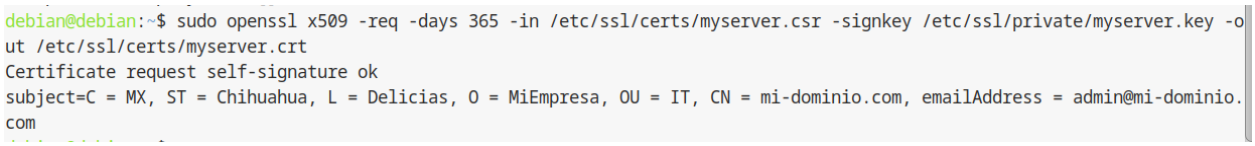
Primero creamos una llave privada RSA de 2048 bits

Despues creamos un CSR certificate signing request

Aqui ingresamos informacion sobre la empresa

Aqui firmamos el CSR con nuestra llave privada para validar el certificado por 265 dias.

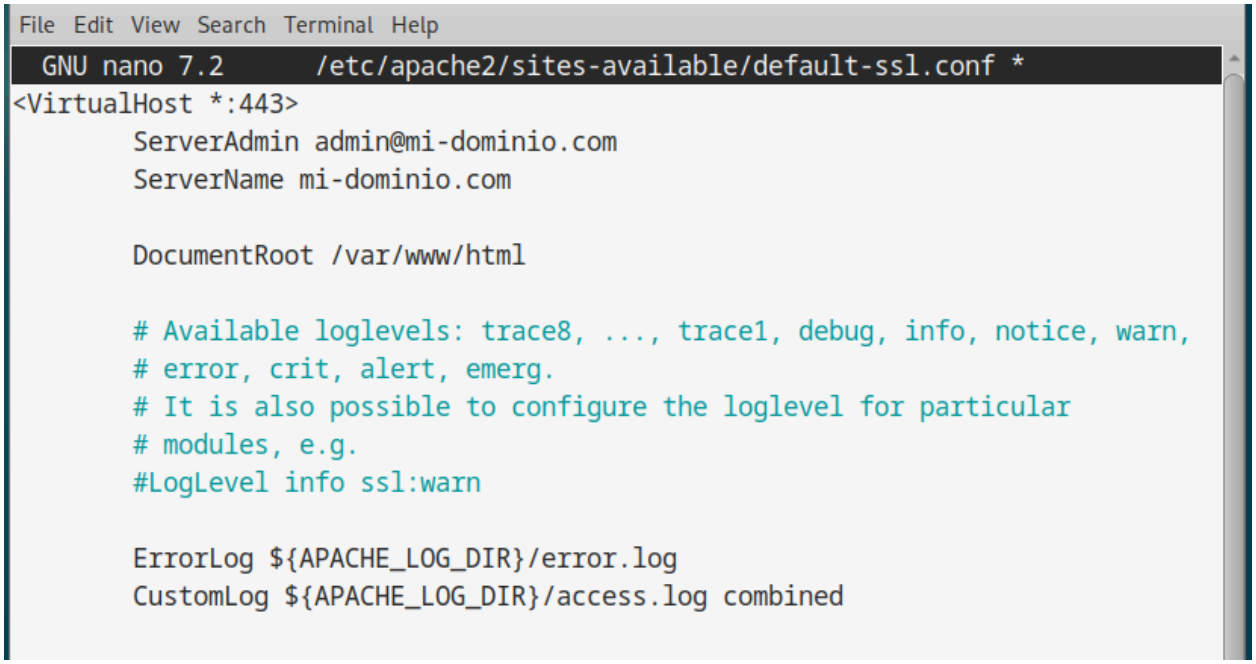


Aqui deditamos el archivo de configuracion

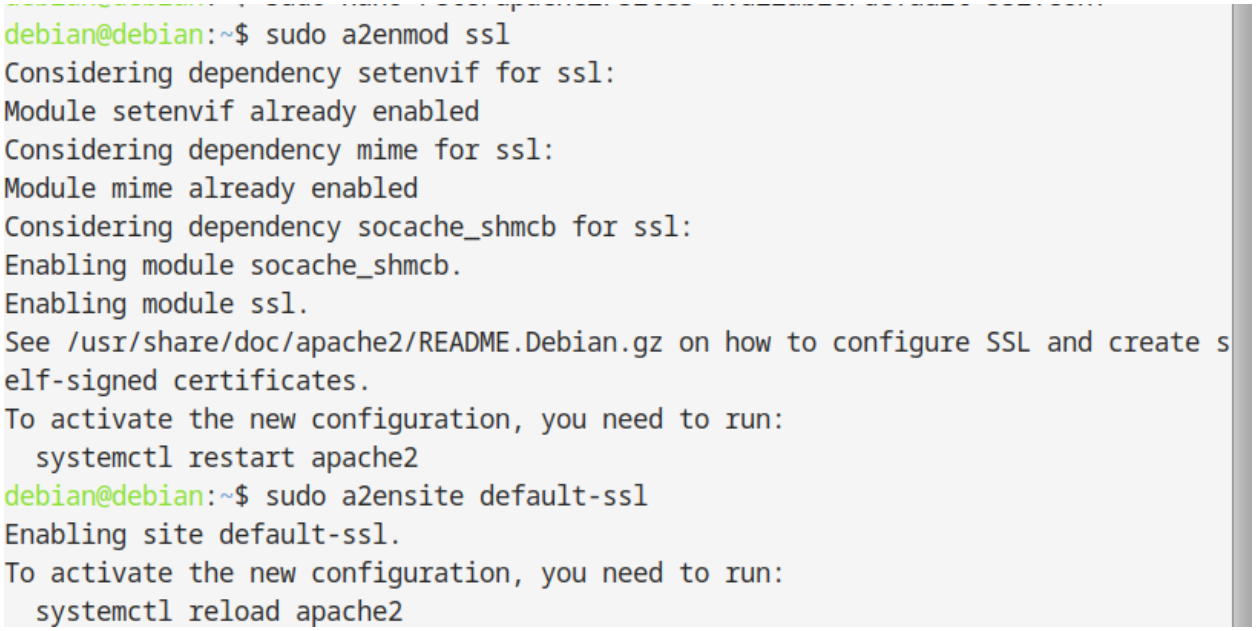
```
 GNU nano 7.2      /etc/apache2/sites-available/default-ssl.conf *
        #    practice often causes hanging connections with brain-dead browsers>
        #    this only for browsers where you know that their SSL implementation
        #    works correctly.
        #   Notice: Most problems of broken clients are also related to the HTTP
        #   keep-alive facility, so you usually additionally want to disable
        #   keep-alive for those clients, too. Use variable "nokeepalive" for t>
        #   Similarly, one has to force some clients to use HTTP/1.0 to workaro>
        #   their broken HTTP/1.1 implementation. Use variables "downgrade-1.0">
        #   "force-response-1.0" for this.
        BrowserMatch "MSIE [2-6]" \
               nokeepalive ssl-unclean-shutdown \
               downgrade-1.0 force-response-1.0

        BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown

</VirtualHost>
```

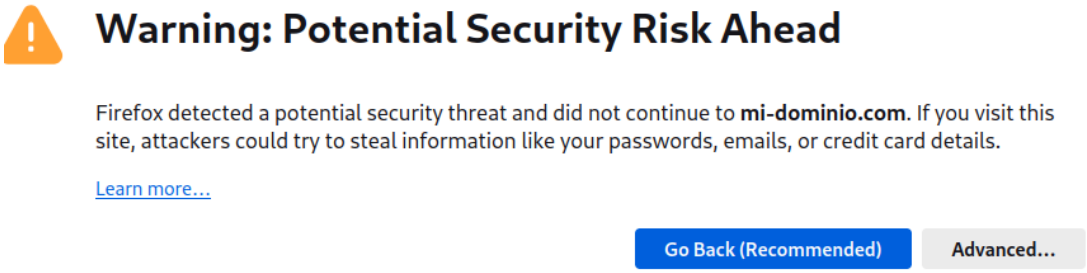
```
        #SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
        <FilesMatch "\.(?:cgi|shtml|phtml|php)$">
                SSLOptions +StdEnvVars
        </FilesMatch>
        <Directory /usr/lib/cgi-bin>
                SSLOptions +StdEnvVars
        </Directory>
```

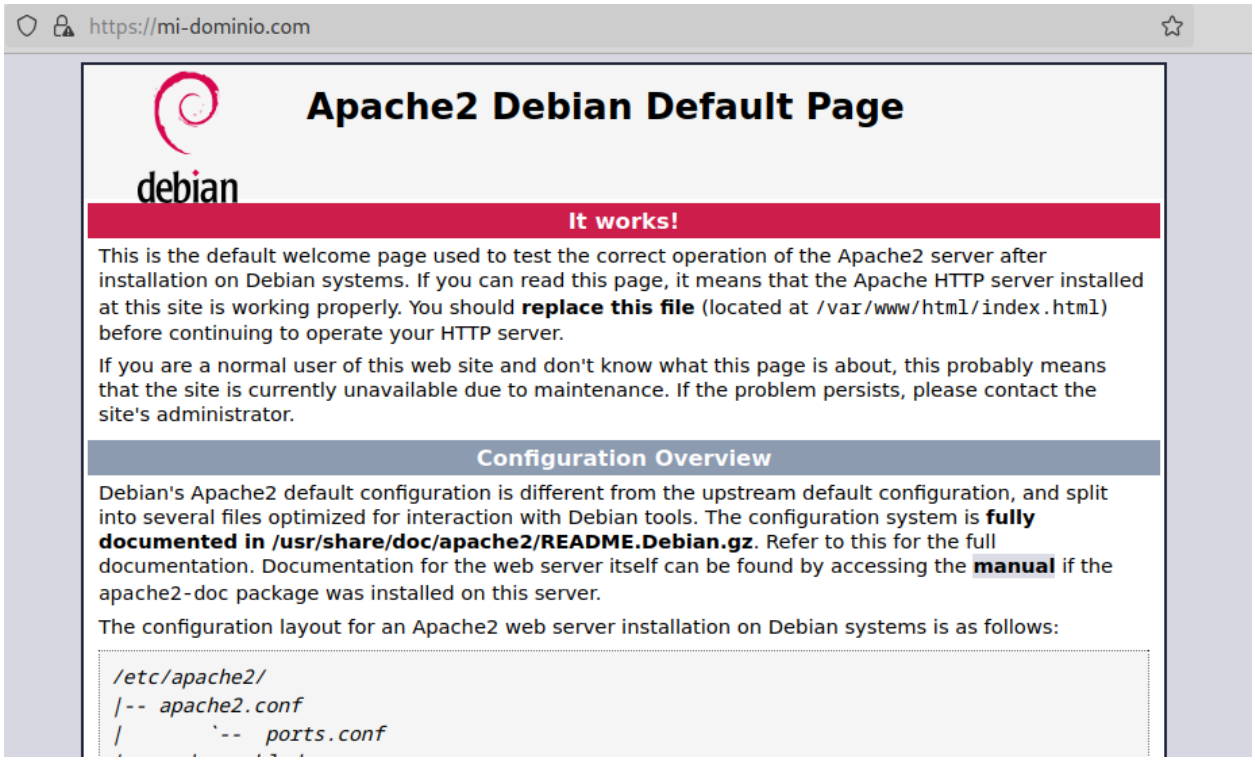
```
 GNU nano 7.2      /etc/apache2/sites-available/default-ssl.conf *

        #   SSL Engine Switch:
        #   Enable/Disable SSL for this virtual host.
        SSLEngine on
        SSLCertificateFile /etc/ssl/certs/myserver.crt
        SSLCertificateKeyFile /etc/ssl/private/myserver.key

        #   A self-signed (snakeoil) certificate can be created by installing
        #   the ssl-cert package. See
        #   /usr/share/doc/apache2/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/certs/ssl-cert-snakeoil.pem
#       SSLCertificateKeyFile   /etc/ssl/private/ssl-cert-snakeoil.key
```



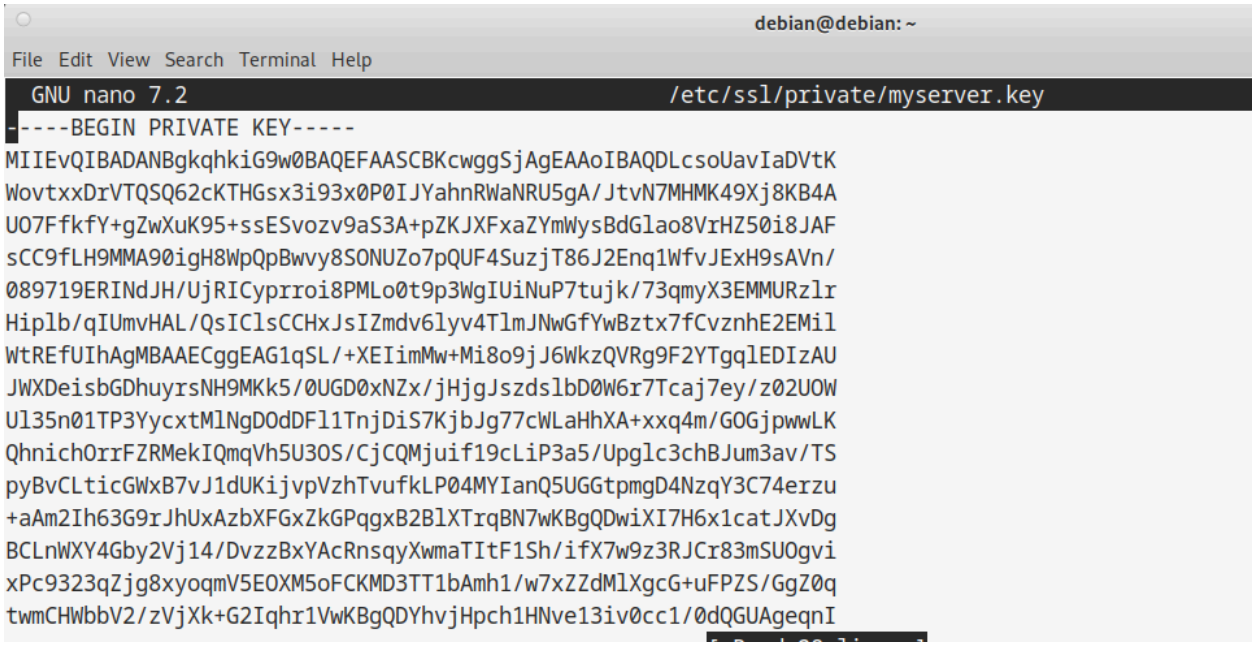
Aqui habilitamos SSL y el modulo SSL







El reporte jSOn menciona que la llave se encuentra en el archivo /etc/ssl/private/myserver.key. Abajo confirmo que si lo esta.


debian@debian: ~
File Edit View Search Terminal Help
GNU nano 7.2 /etc/ssl/private/myserver.key
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDLcsoUavIaDVtK
WovtxxDrVTQSQ62cKTHGsx3i93x0P0IJYahnRWaNRU5gA/JtvN7MHMK49Xj8KB4A
UO7FfkfY+gZwXuK95+ssESvozv9aS3A+pZKJXFxaZYmWysBdGlao8VrHZ50i8JAF
sCC9fLH9MMA90igH8WpQpBwvy8SONUZo7pQUF4SuzjT86J2Enq1WfvJExH9sAVn/
089719ERINdJH/UjRICyprroi8PMLo0t9p3WgIUiNuP7tujk/73qmyX3EMMURzlr
Hiplb/qIUmvHAL/QsIClsCCHxJsIZmdv6lyv4TlmJNwGfYwBztx7fCvznhE2EMil
WtREfUIhAgMBAAECggEAG1qSL/+XEIimMw+Mi8o9jJ6WkzQVRg9F2YTgqlEDIzAU
JWXDeisbGDhuyrsNH9MKk5/0UGD0xNZx/jHjgJszdslbD0W6r7Tcaj7ey/z02UOW
Ul35n01TP3YycxtMlNgDOdDFl1TnjDiS7KjbJg77cWLaHhXA+xxq4m/GOGjpwwLK
QhnichOrrFZRMekIQmqVh5U3OS/CjCQMjuif19cLiP3a5/Upglc3chBJum3av/TS
pyBvCLticGWxB7vJ1dUKijvpVzhTvufkLP04MYIanQ5UGGtpmgD4NzqY3C74erzu
+aAm2Ih63G9rJhUxAzbXFGxZkGPqgxB2BlXTrqBN7wKBgQDwiXI7H6x1catJXvDg
BCLnWXY4Gby2Vj14/DvzzBxYAcRnsqyXwmaTItF1Sh/ifX7w9z3RJCr83mSUOgvi
xPc9323qZjg8xyoqmV5EOXM5oFCKMD3TT1bAmh1/w7xZZdMlXgcG+uFPZS/GgZ0q
twmCHWbbV2/zVjXk+G2Iqhr1VwKBgQDYhvjHpch1HNve13iv0cc1/0dQGUAgeqnI