cgl@www:/$ echo "Enable SSL Module"
Enable SSL Module
cgl@www:/$ }
cgl@www/$ sudo a2enmod ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart

cgl@www/$
cgl@www:/$ echo "Create a certificate"
Create a certificate
cgl@www:/$
cgl@www:/$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/dsufux.us.key -out /etc/ssl/private/dsufux.us.crt
Generating a 2048 bit RSA private key
....+++ 
........................................................................................................................................+++ 
writing new private key to '/etc/ssl/private/dsufux.us.key'
-----
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]:‌
cgl@www:/$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/dsutux.us.key -out /etc/ssl/private/dsutux.us.crt
Generating a 2048 bit RSA private key
.....+++
........................................................................................................................................+++
writing new private key to '/etc/ssl/private/dsutux.us.key'
-----
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]:US
State or Province Name (full name) [Some-State]:UT
Locality Name (eg, city) []:St. George
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DSUTUX
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:www.dsutux.us
Email Address []:root@dsutux.us
cgl@www:/$
cgl@www:/$ sudo ls -l /etc/ssl/private/
total 12
-rw-r--r-- 1 root root 1363 Nov 14 14:13 dsutux.us.crt
-rw-r--r-- 1 root root 1708 Nov 14 14:13 dsutux.us.key
-rw-r----- 1 root ssl-cert 1704 Sep  5 12:56 ssl-cert-snakeoil.key
cgl@www:/$
cgl@www:$ sudo chmod 640 /etc/ssl/private/dsutux.us.key /etc/ssl/private/dsutux.us.crt

cgl@www:$
cgl@www:$
cgl@www:$ sudo ls -l /etc/ssl/private/
total 12
-rw-r----- 1 root root 1363 Nov 14 14:13 dsutux.us.crt
-rw-r----- 1 root root 1708 Nov 14 14:13 dsutux.us.key
-rw-r----- 1 root ssl-cert 1704 Sep 5 12:56 ssl-cert-snakeoil.key

cgl@www:$
cgl@www:/ $ sudo emacs /etc/apache2/sites-available/default-ssl
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
  ServerAdmin webmaster@localhost
  ServerName www.dsutux.us:443
  DocumentRoot /var/www
  <Directory />
    Options FollowSymLinks
    AllowOverride None
  </Directory>
  <Directory /var/www/>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    allow from all
  </Directory>

  ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
  <Directory "/usr/lib/cgi-bin"/>
    AllowOverride None
    Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
    Order allow,deny
  </Directory>
</VirtualHost>
</IfModule>
Allow from 127.0.0.0/255.0.0.0 ::1/128

</Directory>

# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.

SSLCertificateFile /etc/ssl/private/dsutux.us.crt
SSLCertificateKeyFile /etc/ssl/private/dsutux.us.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
cgl@www:/$ echo "Tell apache about the changes"
Tell apache about the changes
cgl@www:/$  

cgl@www:/$ sudo service apache2 restart
  * Restarting web server apache2
    ... waiting

cgl@www:/$ [ OK ]
cgl@www:/$ sudo tail /var/log/apache2/error.log

Tue Nov 12 05:08:32 2013 [error] [client 37.187.77.137] script not found or unable to stat: /usr/lib/cgi-bin/php
Tue Nov 12 15:06:47 2013 [error] [client 142.0.37.201] File does not exist: /var/www/updates
Thu Nov 14 02:57:14 2013 [error] [client 198.199.86.75] File does not exist: /var/www/w00t00t.at.blackhats.romanian.anti-sec:
Thu Nov 14 02:57:14 2013 [error] [client 198.199.86.75] File does not exist: /var/www/phpMyAdmin
Thu Nov 14 02:57:15 2013 [error] [client 198.199.86.75] File does not exist: /var/www/phpmyadmin
Thu Nov 14 02:57:15 2013 [error] [client 198.199.86.75] File does not exist: /var/www/pma
Thu Nov 14 02:57:15 2013 [error] [client 198.199.86.75] File does not exist: /var/www/myadmin
Thu Nov 14 02:57:15 2013 [error] [client 198.199.86.75] File does not exist: /var/www/MyAdmin
Thu Nov 14 14:18:17 2013 [notice] caught SIGTERM, shutting down
Thu Nov 14 14:18:18 2013 [notice] Apache/2.2.22 (Ubuntu) PHP/5.3.10-1ubuntu3.8 with Suhosin-Patch mod_ssl/2.2.22 OpenSSL/1.0.1 configured -- resuming normal operations

cgl@www:/$
cgl@www:/$ echo "Enable SSL site"
Enable SSL site
cgl@www:/$
cgl@www:/$ sudo a2ensite default
default  default-ssl  default-ssl-
cgl@www:/$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
cgl@www:/$
cgl@www:/$ sudo service apache2 restart
  * Restarting web server apache2
    ... waiting
    [ OK ]
cgl@www:/$  

The site's security certificate is not trusted!

You attempted to reach www.dsutux.us, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chromium cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, especially if you have never seen this warning before for this site.

Proceed anyway  Back to safety
It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.