A public scanning platform to assess privacy issues of websites

Matthias Marx
University of Hamburg
Motivation
Who knows that I am visiting social support websites?
Existing Scanning Services are focused on single-site scans
SSL Report: youtube.com (216.58.212.142)
Assessed on: Wed, 01 Mar 2017 20:48:35 UTC | Clear cache

Summary

Overall Rating
A

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/

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

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

Recommended Change

- 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

<table>
<thead>
<tr>
<th>Test</th>
<th>Pass</th>
<th>Score</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Security Policy</td>
<td>✓</td>
<td>0</td>
<td>Content Security Policy (CSP) implemented with unsafe sources inside <strong>style-src</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This includes <code>unsafe-inline</code>, <code>data:</code>, or overly broad sources such as https.</td>
</tr>
</tbody>
</table>
Results for **www.bundestag.de**

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

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/
Existing scanning services

useful for admins for ad-hoc scanning

predefined evaluation methodology
Goals of PrivacyScore

Create incentives for providers to improve security and privacy by publishing results as ranked benchmarks.

users can influence ranking

Released as open source, all results published as open data

USER-DEFINED SITE PROPERTIES

Do Bavarian cities perform better than schools in Hamburg?

Is size of a hospital correlated with its rank?
Screenshots
EDRi Members

Tags: privacy  data-protection  ngo

Author: @malexmave

EDRi members, as of July 2017

Results Overview

This list contains 36 websites (with 6 scan errors).

- 0 passed all checks
- 19 failed one or more checks
- 0 failed all tests in at least one group
- 11 failed at least one critical check
- 6 could not be judged due to missing data
<table>
<thead>
<tr>
<th>#</th>
<th>URL</th>
<th>Name</th>
<th>Location</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="https://www.openrightsgroup.org/">https://www.openrightsgroup.org/</a></td>
<td>Open Rights Group</td>
<td>UK</td>
<td>✔️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
</tr>
<tr>
<td>2</td>
<td><a href="https://www.itpol.dk/">https://www.itpol.dk/</a></td>
<td>ITPol Denmark</td>
<td>DK</td>
<td>✔️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
</tr>
<tr>
<td>3</td>
<td><a href="https://www.vrijschrift.org/">https://www.vrijschrift.org/</a></td>
<td>Vrijschrift</td>
<td>NL</td>
<td>✔️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
</tr>
<tr>
<td>4</td>
<td><a href="https://www.dfri.se/">https://www.dfri.se/</a></td>
<td>DFRI</td>
<td>SE</td>
<td>✔️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
</tr>
<tr>
<td>5</td>
<td><a href="https://netzfreiheit.org/">https://netzfreiheit.org/</a></td>
<td>Netzfreiheit</td>
<td>AT</td>
<td>✔️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
</tr>
<tr>
<td>6</td>
<td><a href="https://digitalcourage.de/">https://digitalcourage.de/</a></td>
<td>Digitalcourage</td>
<td>DE</td>
<td>✔️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
</tr>
<tr>
<td>7</td>
<td><a href="https://edri.org/">https://edri.org/</a></td>
<td>EDRi</td>
<td>International</td>
<td>✔️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
</tr>
<tr>
<td>8</td>
<td><a href="https://www.bof.nl/">https://www.bof.nl/</a></td>
<td>Bits of Freedom</td>
<td>NL</td>
<td>✔️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
<td>⚠️</td>
</tr>
<tr>
<td>Check if 3rd party embeds are being used</td>
<td>reliable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The site does not use any third parties.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check if embedded 3rd parties are known trackers</td>
<td>reliable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The site does not use any known tracking- or advertising companies.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determine how many cookies the website sets</td>
<td>reliable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The website itself is not setting any cookies.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determine how many cookies are set by third parties</td>
<td>reliable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No one else is setting any cookies.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check if Google Analytics is being used</td>
<td>reliable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The site does not use Google Analytics.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check if Google Analytics has the privacy extension enabled</td>
<td>reliable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not checking if Google Analytics data is being anonymized, as the site does not use Google Analytics.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Check whether web server is located in EU</td>
<td>unreliable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All web servers are located in United Kingdom.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A public scanning platform to assess privacy issues of websites