EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

Web Service Self-Assessment Tools

Robert Riemann
IT Policy

Hands-On Exercise
DPO Day

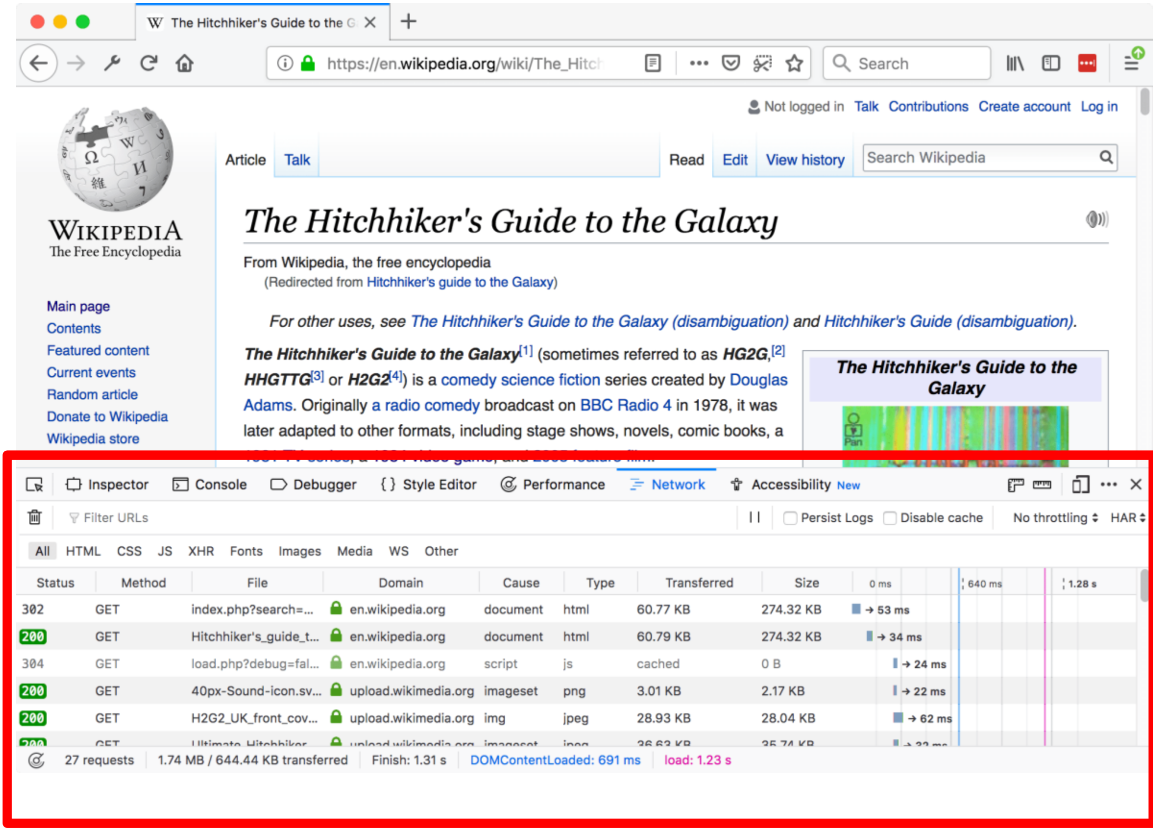
12 December 2018

Don’t wait until a future wave catches you!

Test the waters ahead of time on your own!

Browser Developer Toolbar

- easily available: integrated in all modern browsers
- press in browser: `Ctrl+Shift+I`
- displays browser storage (cookies) and all data traffic in real-time



The Hitchhiker's Guide to the G

https://en.wikipedia.org/wiki/The_Hitch

Search

Not logged in Talk Contributions Create account Log in

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Article Talk Read Edit View history Search Wikipedia

The Hitchhiker's Guide to the Galaxy

From Wikipedia, the free encyclopedia
(Redirected from Hitchhiker's guide to the Galaxy)

For other uses, see The Hitchhiker's Guide to the Galaxy (disambiguation) and Hitchhiker's Guide (disambiguation).

The Hitchhiker's Guide to the Galaxy[1] (sometimes referred to as ***HG2G***,[2] ***HHGTTG***[3] or ***H2G2***[4]) is a comedy science fiction series created by Douglas Adams. Originally a radio comedy broadcast on BBC Radio 4 in 1978, it was later adapted to other formats, including stage shows, novels, comic books, a 1981 TV series, a 1984 video game, and 2005 feature film.

