

Reto1-UD2

Servidor web seguro



DAW – 2

Kerin Aguilera – Mohamed Bada – Freddy de Andrade

Máquina virtual en AWS que responda a https y tenga una carpeta que solicite autenticación.

1. **https:** documenta el proceso explicado en clase, puedes seguir el tutorial del aula virtual u otro. Muestra el aviso del navegador y sus detalles. ¿Puedes añadir el certificado al navegador para decirle que lo considere de confianza?

Primero debemos habilitar el módulo ssl que nos permitirá usar el protocolo https usando el comando **sudo a2enmod ssl** :

```
ubuntu@ip-172-31-26-188: /var/www/html
ubuntu@ip-172-31-26-188:/var/www/html$ sudo a2enmod ssl
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 s
elf-signed certificates.
To activate the new configuration, you need to run:
systemctl restart apache2
```

Reiniciamos el servidor web de Apache para que los cambios se apliquen:

```
ubuntu@ip-172-31-26-188:/var/www/html$ sudo systemctl restart apache2
```

Al intentar verificar que hay un nuevo puerto que escucha en el 443 con el comando **netstat -nat**, no da un error, ya que debemos de instalar el net-tools. Lo instalamos con el comando **sudo apt install net-tools**:

```
ubuntu@ip-172-31-26-188:/var/www/html$ netstat -nat
Command 'netstat' not found, but can be installed with:
sudo apt install net-tools
ubuntu@ip-172-31-26-188:/var/www/html$ sudo apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
net-tools
0 upgraded, 1 newly installed, 0 to remove and 23 not upgraded.
Need to get 207 kB of archives.
After this operation, 1229 kB of additional disk space will be used.
Get:1 http://us-east-1.ec2.ports.ubuntu.com/ubuntu-ports noble-updates/main arm64
4 net-tools arm64 2.10-0.1ubuntu4.4 [207 kB]
Fetched 207 kB in 0s (11.3 MB/s)
Selecting previously unselected package net-tools.
```

Y podemos observar que ahora si funciona y si escucha en el puerto 443:

```
ubuntu@ip-172-31-26-188:/var/www/html$ netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 172.31.26.188:34728     52.87.202.145:80        TIME_WAIT
tcp        0    196 172.31.26.188:22        217.9.26.59:46026       ESTABLISHED
tcp6       0      0 :::443                  :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
```

Ahora creamos el directorio “seguro” y nos movemos a este. Hacemos un **sudo nano** para crear el **index.html**.

```
ubuntu@ip-172-31-26-188:/var/www/html$ sudo mkdir seguro
ubuntu@ip-172-31-26-188:/var/www/html$ cd seguro
ubuntu@ip-172-31-26-188:/var/www/html/seguro$ nano index.html
ubuntu@ip-172-31-26-188:/var/www/html/seguro$ ls
ubuntu@ip-172-31-26-188:/var/www/html/seguro$ sudo nano index.html
ubuntu@ip-172-31-26-188:/var/www/html/seguro$ ls
index.html
```

Volvemos y comprobamos que estamos en home:

```
ubuntu@ip-172-31-26-188:/var/www/html/seguro$ cd ~
ubuntu@ip-172-31-26-188:~$ pwd
/home/ubuntu
```

Creamos una clave privada RSA de 2048 bit con el comando **openssl genrsa -out seguro.key 2048** y comprobamos si se ha creado.

```
ubuntu@ip-172-31-26-188:~$ openssl genrsa -out seguro.key 2048
ubuntu@ip-172-31-26-188:~$ ls
seguro.key
```

Generamos una solicitud de certificado CSR e introducimos los datos que queremos:

```
ubuntu@ip-172-31-26-188:~$ openssl req -new -key seguro.key -out seguro.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]:IES Goya
Organizational Unit Name (eg, section) []:2daw012
Common Name (e.g. server FQDN or YOUR name) []:seguro.2daw012.net
Email Address []:

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

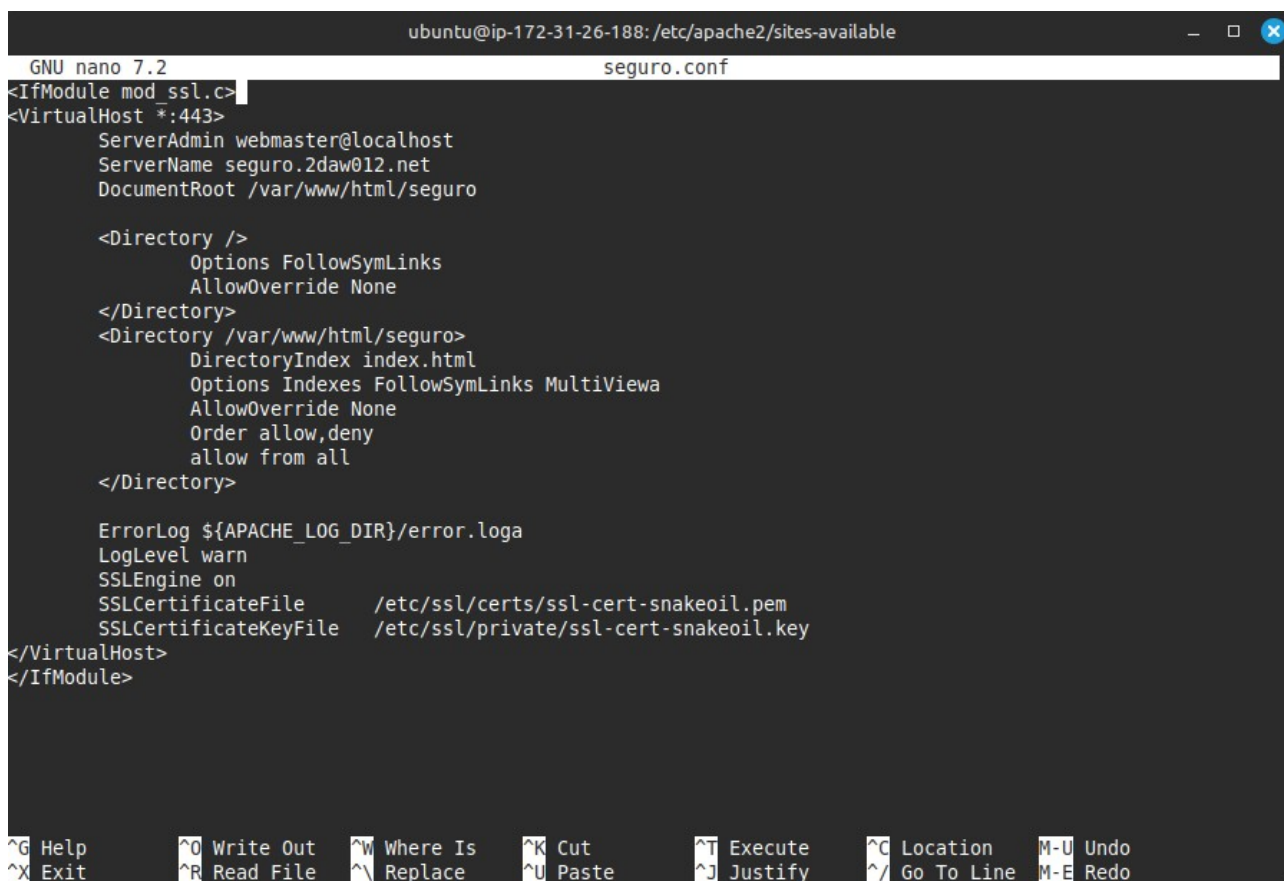
Creamos el certificado digital autofirmado usando la clave privada anterior:

```
ubuntu@ip-172-31-26-188:~$ openssl x509 -req -days 365 -in seguro.csr -signkey seguro.key -out seguro.crt
Certificate request self-signature ok
subject=C = ES, ST = Madrid, L = Madrid, O = IES Goya, OU = 2daw012, CN = seguro.2daw012.net
```

Copiamos la clave y el certificado en el directorio que utiliza por defecto Apache y le otorgamos los permisos necesarios para que funcione correctamente:

```
ubuntu@ip-172-31-26-188:~$ sudo cp seguro.key /etc/ssl/private/
sudo cp seguro.crt /etc/ssl/certs/
sudo chown root:ssl-cert /etc/ssl/private/seguro.key
sudo chmod 640 /etc/ssl/private/seguro.key
sudo chown root:root /etc/ssl/certs/seguro.crt
```

Creamos un fichero **seguro.conf** en la ruta de Apache de sitios disponibles **/etc/apache2/sites-available/seguro.conf** con las mismas directivas que el archivo **default-ssl** que ya venía creado, pero eliminando las líneas sobrantes y modificando el resto:



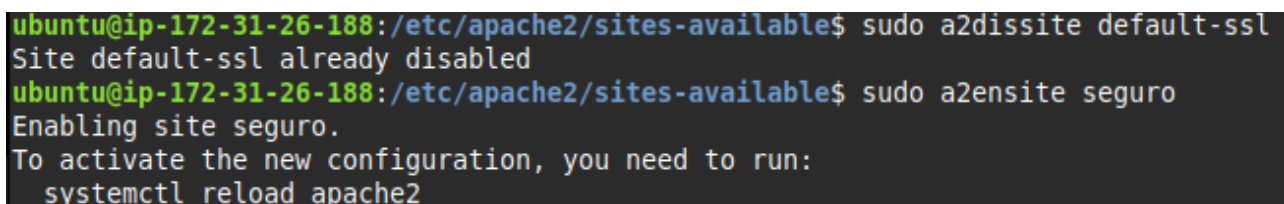
```
ubuntu@ip-172-31-26-188: /etc/apache2/sites-available
GNU nano 7.2                                seguro.conf
<IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName seguro.2daw012.net
    DocumentRoot /var/www/html/seguro

    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    <Directory /var/www/html/seguro>
        DirectoryIndex index.html
        Options Indexes FollowSymLinks MultiView
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    LogLevel warn
    SSLEngine on
    SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile   /etc/ssl/private/ssl-cert-snakeoil.key
</VirtualHost>
</IfModule>

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location  M-U Undo
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo
```

Deshabilitamos el servidor ssl por defecto con el comando **sudo a2dissite default-ssl** y vemos que se deshabilita. Además habilitamos el servidor virtual seguro con el comando **sudo a2ensite seguro** y nos pide reiniciar Apache para que se apliquen los cambios:



```
ubuntu@ip-172-31-26-188:/etc/apache2/sites-available$ sudo a2dissite default-ssl
Site default-ssl already disabled
ubuntu@ip-172-31-26-188:/etc/apache2/sites-available$ sudo a2ensite seguro
Enabling site seguro.
To activate the new configuration, you need to run:
    systemctl reload apache2
```

Intentamos reiniciar el servidor Apache pero nos salta un error. Al ver los detalles de este error con un status, observamos que se encuentra en la línea 13 y se debe a que pusimos mal la palabra MultiViews, poniendo en su lugar MiltiViewa.

```
ubuntu@ip-172-31-26-188:/etc/apache2/sites-available$ sudo systemctl reload apache2
Job for apache2.service failed.
See "systemctl status apache2.service" and "journalctl -xeu apache2.service" for details.
ubuntu@ip-172-31-26-188:/etc/apache2/sites-available$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-10-30 09:53:11 UTC; 1h 7min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 1247 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Process: 7999 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=1/FAILURE)
 Main PID: 1251 (apache2)
    Tasks: 7 (limit: 1080)
  Memory: 16.0M (peak: 19.0M)
     CPU: 333ms
    CGroup: /system.slice/apache2.service
            └─1251 /usr/sbin/apache2 -k start
              1253 /usr/sbin/apache2 -k start
              1254 /usr/sbin/apache2 -k start
              1255 /usr/sbin/apache2 -k start
              1256 /usr/sbin/apache2 -k start
              1257 /usr/sbin/apache2 -k start
              1919 /usr/sbin/apache2 -k start

Oct 30 09:53:11 ip-172-31-26-188 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Oct 30 09:53:11 ip-172-31-26-188 systemd[1]: Started apache2.service - The Apache HTTP Server.
Oct 30 10:59:59 ip-172-31-26-188 systemd[1]: Reloading apache2.service - The Apache HTTP Server.
Oct 30 10:59:59 ip-172-31-26-188 apachectl[8002]: AH00526: Syntax error on line 13 of /etc/apache2/sites-enabled/seguro.conf:
Oct 30 10:59:59 ip-172-31-26-188 apachectl[8002]: Illegal option MultiViewa
Oct 30 10:59:59 ip-172-31-26-188 systemd[1]: apache2.service: Control process exited, code=exited, status=1/FAILURE
Oct 30 10:59:59 ip-172-31-26-188 systemd[1]: Reload failed for apache2.service - The Apache HTTP Server.
```

Volvemos a editar el archivo sustituyendo MultiViewa por MultiViews:

```
ubuntu@ip-172-31-26-188:/etc/apache2/sites-available$ nano seguro.conf
GNU nano 7.2
<IfModule mod ssl.c>
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName seguro.2daw012.net
    DocumentRoot /var/www/html/seguro

