2021

Apache2 Práctica 4

FRANCISCO JAVIER LÓPEZ CALDERÓN

Francisco Javier López Calderón

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.
- Las carpetas de páginas serán**: /var/www/pruebasHTTP** para HTTP y

  /var/www/pruebasHTTPS para HTTPS

```
root@debian2:/var/www/html# ls
index.html  institutofp  pruebasHTTP  pruebasHTTPS
```

```
zone "pruebashttps.net" {
        type master;
        file "/var/lib/bind/pruebashttps.net.maestro";
};
```

```
$TTL 48h
@ IN SOA dns correo ( 1 2 3 4 5 )
 IN NS dns
dns IN A 10.33.1.2
www IN A 10.33.1.2
dns IN A 10.33.1.2
```

```
ServerName www.pruebashttps.net
ServerAlias dns.pruebashttps.net
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/pruebasHTTPS

# Available loglevels: trace8, ..., trace1, debu
# error, crit, alert, emerg.
# It is also possible to configure the loglevel
# modules, e.g.
#LogLevel info ssl:warn

DirectoryIndex index.html

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
```

```
root@debian2:/etc/apache2/sites-available# a2ensite 002-https.conf
Enabling site 002-https.
```

Activaremos el módulo que activa el HTTPS "a2enmod ssl" y reiniciamos apache

```
root@debian2:/var/www/html/pruebasHTTPS# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certifica
tes.
```

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

```
Listen 80

<IfModule ssl_module>
        Listen 443
</IfModule>

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

Ahora modificamos el archivo SSL por defecto para configurar el HTTPS

```
root@debian2:/etc/apache2/sites-available# nano default-ssl.conf _
```

- **Añadimos la ruta en "DocumentRoot"**
- **Creamos la directiva Directory, seleccionamos el documento fijado, permisos**

```
<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webmaster@localhost

                DocumentRoot /var/www/html/pruebasHTTPS

                <Directory /var/www/html/pruebasHTTPS>
                        DirectoryIndex index.html
                        Options Indexes FollowSymlinks MultiViews
                        AllowOverride None
                        Require all granted
                </Directory>
```

Activamos el sitio por defecto HTTPS y reiniciamos Apache

```
root@debian2:/var/www/html/pruebasHTTPS# a2ensite default-ssl
Site default-ssl already enabled
```

- 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

```
root@debian2:/var/www/html/pruebasHTTPS/direcseguro# ls
segubuntu.html
```

```
<html>
        <head>
                <meta charset="utf-8"/>
        </head>
        <body>
                <h1> Página segura solo para ubuntu 1 </h1>
        </body>
</html>
```

Modificamos el archivo index_https.html

```
<li><a href="direcseguro/segubuntu.html">Solo ubuntu 1</a></li>
```

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

```
<p><a href="../index_https.html">Volver</a></p>
```

Página segura solo para ubuntu 1

Volver

Index Seguro

Página Index Segura

-
- Solo ubuntu 1

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.

```
root@debian2:/var/www/img#
```

Se ha creado el directorio img en www

Descargamos las imágenes con lftp

```
lftp 10.33.1.5:/> get conejo.jpg
105859 bytes transferred
lftp 10.33.1.5:/> get perro.jpg
96311 bytes transferred
lftp 10.33.1.5:/> get gato.jpg
96397 bytes transferred
lftp 10.33.1.5:/> bye
root@debian2:/var/www/img# ls
conejo.jpg  gato.jpg  img.html  perro.jpg
```

```
Alias /img /var/www/img

<Directory /var/www/img>
        require all granted
        allowoverride none
        options indexes followsymlinks
</Directory>
```

Creamos el alias "/img"

Accedemos a la página

Index Seguro

Página Index Segura

-
- Solo ubuntu 1
- Carpeta imágenes

Index of /img

Name	Last modified	Size	Description
Parent Directory		-	
conejo.jpg	2021-02-27 01:19	103K	
gato.jpg	2021-02-27 01:19	94K	
img.html	2021-02-27 01:10	143	
perro.jpg	2021-02-27 01:18	94K	

Apache/2.4.38 (Debian) Server at www.pruebashttps.net Port 443

Comprobamos que ha funcionado correctamente y el puerto es el correcto

Francisco Javier López Calderón

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

