MANUAL:

Como comprobar si un SSL está bien instalado (p.e. con el SSL Checker) y donde conseguir de la Web la CA y SubCA si tienen que instalarlas en el Servidor.

Contenido

INTRODUCCIÓN

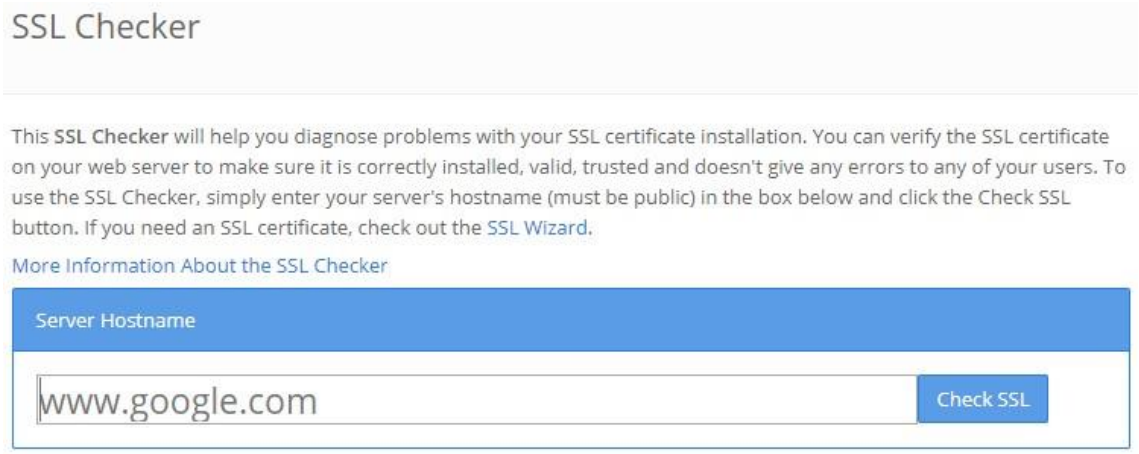
En este manual se va a explicar como realizar la comprobación de su un certificado SSL está bien instalado utilizando la herramienta SSL Checker.

Por otra parte, también se va a indicar de donde obtener la CA y la SubCA dentro de nuestra página web en caso de que sea necesario instalarlas en el servidor.

COMPROBACIÓN DE UN SSL BIEN INSTALADO

Para comprobar que un SSL está bien instalado, basta con acceder a la siguiente página web:

https://www.sslshopper.com/ssl-checker.html



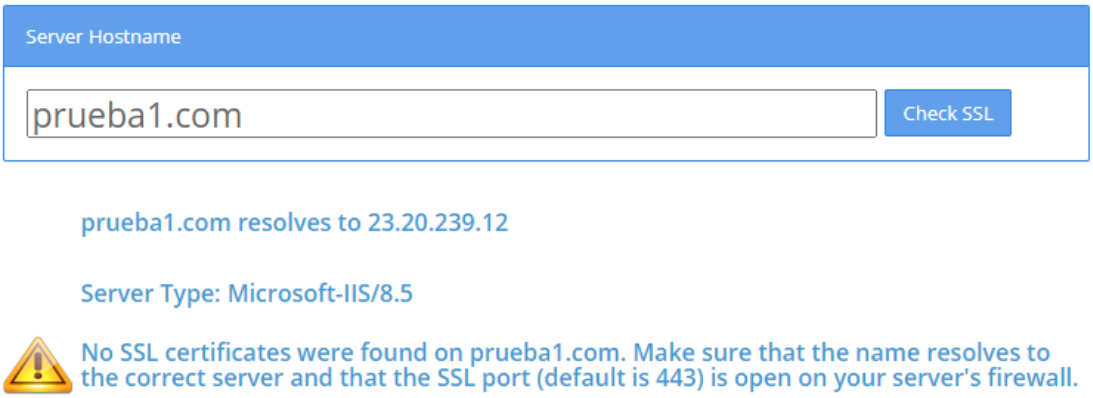
En el recuadro tenemos que poner el dominio que queremos comprobar.

Tras esto, pueden aparecer 2 situaciones:

1. Que el dominio es correcto, por lo que se muestra algo similar como lo que se ve a continuación:


Server Hostname
www.camerfirma.com
Check SSL
These results were cached from August 6, 2019, 12:33 am PST to conserve server resources.
If you are diagnosing a certificate installation problem, you can get uncached results by clicking here.
www.camerfirma.com resolves to 194.140.12.230
Server Type: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16
The certificate should be trusted by all major web browsers (all the correct intermediate certificates are installed).
The certificate will expire in 73 days.
Remind me
The hostname (www.camerfirma.com) is correctly listed in the certificate.
Server
SANs: policy.camerfirma.com, cps.camerfirma.com, pds.camerfirma.com, www.camerfirma.com
Organization: AC CAMERFIRMA S.A. Org. Unit: SISTEMAS
Location: MADRID, ES
Valid from October 19, 2017 to October 19, 2019
Serial Number: 1648000446075557883 (0x16dedfac9a04d7fb)
Signature Algorithm: sha256WithRSAEncryption
Issuer: Camerfirma Corporate Server II - 2015
Chain
Common name: Camerfirma Corporate Server II - 2015
Organization: AC Camerfirma S.A. Org. Unit: AC CAMERFIRMA
Location: Madrid (see current address at https://www.camerfirma.com/address), ES
Valid from January 15, 2015 to December 15, 2037
Serial Number: 7070637242797760822 (0x621ff31c489ba136)
Signature Algorithm: sha256WithRSAEncryption
Issuer: Chambers of Commerce Root - 2008
Chain
Common name: Chambers of Commerce Root - 2008
Organization: AC Camerfirma S.A.
Location: Madrid (see current address at www.camerfirma.com/address), EU
Valid from August 1, 2008 to July 31, 2038
Serial Number: 11806822484801597146 (0xa3da427ea4b1aeda)
Signature Algorithm: sha1WithRSAEncryption
Issuer: Chambers of Commerce Root - 2008

2. Que el dominio no sea correcto o no esté dado de alta, por lo que se mostrará algo como lo siguiente:



DONDE CONSEGUIR DE LA WEB LA CA Y LA SUBCA

Los certificados de la CA raíz y de la SubCA se pueden localizar en nuestra web en los sitios que se muestran a continuación. Instalar los certificados raíz resuelve, por ejemplo en este tipo de certificados, el aviso de que no se puede verificar el certificado porque el emisor es desconocido.

1. Certificado raíz en formato .cer: En https://www.camerfirma.com/politicas-de-certificacion-ac-camerfirma/ se descarga e instala el *CHAMBERS OF COMMERCE ROOT - 2008.cer*.
2. Certificado subordinado .cer: En https://www.camerfirma.com/politicasde-certificacion-ac-camerfirma/ se descarga e instala el *Corporate Server II – 2015.cer*.

Para convertir los certificados anteriores en .pem, hay que realizar el siguiente proceso:

1. Abrir clave pública, desde opciones de Internet o en Status.

2. Ir a la pestaña detalles.
3. Hacer clic en “copiar archivo”.
4. Seleccionar "X.509 codificado base 64 (.cer)" y hacer clic en siguiente.
5. Hacer clic en “Examinar” y guardar el archivo donde se quiera.
6. Hacer clic en siguiente.
7. Hacer clic en finalizar.
8. Ir al archivo creado y cambiar la extensión .cer por .pem.
9. Aceptar el mensaje de advertencia.