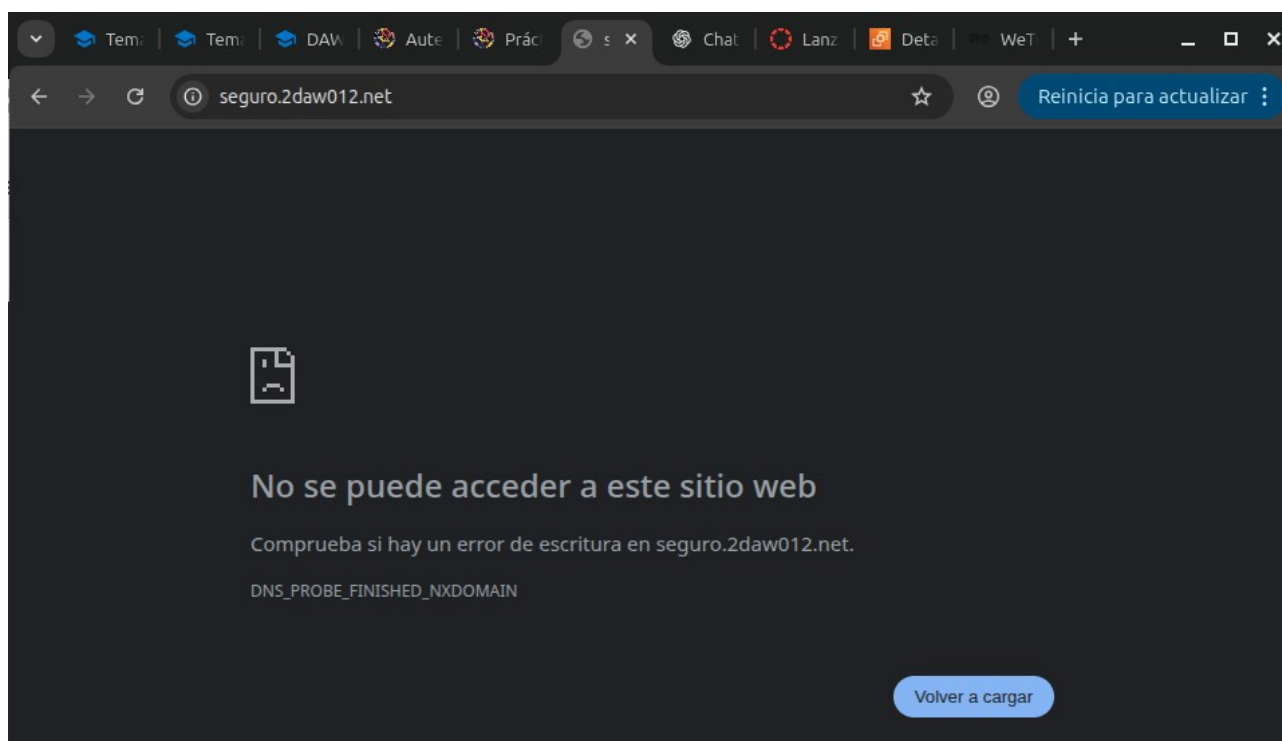
    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    <Directory /var/www/html/seguro>
        DirectoryIndex index.html
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    LogLevel warn
    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
</VirtualHost>
</IfModule>
```


Nos movemos a **sites-enabled** donde se guardan todas las configuraciones de sitios que están activos. Hacemos un **ls -l** para ver una lista detallada de los archivos del directorio y vemos que si se encuentra el archivo **seguro.conf** que hemos creado

```
ubuntu@ip-172-31-26-188:/etc/apache2/sites-available$ cd /etc/apache2/sites-enabled/
ubuntu@ip-172-31-26-188:/etc/apache2/sites-enabled$ ls
000-default.conf  seguro.conf
ubuntu@ip-172-31-26-188:/etc/apache2/sites-enabled$ ls -l
total 0
lrwxrwxrwx 1 root root 35 Oct  9 08:56 000-default.conf -> ../sites-available/000-default.conf
lrwxrwxrwx 1 root root 30 Oct 30 10:59 seguro.conf -> ../sites-available/seguro.conf
ubuntu@ip-172-31-26-188:/etc/apache2/sites-enabled$
```

Al intentar buscar la dirección **seguro.2daw013.net** nos salta un error de que no se pudo acceder a la página web



