PRIVACYSCORE.ORG

Test websites and rank them according to their security and privacy features

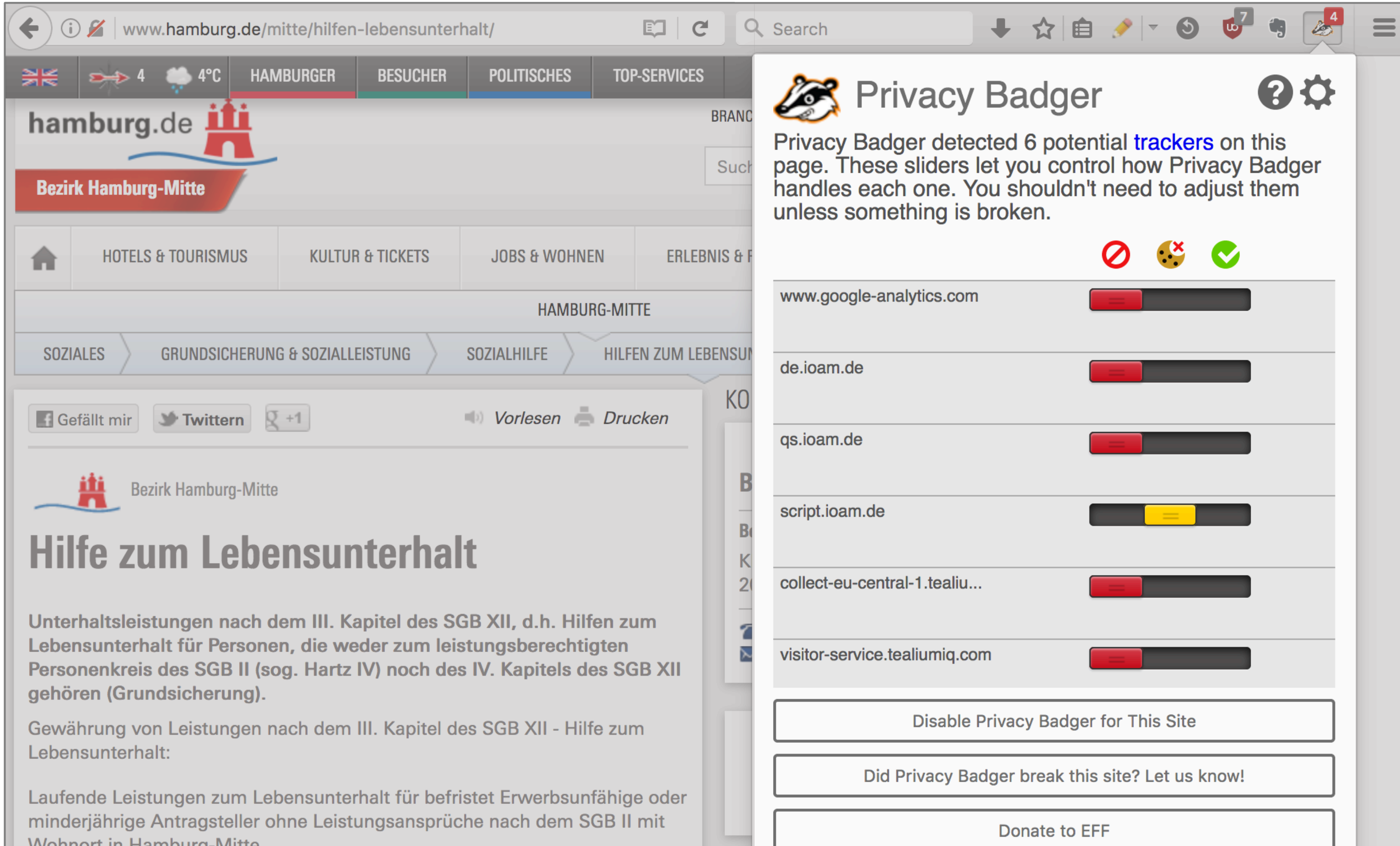
Prof. Dr. **Dominik Herrmann**
Otto-Friedrich-Universität Bamberg

joint work with Anne Laubach (Uni Kassel), Max Maaß (TU Darmstadt), Henning Pridöhl (Uni Bamberg), and Pascal Wichmann (Uni Hamburg)

https://dhgo.to/pw17-slides

Motivation

Who knows that … you are on welfare?



www.hamburg.de/mitte/hilfen-lebensunterhalt/

Search
4 4°C HAMBURGER BESUCHER POLITISCHES TOP-SERVICES
hamburg.de
Bezirk Hamburg-Mitte
BRANC
Such
HOTELS & TOURISMUS KULTUR & TICKETS JOBS & WOHNEN ERLEBNIS & F
HAMBURG-MITTE
SOZIALES GRUNDSICHERUNG & SOZIALLEISTUNG SOZIALHILFE HILFEN ZUM LEBENSUN
Gefällt mir Twittern +1 Vorlesen Drucken
KO

Bezirk Hamburg-Mitte

Hilfe zum Lebensunterhalt

Unterhaltsleistungen nach dem III. Kapitel des SGB XII, d.h. Hilfen zum Lebensunterhalt für Personen, die weder zum leistungsberechtigten Personenkreis des SGB II (sog. Hartz IV) noch des IV. Kapitels des SGB XII gehören (Grundsicherung).

Gewährung von Leistungen nach dem III. Kapitel des SGB XII - Hilfe zum Lebensunterhalt:

Laufende Leistungen zum Lebensunterhalt für befristet Erwerbsunfähige oder minderjährige Antragsteller ohne Leistungsansprüche nach dem SGB II mit Wohnort in Hamburg-Mitte

Privacy Badger

Privacy Badger detected 6 potential trackers on this page. These sliders let you control how Privacy Badger handles each one. You shouldn't need to adjust them unless something is broken.