The Hitchhiker's Guide to the Galaxy

Inspector Console Debugger Style Editor Performance Network Accessibility New

Filter URLs ☐ Persist Logs ☐ Disable cache No throttling HAR

All HTML CSS JS XHR Fonts Images Media WS Other

Status	Method	File	Domain	Cause	Type	Transferred	Size	0 ms ¦ 640 ms ¦ 1.28 s
302	GET	index.php?search=...	en.wikipedia.org	document	html	60.77 KB	274.32 KB	→ 53 ms
200	GET	Hitchhiker's_guide_t...	en.wikipedia.org	document	html	60.79 KB	274.32 KB	→ 34 ms
304	GET	load.php?debug=fal...	en.wikipedia.org	script	js	cached	0 B	→ 24 ms
200	GET	40px-Sound-icon.sv...	upload.wikimedia.org	imageset	png	3.01 KB	2.17 KB	→ 22 ms
200	GET	H2G2_UK_front_cov...	upload.wikimedia.org	img	jpeg	28.93 KB	28.04 KB	→ 62 ms
200	GET	Ultimate_Hitchhiker...	upload.wikimedia.org	imageset	jpeg	36.63 KB	35.74 KB	→ 22 ms

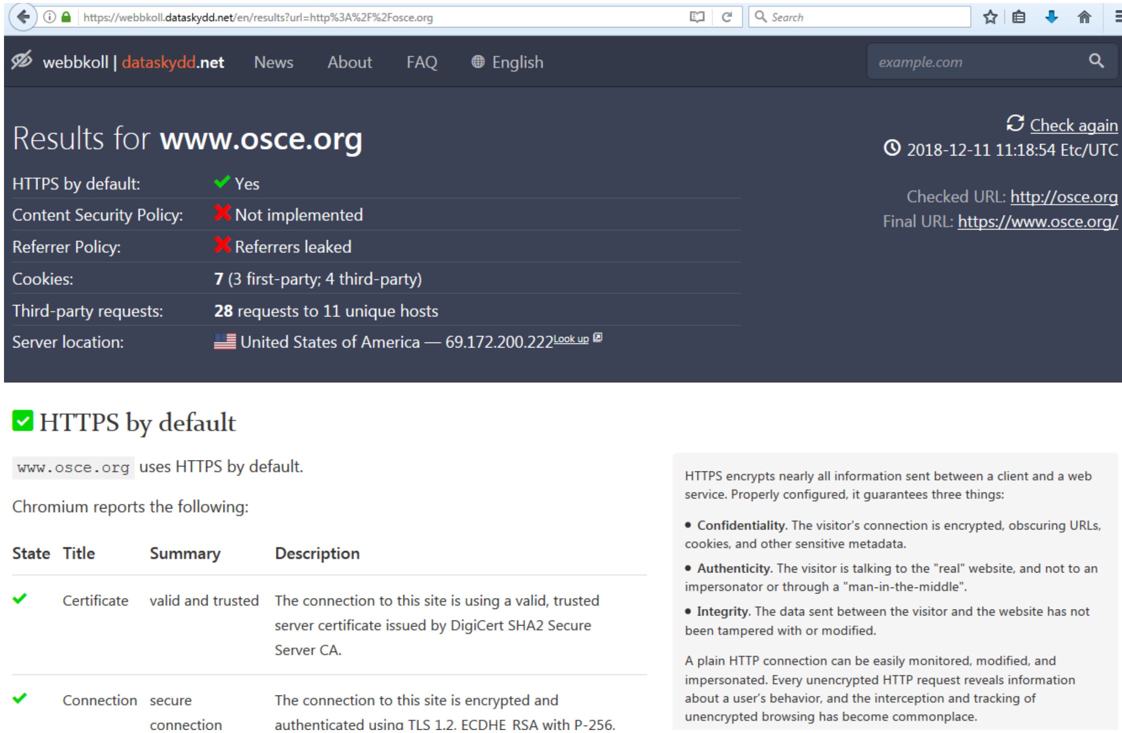
27 requests | 1.74 MB / 644.44 KB transferred | Finish: 1.31 s | DOMContentLoaded: 691 ms | load: 1.23 s

- Firefox: https://developer.mozilla.org/en-US/docs/Tools
- Chrome: https://developers.google.com/web/tools/chrome-devtools/

Online Service *webbkoll*

https://webbkoll.dataskydd.net/en

- service gathers evidence, e.g. cookies, HTTPS
- provides privacy assessment
- assessment is automated and not EUI specific


https://webbkoll.dataskydd.net/en/results?url=http%3A%2F%2Fosce.org
Search
webbkoll | dataskydd.net
News
About
FAQ
English
example.com

Results for **www.osce.org**

Check again
2018-12-11 11:18:54 Etc/UTC

Checked URL: http://osce.org
Final URL: https://www.osce.org/

HTTPS by default:	✓ Yes
Content Security Policy:	✗ Not implemented
Referrer Policy:	✗ Referrers leaked
Cookies:	**7** (3 first-party; 4 third-party)
Third-party requests:	**28** requests to 11 unique hosts
Server location:	United States of America — 69.172.200.222 Look up

☑ HTTPS by default

`www.osce.org` uses HTTPS by default.

Chromium reports the following:

State	Title	Summary	Description
✓	Certificate	valid and trusted	The connection to this site is using a valid, trusted server certificate issued by DigiCert SHA2 Secure Server CA.
✓	Connection	secure connection	The connection to this site is encrypted and authenticated using TLS 1.2, ECDHE_RSA with P-256,

HTTPS encrypts nearly all information sent between a client and a web service. Properly configured, it guarantees three things:

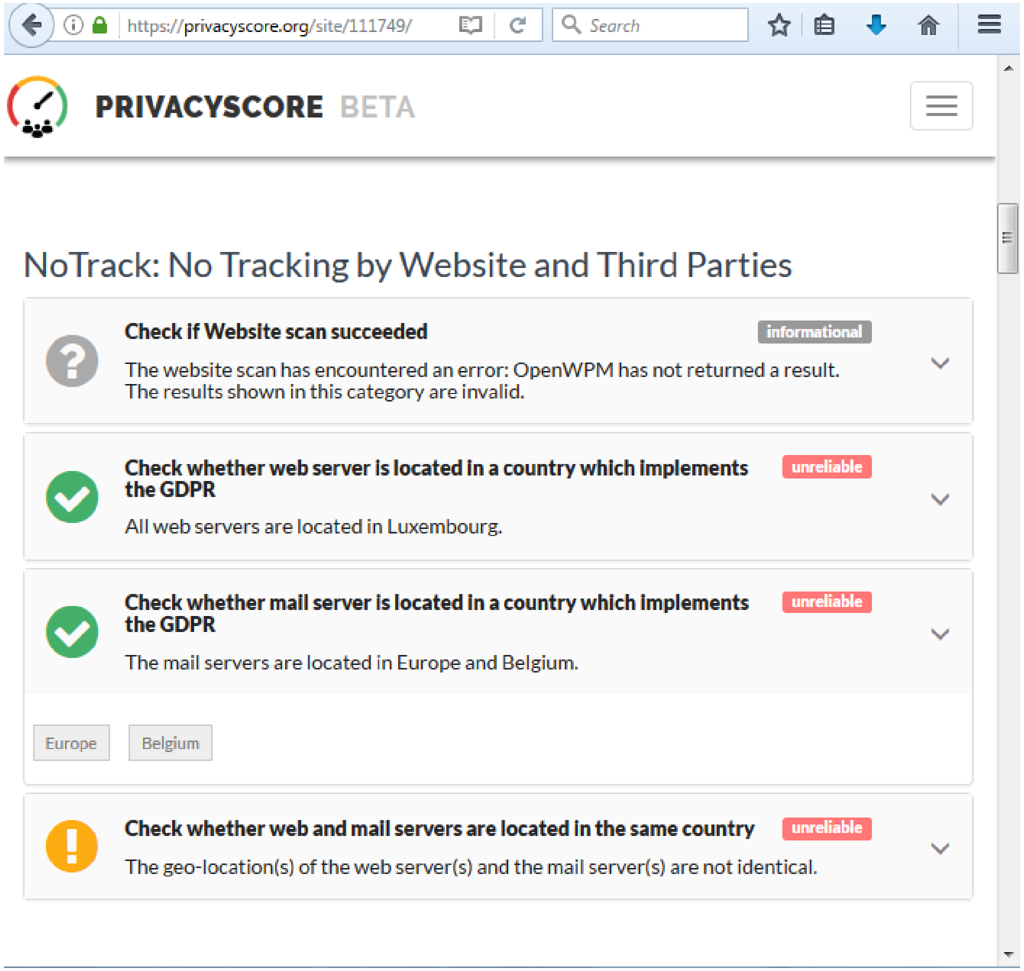
- **Confidentiality.** The visitor's connection is encrypted, obscuring URLs, cookies, and other sensitive metadata.
- **Authenticity.** The visitor is talking to the "real" website, and not to an impersonator or through a "man-in-the-middle".
- **Integrity.** The data sent between the visitor and the website has not been tampered with or modified.