```
$TTL 48h
@ IN SOA dns correo ( 1 2 3 4 5 )
 IN NS dns
dns IN A 10.33.1.2
www IN A 10.33.1.2
dns IN A 10.33.1.2
www2 IN A 10.33.1.2
```

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

```
<html>
        <head>
                <meta charset="utf-8"/>
        </head>
        <body>
                <h1>Index en pruebas2</h1>
                <p><a target="_blank" href="https://www.pruebashttps.net">Index Prueba1</a></p>
        </body>
</html>
```

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

```
root@debian2:/etc/apache2/sites-available# ls
000-default.conf  002-https.conf  default-ssl.conf  sitio2-ssl.conf
```

```
ServerName www2.pruebashttps.net
ServerAdmin webmaster@localhost

DocumentRoot /var/www/pruebas2HTTPS

<Directory /var/www/pruebas2HTTPS>
        DirectoryIndex index.html
        Options Indexes FollowSymlinks MultiViews
        AllowOverride None
        Require all granted
</Directory>
```

Y para completar lo activamos con a2ensite y reiniciamos apache

```
root@debian2:/etc/apache2/sites-available# a2ensite sitio2-ssl.conf
Enabling site sitio2-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

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).

Francisco Javier López Calderón

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

```
zone "verysegura.org" {
        type master;
        file "/var/lib/bind/verysegura.org.maestro";
};
```

```
$TTL 48h
@ IN SOA dns correo ( 1 2 3 4 5 )
 IN NS dns
dns IN A 10.33.1.2
ofertas IN A 10.33.1.2
web IN A 10.33.1.2
```

```
root@debian2:/var/www/html# mkdir verysegura
root@debian2:/var/www/html# cd verysegura/
root@debian2:/var/www/html/verysegura#
```

Creamos el directorio que contendrá los archivos .html

```
root@debian2:/var/www/html/verysegura# ls
oferty.html  weby.html
```

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

```
ServerName ofertas.verysegura.org
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/verysegura

# Available loglevels: trace8, ..., trace1, debug
# error, crit, alert, emerg.
# It is also possible to configure the loglevel
# modules, e.g.
#LogLevel info ssl:warn

DirectoryIndex oferty.html

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

<Directory /var/www/html/verysegura>
        require all granted
        options indexes followsymlinks
        allowoverride none
</Directory>
```

Activamos sus zonas con a2ensite

```
root@debian2:/etc/apache2/sites-available# a2ensite oferty.conf
```

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

```
ServerName web.verysegura.org
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/verysegura

# Available loglevels: trace8, ..., trace1, debu
# error, crit, alert, emerg.
# It is also possible to configure the loglevel
# modules, e.g.
#LogLevel info ssl:warn

DirectoryIndex weby.html

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

<Directory /var/www/html/verysegura>
        require all granted
        options indexes followsymlinks
        allowoverride none
</Directory>
```

Activamos sus zonas con a2ensite

```
root@debian2:/etc/apache2/sites-available# a2ensite weby.conf
Enabling site weby.
```

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

```
root@debian2:/var/www/html/verysegura# ln -s /var/www/documentos doc
root@debian2:/var/www/html/verysegura# ls
doc  oferty.html  weby.html
```

Además, crearemos el href

```
<a href="doc">Carpeta documentos en /var/www/documentos <a/>
```

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.

```
root@debian2:/var/www/html/verysegura# a2dissite default-ssl
Site default-ssl disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

Primero, crearemos nuestra clave privada

```
root@debian2:/var/www/html/verysegura# openssl genrsa -out apache.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................+++++
.....................................................+++++
e is 65537 (0x010001)
```

Ahora crearemos la solicitud del certificado

