# Pràctica 2c: Autenticació i encriptació amb HTTPS

## - Configura HTTPS amb Apache en el servidor Debian

**a)** Crea la carpeta **/var/www/html/daw2s**. Fes que **www-data** sigui el usuari i el grup amb permisos especials sobre la carpeta **/var/www/html/daw2s**. Dóna a permís de **rwx** sobre **/var/www/daw2s** a l'usuari **www-data**. La resta d'usuaris no han de tenir cap permís d'accés a la carpeta.

```
root@debian:/home/daw# mkdir /var/www/html/daw2s
root@debian:/home/daw# ls /var/www/html
asix  dam  daw  daw2s  index.html  info.php
```

```
root@debian:/home/daw# chown www-data:www-data /var/www/html/daw2s/
root@debian:/home/daw# chmod 775 -R /var/www/html/daw2s/
```

**b)** Crea el fitxer **index.html** dins de **/var/www/daw2s**:

```
<html>
        <title>
                web segura del lloc www.daw2s.net
        </title>
        <body>
                <h2>P&agrave;gina d'inici de www.daw2s.net</h2>
                Aquesta web nom&eacute;s &eacute;s accesible via https<br>
                <i>Creador del lloc: Nom PrimerCognom</i><br>
           </
         body>
</html>
```

```
root@debian:/home/daw# cat /var/www/html/daw2s/index.html
<html>
<title>
web segura del lloc www.daw2s.net
</title>
<body>
<h2>P&agrave;gina d'inici de www.daw2s.net</h2>
Aquesta web nom&eacute;s &eacute;s accesible via https<br>
<i>Creador del lloc: Manel Castellvi Cerezuela</i><br>
</body>
</html>
```

Fes que **www-data** sigui el usuari i el grup amb permisos especials sobre **index.html**. Dóna permís de **rwx** sobre **/var/www/daw2s**. La resta d'usuari no han de tenir cap permís d'accés a la carpeta.

```
root@debian:/home/daw# chown www-data:www-data /var/www/html/daw2s/index.html
root@debian:/home/daw#
```

**c)** Instal·la en el teu servidor un certificat de seguretat autosignat i una clau pública, seguint els següents passos:

NO ES EL DEL MOODLE, EL CREO JO, QUE ES L'APARTAT 4

```
root@debian:/etc/ssl# openssl genrsa -out daw2.key 8192
Generating RSA private key, 8192 bit long modulus (2 primes)
.....
.....
.....
.....
.....
.....
.....+++
.....
.....
.....+++
e is 65537 (0x010001)
```

```
root@debian:/etc/ssl#  openssl req -new -key daw2.key -out daw2.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]:Tarragona
Locality Name (eg, city) []:Tarragona
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Vidal
Organizational Unit Name (eg, section) []:DAW2
Common Name (e.g. server FQDN or YOUR name) []:manel castellvi
Email Address []:admin@daw2s.net

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@debian:/etc/ssl#
```

```
root@debian:/etc/ssl# openssl x509 -req -days 365 -in daw2.csr -signkey daw2.key
 -out daw2.crt
Signature ok
subject=C = ES, ST = Tarragona, L = Tarragona, O = Vidal, OU = DAW2, CN = manel
castellvi, emailAddress = admin@daw2s.net
Getting Private key
root@debian:/etc/ssl# cp daw2.key private/
root@debian:/etc/ssl# cp daw2.crt certs/
root@debian:/etc/ssl# systemctl restart apache2
```

**d)** Crea l'arxiu de configuració d'un lloc virtual **www.daw2s.net** seguint els següents pasos:

**1r pas)** Crea un arxiu de configuració de nom **daw2s.conf** dins del directori **/etc/apache2/sites-available**. amb el següent contingut:

```
<IfModule mod_ssl.c>
    <VirtualHost *:443>
            ServerAdmin webmaster@daw2s.net
            ServerName www.daw2s.net
            ServerAlias web.daw2s.net
            DocumentRoot /var/www/daw2s
            ErrorLog ${APACHE_LOG_DIR}/error.log
            CustomLog ${APACHE_LOG_DIR}/access.log combined
            DirectoryIndex index.html index.php
            SSLEngine on
            SSLCertificateFile /etc/ssl/certs/daw2.crt
            SSLCertificateKeyFile /etc/ssl/private/daw2.key
    </VirtualHost>
</IfModule>
```

```
  GNU nano 5.4          /etc/apache2/sites-available/daw2s.conf
<IfModule mod_ssl.c>
        <VirtualHost *:443>
                ServerAdmin webmaster@daw2s.net
                ServerName www.daw2s.net
                ServerAlias web.daw2s.net
                DocumentRoot /var/www/html/daw2s
                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined
                DirectoryIndex index.html
                SSLEngine on
                SSLCertificateFile /etc/ssl/certs/daw2.crt
                SSLCertificateKeyFile /etc/ssl/private/daw2.key
                #SSLEngine off
        </VirtualHost>
</IfModule>
```

**e)** Activa el lloc web virtual **www.daw2s.net** executant **a2ensite daw2s.conf**.

```
root@debian:/etc/apache2/sites-available# a2ensite daw2s.conf
Site daw2s already enabled
root@debian:/etc/apache2/sites-available#
```

**f)** Carrega el mòdul **SSL** del servidor **Apache**. Executa: **a2enmod ssl**. Comprova que s'ha carregat amb l'ordre. Executa: **apachectl -M**.

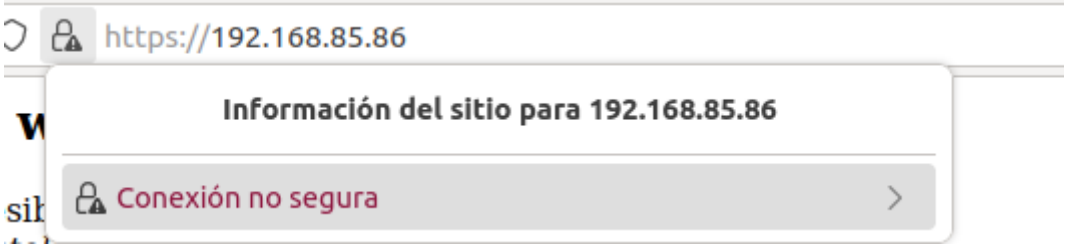
```
root@debian:/etc/apache2/sites-available# apachectl -M
Loaded Modules:
 core_module (static)
 so_module (static)
 watchdog_module (static)
 http_module (static)
 log_config_module (static)
 logio_module (static)
 version_module (static)
 unixd_module (static)
 access_compat_module (shared)
 alias_module (shared)
 auth_basic_module (shared)
 authn_core_module (shared)
 authn_file_module (shared)
 authz_core_module (shared)
 authz_host_module (shared)
 authz_user_module (shared)
 autoindex_module (shared)
 deflate_module (shared)
 dir_module (shared)
 env_module (shared)
 filter_module (shared)
 mime_module (shared)
```

**g)** Reinicia **Apache2**.Comprova que el servidor **Apache2** s'executa i **escolta** pel **port 443/tcp**.

```
root@debian:/etc/ssl# systemctl restart apache2
root@debian:/etc/ssl#
```

## 2- Accedint al lloc segur des de la màquina client amb el navegador Firefox

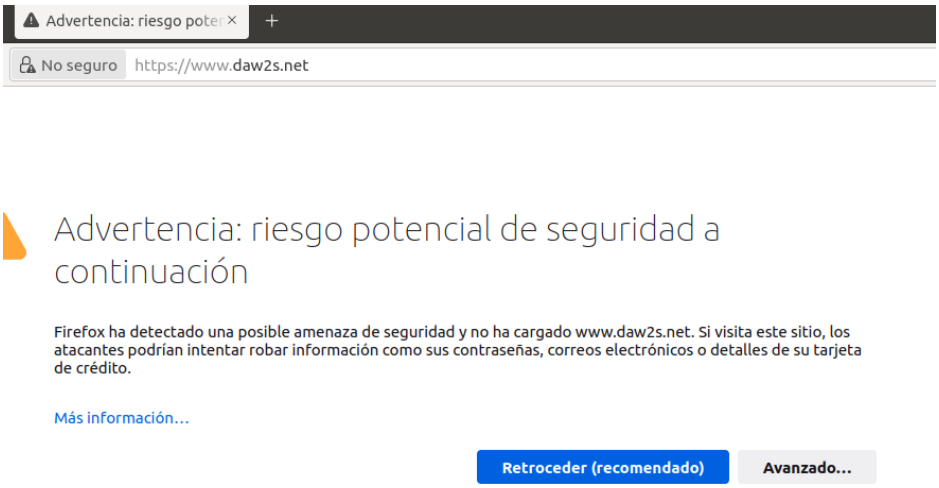
**a)** Comprova l'adreça IP de la màquina virtual a on has creat el lloc virtual segur **www.daw2s.net**.



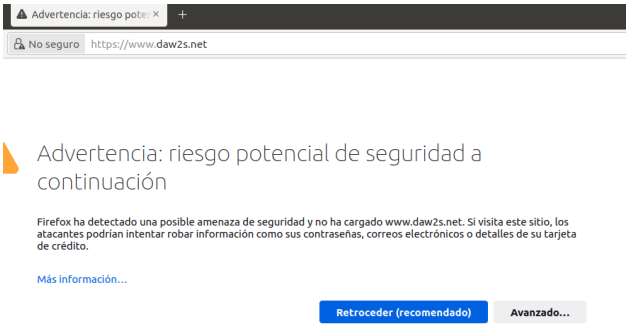

**b)** Modifica el fitxer **/etc/hosts** (Linux/MAC) o **c:\windows\system32\drivers\etc\hosts** (Windows) i afegeix una nova línia a on surti l'adreça IP del servidor debian i el nom del lloc virtual.
Fet anteriorment

**c)** Des del navegador, estableix una connexió segura amb el servidor debian, establint una connexió a la següent URI:

**https://www.daw2s.net**




**d)** En el moment de connectar-te, el navegador dóna l'avís que la connexió no és segura. Fes click a l'opció **Avançat** i comprova el motiu d'aquest avís.



**e)** Afegeix l'excepció de seguretat i aconsegueix el certificat. Visualitza'l. Busca el número de sèrie i la data de venciment i anota'ls.


**f)** Confirma l'excepció de seguretat i comprova que pots accedir a la web del lloc virtual **www.daw2s.net**.

**h)** Comprova que has carregat el certificat en el teu navegador. Des de **Firefox**, obre Edita --> Privadesa i seguretat --> Certificats --> Visualitza els certificats. Troba el certificat del servidor **www.daw2s.net**.

**i)** Tanca el navegador i torna a connectar-te al lloc virtual. Comprova que ara has entrat directament perquè el certificat està carregat.
Fet


**j)** Comprova que passa si realitzes una connexió a **http://www.daw2s.net** (http no https). Quin lloc virtual ens mostra el servidor?
M'envia a la pagina per defecte: