PRIVACYSCORE.ORG

Investigating security and privacy properties of related Web sites

Tobias Mueller
Universität Hamburg

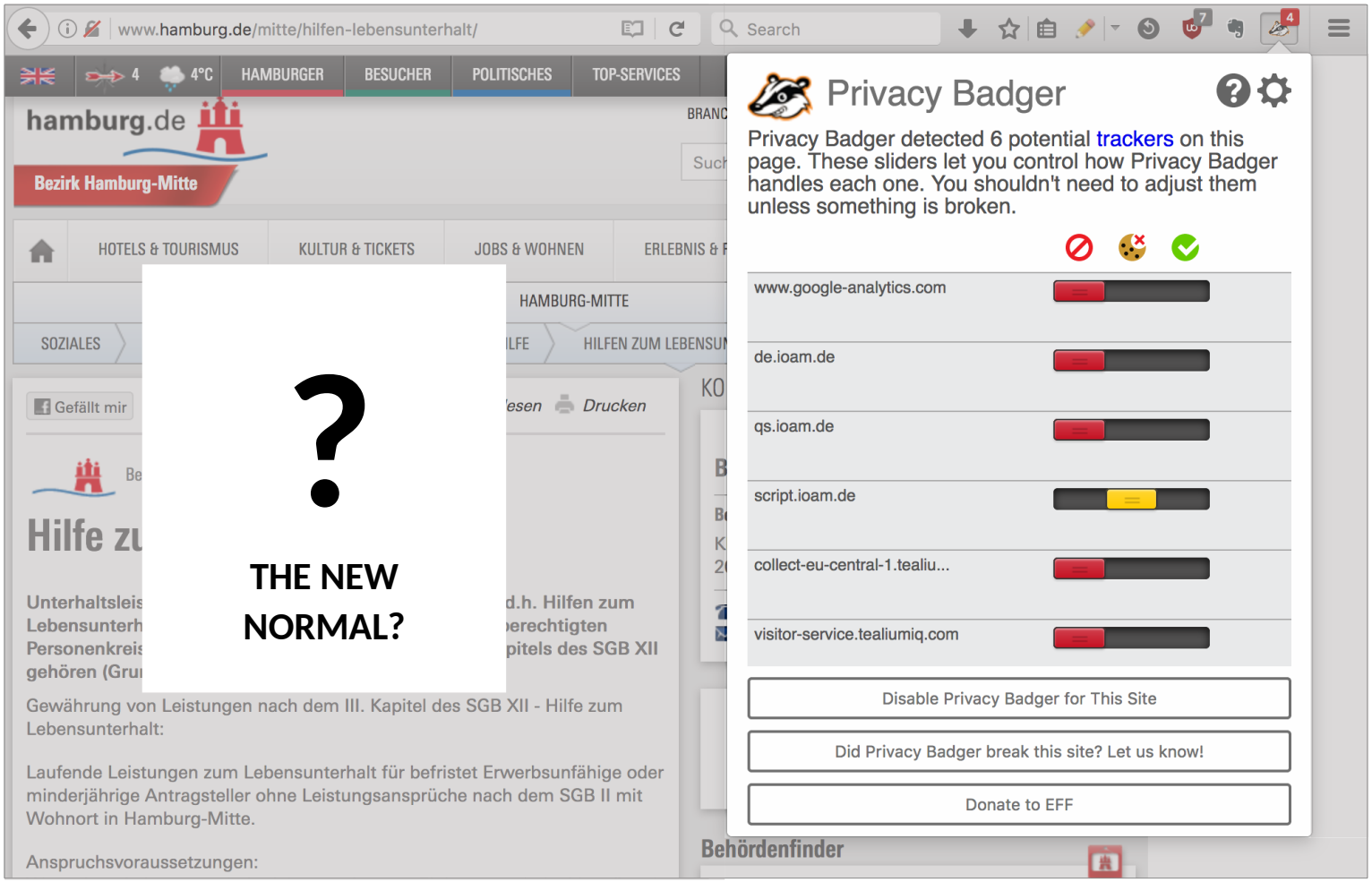
with Pascal Wichmann (Uni Hamburg) Max Maaß (TU Darmstadt) Henning Pridöhl (Uni Bamberg) und Dominik Herrmann (Uni Bamberg)

PRIVACYSCORE.ORG

Tobias Mueller
Universität Hamburg

Motivation

Who knows that I'm interested in social welfare?