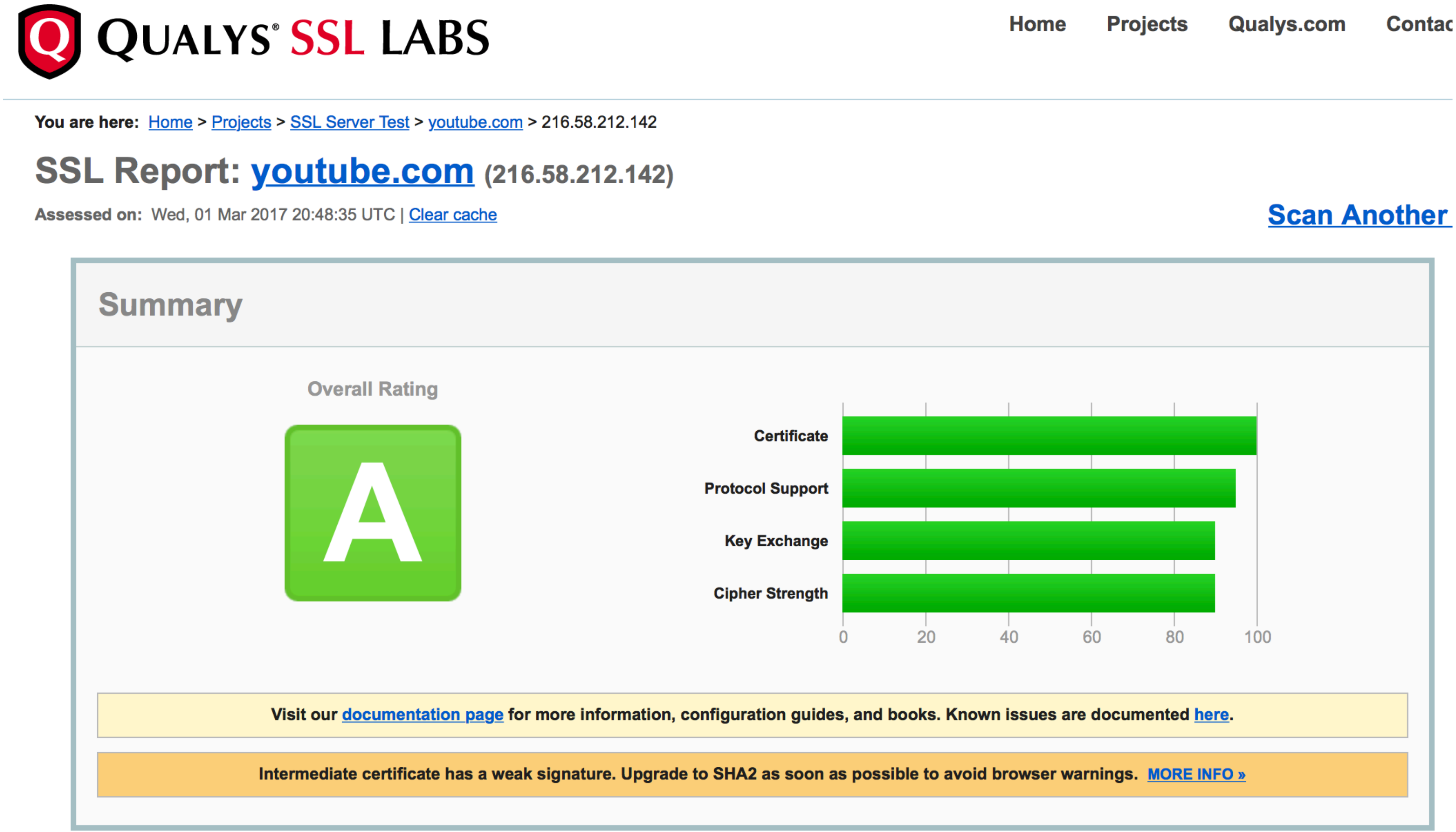
www.google-analytics.com	🟥
de.ioam.de	🟥
qs.ioam.de	🟥
script.ioam.de	🟨
collect-eu-central-1.tealiu...	🟥
visitor-service.tealiumiq.com	🟥

Disable Privacy Badger for This Site
Did Privacy Badger break this site? Let us know!
Donate to EFF

THE NEW NORMAL?

Existing Website Scanning Services

focus on single sites



You are here: Home > Projects > SSL Server Test > youtube.com > 216.58.212.142

SSL Report: youtube.com (216.58.212.142)

Assessed on: Wed, 01 Mar 2017 20:48:35 UTC | Clear cache

Scan Another

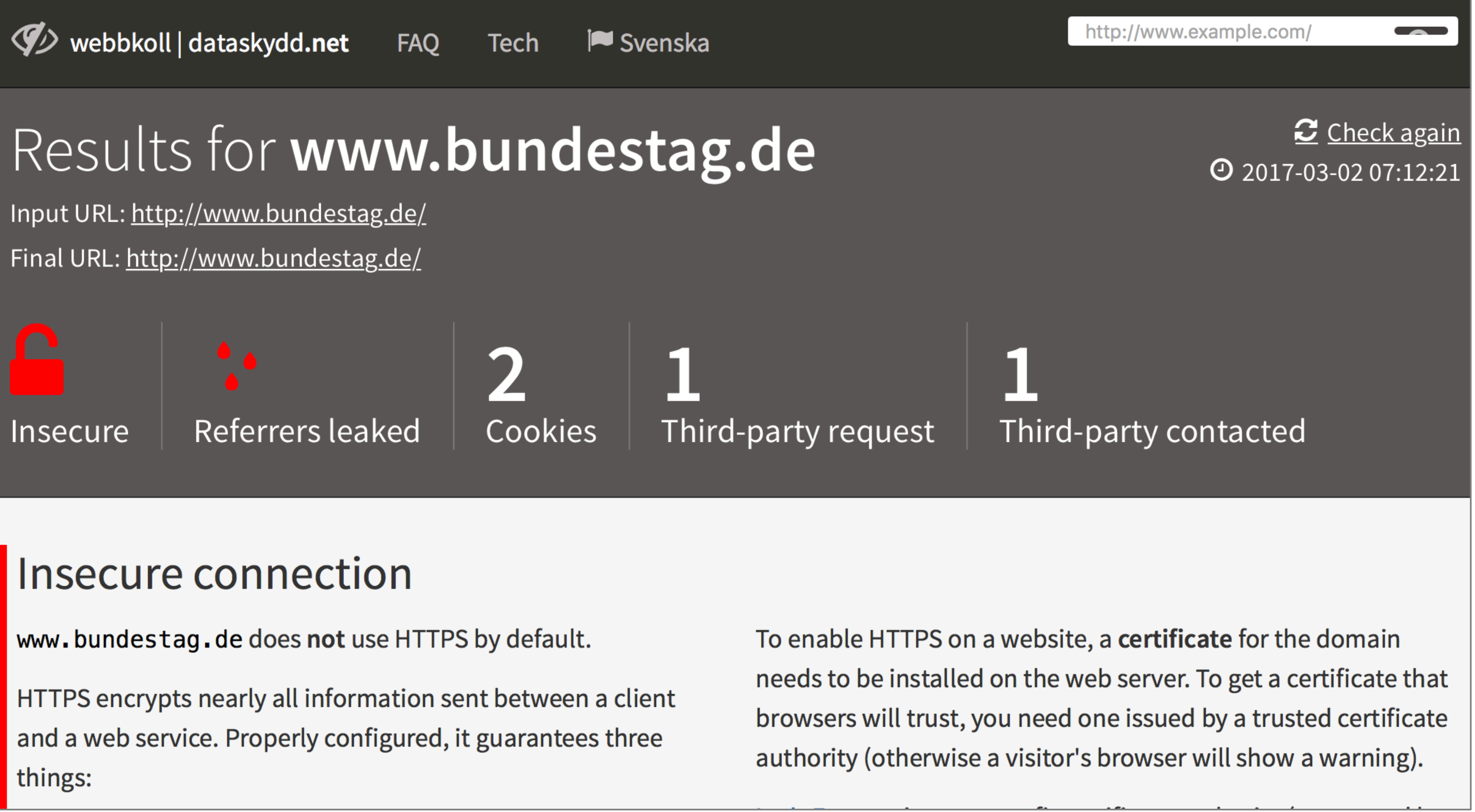
Summary

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

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. MORE INFO »

https://www.ssllabs.com/ssltest

observatory.mozilla.org · securityheaders.io · urlscan.io



Results for **www.bundestag.de**

2017-03-02 07:12:21

Input URL: http://www.bundestag.de/

Final URL: http://www.bundestag.de/

Insecure

Referrers leaked

2 Cookies

1 Third-party request

1 Third-party contacted

Insecure connection

`www.bundestag.de` does **not** use HTTPS by default.

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

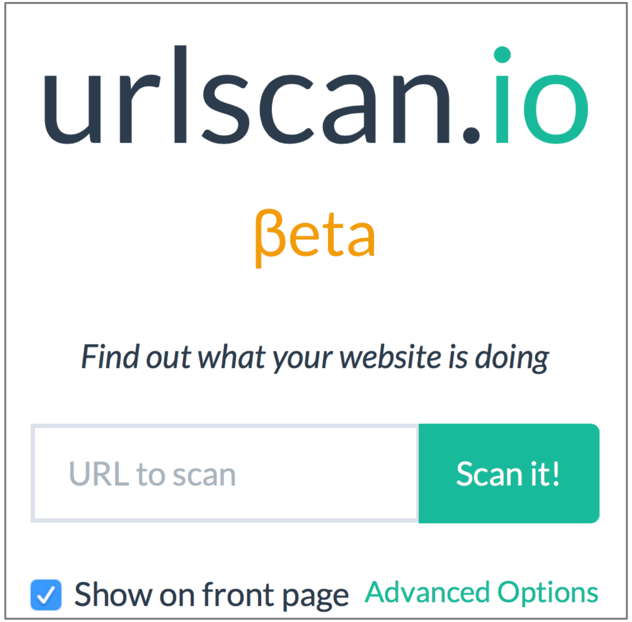
To enable HTTPS on a website, a **certificate** for the domain needs to be installed on the web server. To get a certificate that browsers will trust, you need one issued by a trusted certificate authority (otherwise a visitor's browser will show a warning).

https://www.sit.fraunhofer.de/de/track-your-tracker

https://webbkoll.dataskydd.net/en

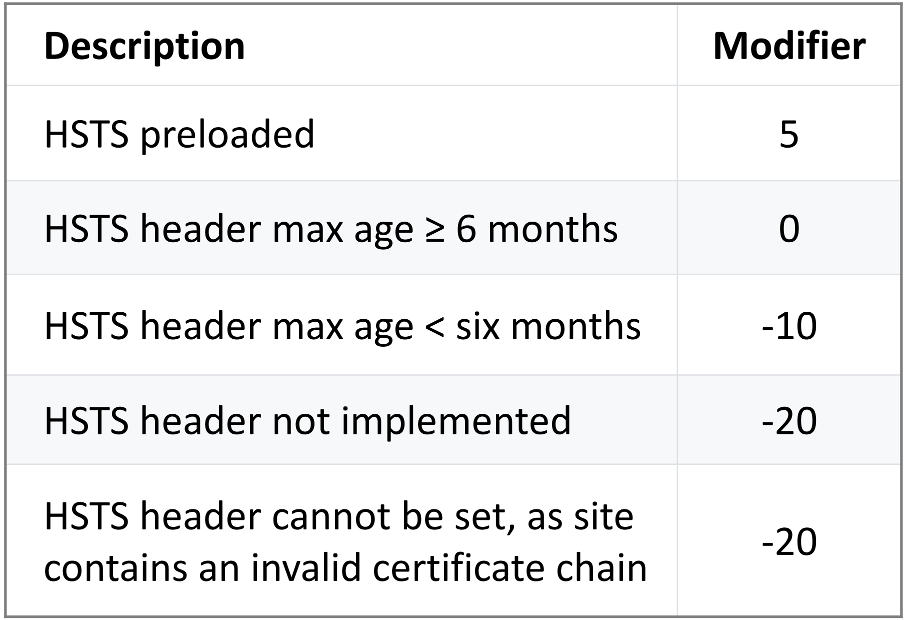
Existing Scanning Services …

are targeted at server operators



Find out what your website is doing

use a pre-defined rating scheme



Description	Modifier
HSTS preloaded	5
HSTS header max age ≥ 6 months	0
HSTS header max age < six months	-10
HSTS header not implemented	-20
HSTS header cannot be set, as site contains an invalid certificate chain	-20

https://github.com/mozilla/http-observatory/blob/master/httpobs/docs/scoring.md

PrivacyScore has a different focus.

Objective: **public rankings** to create incentives for operators to improve privacy and security on their site.

Visitors can upload **annotated lists of websites** and influence the ranking according to their preference (soon™).

All code **open source** (GPLv3+),
all results published as **open data**.

USER-DEFINED ATTRIBUTES

?

Are the sites of **large cities** ***worse than those of*** **smaller** ***cities?***

Any regional differences for websites of, e.g., universities?

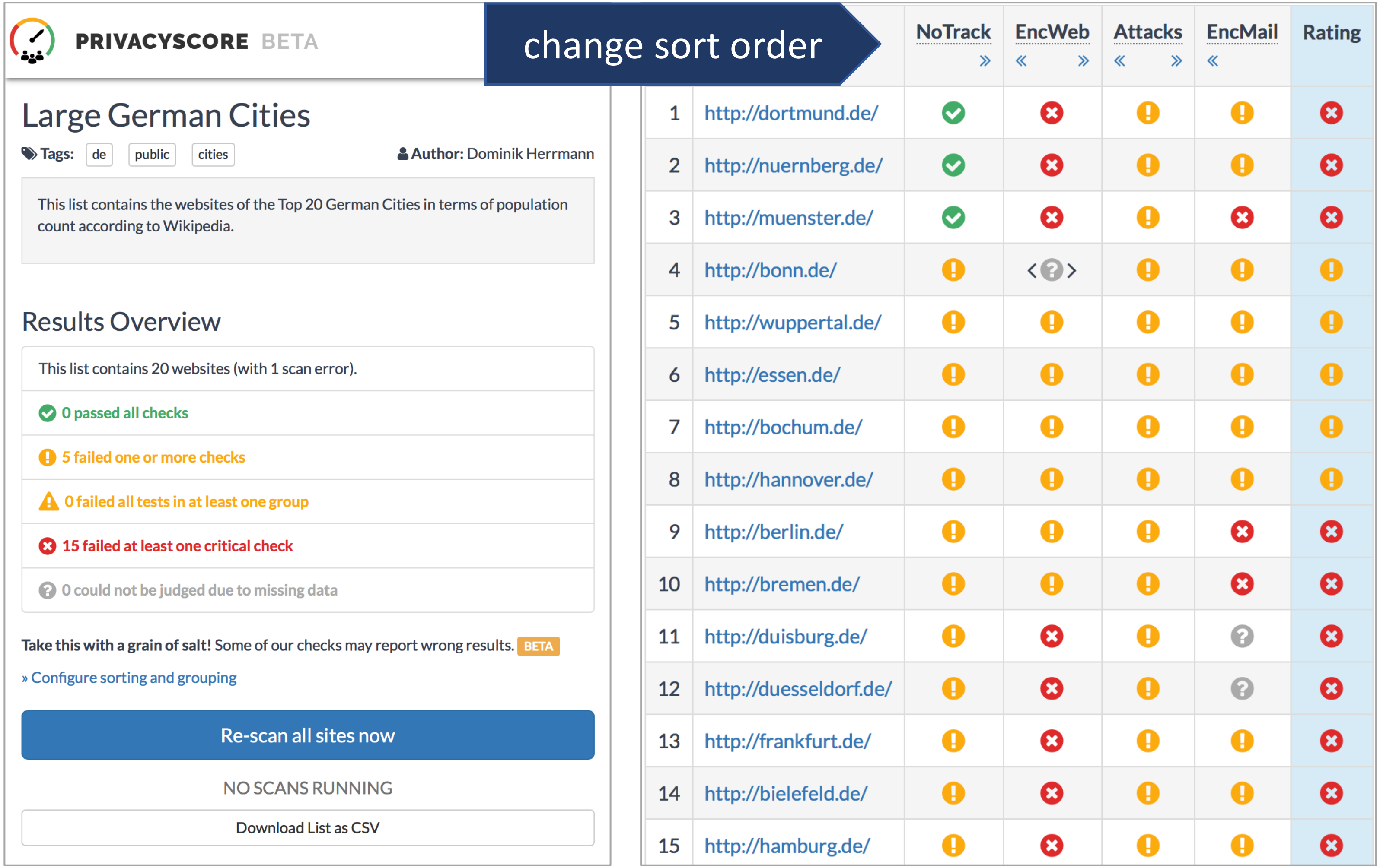
Ranking and Detailed Results

Four categories of checks

- **No Tracking**
- **Encryption to Website**
- **Encryption to Mailserver**
- **Protection Against Other Attacks**

Public Ranking

(as of Oct 2017)



change sort order

PRIVACYSCORE BETA

Large German Cities

Tags: de public cities

Author: Dominik Herrmann

This list contains the websites of the Top 20 German Cities in terms of population count according to Wikipedia.

Results Overview

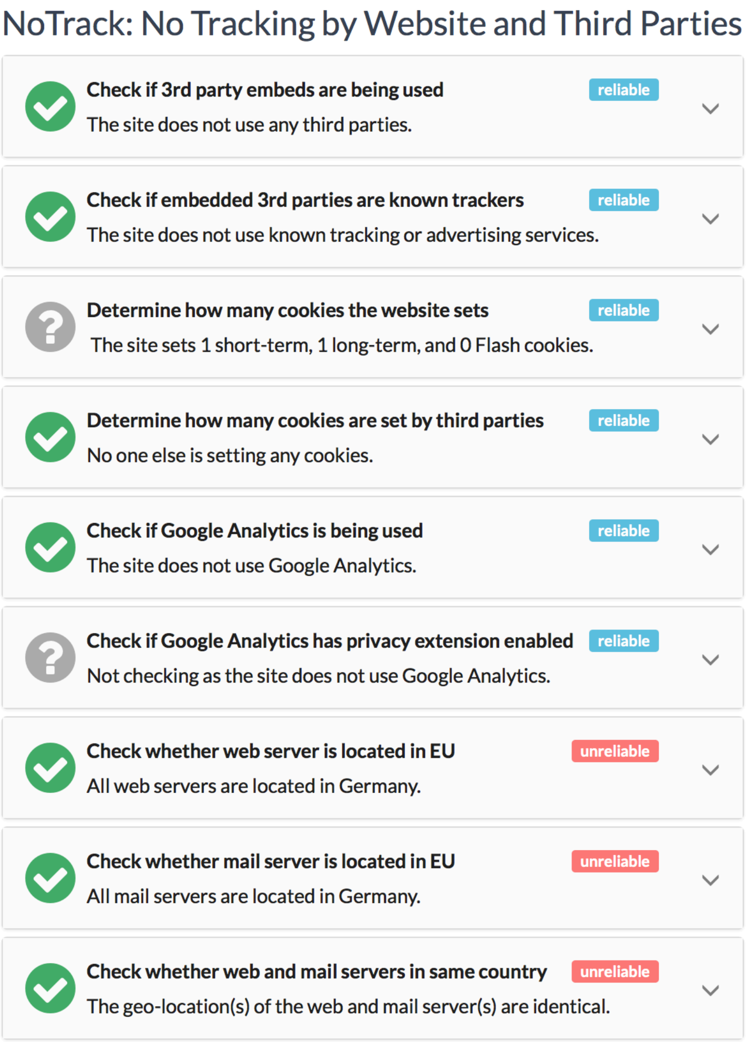
This list contains 20 websites (with 1 scan error).

- ✓ 0 passed all checks
- ! 5 failed one or more checks
- ⚠ 0 failed all tests in at least one group
- ✗ 15 failed at least one critical check
- ? 0 could not be judged due to missing data

Take this with a grain of salt! Some of our checks may report wrong results. BETA

» Configure sorting and grouping

		NoTrack »	EncWeb « »	Attacks « »	EncMail «	Rating
1	http://dortmund.de/	✓	✗	!	!	✗
2	http://nuernberg.de/	✓	✗	!	!	✗
3	http://muenster.de/	✓	✗	!	✗	✗
4	http://bonn.de/	!	<?>	!	!	!
5	http://wuppertal.de/	!	!	!	!	!
6	http://essen.de/	!	!	!	!	!
7	http://bochum.de/	!	!	!	!	!
8	http://hannover.de/	!	!	!	!	!
9	http://berlin.de/	!	!	!	✗	✗
10	http://bremen.de/	!	!	!	✗	✗
11	http://duisburg.de/	!	✗	!	?	✗
12	http://duesseldorf.de/	!	✗	!	?	✗
13	http://frankfurt.de/	!	✗	!	!	✗
14	http://bielefeld.de/	!	✗	!	!	✗
15	http://hamburg.de/	!	✗	!	!	✗



NoTrack: No Tracking by Website and Third Parties

✓ **Check if 3rd party embeds are being used** reliable
The site does not use any third parties.

✓ **Check if embedded 3rd parties are known trackers** reliable
The site does not use known tracking or advertising services.

? **Determine how many cookies the website sets** reliable
The site sets 1 short-term, 1 long-term, and 0 Flash cookies.

✓ **Determine how many cookies are set by third parties** reliable
No one else is setting any cookies.

✓ **Check if Google Analytics is being used** reliable
The site does not use Google Analytics.

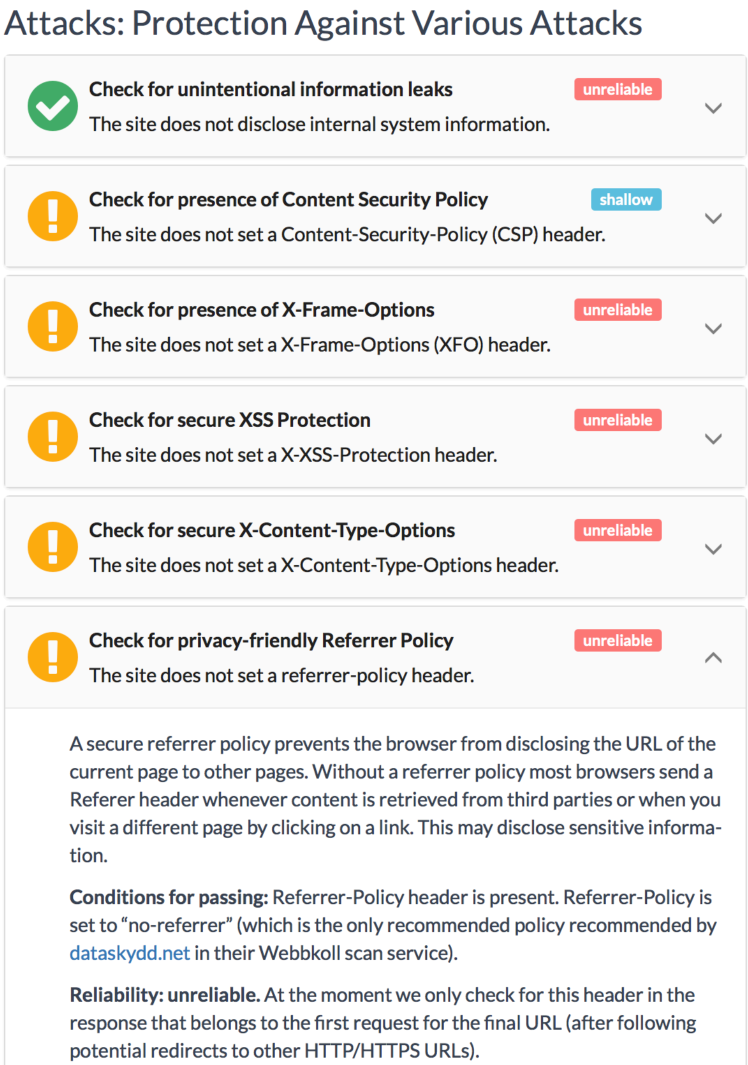
? **Check if Google Analytics has privacy extension enabled** reliable
Not checking as the site does not use Google Analytics.

✓ **Check whether web server is located in EU** unreliable
All web servers are located in Germany.

✓ **Check whether mail server is located in EU** unreliable
All mail servers are located in Germany.

✓ **Check whether web and mail servers in same country** unreliable
The geo-location(s) of the web and mail server(s) are identical.

detailed results of a site



Attacks: Protection Against Various Attacks

✓ **Check for unintentional information leaks** unreliable
The site does not disclose internal system information.