A plain HTTP connection can be easily monitored, modified, and impersonated. Every unencrypted HTTP request reveals information about a user's behavior, and the interception and tracking of unencrypted browsing has become commonplace.

Online Service *PrivacyScore*

https://privacyscore.org

- inspired by *webbkoll*
- evidence and assessment
- curated lists with assessment of EU institutions
- assessment is automated and not EUI specific



NoTrack: No Tracking by Website and Third Parties

Check if Website scan succeeded informational

The website scan has encountered an error: OpenWPM has not returned a result. The results shown in this category are invalid.

Check whether web server is located in a country which implements the GDPR unreliable

All web servers are located in Luxembourg.

Check whether mail server is located in a country which implements the GDPR unreliable

The mail servers are located in Europe and Belgium.

Europe Belgium

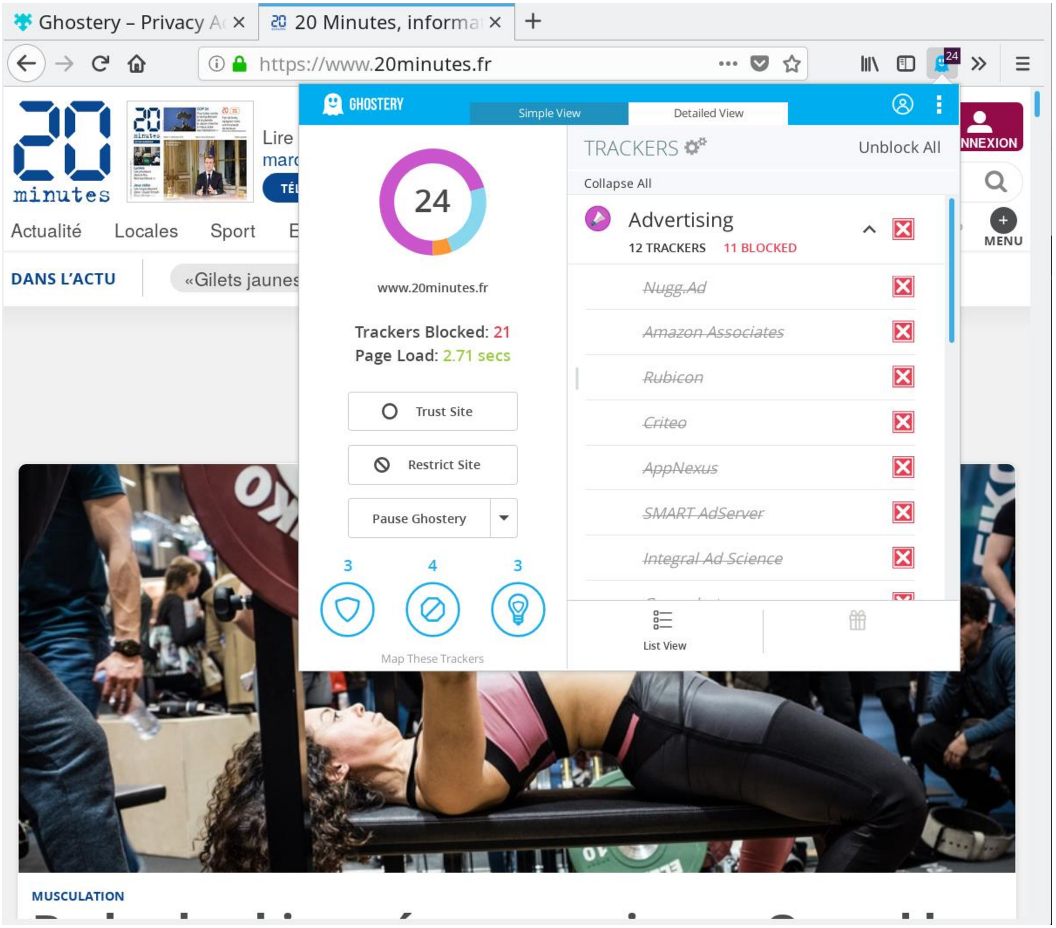
Check whether web and mail servers are located in the same country unreliable

The geo-location(s) of the web server(s) and the mail server(s) are not identical.