Existing Scanning Services

focus on single sites

QUALYS® SSL LABS

Home Projects Qualys.com Contac

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

SSL Report: youtube.com (216.58.212.142)

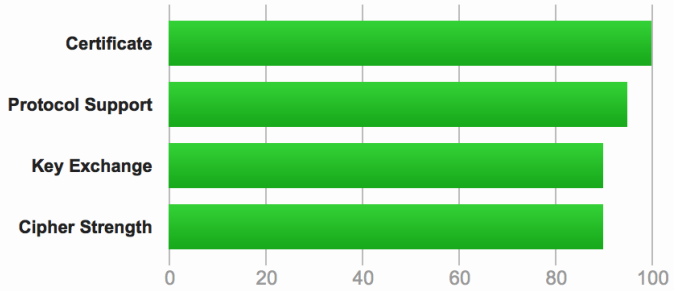
Assessed on: Wed, 01 Mar 2017 20:48:35 UTC | Clear cache

Scan Another

Summary

Overall Rating

A

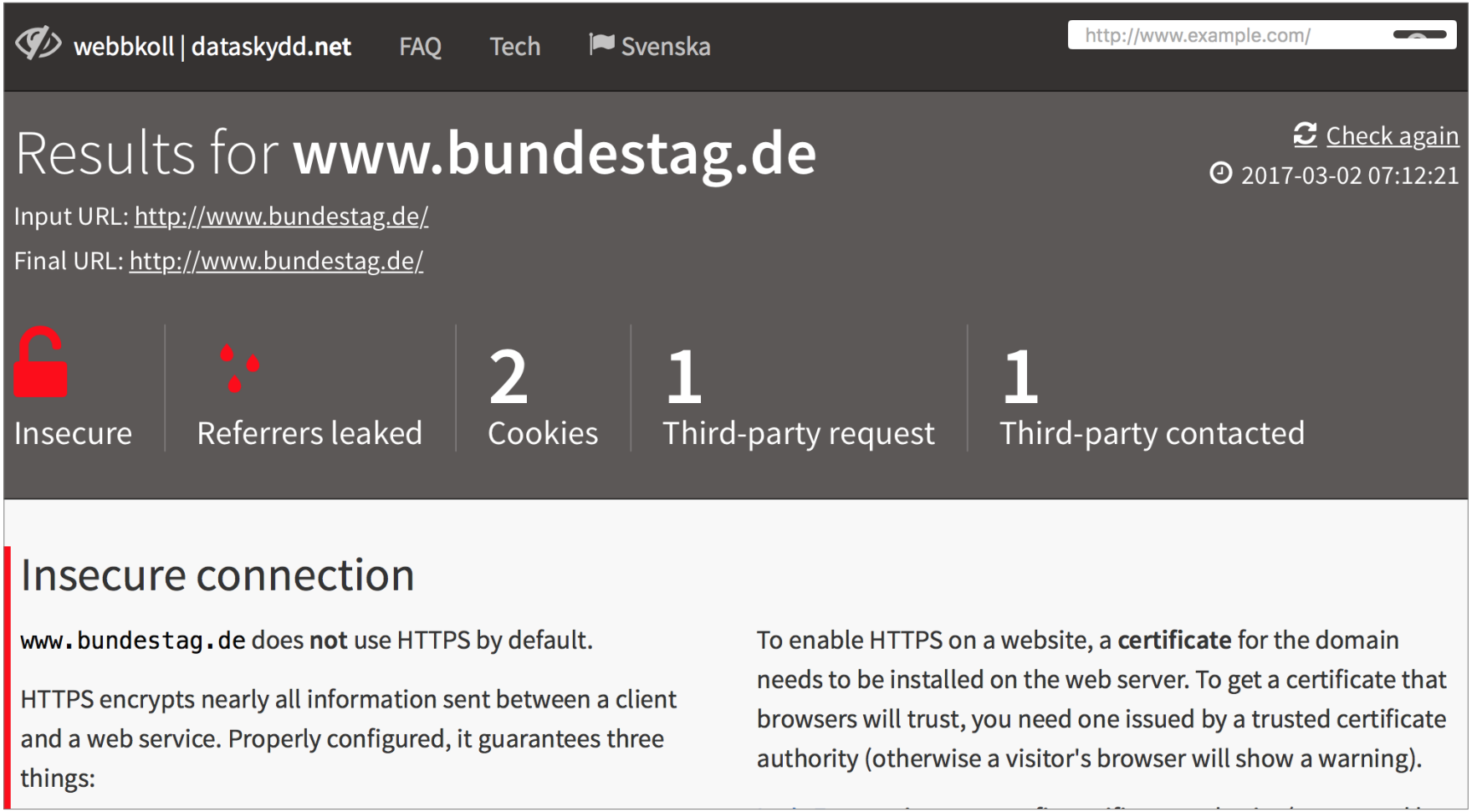


Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

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

https://www.ssllabs.com/ssltest/

https://observatory.mozilla.org/ – https://securityheaders.io/ – http://urlscan.io/

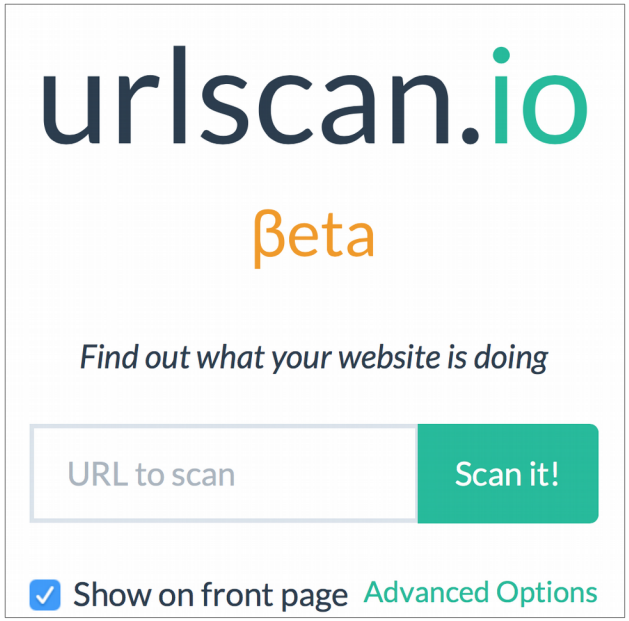


https://webbkoll.dataskydd.net/en/

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

Existing Scanning Services…

target Web site operators



use pre-defined ranking 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:

Idea: **public benchmarks** for **incentivising** operators to introduce privacy friendly enhancements.

The public can create **lists** with properties and **customise the ranking** (soon™).

Free Software (GPLv3+) und Open Data

Out of scope: Pentesting, SQLi, XSS, …

USER DEFINED ATTRIBUTES:

Are cities in the south better than Hamburg (in the north)?

Does the size of a hospital have an influence on the ranking of its Web site?

Are GNOME-based distros more privacy friendly than KDE-based ones?

