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?

THE NEW NORMAL?
Existing Website Scanning Services
focus on single sites
SSL Report: **youtube.com** (216.58.212.142)
Assessed on: Wed, 01 Mar 2017 20:48:35 UTC | Clear cache

**Summary**

- **Overall Rating:** A

- **Certificate:** 100%
- **Protocol Support:** 100%
- **Key Exchange:** 100%
- **Cipher Strength:** 100%

Visit our [documentation page](https://www.ssllabs.com/ssltest) for more information, configuration guides, and books. Known issues are documented [here](https://www.ssllabs.com/ssltest).

Intermediate certificate has a weak signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. [MORE INFO »](https://www.ssllabs.com/ssltest)
Results for www.bundestag.de

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

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).
Existing Scanning Services ...

are targeted at server operators

use a pre-defined rating scheme

<table>
<thead>
<tr>
<th>Description</th>
<th>Modifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSTS preloaded</td>
<td>5</td>
</tr>
<tr>
<td>HSTS header max age ≥ 6 months</td>
<td>0</td>
</tr>
<tr>
<td>HSTS header max age &lt; six months</td>
<td>-10</td>
</tr>
<tr>
<td>HSTS header not implemented</td>
<td>-20</td>
</tr>
<tr>
<td>HSTS header cannot be set, as site contains an invalid certificate chain</td>
<td>-20</td>
</tr>
</tbody>
</table>
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
## Large German Cities

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

### Results Overview

- **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.

Configure sorting and grouping

Re-scan all sites now

<table>
<thead>
<tr>
<th>NoTrack</th>
<th>EncWeb</th>
<th>Attacks</th>
<th>EncMail</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✔</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>2</td>
<td>✔</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>3</td>
<td>✔</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>4</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>5</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>6</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>7</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>8</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>9</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>10</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>11</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>12</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>13</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>14</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
<tr>
<td>15</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
<td>☠</td>
</tr>
</tbody>
</table>
NoTrack: No Tracking by Website and Third Parties

- Check if 3rd party embeds are being used: The site does not use any third parties.
- Check if embedded 3rd parties are known trackers: The site does not use known tracking or advertising services.
- Determine how many cookies the website sets: The site sets 1 short-term, 1 long-term, and 0 Flash cookies.
- Determine how many cookies are set by third parties: No one else is setting any cookies.
- Check if Google Analytics is being used: The site does not use Google Analytics.
- Check if Google Analytics has privacy extension enabled: Not checking as the site does not use Google Analytics.
- Check whether web server is located in EU: All web servers are located in Germany.
- Check whether mail server is located in EU: All mail servers are located in Germany.
- Check whether web and mail servers are in the same country: The geo-location(s) of the web and mail server(s) are identical.

Attacks: Protection Against Various Attacks

- Check for unintentional information leaks: The site does not disclose internal system information.
- Check for presence of Content Security Policy: The site does not set a Content-Security-Policy (CSP) header.
- Check for presence of X-Frame-Options: The site does not set a X-Frame-Options (XFO) header.
- Check for secure XSS Protection: The site does not set a X-XSS-Protection header.
- Check for secure X-Content-Type-Options: The site does not set a X-Content-Type-Options header.
- Check for privacy-friendly Referrer Policy: 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 dataskyd.net in their Webkoll 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.

### 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 attack.
Predefined analyses for more transparency (under development)

<table>
<thead>
<tr>
<th>Top 20 Cities</th>
<th>Known Trackers</th>
<th>Third Party Servers</th>
<th>Third Party Cookies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hamburg</td>
<td>40</td>
<td>81</td>
<td>49</td>
</tr>
<tr>
<td>Berlin</td>
<td>22</td>
<td>37</td>
<td>17</td>
</tr>
<tr>
<td>Leipzig</td>
<td>6</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>München</td>
<td>5</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>Bremen</td>
<td>4</td>
<td>13</td>
<td>3</td>
</tr>
<tr>
<td>Dresden</td>
<td>3</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Düsseldorf</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Hannover</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Köln</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Stuttgart</td>
<td>1</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>Top 20 Cities</td>
<td>Known Trackers</td>
<td>Third Party Servers</td>
<td>Third Party Cookies</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------</td>
<td>---------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Hamburg</td>
<td>40</td>
<td>81</td>
<td>49</td>
</tr>
<tr>
<td>Berlin</td>
<td>22</td>
<td>37</td>
<td>17</td>
</tr>
<tr>
<td>Leipzig</td>
<td>6</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>München</td>
<td>5</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>Bremen</td>
<td>4</td>
<td>13</td>
<td>3</td>
</tr>
<tr>
<td>Dresden</td>
<td>3</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Düsseldorf</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Hannover</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Köln</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Stuttgart</td>
<td>1</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>Bielefeld</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Bonn</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Duisburg</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>Essen</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Wuppertal</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Münster</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Dortmund</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Nürnberg</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bochum</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Frankfurt</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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

- adnxs.com
- google-syndication.com
- mxcdn.net
- adsafe-protected.com
- tdcdn.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 [...]

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

BETA

some results may be wrong
Visualizing changes over time to track progress (under development)

All submitted websites are rescanned periodically.
Geographic analysis of university sites uncovers regional peculiarities (under development)

<table>
<thead>
<tr>
<th>#</th>
<th>URL</th>
<th>Land</th>
<th>Traeger</th>
<th>Promotionsrecht</th>
<th>NoTrack</th>
<th>EncWeb</th>
<th>Attacks</th>
<th>EncMail</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td><a href="http://www.tuhh.de/">http://www.tuhh.de/</a></td>
<td>HH</td>
<td>staatlich</td>
<td>ja</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>12</td>
<td><a href="http://www.hfmt-hamburg.de/">http://www.hfmt-hamburg.de/</a></td>
<td>HH</td>
<td>staatlich</td>
<td>ja</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>13</td>
<td><a href="http://www.hft-leipzig.de/">http://www.hft-leipzig.de/</a></td>
<td>SN</td>
<td>privat</td>
<td>nein</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

![Map of Germany showing percentage of websites with NoTrack and EncWeb features. Fractions with NoTrack are marked with a green check, while those with EncWeb are marked with a red cross. Darker shades indicate worse conditions.](image-url)
PrivacyScore also checks for typical information leaks

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

Try to retrieve …

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

 [...]
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

<table>
<thead>
<tr>
<th>#</th>
<th>URL</th>
<th>Name</th>
<th>Ort</th>
<th>Bundesland</th>
<th>Land</th>
<th>Typ</th>
<th>NoTrack</th>
<th>EncWeb</th>
<th>Attacks</th>
<th>EncMail</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="http://c3w.at/">http://c3w.at/</a></td>
<td>C3W</td>
<td>Wien</td>
<td>-</td>
<td>Österreich</td>
<td>Erfa</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>2</td>
<td><a href="https://bodensee.space/chaostreff-markdorf">https://bodensee.space/chaostreff-markdorf</a></td>
<td>Toolbox Bodensee e.V.</td>
<td>Markdorf</td>
<td>Baden-Württemberg</td>
<td>Deutschland</td>
<td>Chaostreff</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>&lt;❓&gt;</td>
<td>✔️</td>
</tr>
<tr>
<td>3</td>
<td><a href="http://www.c3d2.de/">http://www.c3d2.de/</a></td>
<td>CCC Dresden</td>
<td>Dresden</td>
<td>Sachsen</td>
<td>Deutschland</td>
<td>Erfa</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>?</td>
<td>✔️</td>
</tr>
</tbody>
</table>
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.


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!