! **Check for presence of Content Security Policy** shallow
The site does not set a Content-Security-Policy (CSP) header.

! **Check for presence of X-Frame-Options** unreliable
The site does not set a X-Frame-Options (XFO) header.

! **Check for secure XSS Protection** unreliable
The site does not set a X-XSS-Protection header.

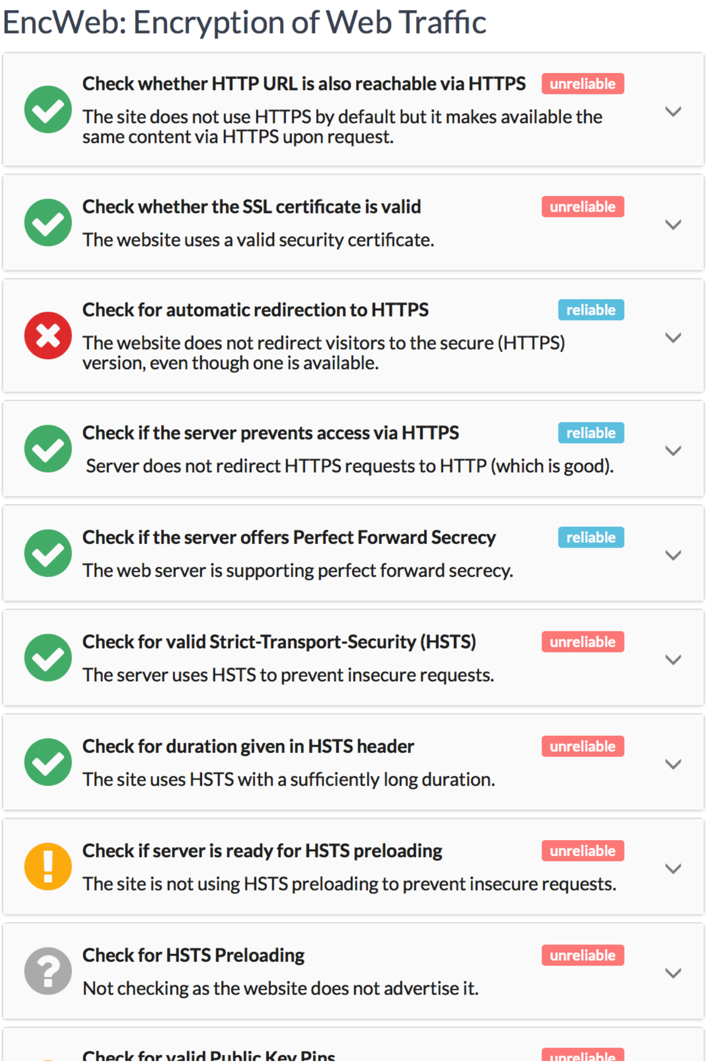
! **Check for secure X-Content-Type-Options** unreliable
The site does not set a X-Content-Type-Options header.

! **Check for privacy-friendly Referrer Policy** unreliable
The site does not set a referrer-policy header.

A secure referrer policy prevents the browser from disclosing the URL of the current page to other pages. Without a referrer policy most browsers send a Referer header whenever content is retrieved from third parties or when you visit a different page by clicking on a link. This may disclose sensitive information.

Conditions for passing: Referrer-Policy header is present. Referrer-Policy is set to "no-referrer" (which is the only recommended policy recommended by dataskydd.net in their Webbkoll scan service).

Reliability: unreliable. At the moment we only check for this header in the response that belongs to the first request for the final URL (after following potential redirects to other HTTP/HTTPS URLs).



EncWeb: Encryption of Web Traffic

✓ **Check whether HTTP URL is also reachable via HTTPS** unreliable
The site does not use HTTPS by default but it makes available the same content via HTTPS upon request.

✓ **Check whether the SSL certificate is valid** unreliable
The website uses a valid security certificate.

✗ **Check for automatic redirection to HTTPS** reliable
The website does not redirect visitors to the secure (HTTPS) version, even though one is available.

✓ **Check if the server prevents access via HTTPS** reliable
Server does not redirect HTTPS requests to HTTP (which is good).

✓ **Check if the server offers Perfect Forward Secrecy** reliable
The web server is supporting perfect forward secrecy.

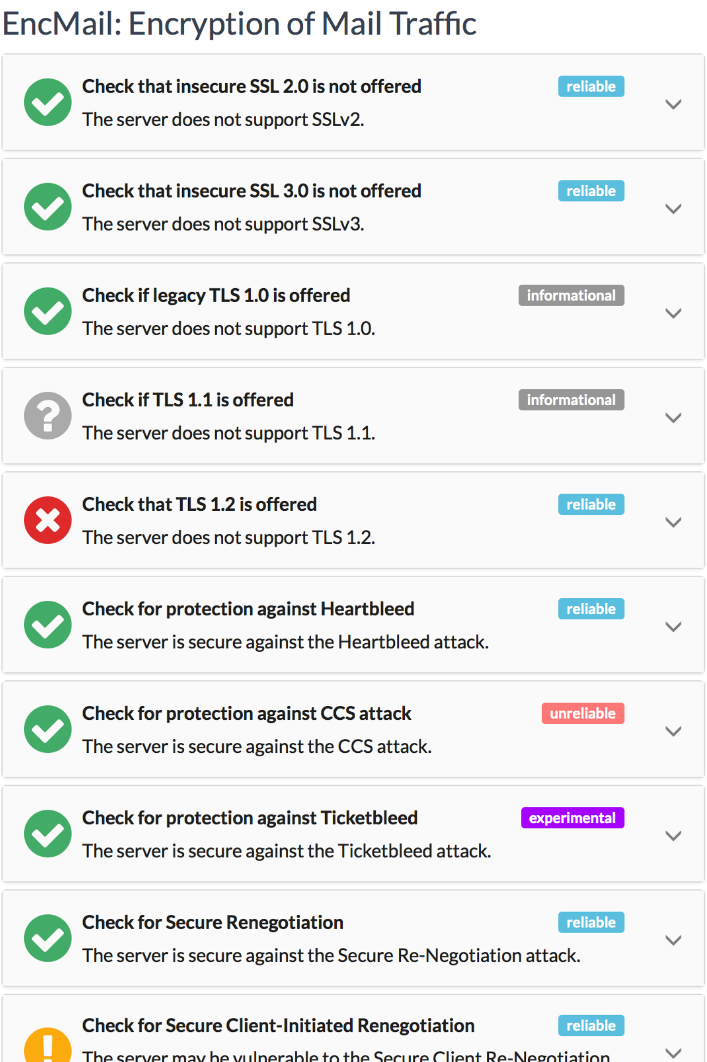
✓ **Check for valid Strict-Transport-Security (HSTS)** unreliable
The server uses HSTS to prevent insecure requests.

✓ **Check for duration given in HSTS header** unreliable
The site uses HSTS with a sufficiently long duration.

! **Check if server is ready for HSTS preloading** unreliable
The site is not using HSTS preloading to prevent insecure requests.

? **Check for HSTS Preloading** unreliable
Not checking as the website does not advertise it.

Check for valid Public Key Pins unreliable



EncMail: Encryption of Mail Traffic

✓ **Check that insecure SSL 2.0 is not offered** reliable
The server does not support SSLv2.

✓ **Check that insecure SSL 3.0 is not offered** reliable
The server does not support SSLv3.

✓ **Check if legacy TLS 1.0 is offered** informational
The server does not support TLS 1.0.

? **Check if TLS 1.1 is offered** informational
The server does not support TLS 1.1.

✗ **Check that TLS 1.2 is offered** reliable
The server does not support TLS 1.2.

✓ **Check for protection against Heartbleed** reliable
The server is secure against the Heartbleed attack.

✓ **Check for protection against CCS attack** unreliable
The server is secure against the CCS attack.

✓ **Check for protection against Ticketbleed** experimental
The server is secure against the Ticketbleed attack.

✓ **Check for Secure Renegotiation** reliable
The server is secure against the Secure Re-Negotiation attack.

! **Check for Secure Client-Initiated Renegotiation** reliable
The server may be vulnerable to the Secure Client Re-Negotiation

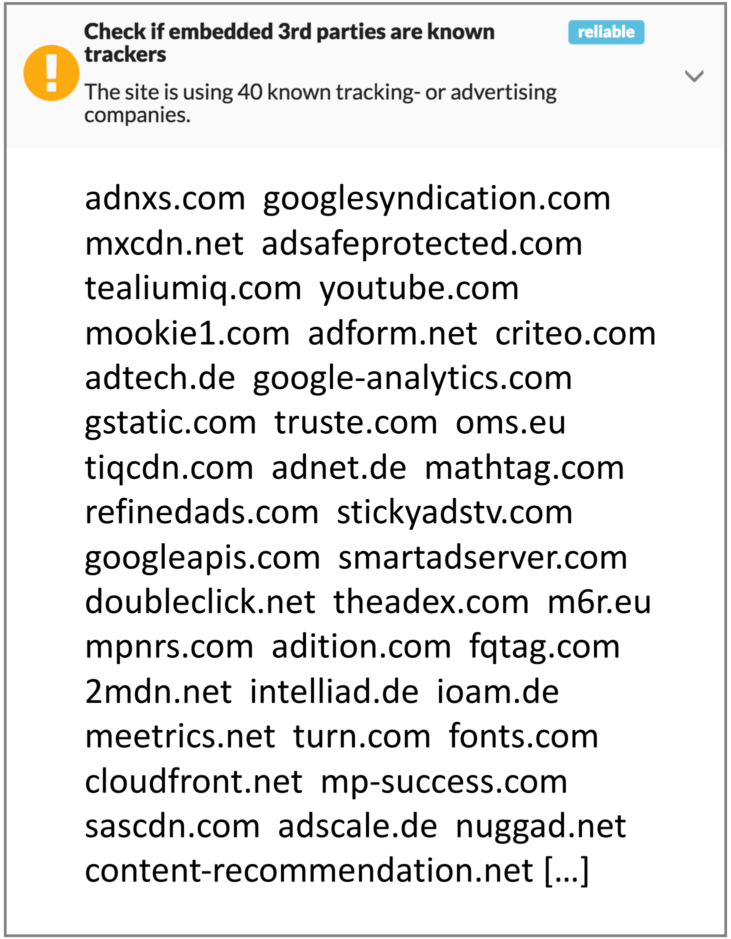
Predefined analyses for more transparency

(under development)

Top 20 Cities	Known Trackers	Third Party Servers	Third Party Cookies
Hamburg	**40**	**81**	**49**
Berlin	**22**	**37**	**17**
Leipzig	**6**	**10**	**5**
München	**5**	**11**	3
Bremen	4	**13**	3
Dresden	3	**8**	4
Düsseldorf	2	3	3
Hannover	2	3	1
Köln	2	3	1
Stuttgart	1	**7**	2

operated by media agencies

	Top 20 Cities	Known Trackers	Third Party Servers	Third Party Cookies
●	Hamburg	**40**	**81**	**49**
●	Berlin	**22**	**37**	**17**
	Leipzig	**6**	**10**	**5**
●	München	**5**	**11**	3
●	Bremen	4	**13**	3
●	Dresden	3	**8**	4
	Düsseldorf	2	3	3
●	Hannover	2	3	1
	Köln	2	3	1
●	Stuttgart	1	**7**	2
●	Bielefeld	1	2	0
●	Bonn	1	1	0
	Duisburg	0	4	0
	Essen	0	2	1
	Wuppertal	0	2	0
	Münster	0	0	0
	Dortmund	0	0	0
	Nürnberg	0	0	0
	Bochum	0	0	0
	Frankfurt	0	0	0



Check if embedded 3rd parties are known trackers reliable

The site is using 40 known tracking- or advertising companies.

adnxs.com googlesyndication.com mxcdn.net adsafeprotected.com tealiumiq.com youtube.com mookie1.com adform.net criteo.com adtech.de google-analytics.com gstatic.com truste.com oms.eu tiqcdn.com adnet.de mathtag.com refinedads.com stickyadstv.com googleapis.com smartadserver.com doubleclick.net theadex.com m6r.eu mpnrs.com adition.com fqtag.com 2mdn.net intelliad.de ioam.de meetrics.net turn.com fonts.com cloudfront.net mp-success.com sascdn.com adscale.de nuggad.net content-recommendation.net [...]

Top 20 Cities	Known Trackers	Third Party Servers	Third Party Cookies	Web: HTTPS	Mail: STARTTLS
Hamburg	**40**	**81**	**49**	**no redirection**	minor issues
Berlin	**22**	**37**	**17**	minor issues	**no TLS 1.2**
Leipzig	**6**	**10**	**5**	**no redirection**	minor issues
München	**5**	**11**	3	**enforces HTTP !**	minor issues
Bremen	4	**13**	3	minor issues	**no TLS 1.2**
Dresden	3	**8**	4	**no redirection**	minor issues
Düsseldorf	2	3	3	certificate issue	check timed out
Hannover	2	3	1	minor issues	minor issues
Köln	2	3	1	**enforces HTTP !**	minor issues
Stuttgart	1	**7**	2	**no redirection**	minor issues
Bielefeld	1	2	0	**no redirection**	minor issues
Bonn	1	1	0	check timed out	minor issues
Duisburg	0	4	0	**no redirection**	check timed out
Essen	0	2	1	minor issues	minor issues
Wuppertal	0	2	0	minor issues	minor issues
Münster	0	0	0	minor issues	**no TLS 1.2**
Dortmund	0	0	0	**no TLS 1.2**	minor issues
Nürnberg	0	0	0	**no TLS 1.2**	minor issues
Bochum	0	0	0	minor issues	minor issues
Frankfurt	0	0	0	minor issues	minor issues

BETA

some results may be wrong

Visualizing changes over time to track progress (under development)

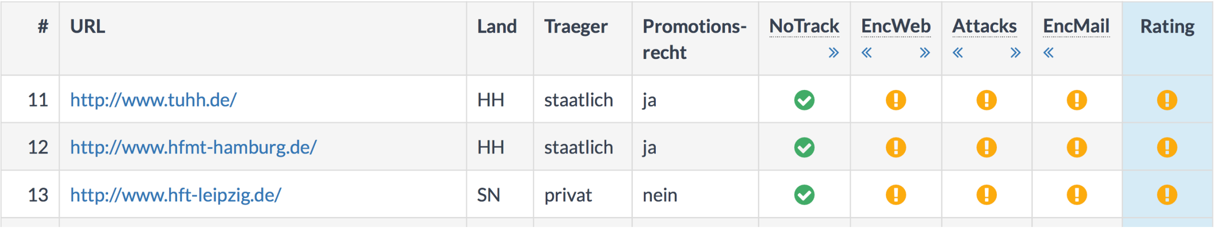
All submitted websites are rescanned periodically.

