

# PrivacyScore

**A public scanning platform to  
assess privacy issues of websites**

Dominik Herrmann

Universities of Siegen & Hamburg

<http://herdom.net/>

# Who learns what about me?

← ⓘ | symptoms.webmd.com/default.htm#introView

🗨️ ↺ 🔍 Search

⬇️ ☆ 📅 🖨️ ⌵ ⌂ 📶 24 📞 10 ☰

CHECK YOUR SYMPTOMS

FIND A DOCTOR

FIND LOWEST DRUG PRICES

SIGN IN

SIGN UP

SUBSCRIBE

WebMD

HEALTH A-Z

DRUGS & SUPPLEMENTS


LIVING HEALTHY

FAMILY & PREGNANCY

NEWS & EXPERTS

SEARCH 🔍

WebMD Home > Symptom Checker



WebMDsymptomchecker

Take the Tour 🗺️

Take the first step and see what could be causing your symptoms. Then learn about possible next steps.

For

Me

Gender

☒ Male

☐ Female

Age

25-34 years

Zip code

Optional

Email

Optional

Stay informed with the latest health news and features from WebMD. Get our [Men's Health Newsletter](#) delivered right to your inbox. By clicking Submit, you agree to the [WebMD Terms & Conditions](#) & [Privacy Policy](#) and understand that you may opt out of WebMD subscriptions at any time.

Submit

If you are a WebMD member, [sign in](#) to save your Symptom Checker history.

The Air Quality Index

How healthy is the air in your area? See if pollution levels where you live could make it hard to breathe today.

Zip Code

Go

☐ Remember my zip code

# Who learns what about me?

The screenshot shows a web browser window with the URL `www.hamburg.de/mitte/hilfen-lebensunterhalt/`. The browser's address bar and tabs are visible. The website content includes a navigation bar with links like 'HAMBURGER', 'BESUCHER', 'POLITISCHES', and 'TOP-SERVICES'. The main content area is titled 'Hilfe zum Lebensunterhalt' and contains text about social security benefits. A Privacy Badger extension overlay is active, displaying a list of detected trackers and their status.

**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.

Tracker	Status
www.google-analytics.com	Blocked
de.ioam.de	Blocked
qs.ioam.de	Blocked
script.ioam.de	Allowed
collect-eu-central-1.tealiu...	Blocked
visitor-service.tealiumiq.com	Blocked

Buttons at the bottom of the overlay:

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

**hamburg.de**

**Bezirk Hamburg-Mitte**

HOTELS & TOURISMUS KULTUR & TICKETS JOBS & WOHNEN ERLEBNIS & F

HAMBURG-MITTE

SOZIALES GRUNDSICHERUNG & SOZIALLEISTUNG SOZIALHILFE HILFEN ZUM LEBENSUNT

Gefällt mir Twittern +1 Vorlesen Drucken

**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.

Anspruchsvoraussetzungen:

Behördenfinder

# Existing Scanning Services

# Results for **www.bundestag.de**

[↻ Check again](#)

🕒 2017-03-02 07:12:21

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

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

		<b>2</b>	<b>1</b>	<b>1</b>
Insecure	Referrers leaked	Cookies	Third-party request	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://webbkoll.dataskydd.net/en/>

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [youtube.com](#) > 216.58.212.142

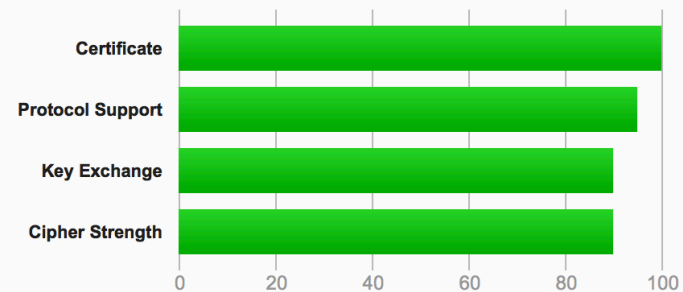
## SSL Report: [youtube.com](#) (216.58.212.142)

Assessed on: Wed, 01 Mar 2017 20:48:35 UTC | [Clear cache](#)

[Scan Another](#)

