Junta de Andalucía
Consejería de Educación y Deporte
Unión Europea
Fondo Social Europeo
"El FSE invierte en tu futuro"
GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

En esta tarea habilitaremos el uso de HTTPS mediante el uso de certificados TLS para cifrar el tráfico de información entre el cliente y el servidor.

Módulos de Apache

Antes de comenzar con la tarea de certificados TLS, tenemos que hablar acerca de los módulos de Apache. En la anterior tarea, a la hora de utilizar la autenticación haciendo uso de grupos tuvimos que habilitar el uso de la directiva `AuthGroupFile` mediante el siguiente comando:

```
a2enmod authz_groupfile
```

Apache tiene un sinfín de características adicionales que si estuvieran siempre incluidas, harían de él un programa demasiado grande y pesado. En lugar de esto, Apache se compila de forma modular y se cargan en memoria sólo los módulos necesarios en cada caso.

Los módulos se guardan en la configuración de apache2 en dos directorios de forma similar que con la configuración de virtualhosts:

- */etc/apache2/mods-available/*: Directorio que contiene los módulos disponibles en la instalación actual.
- */etc/apache2/mods-enabled/*: Directorio que incluye mediante enlaces simbólicos al directorio anterior, los módulos que se van a cargar en memoria la próxima vez que se inicie Apache.

Los módulos de apache se pueden encontrar de dos maneras, compilados dentro del ejecutable apache2 o compilados de forma individual como una biblioteca de enlace dinámico (con extensión .so). Para saber qué módulos incluye el ejecutable de nuestra instalación de apache, podemos utilizar la siguiente instrucción:

```
# apache2 -l
Compiled in modules:
  core.c
  mod_so.c
  mod_watchdog.c
  http_core.c
  mod_log_config.c
  mod_logio.c
  mod_version.c
  mod_unixd.c
```

El resto de módulos disponibles para cargar en tiempo de ejecución se encuentran en el directorio */usr/lib/apache2/modules/*:

```
# ls /usr/lib/apache2/modules/

httpd.exp          mod_dav.so       mod_proxy_fcgi.so
mod_access_compat.so  mod_dbd.so       mod_proxy_fdpass.so
mod_actions.so         mod_deflate.so       mod_proxy_ftp.so
...
```

Pueden parecer muchos, pero son sólo los módulos de la instalación estándar y se incluyen dentro del paquete apache2-data. Hay otros muchos módulos que se distribuyen en paquetes separados, que en debian reciben el nombre libapache2-mod-*:

```
# apt-cache search libapache2-mod
libapache2-mod-auth-ntlm-winbind - apache2 module for NTLM
authentication against Winbind
libapache2-mod-upload-progress - upload progress support for
the Apache web server
```

Para ver los módulos activados en apache2:

```
# apache2ctl -M

Loaded Modules:
 core_module (static)
 so_module (static)
 watchdog_module (static)
 http_module (static)
 log_config_module (static)
```

Uso de módulos

Si vamos al directorio donde se ubican los módulos disponibles de Apache */etc/apache2/mods-available* y hacemos un listado encontramos ficheros *.load y *.conf.

Los ficheros con extensión load suelen incluir una línea con la directiva LoadModule, por ejemplo:

```
# cat userdir.load
```

```
LoadModule                                    userdir_module
/usr/lib/apache2/modules/mod_userdir.so
```

Además de cargar el módulo, en muchos casos es necesario realizar alguna configuración mediante directivas, por lo que en esos casos se existe un fichero con extensión .conf.

Si queremos que Apache utilice cualquier módulo, lo que tendríamos que hacer es un enlace simbólico del fichero de extensión .load (y del .conf si existe) en el directorio */etc/apache2/mods-enabled*. Este enlace lo podemos hacer con la instrucción `a2enmod`, por ejemplo:

```
# a2enmod userdir
Enabling module userdir.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

Para desactivarlo (borrar el enlace simbólico) utilizamos la instrucción `a2dismod`. Después de utilizar estos comandos hay que reiniciar el servicio.

Junta de Andalucía
Consejería de Educación y Deporte
Unión Europea
Fondo Social Europeo
"El FSE invierte en tu futuro"
GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

HTTPS

Consulta el siguiente tutorial.

Una vez consultado, **implementa una web HTTPS** con los siguientes requisitos:

- **Estructura y contenidos de la web**:

```
-- Raíz
    |-- vips
        -- index.html
        |-- recursos
            -- imagen.jpg
            -- imagen2.jpg
            -- informacion.txt
    |-- assets
        |-- images
            -- imagen.jpg
        -- style.css
    -- contacto
        -- index.html
    -- index.php
```

- **Descripción de las secciones**:
  - **Raíz**: directorio raíz de la web, debe estar ubicado en */var/www/https*. Debe de contener la página principal de la web (un index.php a tu gusto que muestre la imagen almacenada en *assets/images/*) .
  - **admin**: sección habilitada solo para vips, debe de dar la enhorabuena por ser vip.

        - **recursos**: sección que no contiene un index.html, tan solo distintos archivos.
    - **assets**: directorio que contiene recursos empleados para el renderizado de la página principal, tales como el css o imágenes.
    - **contacto**: sección de contacto de tu sitio web, introduce datos de contacto ficticios para los números de contacto, localización e inserta tu correo del centro.
- **Requisitos de configuración**:
    - Generales:
        - En toda la web se hallará deshabilitado el indexado de contenido o el listado de directorios.
        - No se emplearán ficheros .htaccess
        - Sólo será accesible mediante HTTPS y el puerto 443.
        - Debe estar ubicada en */var/www/https*
        - Será accesible por los dominios www.https.com y www.https.edu
    - sección vips: sólo será accesible para los usuarios del grupo vip. Introduce 2 o 3 usuarios en el grupo.
        - sección recursos: tendrá habilitado el indexado de contenido o el listado de directorios.
    - Habilita el uso de PHP en apache habilitando el módulo correspondiente. Para ello primero tendrás que instalar la librería:

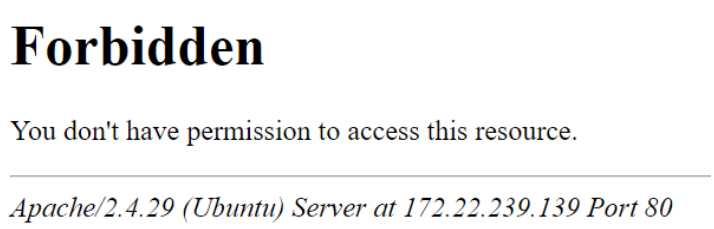
      ```
      sudo apt install libapache2-mod-phpX.X
      ```

      También deberás modificar el index.php de forma que tenga un campo de búsqueda y al buscar muestre la palabra buscada. Para ello utiliza una url de este estilo `https://www.https.com/buscar/palabra`. Consulta la siguiente referencia del módulo rewrite que nos permite hacer esto. Javascript.

Hardening

Ahora realizaremos una pequeña securización de Apache limitando la información que este muestra.

Junta de Andalucía
Consejería de Educación y Deporte
Unión Europea
Fondo Social Europeo
"El FSE invierte en tu futuro"
GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

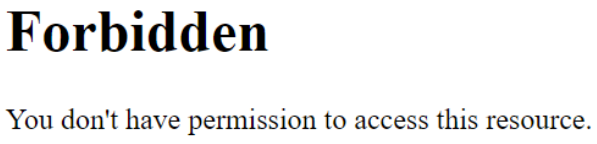


Hay dos directivas que necesitas cambiar en el archivo de configuración */etc/apache2/conf-avaliable/security.conf*

```
ServerSignature Off
ServerTokens Prod
```

El *ServerSignature* aparece en la parte inferior de las páginas generadas por Apache, por ejemplo al mostrar el error 404 (documento no encontrado).

La directiva *ServerTokens* sirve para determinar lo que pondrá Apache en la cabecera de la respuesta HTTP del servidor.



Comprueba que la configuración ha surtido efecto.

Entrega

Un documento pdf con todos los pasos seguidos para cumplir los requisitos, así como pruebas de funcionamiento.

Junta de Andalucía
Consejería de Educación y Deporte

Unión Europea
Fondo Social Europeo
"El FSE invierte en tu futuro"

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL