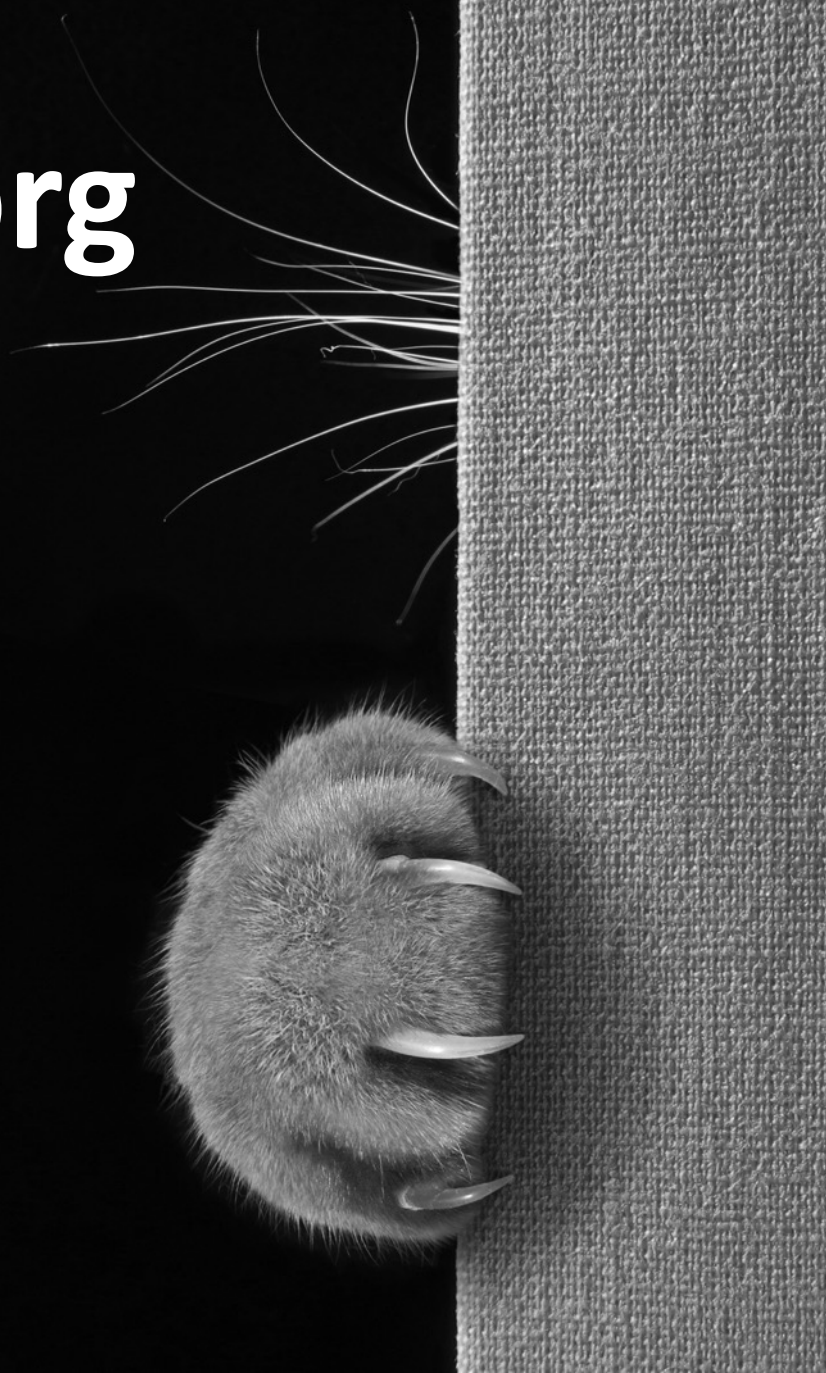
PrivacyScore.org

Eine Plattform zum Vergleich von Privacy- und Security-Eigenschaften von Webseiten

Prof. Dr. Dominik Herrmann
Lehrstuhl für Privatsphäre und Sicherheit in Informationssystemen

Otto-Friedrich Universität Bamberg

Folien: https://dhgo.to/ps-20190430



Die meisten Scan-Dienste für Webseiten untersuchen lediglich einzelne Seiten.

PRIVACYSCORE BETA

LISTS CODE TEAM FAQ

Webseiten vergleichen mit PrivacyScore

PrivacyScore erlaubt Ihnen, Websites hinsichtlich einer Reihe von Sicherheits- und Datenschutzfunktionen zu bewerten.

