Tasca 1. Mira aquest vídeo i explica els seguents punts:
https://www.youtube.com/watch?v=THxIyHz191A&ab_channel=HighPerformanceProgramming

a)Quin és el protocol de xifrat que fa servir HTTPS?

- ➔ HTTPS uses the TLS protocol.

b)Quina és la diferència entre SSL i TLS?

- ➔ SSL is the older version of TLS which is the updated and more secure version of SSL.

c)De quines dues fases consta el protocol TLS?

Consist of 2 phases:

- ➔ Handshake phase
  - ◆ It is for authentication, the server provides a TLS certificate and then they use public key protocol for the authentication. Its purpose is to establish a shared secret key that will be used in the second phase.
- ➔ Encryption phase
  - ◆ The shared secret key will be used to encrypt all outgoing messages, first the encrypted messages are transmitted to the other side than they'll verify to see if there where any modification during the transmission if not the message will be decrypted with the same symmetric secret key (symmetric cuz its used to encrypt and decrypt them)

d)A la fase de handshake, quin extrem HTTP proporciona el certificat SSL/TLS?

- ➔ In the handshake phase the server provides a TLS/SSL certificate to the client to verify its identity.

e)Com s'aconsegueix un certificat SSL/TLS?

- ➔ An TLS/SSL certificate is obtained from Certificate Authority(CA) which verifies the identity of the company or organization and issues the certificate.

f)Com es pot garantir que la clau de sessió generada pel client a la fase de handshake només podrà ser desencriptada pel servidor que ha presentat el certificat?

- ➔ The session key is encrypted with the server's public key, which can only be decrypted using the corresponding private key held by the server.

g)Quina clau es fa servir per encriptar els missatges HTTP: la clau pública o la privada (clau de sessió)?

- ➔ After the handshake, the session key is used for encrypting HTTP messages as it is faster and more efficient.

h)El procés d'encriptació és simètric o asimètric?

- ➔ During the handshake, encryption is asymmetric (public and private keys).
- ➔ During data transmission, encryption is symmetric (session key).

i)Què vol dir que el protocol TLS proporciona també integritat de dades?

Tasca 2. Crea un servidor virtual pel domini www.securesite.org. Comprova que pots accedir-hi des del navegador i que aquest la considera una web no segura.

- En nano /etc/hosts

```
 GNU nano 7.2                                    /etc/hosts *
127.0.0.1 localhost
127.0.1.1 aarati
127.0.0.1 www.securesite.org
```

- crear fichero

```
root@aarati:~# mkdir -p /var/www/securesite
```

```
root@aarati:~# sudo chown -R www-data:www-data /var/www/securesite
```

- index de página

```
root@aarati:~# nano /var/www/securesite/index.html
```

```
 GNU nano 7.2                          /var/www/securesite/index.html *
<!DOCTYPE html>
<html lang="en">
<head>
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <title>Secure site</title>
</head>
<body>
        <h1>Welcome to SecureSite.org!</h1>
</body>
</html>
```

- virtual host file

```
root@aarati:~# nano /etc/apache2/sites-available/securesite.org.conf
```

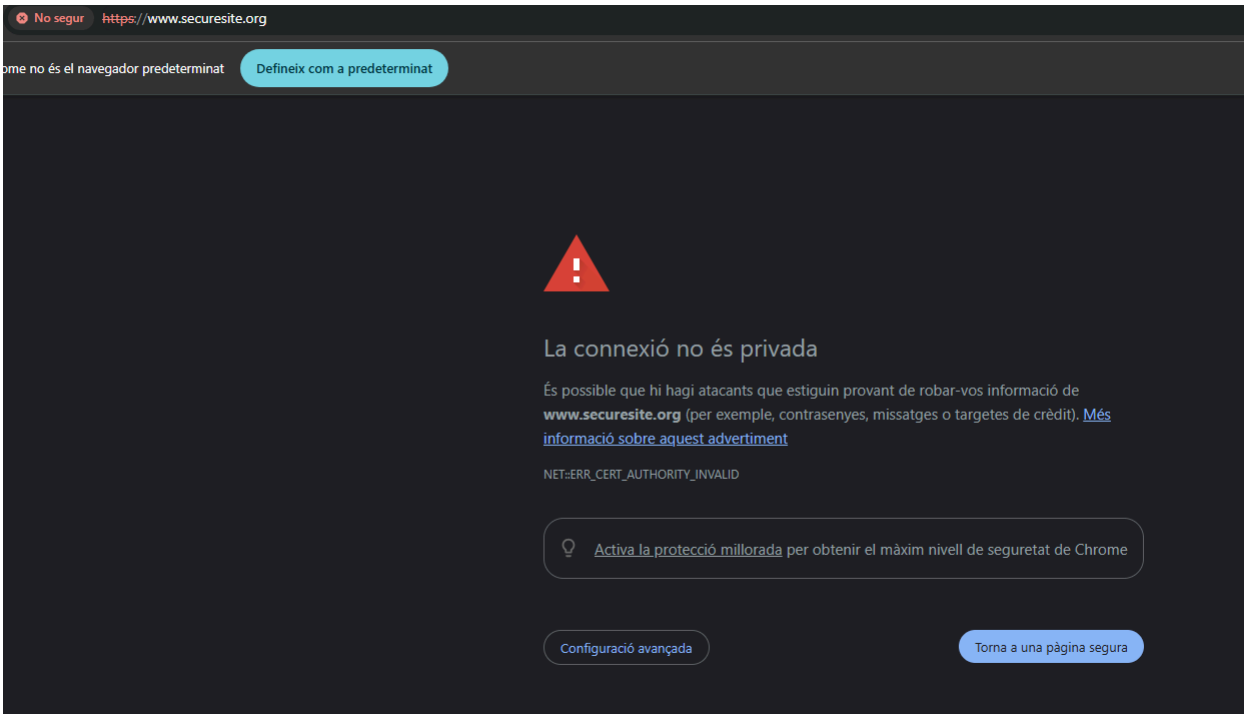
- enable

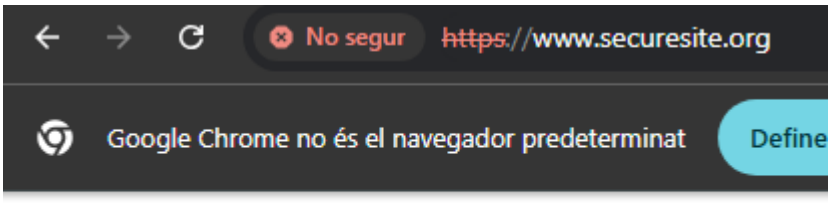
```
root@aarati:~# sudo a2ensite securesite.org.conf
Enabling site securesite.org.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@aarati:~# sudo systemctl reload apache2
root@aarati:~#
```

```
<VirtualHost *:80>
        ServerName www.securesite.org
        DocumentRoot /var/www/html/securesite

        <Directory /var/www/html/securesite>
                Options -Indexes +FollowSymLinks
                AllowOverride All
                Require all granted
        </Directory>

</VirtualHost>
```





Welcome to Secure site

Tasca 3. A continuació, aconseguirem un certificat (més una clau pública) per a que el nou servidor virtual en faci ús.

a)Crea una carpeta certs al directori principal de configuració d'Apache.

```
root@aarati:~# mkdir /etc/apache2/certs
```

b)Utilitza l'eina openssl per a crear un parell certificat + clau pública pel teu servidor: sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout dawac6.key -out dawac6.crt
Openssl et demanarà una serie de dades per a incloure en el certificat:

```
root@aarati:/etc/apache2/certs# sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout dawac6.key -o
ut dawac6.crt
.....+.........+...+..+.........................+...+.........+.....++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++*.....+.........++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
...........+.+........+.+...+........+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.+.....+....+.....+.....+.+.........+.........+........+...+.+.........+........+..+.........+...+..+.....
....+.........+..+....+.....+....+.....+......+.........+...+.....+.........+..+.+...+.....+....++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++*....+........+.+......+................+...+.........+.....+....+.....+.+...+..+.........+.+
...+......+.........+.....+.......+...+..+.......+..+.........+........+.+.....+.+................+...+....
.+.......+...+................+...+...+.+...+......+..+...+.........+.................+...+.....+.......
.....+.+...+..+.......+..+....+...........+....+.........+.....+.+..+...+.............+.+.............+++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
-----
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]:Barcelona
Locality Name (eg, city) []:Barcelona
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ETPX
Organizational Unit Name (eg, section) []:DAW
Common Name (e.g. server FQDN or YOUR name) []:www.securesite.org
Email Address []:
```

c)Comprova que s'han generat els fitxers dawac6.crt i dawac6.key.

```
root@aarati:/etc/apache2/certs# ls
dawac6.crt  dawac6.key
root@aarati:/etc/apache2/certs#
```

d)Abans de continuar, analitzem la comanda que hem fet servir: per què hem fet servir l'opció -x509?

➔ La opción -x509 indica a OpenSSL que debe crear un certificado autosignado en formato X.509. Este formato es un estándar utilizado en protocolos de seguridad como TLS/SSL para garantizar que las comunicaciones sean seguras y auténticas.

Tasca 4. En aquest cas, hem generat un certificat autosignat: és a dir, un certificat signat, no per una autoritat certificadora, sinò pel propi administrador del servidor. Tot i que hi ha CAs (certification authorities) que proveeixen certificats de manera gratuïta (per exemple, cacert.org), és necessari tenir un domini propi (i públic) per a poder demanar-ne un.

a)Investiga quina és la limitació, de cara als clients, de l'ús de certificats autosignats.

➔ No es confiable para el navegador porque el certificado no está firmado por una Autoridad de Certificación (CA)..

b)Investiga quines són les principals autoritzats certificadores actuals.

➔ Let's Encrypt, DigiCert, GlobalSign, etc.

Tasca 5. (Continuem amb tasca 3). Per a poder fer servir el xifrat SSL en el nostre servidor, hem de fer algunes configuracions:

a)Activa el mòdul ssl.

```
root@aarati:~# 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
root@aarati:~# systemctl restart apache2
root@aarati:~#
```

b)Canvia la configuració del servidor virtual que volem securitzar (www.securesite.org), de la següent manera:

```
<VirtualHost *:80>
        ServerName www.securesite.org
        DocumentRoot /var/www/securesite

        <Directory /var/www/securesite>
                Options Indexes FollowSymLinks
                AllowOverride None
                Require all granted
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/securesite_error.log
        CustomLog ${APACHE_LOG_DIR}/securesite_access.log combined

        SSLEngine on
        SSLCertificateFile /etc/apache2/certs/dawac6.crt
        SSLCertificateKeyFile /etc/apache2/certs/dawac6.key
</VirtualHost>
```

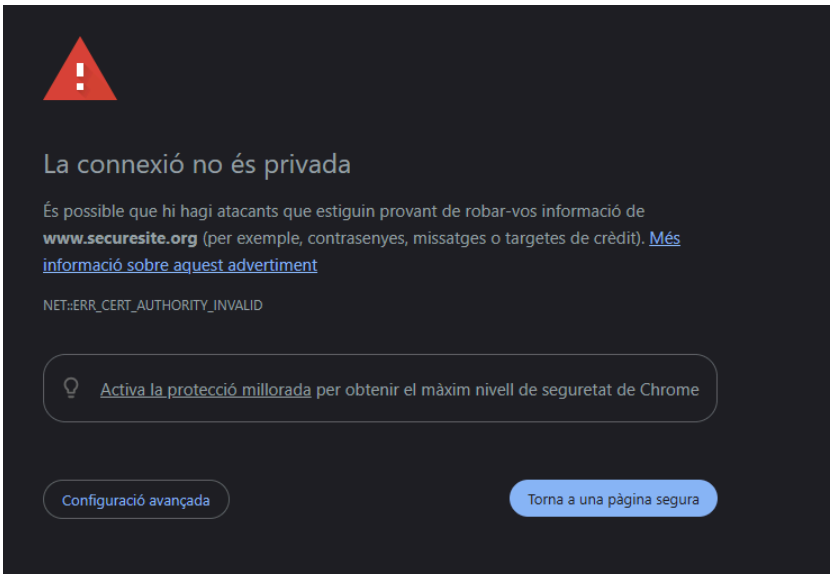
c)Reinicia el servidor per vere aplicats els canvis, i comprova què ocorre quan el navegador demana la web https://www.securesite.org.

```
root@aarati:~# systemctl restart apache2
root@aarati:~#
```

d)Per què el navegador continua considerant el lloc insegur?

