



4.2 El panel de Seguridad

¡BIENVENIDOS!

Soy Juan Diego Pérez Jiménez

Profesor de Informática en FP



<https://www.linkedin.com/in/juandiegoperez>



@pekechis

ÍNDICE

- Definición
- Apariencia
- Información detallada
- Posibles problemas

Definición

“ El **panel de seguridad** sirve para comprobar que la página está usando **correctamente** el protocolo **HTTPS**, los **certificados** asociados etc... ”

Apariencia

Información de Seguridad

Overview

Main origin

Reload to view details

Secure origins

- https://api.twitter.com
- https://twitter.com
- https://pbs.twimg.com

Orígenes

TODO OK

PROBLEMAS

Security overview



This page is secure (valid HTTPS).

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by DigiCert SHA2 High Assurance Server CA.

[View certificate](#)

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM.

Resources - all served securely

All resources on this page are served securely.

Certificado

Encriptación

Resumen recursos
servidos

Información detallada

Visor de certificados: *.openwebinars.net

General Detalles

Este certificado se ha verificado para los siguientes usos:

Certificado de servidor SSL

Enviado a

Nombre común (CN)	*.openwebinars.net
Organización (O)	<No incluido en el certificado>
Unidad organizativa (OU)	<No incluido en el certificado>

Emitido por

Nombre común (CN)	Sectigo RSA Domain Validation Secure Server CA
Organización (O)	Sectigo Limited
Unidad organizativa (OU)	<No incluido en el certificado>

Periodo de validez

Emitido el	martes, 3 de marzo de 2020, 1:00:00
Vencimiento el	viernes, 4 de marzo de 2022, 0:59:59

Huellas digitales

Huella digital SHA-256	25 B4 C9 D2 15 97 4F E5 A6 D3 45 F4 57 33 D0 B9 78 FE 52 16 C8 F3 D8 37 88 19 28 BD 73 C4 17 86
Huella digital SHA-1	19 47 8D AD 7A A8 90 6A 73 69 6F 6F D4 59 F8 A3 87 0D 09 20

Overview

Main origin

Reload to view details

Secure origins

- https://api.twitter.com
- https://twitter.com
- https://pbs.twimg.com
- https://video.twimg.com
- https://abs-0.twimg.com

Origin

- https://api.twitter.com

[View requests in Network Panel](#)

Connection

Protocol	TLS 1.2
Key exchange	ECDHE_RSA
Key exchange group	P-256
Cipher	AES_128_GCM

Certificate

Subject	api.twitter.com
SAN	api.twitter.com
Valid from	Thu, 26 Mar 2020 00:00:00 GMT
Valid until	Thu, 25 Mar 2021 12:00:00 GMT
Issuer	DigiCert SHA2 High Assurance Server CA

[Open full certificate details](#)

Certificate Transparency

SCT	Google 'Argon2021' log (Embedded in certificate, Verified)
SCT	DigiCert Yeti2021 Log (Embedded in certificate, Verified)

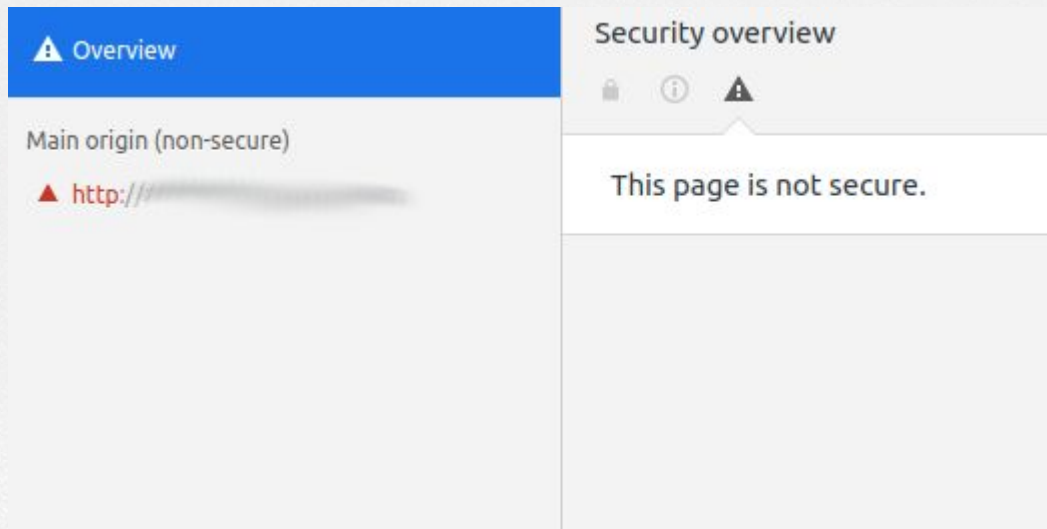
[Show full details](#)

Posibles problemas

- **Página no segura (HTTP)**
- **Elementos seguros y no seguros**

Posibles problemas

(Página no segura HTTP)



Posibles problemas

(Elementos seguros y no seguros)

Overview

Main origin (secure)

- https://www.juntadeandalucia.es

Secure origins

- https://ssl.google-analytics.com

Security overview

This page is not secure.

Resources - non-secure form

This page includes a form with a non-secure "action" attribute.

Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by GlobalSign RSA OV SSL CA 2018.

View certificate

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM.

Posibles problemas

(Elementos seguros y no seguros)



Overview

Main origin (secure)

- https://www.juntadeandalucia.es

Secure origins

- https://ssl.google-analytics.com

Security overview

This page is not secure.

- Resources - non-secure form
This page includes a form with a non-secure "action" attribute.
- Certificate - valid and trusted
The connection to this site is using a valid, trusted server certificate issued by GlobalSign RSA OV SSL CA 2018.
[View certificate](#)
- Connection - secure connection settings
The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with P-256, and AES_128_GCM.

THANKS!

Any questions?

You can find me at @pekechis &
<https://github.com/pekechis>