```
root@debian2:/var/www/html/verysegura# openssl req -new -key apache.key -out apache.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]:ES
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Madrid
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Seguras
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:web.veryseguras.org
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123
string is too short, it needs to be at least 4 bytes long
A challenge password []:1234
An optional company name []:
```

Finalmente, se hará el certificado con un año de duración

```
root@debian2:/var/www/html/verysegura# openssl x509 -req -days 365 -in apache.csr -signkey apache.ke
y -out apache.crt
Signature ok
subject=C = ES, ST = Madrid, L = Madrid, O = Seguras, CN = web.veryseguras.org
Getting Private key
```

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

```
root@debian2:/var/www/html/verysegura# mv apache.key /etc/ssl/private
root@debian2:/var/www/html/verysegura# mv apache.crt /etc/ssl/certs
```

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

```
root@debian2:/etc/ssl/private# ls
apache.key  ssl-cert-snakeoil.key
root@debian2:/etc/ssl/private# chown root:ssl-cert apache.key
root@debian2:/etc/ssl/private# chmod 640 apache.key
```

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

```
ServerName web.verysegura.org
ServerAdmin webmaster@localhost

DocumentRoot /var/www/html/verysegura

DirectoryIndex weby.html

<Directory /var/www/html/verysegura>
        require all granted
        allowoverride none
        options indexes followsymlinks
</Directory>

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

SSLEngine on

SSLCertificateFile      /etc/ssl/certs/apache.crt
SSLCertificateKeyFile /etc/ssl/private/apache.key
```

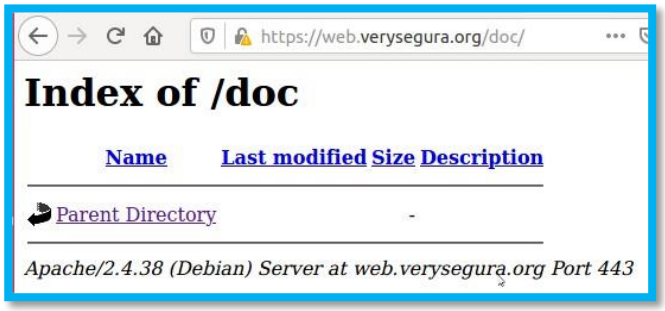
Ahora crearemos el Alias que irá a /var/www/confidencial, llamado pepino

```
Alias /pepino /var/www/confidencial

<Directory /var/www/confidencial>
        require all granted
        options indexes followsymlinks
        allowoverride none_
</Directory>
```