Eigene Liste erstellen

— oder eine bestimmte Seite direkt scannen —

URL, z.B. privacyscore.org | LOS

Öffentliche Benchmarks, als **Anreiz** für Betreiber, den Schutz der Privatsphäre zu verbessern.

Jeder kann (annotierte) **Listen** von Webseiten hochladen und das **Ranking beeinflussen**.

Open Source (GPLv3+) und Open Data

Öffentliches Ranking

Sortierung ändern

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

Re-scan all sites now

NO SCANS RUNNING

Download List as CSV

		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/	!	✗	!	!	✗
16	http://dresden.de/	!	✗	!	!	✗
17	http://stadt-koeln.de/	!	✗	!	!	✗
18	http://leipzig.de/	!	✗	!	!	✗
19	http://stuttgart.de/	!	✗	!	!	✗
20	http://muenchen.de/	!	✗	!	!	✗

Detail-Ergebnisse

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.

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).

Potential scan errors: We may miss security problems on sites that redirect multiple times. We may also miss security problems on sites that issue multi-

Tests von PrivacyScore

Privatsphäre und Tracking

Third Parties

Bekannte Tracker

Server-Standorte

Verschlüsselung Webserver

HTTPS/STARTTLS verfügbar?

Zertifikat: gültig / Schlüssellänge

Unsichere Protokolle: SSLv3, …

Schwachstellen: Heartbleed, …

HSTS

Mixed Content

Automatische Umleitung zu HTTPS

Verschlüsselung Mailserver

andere Angriffe

Referer-Policy

Security-Header

Problematische Inhalte

server-status

phpinfo.php

server.key

backup.sql

.git

core

.svn

2 Jahre Betriebserfahrung

knapp 120.000 Webseiten

über 1.600.000 Scans

etwa 250 Listen

Banken, Versicherungen, Schulen, Kommunen, Parteien, Politiker, EU-Behörden, Alexa Top 500, Datenschutzbeauftragte, Ärztekammern, IHKs, Kinderseiten, Einzelhändler, Buchungsportale, Apotheken, Mitglieder der ARD, Newsseiten, Hochschulen, Buchverlage, Automobilhersteller

Sicherheitslücke betraf mehr als 170 Online-Apotheken

Wer kauft gerade welche Medikamente ein? Dritte konnten solche sensiblen Informationen bei zahlreichen Internetapotheken einsehen. Die Panne betraf Dutzende Websites auf einmal.

Von Markus Böhm

Donnerstag, 24.05.2018 14:44 Uhr

Auf die Fährte des Problems hatte die Bamberger Forscher ein Nutzer ihrer Website "PrivacyScore" gebracht. Das Portal ermöglicht es, Websites automatisch auf gängige Datenschutz- und Sicherheitsprobleme hin untersuchen zu lassen.

Im Februar hatte ein Nutzer dort mehrere Listen mit dem Titel "Registered Internet Pharmacies in Germany (which are pharmacies)" hochgeladen, was dazu führte, dass der Onlinedienst die Apotheken-Websites überprüfte. Ergebnis der technischen Analyse war, dass auffallend viele der Websites dasselbe Sicherheitsproblem hatten.

https://www.apc .de/server-status

Szenario nachgestellt

Apache Server Status for

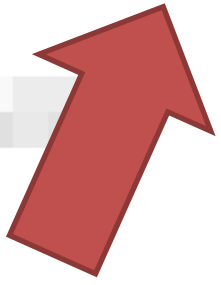
Server Version: Apache/2.2.8 (Ubuntu) mod_auth_pgsql/2.0.3 mod_python/3.3.1 Python/2.5.2 PHP/5.2.4-2ubuntu5.27 with Suhosin-Patch mod_ruby/1.2.6 Ruby/1.8.6(2007-09-24) mod_ssl/2.2.8 OpenSSL/0.9.8g mod_perl/2.0.3 Perl/v5.8.8
Server Built: Mar 8 2013 17:04:27

Current Time: Monday, 11-Jun-2018 11:07:53 NZST
Restart Time: Tuesday, 22-May-2018 15:24:04 NZST
Parent Server Generation: 13
Server uptime: 19 days 19 hours 43 minutes 48 seconds
Total accesses: 138469 - Total Traffic: 5.9 GB
CPU Usage: u20.71 s3.32 cu0 cs0 - .0014% CPU load
.0809 requests/sec - 3719 B/second - 44.9 kB/request
1 requests currently being processed, 9 idle workers

____._._W.___.....

Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-13	4978	0/8/11203	_	0.37	345	0	0.0	0.01	495.05			NULL
1-13	4501	0/26/10972	_	0.49	346	230	0.0	18.34	435.15			GET /keywordsearch;jsessionid=83D21A252177B8
2-13	5207	0/1/10580	_	0.01	138	8	0.0	0.00	364.21			
3-13	3210	0/102/10603	_	2.68	344	0	0.0	18.22	534.61			
4-13	-	0/0/10030	.	0.01	341	8	0.0	0.00	335.80			
5-13	4437	0/35/10152	_	0.90	346	0	0.0	47.02	371.89			
6-												



Nicht immer erwünschte Wirkung

„Unterlassen Sie weitere Tests. Sonst stellen wir Strafanzeige nach § 202a StGB.“

Auf Wunsch von weiteren Scans ausgeschlossen.

Letzte Ergebnisse bleiben aber sichtbar.

Betrieb in Deutschland rechtlich zulässig

siehe *arxiv.org/abs/1705.08889* (GI INFORMATIK 2017)

Von weiteren Scans ausgenommen

Die Betreiber der hier aufgeführten Seiten haben uns gebeten, keine weiteren Scans durchzuführen. Aus Gründen der Transparenz archivieren wir das Ergebnis des letzten erfolgreichen Scans in der folgenden Tabelle. Beachten Sie, dass es möglich ist, dass Seitenbetreiber in der Zwischenzeit Änderungen an ihrer Website vorgenommen haben, die sich nicht in diesen veralteten Ergebnissen widerspiegeln.

#	Adresse (URL)	Name	Versicherte	Typ	Kategorie	NoTrack »	EncWeb « »	Attacks « »	EncMail «	Rating
1	http://www.meine-krankenkasse.de/ / 2018-01-12 @ 06:51:56	BKK Verkehrsbau Union	498.000	gesetzl	BKK	!	!	!	?	!
2	http://www.novitas-bkk.de/ (1 Fehler) / 2018-01-16 @ 13:18:50	Novitas BKK	410.216	gesetzl	BKK	!	!	!	?	!
3	http://www.bmwbkk.de/ / 2017-12-18 @ 13:53:50	Betriebskrankenkasse der BMW AG – betriebsbezogen	157.839	gesetzl	BKK	!	!	!	!	!

11

Einige Betreiber
hören tatsächlich zu.

ANZAHL DER TRACKER

	14 Aug	27 Okt	Delta
Piraten	0	0	–
Linke	0	1	!!
Die PARTEI	0	0	–
CDU	1	1	–
Grüne	1	2	!!
SPD	1	0	gut!
FDP	2	2	–
AFD	4	4	–
CSU	5	38	!!

??

Update 30. Jan. 2019:
nur noch 1 Tracker auf *csu.de*

In Entwicklung

- Überprüfung der Aktualität der Serversoftware
- Automatisierte Benachrichtigung der Seitenbetreiber
- Nutzerdefinierte Rankings und Ratings
- Vergleichsfunktionen

German Institutions of Higher Education

Submitted 6 months ago by foobar123

- sites passed all checks 0
- sites with issues 331
- sites failed an area 3
- sites with critical issues 0

Total number of sites 426
Sites with scan errors 120
No rating (missing data) 3
Excluded from scans 0

HTTPS available: 79%

HTTPS used by default: 45%

Average trackers per site: 56

Sites with leaks: 5%

Sites with known trackers: 30%

Rank	URL	Name	HSTS	# Trackers	EncWeb	Attacks	NoTrack
1	http://www.uni-bamberg.de	University of Bamberg	■	14	✓	!	!
2	http://www.uni-regensburg.de	University of Regensburg	☐	0	✗	!	!
3	http://www.tum.de	University of TUM	☐	3	✗	!	!

TRACKING BY SITE OPERATOR AND THIRD PARTIES

Third Parties — 4 CHECKS

- **3** known trackers — de.ioam.de, double... [more]

  https://**de.ioam.de**/tx.io?st=heise&cp=homepage&sv=ke&pt=CP&ps=lin&er=N2f=&r2=...
  https://**securepubads.g.doubleclick.net**/gpt/pubads_impl_rendering_2019041601.js
  https://**cdn.mateti.net**/mcp/onsite.min.js

- No Google Analytics
- **10** other third parties — youtube.com, google.com... [more]
- **5** third-party cookies

Site Operator — 5 CHECKS

- No first-party cookies
- Webserver in GDPR-implementing country: Germany [more]
- Mailserver in GDPR-implementing country: Germany [more]
- Webserver and mailserver are located in the very same country
- Privacy-preserving Referer header present

show over time | compare sites

2018-09-10 – 2019-04-14

min: 0 max: 20

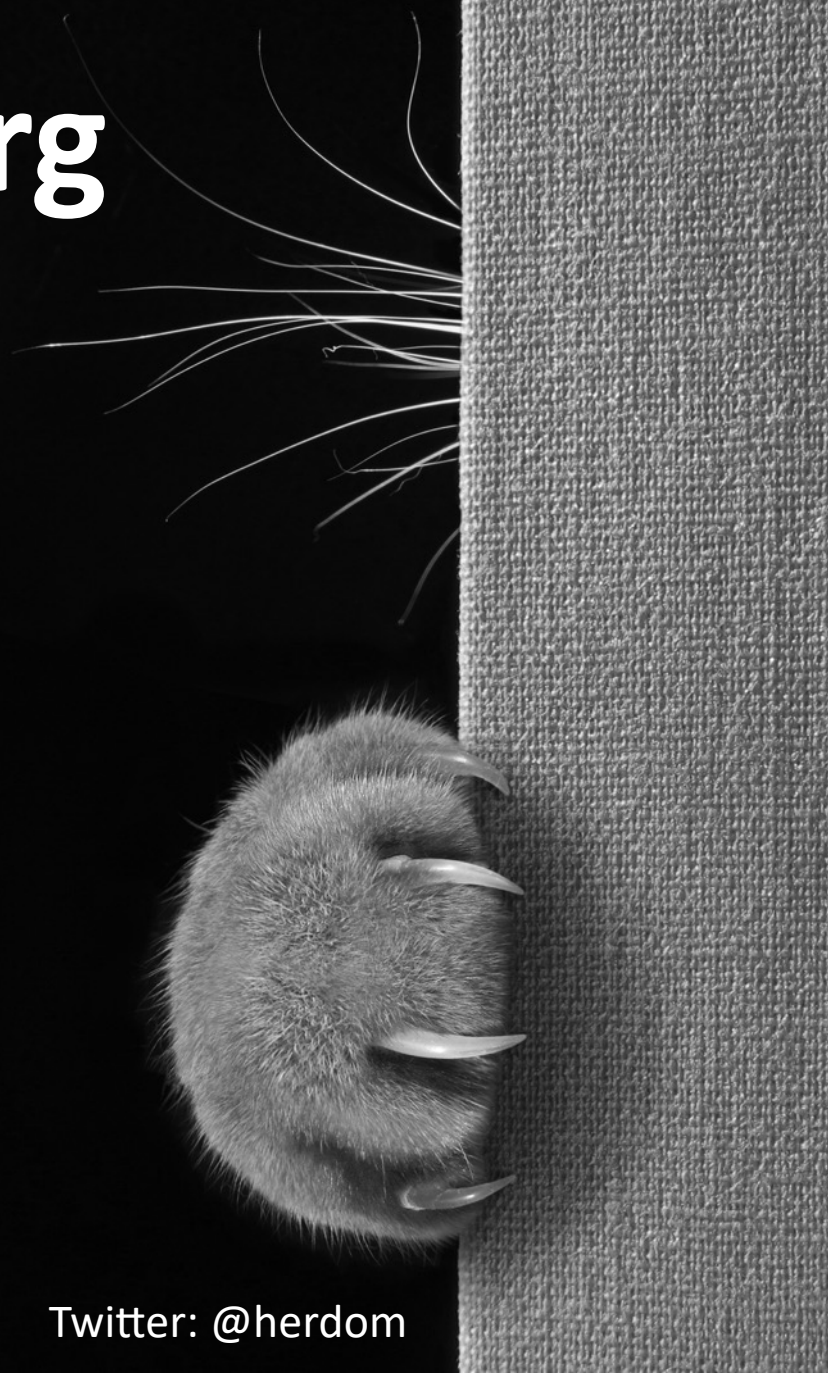
German Institutions of ... | v

90% of sites in list have less
40% of sites in list have 0

Many websites are using services provided by third parties to enhance their websites. However, this use of third parties has pri-

PrivacyScore.org

Eine Plattform zum Vergleich von Privacy- und Security-Eigenschaften von Webseiten



Prof. Dr. Dominik Herrmann
Lehrstuhl für Privatsphäre und Sicherheit in Informationssystemen

Otto-Friedrich Universität Bamberg

Folien: https://dhgo.to/ps-20190430

Twitter: @herdom