

# **Práctica 2.6. Servidor Web Seguro**

Alejandro Priego Izquierdo

## 1. Describe con tus palabras:

- ¿Qué es un servidor web seguro?

Este es aquel en el cual el tráfico entre el cliente y el propio servidor circula de forma cifrada.

¿Qué es el archivo .pem?

Esto significa que es un archivo de certificado.

- ¿Qué es el archivo .csr y qué contiene?

Este es un archivo que contiene información codificada sobre la compañía, y suele usarse para pedir certificados como por ejemplo el de SSL.

- ¿Qué es archivo .key?

Esta es la llave privada que corresponde a una llave pública.

- ¿Cuál/es de todos estos tiene el servidor? ¿Y los clientes?

El servidor tiene el .key (Llave privada) mientras que los clientes tienen el .pem (Llave pública)

## 2. Genera tu propio certificado con OpenSSL.

2.1. Instala previamente el openssl: apt install openssl

```
apriego@priegoDAWServer:/var/www/ww2/apache$ sudo apt install openssl
[sudo] password for apriego:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssl is already the newest version (3.0.2-0ubuntu1.14).
openssl set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 47 not upgraded.
```

2.2. Modifica el fichero openssl.conf con información de la empresa, país, etc.

```
[ req_distinguished_name ]
countryName               = Country Name (2 letter code)
countryName_default       = ES
countryName_min           = 2
countryName_max           = 2

stateOrProvinceName       = Cordoba
stateOrProvinceName_default = Cordoba

localityName              = Cordoba

0.organizationName        = priegoDAW2
0.organizationName_default = priegoDAW2

# we can do this but it is not needed normally :-))
#1.organizationName       = Second Organization Name (eg, company)
#1.organizationName_default = World Wide Web Pty Ltd

organizationalUnitName     = Organizational Unit Name (eg, section)
#organizationalUnitName_default =

commonName                 = Alejandro Priego
commonName_max             = 64

emailAddress               = alejandro@pfagot.com
emailAddress_max           = 64

# SET-ex3                  = SET extension number 3


[ req_attributes ]
```

### 2.3. Genera el .pem

[illegible]

### 3. Configuración del sitio web seguro y acceso desde un cliente.

3.1. Sigue los pasos del curso para conseguir acceder también en modo seguro (https) a tu página web de prueba.



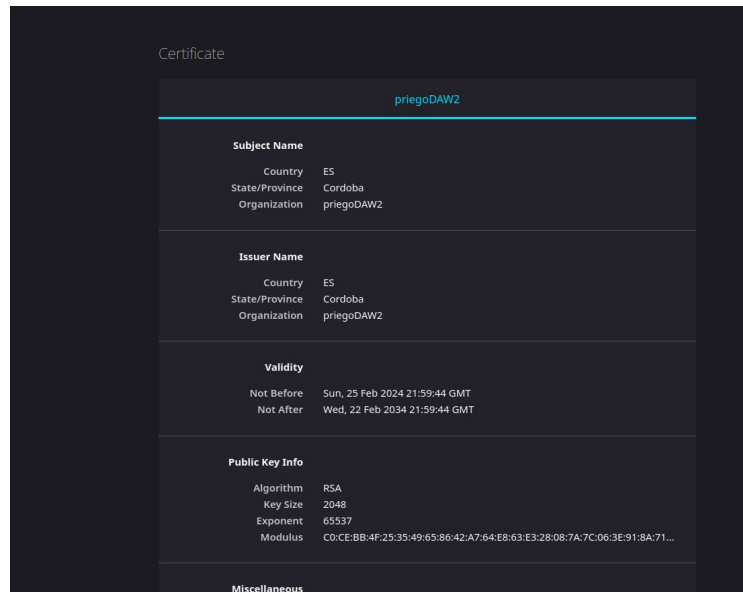
## Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **ww3.priegotaw2.org**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

[Learn more...](#)

Go Back (Recommended)

Advanced...



### 3.2. Configurar el servidor web para acceder por https.

Muestra los cambios en el fichero de configuración del sitio web.

```
GNU nano 6.2 /etc/nginx/sites-available
server {
    listen 443 ssl;
    listen [::]:443 ssl;

    ssl_certificate /etc/ssl/certs/priego.pem;
    ssl_certificate_key /etc/ssl/private/priego.key;
    ssl_password_file /var/lib/nginx/ssl_passwords.txt;

    root /var/www/ww3/nginx;

    index index.html index.htm index.nginx-debian.html;

    server_name ww3.priegodaw2.org;

    location / {
        try_files $uri $uri/ =404;
        autoindex on;
    }
}
```

### 3.3. Prueba el servidor web seguro:

a) Haz una captura de pantalla, tanto de forma segura (https)

<https://IPdelservidorwebvirtual>



b) ....como de forma 'insegura' (http):

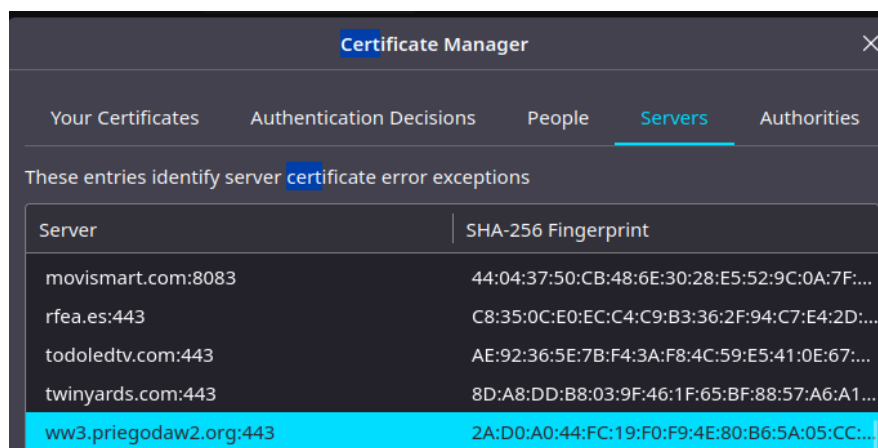
<http://IPdelservidorwebvirtual>



¿Qué ocurre? ¿Cuál está funcionando correctamente y cuál no?

Está cargando WW2 ya que no tiene configuración para la escucha en :81 por WW3.

c) muestra el certificado que se ha añadido a tu lista de certificados del navegador.



### 3.4. Forzar ahora que lo anterior funcione, es decir, aunque se acceda de modo no seguro (http) hacer que se pase a modo seguro (https).

<https://techexpert.tips/es/nginx-es/nginx-redirigir-http-a-https/>

Usar para ello "RETURN" (REDIRECT en Apache) de modo que al acceder por http automaticamente te redirija a https.

Ahora la configuración del \*:80 se elimina y sólo queda la mínima para que se acceda e inmediatamente se redirija al site seguro (return)

La configuración del site completa estará en el \*:443

```
GNU nano 6.2 /etc/nginx/sites-avail
server {
    listen 80;
    listen [::]:80;
    server_name ww3.priegodaw2.org;
    return 301 https://$host$request_uri;
}

server {
    listen 443 ssl;
    listen [::]:443 ssl;

    ssl_certificate /etc/ssl/certs/priego.pem;
    ssl_certificate_key /etc/ssl/private/priego.key;
    ssl_password_file /var/lib/nginx/ssl_passwords.txt;

    root /var/www/ww3/nginx;

    index index.html index.htm index.nginx-debian.html;

    server_name ww3.priegodaw2.org;

    location / {
        try_files $uri $uri/ =404;
        autoindex on;
    }
}
```