Browser-Plugin *Ghostery*

https://www.ghostery.com/

- plug-in to block and report on tracking and advertising of web services
- for all browsers
- easy to use



Ghostery – Privacy A

20 Minutes, informa

https://www.20minutes.fr

GHOSTERY

24

www.20minutes.fr

Trackers Blocked: 21

Page Load: 2.71 secs

TRACKERS

Advertising

12 TRACKERS 11 BLOCKED

~~Nugg.Ad~~

~~Amazon Associates~~

~~Rubicon~~

~~Criteo~~

~~AppNexus~~

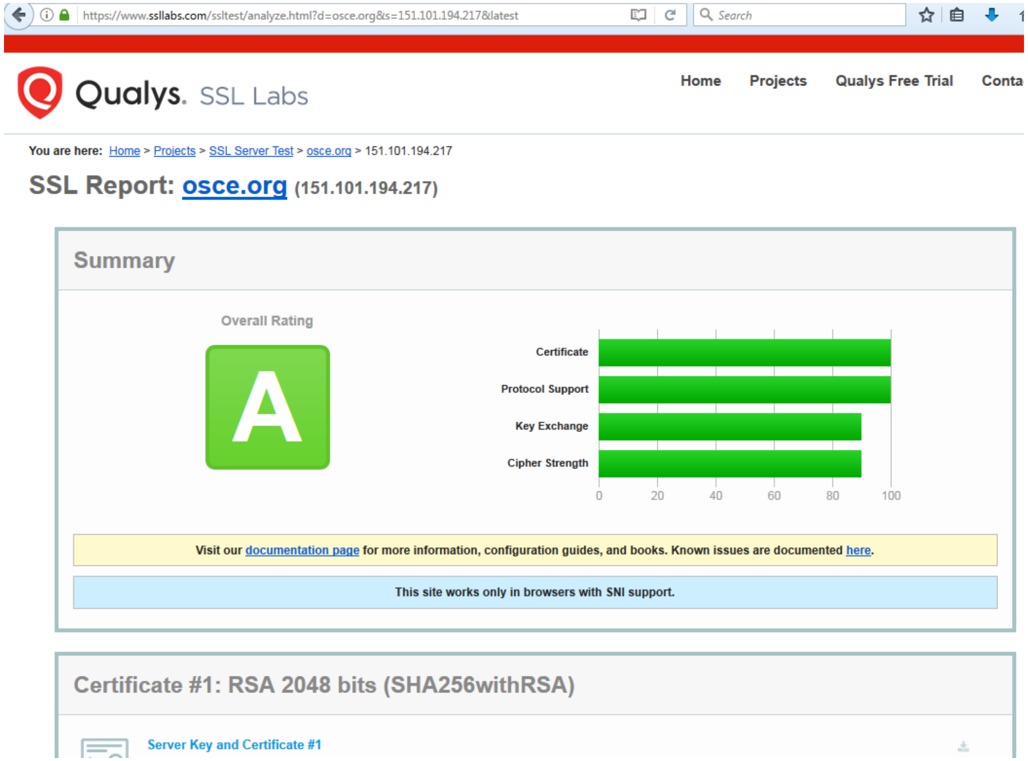
~~SMART AdServer~~

~~Integral Ad Science~~

Online Service Qualys SSL Labs

https://www.ssllabs.com/ssltest/

- online service to assess HTTPS configuration
- tests for known vulnerabilities
- easy to use
- traffic light feedback



https://www.ssllabs.com/ssltest/analyze.html?d=osce.org&s=151.101.194.217&latest

You are here: Home > Projects > SSL Server Test > osce.org > 151.101.194.217

SSL Report: osce.org (151.101.194.217)

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Alternative open source software: https://testssl.sh/