```
<a href="pepino"> Carpeta alias en confidencial </a>
```

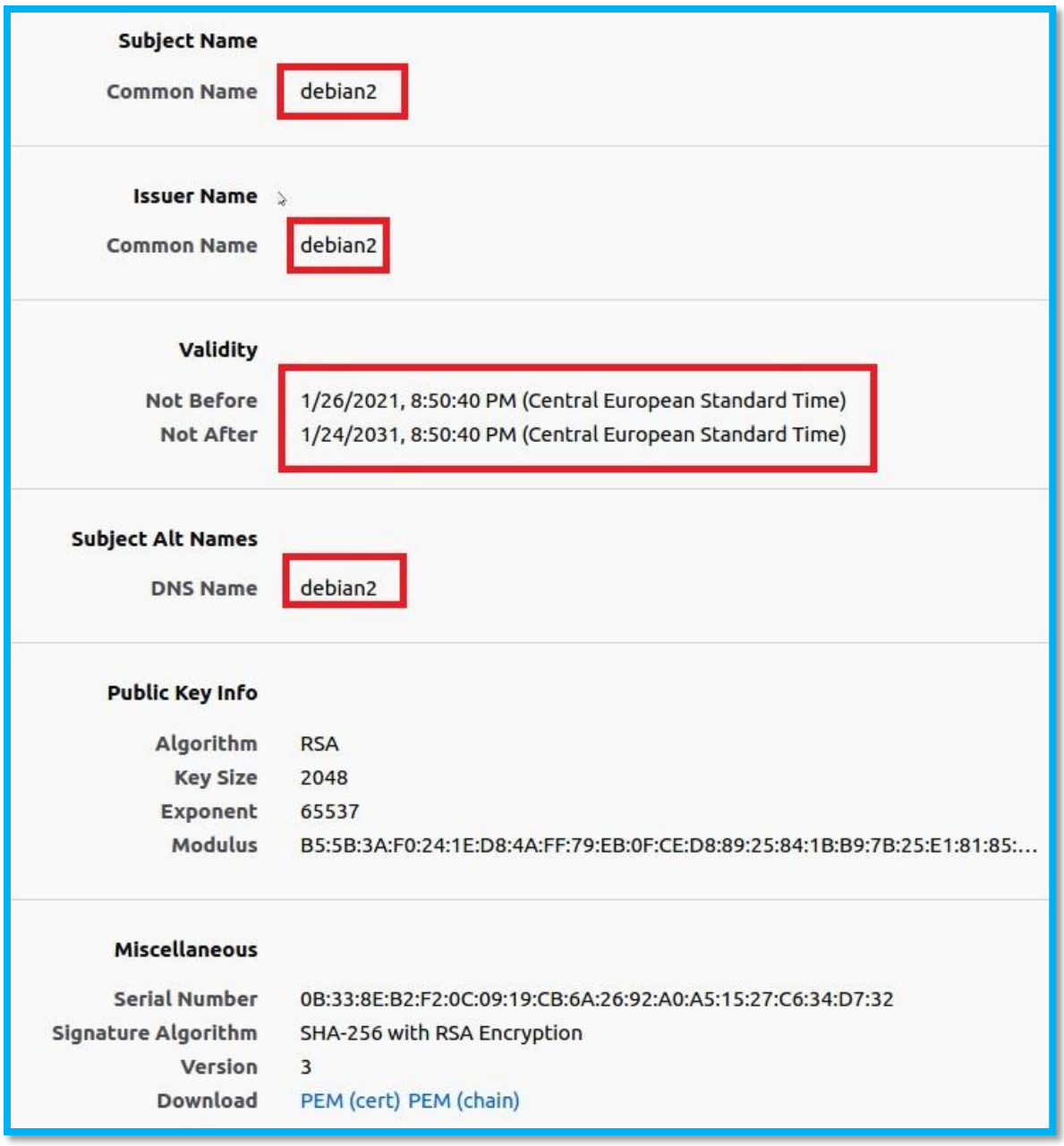
Probamos el funcionamiento de la página web



Ahora observaremos el certificado.

Le damos clic a ver el certificado

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



Francisco Javier López Calderón

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

```
web IN A 10.33.1.2
confidencial IN A 10.33.1.2
```

```
root@debian2:/var/www# mkdir superconfidencial
root@debian2:/var/www# cd superconfidencial/
```

Creamos el directorio superconfidencial

Creamos la página index y hacemos href con su alias

```
<h1>Página en confidencial</h1>
<a href="pepinaco"> Camino a superconfidencial </a>
```

```
<IfModule ssl_module>
        Listen 443
        Listen 444_
</IfModule>
```

Habilitamos el puerto 444 en el módulo ssl

Creamos y modificamos el archivo.conf

```
<VirtualHost _default_:444>

        ServerName confidencial.verysegura.org
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www/confidencial

        DirectoryIndex confi.html

        <Directory /var/www/confidencial>
                require all granted
                allowoverride none
                options indexes followsymlinks
        </Directory>

        Alias /pepinaco /var/www/superconfidencial

        <Directory /var/www/superconfidencial>
                require all granted
                options indexes followsymlinks
                allowoverride none
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        SSLEngine on

        SSLCertificateFile      /etc/ssl/certs/apache.crt
        SSLCertificateKeyFile /etc/ssl/private/apache.key
```

Y Activamos la zona

```
root@debian2:/etc/apache2/sites-available# a2ensite Segunport-ssl.conf
Enabling site Segunport-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

Podemos comprobar

Además, haciendo clic en el href accedemos a /superconfidencial