### Summary

#### Overall Rating



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/>

# Scan your site now

<https://scotthelme.co.uk/>

Scan

☐ Hide results ☐ Follow redirects

## Security Report Summary



**Site:** <https://scotthelme.co.uk/>

**IP Address:** 2604:a880:1:20::207:b001

**Report Time:** 02 Mar 2017 07:05:57 UTC

**Report Short URL:** <https://schd.io/13u>

**Headers:**

✓ Strict-Transport-Security

✓ Content-Security-Policy

✓ Public-Key-Pins

✓ X-Frame-Options

✓ X-XSS-Protection

✓ X-Content-Type-Options

✓ Referrer-Policy

<https://securityheaders.io/>

## Scan Summary



<b>Host:</b>	crash-stats.mozilla.com
<b>Scan ID #:</b>	3436353
<b>Test Time:</b>	March 2, 2017 5:30 AM
<b>Test Duration:</b>	2 seconds
<b>Score:</b>	90/100
<b>Tests Passed:</b>	10/12

## Recommended Change

[Initiate Rescan](#)

You're halfway finished! Nice job!

The `X-Content-Type-Options` header tells browsers to stop automatically detecting the contents of files. This protects against attacks where they're tricked into incorrectly interpreting files as JavaScript.

- [Mozilla Web Security Guidelines \(X-Content-Type-Options\)](#)

Once you've successfully completed your change, click [Initiate Rescan](#) for the next piece of advice.

## Test Scores

Test	Pass	Score	Explanation
<a href="#">Content Security Policy</a>	✓	0	<p>Content Security Policy (CSP) implemented with unsafe sources inside <code>style-src</code>.</p> <p>This includes <code>'unsafe-inline'</code>, <code>data:</code> or overly broad sources such as <code>https:</code>.</p> 

<https://observatory.mozilla.org/>



## Summary of heise.de SSL/TLS Security Test

**FINAL GRADE**

A

**COMPLIANT WITH**


☒ PCI DSS


**HOST**

SERVER IP : PORT  
193.99.144.80:443

DATE OF TEST  
February 24th 2017, 20:45 CET

**OPTIONS**

 Refresh results

 Download PDF

The server prefers cipher suites supporting Perfect-Forward-Secrecy.

Good configuration


The server supports cipher suites that are not approved by NIST guidelines and HIPAA guidance.

Non-compliant with NIST and HIPAA

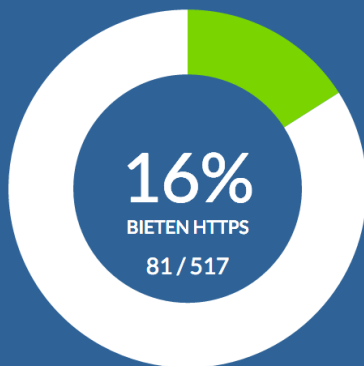
## Relevant Subdomains



Hostname	Port	Service/Protocol	Date/Time	Grade	Compliant with	Archived Result
beta.heise.de	443	HTTPS	February 25th 2017, 01:10	A		<a href="#">View &gt;</a>
business-services.heise.de	443	HTTPS	February 25th 2017, 01:09	A+	PCI DSS	<a href="#">View &gt;</a>
spiele.heise.de	443	HTTPS	February 27th 2017, 01:10	A+	PCI DSS	<a href="#">View &gt;</a>

 SHOW 12 MORE

<https://www.htbridge.com/ssl/>



# Sicheres HTTP (HTTPS)

Letzter Update: 26. Februar 2017

Diese Daten zeigen, ob Domains deutscher Behörden das HTTPS-Protokoll (`https://`) unterstützen, und - falls ja - wie stark diese Unterstützung ist. **HTTPS** ermöglicht eine sichere Verbindung zwischen Webseiten und ihren Besuchern und wird zum Mindeststandard für öffentliche Web-Services. So empfiehlt auch das BSI den **Einsatz von HTTPS als Mindeststandard für die öffentliche Verwaltung**.

Auch wenn HTTPS eingesetzt wird, bedeutet das nicht, dass eine Webseite nicht trotzdem gehackt werden kann. Für mehr Informationen, was HTTPS tut (und was es nicht tun kann), **besuche die HTTPS FAQ** (in Englisch).

Nach Domain

Nach Behörde

Info

Zeige [10](#) | [25](#) | [50](#) | [100](#) Einträge

Suche:

Behörde	Anzahl Domains	Bietet HTTPS	Erzwingt HTTPS	Strict Transport Security (HSTS)
Bundesministerium für Arbeit und Soziales	<a href="#">160</a>	3% <div></div>	3% <div></div>	1% <div></div>
Deutscher Wetterdienst	<a href="#">70</a>	40% <div></div>	0% <div></div>	0% <div></div>
Bundestag	<a href="#">48</a>	2% <div></div>	0% <div></div>	0% <div></div>

<https://https.jetzt/>

# Alexa Top 1 Million Analysis - Feb 2017

*February 27, 2017*

## Previous Crawls

I've done 3 previous crawls before now and they were [Aug 2015](#), [Feb 2016](#) and [Aug 2016](#). They've shown some awesome trends in our adoption of security headers and HTTPS and I've also made several improvements to my crawlers along the way. These latest results are literally fresh off the press as I'm now running my crawl every single day, but more on that later, so let's dig in.

	Aug 2016	Aug 2016	Feb 2017	Feb 2017	% change
CSP	4,139	0.4410%	11,010	1.1736%	166.01%
CSPRO	6118	0.6518%	1,435	0.1530%	-76.54%
XWCSP	383	0.0408%	368	0.0392%	-3.92%
XCSP	743	0.0792%	882	0.0940%	18.71%
PKP	375	0.0400%	501	0.0534%	33.60%
PKPRO	76	0.0081%	74	0.0079%	-2.63%
STS	29,908	3.1863%	41,032	4.3738%	37.19%
XCTO	69,414	7.3951%	90,333	9.6290%	30.14%
XFO	90,124	9.6015%	95,774	10.2090%	6.27%
XXSSP	54,499	5.8061%	71,966	7.6712%	32.05%
XDO	613	0.0653%	6,952	0.7410%	1034.09%
XPCDP	690	0.0735%	6,935	0.7392%	905.07%
HTTPS	129,149	13.7590%	187,245	19.9593%	44.98%

<https://scotthelme.co.uk/alex-top-1-million-analysis-feb-2017/>



# Hur privatlivsvänlig är din kommun?

Vi har undersökt webbplatserna för Sveriges 290 kommuner och tagit reda på vilka dataskyddande funktioner de använder — eller *inte* använder — för att hjälpa dig utöva makt över ditt privatliv.

Webbplatserna [betygsattes](#) enligt en skala A-E. Klicka på ett kommunnamn för detaljerad information.

**I korthet:**0 **A**0 **B**17 **C**58 **D**214 **E**

Antal med HTTPS: 22

*Tips: använd [Dataskydd.net:s Webb koll](#) för att testa din egen sajt (eller någon annans)!*

Visa  kommunerSök : 

Kommun	Betyg	HTTP/HTTPS	Läcker refererrs	Kakor totalt
<a href="#">Ale</a>	<b>D</b>	HTTP	Ja	6
<a href="#">Alingsås</a>	<b>D</b>	HTTP	Ja	9
<a href="#">Alvesta</a>	<b>E</b>	HTTP	Ja	5
<a href="#">Aneby</a>	<b>D</b>	HTTP	Ja	6
<a href="#">Arboga</a>	<b>D</b>	HTTP	Ja	4



## Pressemitteilung

9. September 2014

### Datenschutzprüfung bei Mailservern bayerischer Unternehmen

**Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat Anfang September 2014 bei insgesamt 2.236 bayerischen Unternehmen das Sicherheitsniveau der eingesetzten Mailserver automatisiert überprüft. 772 Unternehmen genügten dabei den gestellten datenschutzrechtlichen Anforderungen nicht und wurden deshalb vom BayLDA schriftlich aufgefordert, ihre Mailserver an den Stand der Technik anzupassen.**

Allgemein bekannt ist die Tatsache, dass das Versenden unverschlüsselter E-Mails vom Grad der Geheimhaltung wie das Verschicken einer Postkarte bewertet wird. Jeder, der die Karte zu Gesicht bekommt, kann ohne größeren Aufwand den Inhalt lesen, auswerten oder sogar ändern. Dass ein solches Mitlesen unverschlüsselter E-Mails nicht nur für Geheimdienste problemlos möglich ist, ist nicht erst seit den Enthüllungen von Edward Snowden bekannt, aber sicherlich mehr in das Bewusstsein der Allgemeinheit gedrungen. Aus diesem Grund sind Unternehmen darauf hinzuweisen, dass sie nach den Vorschriften des Bundesdatenschutzgesetzes (BDSG) verpflichtet sind, im Rahmen der Zugangs-, Zugriffs- und Weitergabekontrolle Verschlüsselungsverfahren in angemessenem Umfang bei den von Ihnen eingesetzten Mailservern nach dem Stand der Technik zu verwenden.

### Verschlüsselung mit STARTTLS und Perfect Forward Secrecy

Wenn eine E-Mail verschickt werden soll, „handeln“ die beteiligten Mailserver zunächst einen Standard für die Übertragung der Nachricht aus, bevor die E-Mail tatsächlich verschickt wird. Das heißt, die Mailserver fragen, sofern sie entsprechend konfiguriert sind, jeweils bei dem anderen nach, ob eine Transport-Verschlüsselung (Transport Layer Security, kurz TLS) unterstützt wird und übertragen dann die E-Mail mit dem bestmöglichen Grad der Verschlüsselung. Mailserver von Unternehmen müssen deshalb das hierbei angewandte Verfahren **STARTTLS** zur Verschlüsselung unterstützen, damit eine Transport-Verschlüsselung bei der Übermittlung von E-Mails überhaupt ermöglicht werden kann. Zusätzlich ist das so genannte **Perfect Forward Secrecy** einzusetzen, damit selbst bei

<https://heise.de/-2390692>

# Existing scanning services

- mainly **useful for admins** who want to check their own site
- some provide **APIs**, some perform **regular rescans**
- typically **do not offer access to whole database** and history
- only very few datasets are publically available

# PrivacyScore



(to be released “soon”)

# Goals of PrivacyScore

Improve privacy for consumers by publicly exposing “opportunities for improvement” found by **automatically scanning websites**.

Increase motivation for providers to act by publishing results as a **benchmark with their peers**.

Provide an easily accessible tool for **federal data protection officers**.

**Targets:** websites run by corporations, government and NGOs

**Crowdsourcing:** everyone should be able to set up a new benchmark (list of sites) at any time.

Analyze at SSL, HTTP headers, 3<sup>rd</sup> party cookies – **and much more**.

**Automated rescans** of lists

**Private benchmarks**

Provide basis for **arbitrary queries**:

- Do Bavarian schools perform better than schools in Hamburg?
- Private vs. public banking sector



Name

German University Websites

Private lists won't  
show up publically☐ Privat**i** Beschreibung

Source of URLs: Wikipedia

**Tags**

de, university

Erstellen Sie hier Ihre Tabelle. Zusätzlich zur URL können Sie zu jeder Website weitere Attribute angeben, wie Land, Sprache oder Branche der Website.

⊗: Reihe/Spalte löschen. ⇌: Spalte verschieben. 👁: Spalte standardmäßig sichtbar. 🔒: Spalte standardmäßig versteckt.

Spalte hinzufügen

Reihe hinzufügen

10 Reihe hinzufügen

Arbitrary columns allow to  
group/aggregate results.

URL (http://...)

⊗ 👁

State

⊗ http://www.uni-siegen.de/

NRW

⊗ https://www.uni-hamburg.de/

HH

⊗ http://www.uni-regensburg.de/

BY

⊗ http://...

alternative:  
CSV upload



<http://www.uni-regensburg.de/>



Liste speichern



Liste scannen

Ihre Liste wurde gespeichert unter dem Token


iiiDwDFf2GgOtbZnq3fpkYEA0uwjXIWDTVE021j4Bsu7mRdGXM

Lightweight design:  
no user management

List creators receive a token  
(can edit/delete their list).

# German University Websites

 Source of URLs: Wikipedia

 de, university

 3/2/2017 - 09:05 Uhr →

Durchschnittliche  
Bewertung

der Seiten bieten  
HTTPS an

Durch  
Anzahl

**Lists are immutable**

but new lists can be  
derived from them


Liste wird gerade  
gescannt - Momentan  
kein erneuter Scan  
möglich

Neue Liste aus dieser  
erstellen

**Scan anzeigen**

3/2/2017 - 09:05 Uhr

☐ **Vergleichs-Scan**

 **Scan läuft seit 3/2/2017 - 09:05 Uhr**  
**Status: Retrieving URL 2/3**  
**11 seconds elapsed**

## Liste suchen

ID, Name, Tags, ...

Suchen

Full text search

**German University Websites** ➔

**i** Source of URLs: Wikipedia

**🔖** de, university

**🕒** wird gescannt...

Start: 3/2/2017 - 09:05 Uhr

**Doo** ➔

**i**

**🔖**

**🕒** 3/1/2017 - 19:55 Uhr

**Doo** ➔

**i**


**🔖**

**Most recently added lists**


directory-like access  
also conceivable

7 - 14:37 Uhr

# German University Websites

 Source of URLs: Wikipedia

 de, university

 3/2/2017 - 09:05 Uhr → 3/2/2017 - 09:13 Uhr

Erneuter Scan möglich  
in 90 Minuten

Neue Liste aus dieser  
erstellen

?

Durchschnittliche  
Bewertung


33.33%

der Seiten bieten  
HTTPS an

2

Durchschnittliche  
Anzahl an Cookies

Scan anzeigen

3/2/2017 - 09:05 Uhr 

Overview of a benchmark

State	Bewertung	HTTPS	HTTPS-Umleitung	Anzahl Cookies	Third Parties	Third Party R
http://www.uni-siegen.de/	NRW	?	✗	✗	2	5
https://www.uni-hamburg.de/	HH	?	✓	✗	4	2
http://www.uni-regensburg.de/	BY	?	✗	✗	0	0

Einträge pro Seite

Liste ausklappen

Spalten anzeigen / verbergen

CSV-Export

PDF-Export

Results of a single page

# Ergebnisse für https://www.uni-hamburg.de/

🕒 02.03.2017 - 08:06 Uhr

Finale URL: https://www.uni-hamburg.de/

?

Bewertung



Zertifizierte HTTPS-  
Verbindung

2 (4)

Third Party Hosts  
(Third Party Requests)

4

Anzahl Cookies

0/0

Gesetzte  
HTTP-Header

Scan anzeigen

02.03.2017 - 08:06 Uhr



## Sichere Verbindung

https://www.uni-hamburg.de/ bietet HTTPS als Standard an.

## Third Parties (2)

Domain
ad1.adfarm1.adition.com
imagesrv.adition.com

## Third Party Requests (4)

Domain
https://ad1.adfarm1.adition.com/js/wp_id=2549993
https://imagesrv.adition.com/js/acb/uid.html
https://ad1.adfarm1.adition.com/banner?sid=2549993&adsver=3&co=1&fvers=24&iframe=0&ref=&os=6&browser=6&h5=-1&h5s=0&wi=1890145534&ac=1&screen_res=175&wpt=J&clickurl=
https://imagesrv.adition.com/banners/372/files/00/08/6d/00/000000552192.gif

## Cookies (4)

Domain	Host	Name	Wert	Gültigkeit
adition.com	.adfarm1.adition.com	UserID1	6392794104089542848	19.03.2017 - 18:03 Uhr
adition.com	ad1.adfarm1.adition.com	fc2	100c0	19.03.2017 - 18:03 Uhr
uni-hamburg.de	www.uni-hamburg.de	_pk_id.83.8f48	17047bb02f69467a.1488438393.1.1488438393.1488438393.	19.03.2017 - 23:10 Uhr
uni-hamburg.de	www.uni-hamburg.de	_pk_ses.83.8f48	*	19.03.2017 - 13:44 Uhr

# Geo-IP

Alle Web-Server in Deutschland.  
Alle Mail-Server in Deutschland.

Feld	Value	Erklärung
MX_LOCATIONS	Germany	Erklärung
A_LOCATIONS	Germany	Erklärung
A_CNAME	www-fiona.rrz.uni-hamburg.de	Erklärung
MX_REVERSE_LOOKUP	mx04.rrz.uni-hamburg.de, mx05.rrz.uni-hamburg.d e, mx03.rrz.uni-hamburg.de	Erklärung
A_REVERSE_LOOKUP	www-fiona.rrz.uni-hamburg.de	Erklärung
MX_ADDRESSES	134.100.38.104, 134.100.38.105, 134.100.38.103	Erklärung
MX_CNAMES		Erklärung
A_ADDRESSES	134.100.56.130	Erklärung
MX_NAMES	mx04.rrz.uni-hamburg.de, mx05.rrz.uni-hamburg.d e, mx03.rrz.uni-hamburg.de	Erklärung



?

Durchschnittliche  
Bewertung

100%

der Seiten bieten  
HTTPS an

39

Durchschnittliche  
Anzahl an Cookies

Scan anzeigen

2/28/2017 - 11:30 Uhr

☒ Vergleichs-Scan

2/28/2017 - 12:09 Uhr

Diagramm anzeigen

TTPS-Umleitung

Anzahl Cookies

Third Parties

Third Party Requests

Alle Webserver in Deutschland

×

39 ↗ 40

32

175

true

Comparisons over time

# Ergebnisse für http://www.spiegel.de/

🕒 02.03.2017 - 08:30 Uhr

Finale URL: http://www.spiegel.de/

?

Bewertung



Unsichere  
HTTP-Verbindung

42 (112)

Third Party Hosts  
(Third Party Requests)

39

Anzahl Cookies

0/0

Gesetzte  
HTTP-Header

Scan anzeigen

02.03.2017 - 08:30 Uhr ▼

## Third Parties (42)

Domain
securepubads.g.doubleclick.net
mep-de.sensic.net
ssl.ligatus.com
s290.mxcdn.net
tpc.googlesyndication.com
sc.iasds01.com
sync.ligadx.com
x.ligatus.com
rtax.criteo.com
h-ssl.ligatus.com
adx.ligadx.com

⌵ Alle anzeigen

## Third Party Requests (112)

Domain
https://script.ioam.de/iam.js
http://imagesrv.adition.com/js/srp.js
http://ad.yieldlab.net/yp/504572,87001?ts=1488439806356
http://rtax.criteo.com/delivery/rta/rta.js?netId=3335&cookieName=cookieName&rnd=43895474138&varName=criteoContent
http://ad8.adfarm1.adition.com/s?t=i0zf.Nl&v=1&w=1446214867&a=1&b=6&f=24&o=6&r=175&p=vpaid(false)device(desktop&s=3505455*3505456*3505447*3554757*3505460*3535055*3505461*3505462*3505463*3505464*3505465*3505466*3505467*3505468*3505469*3505470*3505471*3505472*3505473*3505452*3505451*3505449*3505450*3505454*3505453*3505457
http://de.ioam.de/tx.io?st=spiegel&cp=spon-www-18-0&sv=ke&pt=CP&rf=&r2=&ur=www.spiegel.de&xy=1366x768x24&lo=DE%2Fn.a.&cb=000d&vr=310&id=gdt2b9<=1488439806409&ev=&cs=h05mep&mo=1
http://de.ioam.de/tx.io?st=spiegel&cp=spon-www-18-0&sv=ke&nt=CP

# Cookies (39)

Domain	Host	Name	Wert	Gültigkeit
spiegel.de	www.spiegel.de	spiegelsans	1	19.03.2017 - 14:11 Uhr
spiegel.de	www.spiegel.de	spiegelserif	1	19.03.2017 - 14:11 Uhr
spiegel.de	www.spiegel.de	misobold	1	19.03.2017 - 14:11 Uhr
spiegel.de	www.spiegel.de	fontawesome	1	19.03.2017 - 14:11 Uhr
yieldlab.net	.yieldlab.net	id	9c43da98-fd8a-4018-bed3-d ceb0a19297c	19.03.2017 - 22:52 Uhr
adition.com	.adfarm1.adition.com	UserID1	243716154397517791H	19.03.2017 - 18:26 Uhr
adition.com	ad8.adfarm1.adition.com	fc9	1017blzNqAAEDyrdYywBrAA EByrdYq1lrAAEByrdY	19.03.2017 - 18:26 Uhr
ioam.de	.ioam.de	i00	002d9f418b8819f5d58b7c9f e0001%3B58b7c9fe%3B59ff 4eff	19.03.2017 - 20:04 Uhr
spiegel.de	.spiegel.de	spVcTimeout	1	19.03.2017 - 14:07 Uhr

⌵ Alle anzeigen

# Geo-IP

Alle Web-Server in Deutschland.

Nicht alle Mail-Server in Deutschland.

Who knows that I am visiting *www.spiegel.de* or that I am sending them an e-mail?

Feld	Value
MX_LOCATIONS	Ireland, United Kingdom
A_LOCATIONS	Germany
A_CNAME	null
MX_REVERSE_LOOKUP	mail-am14023.inbound.protection.outlook.com, mail-db34087.inbound.protection.outlook.com
A_REVERSE_LOOKUP	
MX_ADDRESSES	213.199.154.23, 213.199.154.87
MX_CNAMES	
A_ADDRESSES	62.138.116.25
MX_NAMES	spiegel-de.mail.protection.outlook.com

Architecture

# OpenWPM

- <https://github.com/citp/OpenWPM>
- Uses Selenium to instrument Firefox

```
class ScannerConnector():
```

```
    def startscan(self, url_List, list_id, scangroup_id):
```

```
        sites = url_List
```

```
        manager_params, browser_params = TaskManager.load_default_params(1)
```

```
        browser_params[0]['disable_flash'] = False
```

```
        browser_params[0]['headless'] = True
```

```
        browser_params[0]['bot_mitigation'] = True
```

```
        manager = TaskManager.TaskManager(manager_params, browser_params)
```

```
        for site in sites:
```

```
            command_sequence = CommandSequence.CommandSequence(site["url"])
```

```
            command_sequence.get(sleep=10, timeout=60)
```

```
            command_sequence.run_custom_function(determine_final_url, ('final_urls', site['url']))
```

```
            command_sequence.dump_profile_cookies(120)
```

```
            manager.execute_command_sequence(command_sequence, index='**')
```

```
        manager.close()
```

# testssl.sh

by Dirk Wetter

## Testing protocols via sockets except SPDY+HTTP2

SSLv2	not offered (OK)
SSLv3	not offered (OK)
TLS 1	offered
TLS 1.1	offered
TLS 1.2	offered (OK)
SPDY/NPN	not offered
HTTP2/ALPN	not offered

## Testing ~standard cipher lists

Null Ciphers	not offered (OK)
Anonymous NULL Ciphers	not offered (OK)
Anonymous DH Ciphers	not offered (OK)
40 Bit encryption	not offered (OK)
56 Bit export ciphers	not offered (OK)
Export Ciphers (general)	not offered (OK)
Low (<=64 Bit)	not offered (OK)
DES Ciphers	not offered (OK)
"Medium" grade encryption	not offered (OK)
Triple DES Ciphers	offered
High grade encryption	offered (OK)

## Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4

PFS is offered (OK)	ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA-AES128-SHA256	ECDHE-RSA-AES128-SHA
	ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA-AES256-SHA384	ECDHE-RSA-AES256-SHA



# testssl.sh

by Dirk Wetter

## Testing vulnerabilities

**Heartbleed** (CVE-2014-0160)  
**CCS** (CVE-2014-0224)  
**Secure Renegotiation** (CVE-2009-3555)  
**Secure Client-Initiated Renegotiation**  
**CRIME, TLS** (CVE-2012-4929)  
**BREACH** (CVE-2013-3587)  
**POODLE, SSL** (CVE-2014-3566)  
**TLS\_FALLBACK\_SCSV** (RFC 7507)  
**SWEET32** (CVE-2016-2183, CVE-2016-6329)  
**FREAK** (CVE-2015-0204)  
**DROWN** (CVE-2016-0800, CVE-2016-0703)

**LOGJAM** (CVE-2015-4000), experimental  
**BEAST** (CVE-2011-3389)

**LUCKY13** (CVE-2013-0169)  
**RC4** (CVE-2013-2566, CVE-2015-2808)

**not vulnerable (OK)**, no heartbeat extension

**not vulnerable (OK)**

**not vulnerable (OK)**

**not vulnerable (OK)**

**not vulnerable (OK)**

**no HTTP compression (OK)** - only supplied "/" tested

**not vulnerable (OK)**

Downgrade attack prevention supported (OK)

**VULNERABLE**, uses 64 bit block ciphers

**not vulnerable (OK)**

**not vulnerable on this port (OK)**

make sure you don't use this certificate elsewhere with SSLv2 e

<https://censys.io/ipv4?q=2CD448773C1B6C1C2672A5D01925789D18DAE2>

**not vulnerable (OK)**: no DH EXPORT ciphers, no DH key detected

TLS1: **ECDHE-RSA-AES128-SHA AES128-SHA ECDHE-RSA-AES256-SHA**

**AES256-SHA ECDHE-RSA-DES-CBC3-SHA DES-CBC3-SHA**

**VULNERABLE** -- but also supports higher protocols (possible miti

**VULNERABLE**, uses cipher block chaining (CBC) ciphers

**no RC4 ciphers detected (OK)**

# MongoDB

<input type="checkbox"/> T/F	redirected_to_https	true	Boolean
<input type="checkbox"/> T/F	geoip_all_webserverns_in_germany	true	Boolean
<input type="checkbox"/>	site_id	ObjectId("58b5a5b4137ed659c5f89c77")	ObjectId
<input type="checkbox"/>	third_parties_anzahl	36	Int32
▶ <input type="checkbox"/>	flashcookies	[ 0 elements ]	Array
<input type="checkbox"/>	cookies_anzahl	29	Int32
▶ <input type="checkbox"/>	profilecookies	[ 29 elements ]	Array
▶ <input type="checkbox"/>	testssl	{ 8 fields }	Object
<input type="checkbox"/>	scan_group_id	ObjectId("58b70b2a137ed61e1aaa04c5")	ObjectId
<input type="checkbox"/>	third_party_requests_anzahl	176	Int32
<input type="checkbox"/>	score	?	String
<input type="checkbox"/> T/F	https	true	Boolean
▶ <input type="checkbox"/>	responses	[ 239 elements ]	Array
<input type="checkbox"/> T/F	domain_has_mailserverns	true	Boolean
▶ <input type="checkbox"/>	third_party_requests	[ 176 elements ]	Array
▼ <input type="checkbox"/>	testsslmx	{ 8 fields }	Object
<input type="checkbox"/>	scanTime	46	String
<input type="checkbox"/>	target host	heise.de	String
<input type="checkbox"/>	openssl	1.0.2-chacha from Jun 22 19:32:29 2016	String
▼ <input type="checkbox"/>	scanResult	[ 1 element ]	Array
▼ <input type="checkbox"/>	[0]	{ 12 fields }	Object
▶ <input type="checkbox"/>	ciphers	[ 11 elements ]	Array
▼ <input type="checkbox"/>	headerResponse	[ 0 elements ]	Array
<input type="checkbox"/>	service	smtp	String
<input type="checkbox"/>	ip	193.99.145.50	String
<input type="checkbox"/>	hostname	relay.heise.de	String
▶ <input type="checkbox"/>	serverDefaults	[ 20 elements ]	Array
▼ <input type="checkbox"/>	pfs	[ 3 elements ]	Array
▼ <input type="checkbox"/>	[0]	{ 3 fields }	Object
<input type="checkbox"/>	finding	(Perfect) Forward Secrecy : PFS is offered	String
<input type="checkbox"/>	id	pfs	String
<input type="checkbox"/>	severity	OK	String
▶ <input type="checkbox"/>	[1]	{ 3 fields }	Object

(Lots of) Future Work

# Planned Checks 1

- SSL: http URL **redirects** to https?
- SSL **handshake** of **web** and **mail** server (first MX record)
  - Protocols (TLS 1.2?)
  - Weaknesses (Heartbleed, ...)
  - Handshake (PFS, ...)
- **Certificate**
  - Common Name == hostname?
  - Certificate expired?
  - key length “sufficient”?
  - signature algorithm  
(no MD5, no SHA-1)
- **HTTP headers** related to security
  - Strict-Transport-Security
  - Content Security Policy
  - X-XSS-Protection
  - X-Frame-Options
  - X-Content-Type-Options
  - Subresource Integrity
  - HTTP Public Key Pinning
  - Referrer-Policy

# Planned Checks 2

- First and Third party hostnames
  - look up in *disconnect.me* tracking protection list (local DB)
  - correlate with *Google Safebrowsing* list (partly local, may require lookup)
- Browser fingerprinting employed by first/third parties
- All data stays in Germany?
  - geolocation of webserver and mailserver (first mx)
  - using MaxMind GeoLite2 (with a local DB)
- Server software outdated?
  - bonus: look up matching CVEs based on version in banner string 😊

# Open Questions

# Open Questions 1

- Even more **checks**?
- How to **visualize** results?
- What **properties** might be interesting for data mining?
  - country, state, public/private, # of employees/citizens
  - standardize some of the labels?
- Calculate **ratings**: A<sup>+</sup>, A, B
  - weights for checks needed
  - alternative: provide fraction of passed checks
- Global public hall of (sh|f)ame?
  - Top Lists for *Third Parties* and *Cookie-setting Third Parties*
- Should we implement all checks ourselves (have keep it up to date) or tap **APIs of other scanners** (privacy issue)?
- Should we perform the scan if **robots.txt** disallows automated retrieval?

# Open Questions 2

**Bootstrapping:** Populate portal with interesting lists before launch

- all German “gov” domains
- universities, schools, cities
- health insurers, “netdokter.de et al.”
- banking sites
- (free) webmailers

**Publicity:** reached out to *digital-courage.de* and German Data Protection Commissioners

**Who else should know?**

[https://de.wikipedia.org/wiki/Liste\\_der\\_Gro%C3%9F-\\_und\\_Mittelst%C3%A4dte\\_in\\_Deutschland](https://de.wikipedia.org/wiki/Liste_der_Gro%C3%9F-_und_Mittelst%C3%A4dte_in_Deutschland)

[github.com/robby5/german-gov-domains](https://github.com/robby5/german-gov-domains)

**Ethical issues?**

**Research questions:** assess how providers react if confronted with the results

- personal communications
- security improvements (duration)



# PrivacyScore



**A public scanning platform to  
assess privacy issues of websites**

**Dominik Herrmann**

who is grateful to **Nico Vitt** and **Marvin Hebis**ch for their help  
and **Max Maaß** who came up with the initial idea

<http://herdom.net/>