```
ubuntu@ip-172-31-26-188:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 0a:ff:f8:10:4f:85 brd ff:ff:ff:ff:ff:ff
    inet 172.31.26.188/20 metric 100 brd 172.31.31.255 scope global dynamic ens5
        valid_lft 2706sec preferred_lft 2706sec
    inet6 fe80::8ff:f8ff:fe10:4f85/64 scope link
        valid_lft forever preferred_lft forever
```

Tampoco nos deja conectarnos a la página usando el comando curl, ya que el equipo del aula no tiene los permisos para editar los archivos necesarios para entrar en https:

```
ubuntu@ip-172-31-26-188:~$ curl -k --resolve seguro.2daw012.net:443:172.31.26.188 https://seguro.2daw012.net
```


Máquina virtual con ubuntu server 24.04 sin entorno gráfico.

Configurarás la redirección de puertos para que responda a <https://localhost:8443/privado/>

1. <https://localhost:8443/privado/>: documenta el proceso explicado en clase, puedes seguir el tutorial del aula virtual u otro. Muestra el aviso del navegador y sus detalles. ¿Puedes añadir el certificado al navegador para decirle que lo considere de confianza?

Primero instalamos Apache en nuestra maquina de Ubuntu Server y vemos que se ha instalado correctamente:

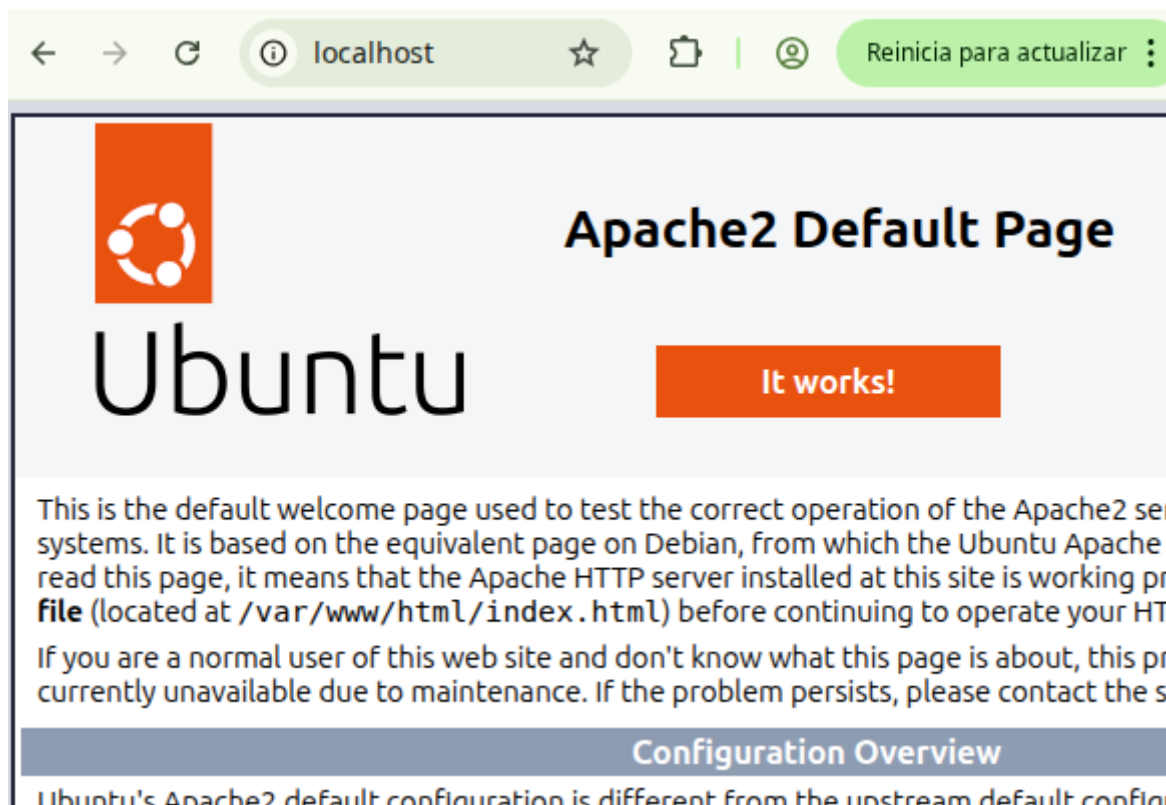
```
sif in 🌐 patoLaVida in ~
> sudo apt install apache2 -y
[sudo] password for sif:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
El paquete indicado a continuación se instaló de forma automática y ya no es necesario.
libstdc++-13-dev
```

Comprobamos el estado del servidor con un status y observamos que se encuentra activo y funciona correctamente:

```
sif in 🌐 patoLaVida in ~
+ > sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-10-30 09:50:03 UTC; 1min 35s ago
     Docs: https://httpd.apache.org/docs/2.4/
  Main PID: 2653 (apache2)
    Tasks: 55 (limit: 4524)
   Memory: 5.2M (peak: 5.5M)
      CPU: 34ms
   CGroup: /system.slice/apache2.service
           └─2653 /usr/sbin/apache2 -k start
             └─2656 /usr/sbin/apache2 -k start
               └─2657 /usr/sbin/apache2 -k start

oct 30 09:50:03 patoLaVida systemd[1]: Starting apache2.service - The Apache HTTP Server..
oct 30 09:50:03 patoLaVida apachectl[2652]: AH00558: apache2: Could not reliably determine
oct 30 09:50:03 patoLaVida systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-16/16 (END)
```

Al buscar <http://localhost> nos devuelve la página por defecto de Apache:



Desde el VirtualBox hacemos unas modificaciones en los ajustes para que nos reenvíe desde el puerto 8443 al 443 :

Reglas de reenvío de puertos					
Nombre	Protocolo	IP anfitrión	Puerto anfitrión	IP invitado	Puerto invitado
APACHEHTTPS	TCP		8443		443

Ahora habilitamos el certificado SSL con el comando **sudo a2enmod ssl**:

```
/etc/apache2#  
2 ■ sudo a2enmod ssl  
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 certificates.  
To activate the new configuration, you need to run:  
systemctl restart apache2
```

Además activamos el sitio SSL por defecto en Apache:

```

/etc/apache2 ■
■ ■ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2

/etc/apache2 ■
■ ■

```

Reiniciamos el servidor apache para aplicar el cambio:

```

/etc/apache2#
#2 # sudo systemctl restart apache2.service

/etc/apache2#
#2 #

```

Intentamos crear un certificado ssl valido para 1 año (365 dias) y que cifre las comunicaciones ente el servidor y el cliente pero nos salta un error:

```

/etc/apache2#
02 # sudo openssl req -x509 -nodes -day 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt
req: Use -help for summary.

/etc/apache2#
02 # r

```

Finalmente lo conseguimos :

[illegible]

Y lo configuramos a nuestro gusto, en Country Name ponemos España pero no nos deja porque admite solo 2 bytes, por lo que ponemos solo sp. En Province y en Locality ponemos Madrid. Como nombre de organización ponemos Bernabeu:

```
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]: España
String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]: esp
String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]: sp
State or Province Name (full name) [Some-State]: Madrid
Locality Name (eg, city) []: Madrid
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Bernabeu
Organizational Unit Name (eg, section) []: Bernabeu
Common Name (e.g. server FQDN or YOUR name) []: Beu
Email Address (e.g. jdoe@example.com):
```

Creamos un archivo **apacheSeguro.conf** con el comando `sudo nano`:

```
/etc/apache2 ■
■2 ■ sudo nano /etc/apache2/sites-available/apacheSeguro.conf
```

Añadimos la configuraciones mínimas para el archivo **apacheSeguro.conf**, como por ejemplo que escuche en el puerto 443, el nombre del servidor, la ruta, etc.:

```
/etc/apache2 ■
■2 ■ cat /etc/apache2/sites-available/apacheSeguro.conf
<VirtualHost *:443>
    ServerName apacheSeguro
    DocumentRoot /var/www/apacheSeguro

    SSLEngine on
    SSLCertificate /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
</VirtualHost>

/etc/apache2 ■
■2 ■ _
```

Habilitamos la configuración de apacheSeguro con el comando **sudo a2ensite**:

```
/var/www/privado ■  
#2 ■ sudo a2ensite apacheSeguro.conf  
Site apacheSeguro already enabled  
  
/var/www/privado ■  
#2 ■
```

Realizamos una prueba para ver que no hay errores en la configuración, y vemos que tenemos varios errores de sintaxis:

```
/var/www/privado ■  
#2 ■ sudo apache2ctl configtest  
apache2: Syntax error on line 225 of /etc/apache2/apache2.conf: Syntax error on line 1 of /etc/apache2/sites-enabled/apacheSeguro.conf: /etc/apache2/sites-enabled/apacheSeguro.conf:8: <VirtualHost> was not closed.\n/etc/apache2/sites-enabled/apacheSeguro.conf:1: <VirtualHost> was not closed.  
  
/var/www/privado ■  
#2 ■
```