➔ El navegador lo considera inseguro porque el certificado es **autofirmado** (no está firmado por una Autoridad de Certificación confiable). Los navegadores solo confían en los certificados emitidos por una CA reconocida.

e)No obstant, comprova, amb les Eines del Programador del navegador, a la pestanya de Seguretat, que la connexió està xifrada.



f)Compara l'anterior amb el contingut de la pestanya Seguretat quan el servidor demana una pàgina HTTP convencional (per exemple, qualsevol dels servidors virtuals configurats en pràctiques anteriors).

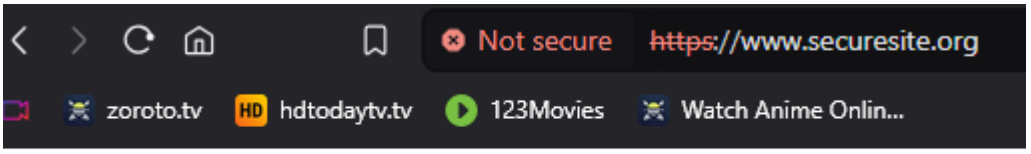
Tasca 6. Amb les directives de configuració d'Apache treballades fins ara, com faries per a que el servidor servís, a una petició de http://www.securesite.org, el recurs segur https://www.securesite.org?

```
<VirtualHost *:80>

        ServerAdmin webmaster@localhost
        ServerName www.securesite.org
        DocumentRoot /var/www/securesite
        Redirect permanent / https://www.securesite.org/

        <Directory /var/www/securesite>
                Options Indexes FollowSymLinks
                AllowOverride None
                Require all granted
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/securesite_error.log
        CustomLog ${APACHE_LOG_DIR}/securesite_access.log combined
</VirtualHost>
```



Welcome to Secure site

Tasca 7. Finalment, senyalarem algunes bones pràctiques de de seguretat en l'ús de servidors Apache. Investiga, per cada una d'aquestes bones pràctiques, 1) per què creus que es aconsellable, i 2) com la posaries en pràctica.

a)Ocultar la versió d'Apache instal·lada, la nostra IP i port, a les pàgines d'error proporcionades pel servidor.

```
root@aarati:~# nano /etc/apache2/conf-enabled/security.conf
```

```
ServerTokens Prod
#ServerTokens Full

#
# Optionally add a l
# name to server-gen
# listings, mod_stat
# documents or custo
# Set to "EMail" to
# Set to one of:  On
#ServerSignature Off
ServerSignature off
```

b)Desactivar l'opció de llistat del contingut dels directoris sense index

```
root@aarati:~# nano /etc/apache2/sites-available/securesite.org
```

```
<Directory /var/www/securesite>
        Options -Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>
```

c)Deshabilitar els mòduls que no fem servir.

d)Deshabilitar els enllaços simbòlics.

```
<Directory /var/www/securesite>
        Options -Indexes -FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>
```

e)Limitar el tamany de les peticions.

f)Mantenir el servidor actualitzat.

```
root@aarati:~# sudo apt update && sudo apt upgrade
Hit:1 http://es.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://es.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:4 http://es.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:5 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [466 kB]
Fetched 718 kB in 4s (196 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
63 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  python3-boto3 python3-botocore python3-dateutil python3-jmespath python3-packaging
```

g)Fer servir algún firewall d'aplicacions web per Apache.
protects against attack

```
root@aarati:~# sudo apt install libapache2-mod-security2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  liblua5.1-0 libyajl2 modsecurity-crs
Suggested packages:
  lua geoip-database-contrib ruby python
The following NEW packages will be installed:
  libapache2-mod-security2 liblua5.1-0 libyajl2 modsecurity-crs
0 upgraded, 4 newly installed, 0 to remove and 2 not upgraded.
Need to get 542 kB of archives.
After this operation, 2,481 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://es.archive.ubuntu.com/ubuntu noble/universe amd64 liblua5.1-0 amd64 5.1.5-9build2 [120
]
```