicio anterior, añadir un segundo sitio web seguro accesible por HTTPS (www2.pruebas.net) con DocumentRoot **/var/www/pruebas2HTTPS,** en cuya página index se incluirá un enlace al primer sitio seguro HTTPS (creado en el ejercicio anterior).

****

**Creamos el nuevo nombre**

**Creamos el index en /var/www/pruebas2HTTPS y añadimos la ruta**

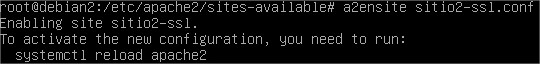
****

**En la /sites-available creamos el archivo “sitio2-ssl.conf” que posteriormente configuraremos**

****

****

**Y para completar lo activamos con a2ensite y reiniciamos apache**

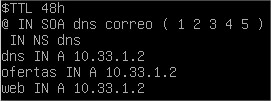
****

Además, en la página a mostrar por defecto en el primer sitio web seguro por HTTPS (ejercicio anterior) e debe incluir un enlace hasta el segundo sitio HTTPS. (Ver imagen aclaratoria).



## Práctica 3

Dada la empresa Verysegura S.L. en la que se dispone de un servidor web Apache sobre Linux, configurarlo para disponer dos sitios web distintos al de defecto (desactivar sitio defecto), en el que se mostrarán las páginas no seguras de la empresa. El primero de ellos será accesible con el nombre de dominio **web.verysegura.org** y el segundo mediante **ofertas.verysegura.org**.

****

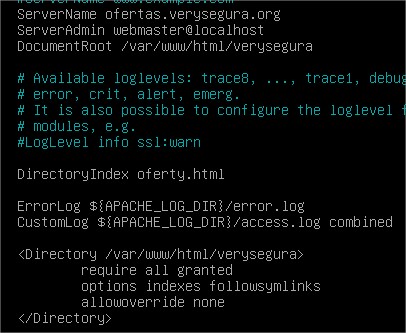
**Creamos la nueva zona**

****

**Creamos el directorio que contendrá los archivos .html**

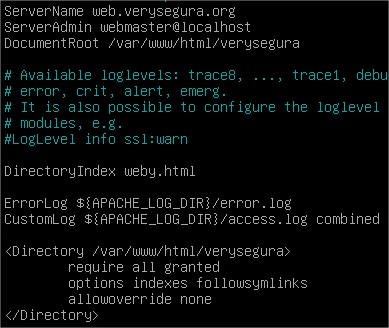
****

**Creamos la zona oferty.con para ofertas.verysegura.org**

****

**Activamos sus zonas con a2ensite**

**Creamos la zona weby.conf para web.verysegura.org**

****

**Activamos sus zonas con a2ensite**

****

Los dos sitios no seguros podrán acceder, además de a las páginas de su DocumentRoot, al contenido de la carpeta */var/www/documentos, utilizando enlace simbólico con el nombre que quieras.*

**Creamos el enlace simbólico llamado doc**

****

**Además, crearemos el href**

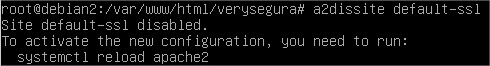
****

**No se podrá utilizar los certificados por defecto** y necesitaremos crear nuestro propio certificado autofirmado de empresa, válido sólo en un ámbito local y por un periodo de 2 años.

**El sitio no seguro podrá acceder, además de a las páginas de su DocumentRoot, al contenido de la carpeta */var/www/confidencial, utilizando ALIAS con el nombre que quieras.***

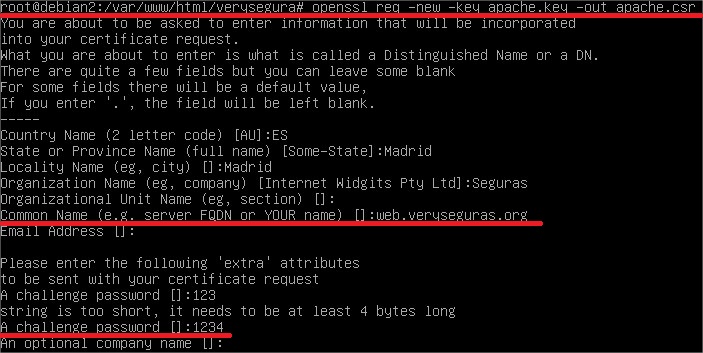
**Crearemos los certificados.**

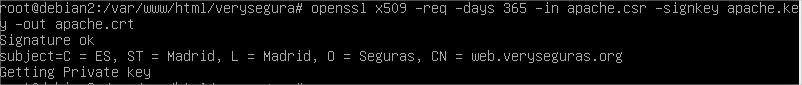
**Primero debemos desactivar el sitio HTTPS default ya que usa el mismo puerto.**