NO. OF KNOWN TRACKERS

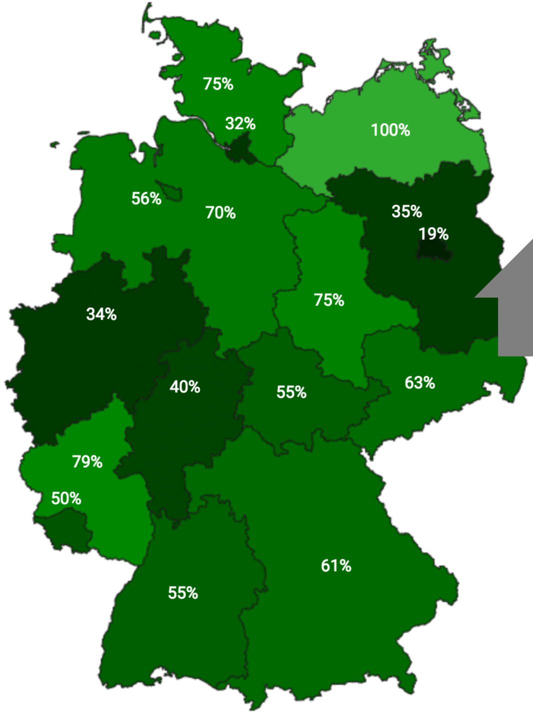
	14 Aug	27 Oct	Delta
Piraten	0	0	–
Linke	0	1	‼
Die PARTEI	0	0	–
CDU	1	1	–
Grüne	1	2	‼
SPD	1	0	☺
FDP	2	2	–
AFD	4	4	–
CSU	5	38	‼

⁉

Geographic analysis of university sites uncovers regional peculiarities (under development)

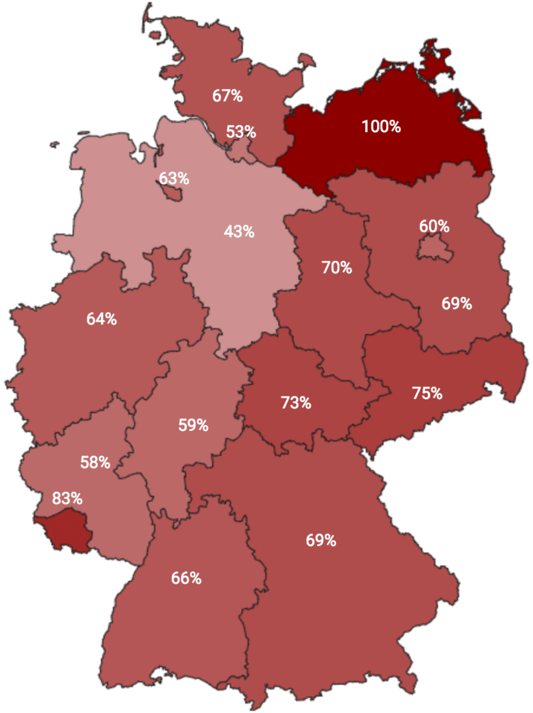


#	URL	Land	Traeger	Promotions-recht	NoTrack »	EncWeb « »	Attacks « »	EncMail «	Rating
11	http://www.tuhh.de/	HH	staatlich	ja	✓	!	!	!	!
12	http://www.hfmt-hamburg.de/	HH	staatlich	ja	✓	!	!	!	!
13	http://www.hft-leipzig.de/	SN	privat	nein	✓	!	!	!	!



Fraction with NoTrack ✓

darker is worse



Fraction with EncWeb ✗

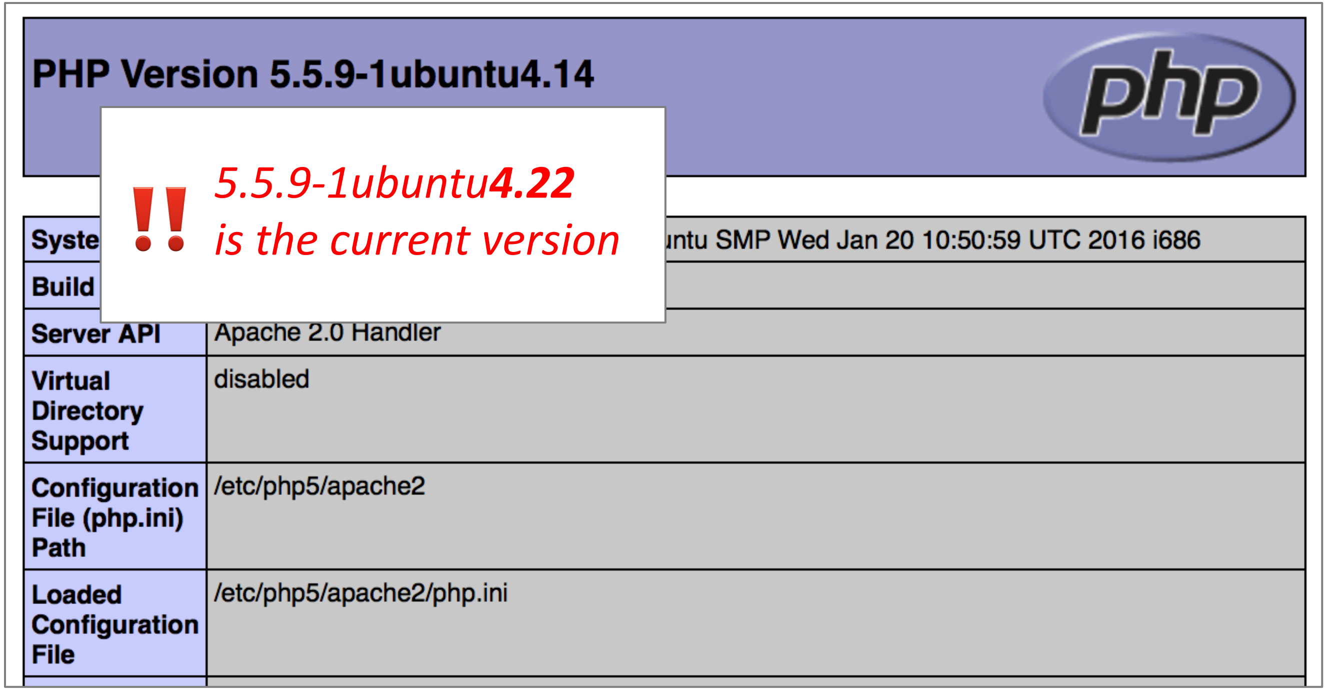
PrivacyScore also checks for typical information leaks

Try to retrieve …

/phpinfo.php
/.git/ and /.svn/
/server.key
/backup.sql
/server-status/

[…]

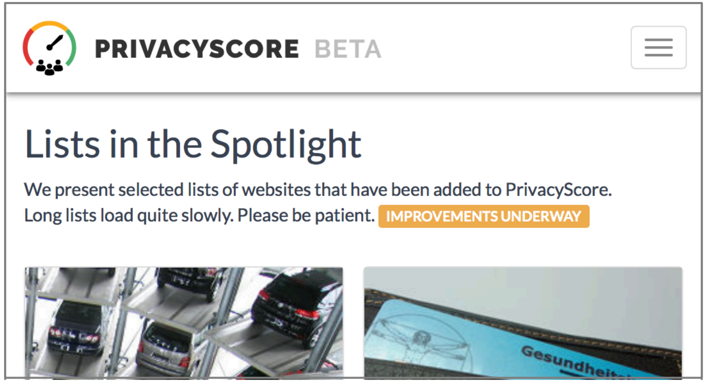
http://www. REDACTED .bg/phpinfo.php



PHP Version 5.5.9-1ubuntu4.14

Syste	untu SMP Wed Jan 20 10:50:59 UTC 2016 i686
Build	
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini

‼ *5.5.9-1ubuntu**4.22***
is the current version



PRIVACYSCORE BETA

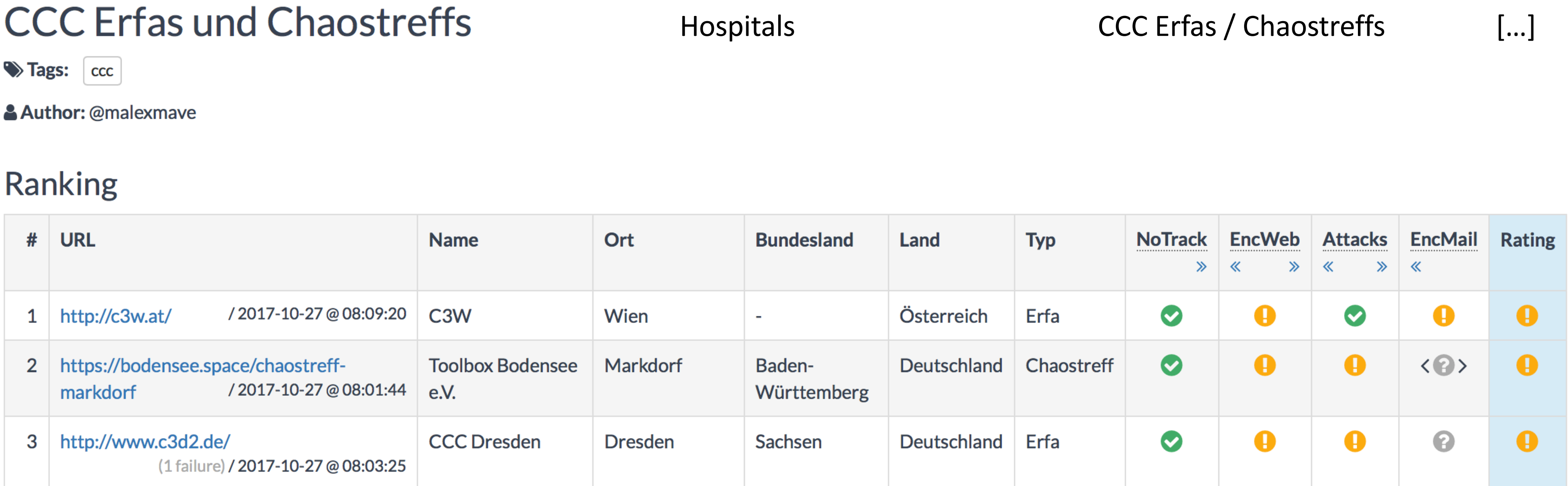
Lists in the Spotlight

We present selected lists of websites that have been added to PrivacyScore.
Long lists load quite slowly. Please be patient. IMPROVEMENTS UNDERWAY

More than 20 lists so far

- Health insurers
- Universities
- Political parties
- Authorities
- Municipalities
- Hospitals
- Data protection authorities
- Global Top 500 (moz.com)
- Internet Service Providers
- Banks
- News Sites
- CCC Erfas / Chaostreffs

[…]



CCC Erfas und Chaostreffs

Tags: ccc

Author: @malexmave

Ranking

#	URL	Name	Ort	Bundesland	Land	Typ	NoTrack »	EncWeb « »	Attacks « »	EncMail «	Rating
1	http://c3w.at/ / 2017-10-27 @ 08:09:20	C3W	Wien	-	Österreich	Erfa	✓	!	✓	!	!
2	https://bodensee.space/chaostreff-markdorf / 2017-10-27 @ 08:01:44	Toolbox Bodensee e.V.	Markdorf	Baden-Württemberg	Deutschland	Chaostreff	✓	!	!	< ? >	!
3	http://www.c3d2.de/ (1 failure) / 2017-10-27 @ 08:03:25	CCC Dresden	Dresden	Sachsen	Deutschland	Erfa	✓	!	!	?	!

Ethical
Considerations

1	Aren’t you helping the bad guys?	dual use
2	We don’t want to overload servers.	rate limiting

Legal

Considerations

Legal considerations for running PrivacyScore (in Germany)

1 – Websites are analyzed without consent of owners

2 – Results are interpreted and used to obtain a ranking

3 – Rankings are published on the PrivacyScore website

Received **one abuse report** since June 2017 after scanning a mailserver.

Whitelisting policy: We may stop scanning upon request, but publish this fact on the site.

M Maaß, A. Laubach, D. Herrmann:
PrivacyScore: Analyse von Webseiten auf Sicherheits- und Privatheitsprobleme – Konzept und rechtliche Zulässigkeit.
GI INFORMATIK 2017, Workshop Recht und Technik: https://arxiv.org/abs/1705.08889 (2017)

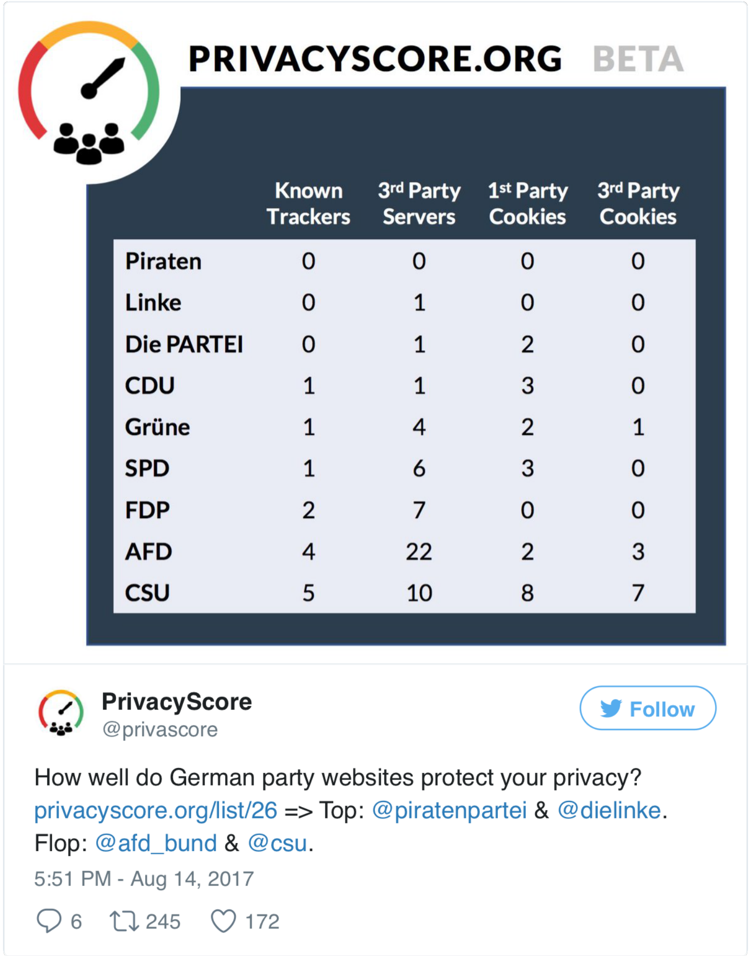
Summary

PrivacyScore: **test and rank websites** according to security and privacy features

Creates transparency, awareness, and incentives for site operators

What checks would you want to see?

Upload your own lists today!



PRIVACYSCORE.ORG BETA

	Known Trackers	3rd Party Servers	1st Party Cookies	3rd Party Cookies
Piraten	0	0	0	0
Linke	0	1	0	0
Die PARTEI	0	1	2	0
CDU	1	1	3	0
Grüne	1	4	2	1
SPD	1	6	3	0
FDP	2	7	0	0
AFD	4	22	2	3
CSU	5	10	8	7

PrivacyScore
@privascore

How well do German party websites protect your privacy? privacyscore.org/list/26 => Top: @piratenpartei & @dielinke. Flop: @afd_bund & @csu.

5:51 PM - Aug 14, 2017