****

**Primero, crearemos nuestra clave privada**

**Ahora crearemos la solicitud del certificado**

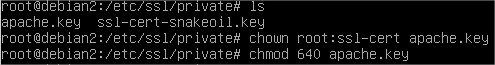
****

**Finalmente, se hará el certificado con un año de duración**

**Ahora es necesario mover los archivos a un directorio que apache pueda utilizar**

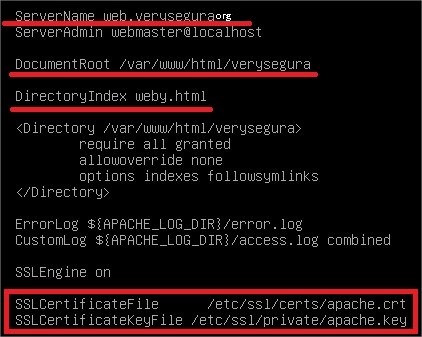
****

**Modificamos el grupo de pertenencia para asociarlo a ssl-cert y modificamos sus permisos para que solo los de su grupo puedan leerlo**

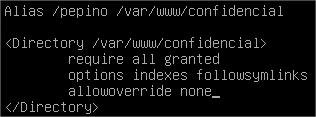
****

**De esta manera, completamos el certificado y la llave privada**

**Crearemos el archivo weby-seguro.conf y lo modificamos agregando las llaves y certificados nuevos**

****

**Ahora crearemos el Alias que irá a /var/www/confidencial, llamado pepino**

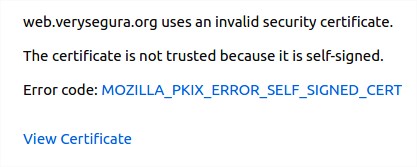
****

****

**Probamos el funcionamiento de la página web**

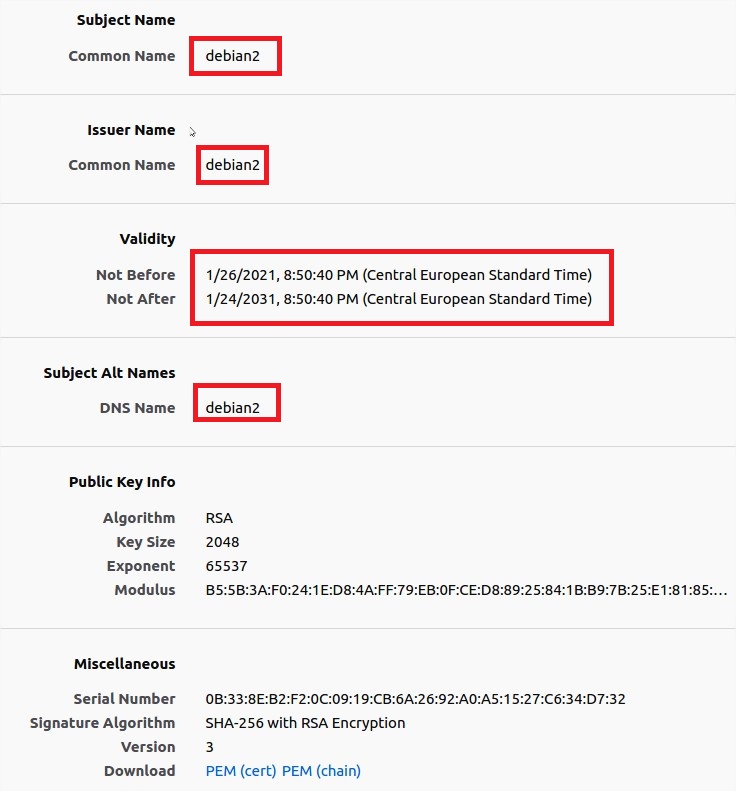
****

**Ahora observaremos el certificado.**

****

**Le damos clic a ver el certificado**

**Podemos comprobar que nuestro querido certificado que creamos previamente funciona correctamente UwU**

****

## Práctica 4

Configurar un segundo sitio seguro para la empresa anterior con el nombre confidencial.verysegura.org, que funcione bajo un puerto distinto del anterior.

Su DocumentRoot será la carpeta /var/www/confidencial creada en el apartado anterior, pero también podrá acceder mediante un alias al contenido de la carpeta

/var/www/superconfidencial

****

**Creamos el nombre “confidencial” en el dominio**

****

**Creamos el directorio superconfidencial**

****

**Creamos la página index y hacemos href con su alias**

****

**Habilitamos el puerto 444 en el módulo ssl**

**Creamos y modificamos el archivo.conf**

****

**Y Activamos la zona**

****

**Podemos comprobar**

****

**Además, haciendo clic en el href accedemos a /superconfidencial**