Selected Lists

News Sites Popular in Germany

Active GNU, Linux, and BSD Distributions from Distrowatch

Projects with a stand at FOSDEM

Desktop Environments

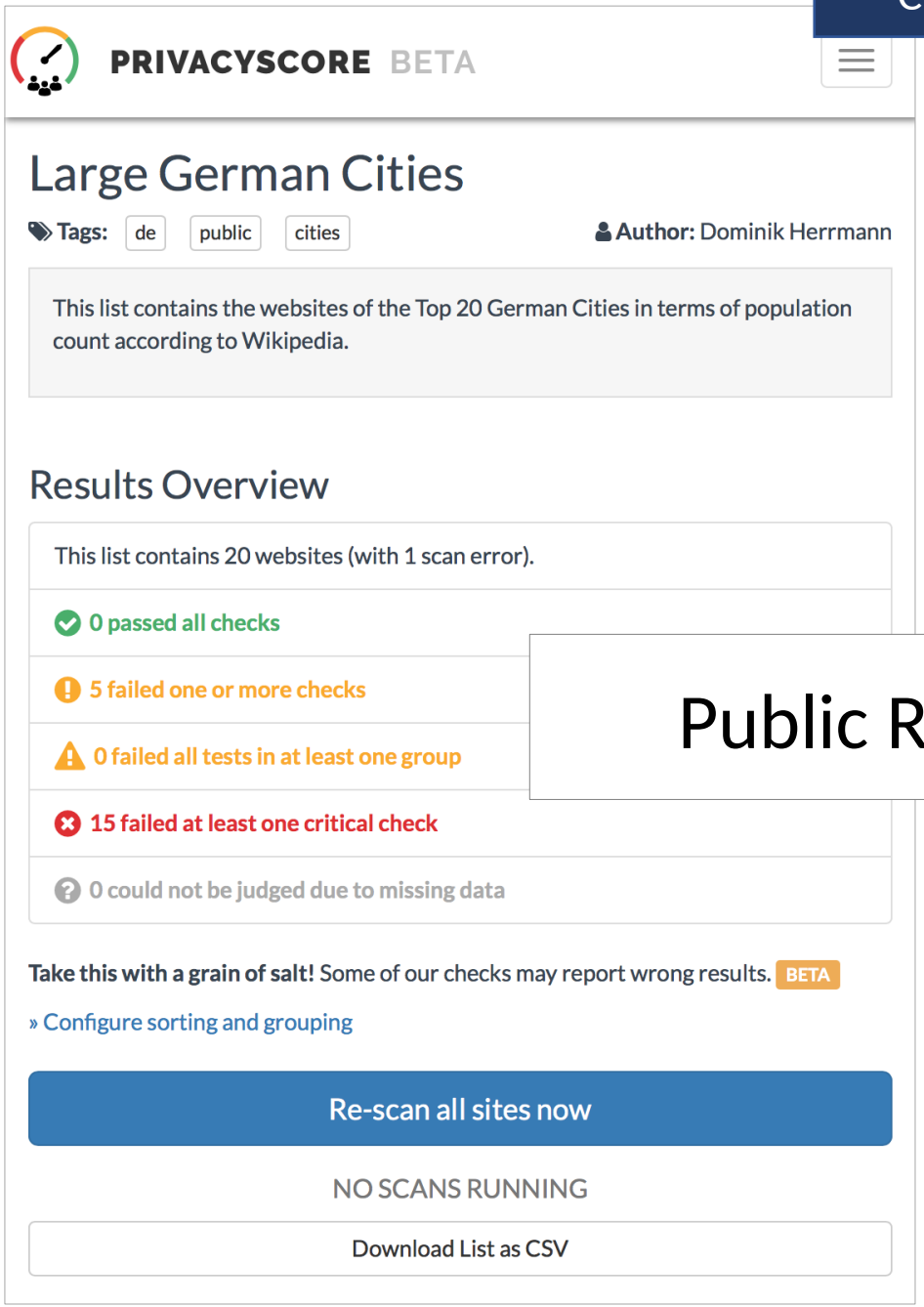
PRIVACYSCORE BETA

								LISTS	CODE	TEAM
1	http://xfce.org/ / 2018-01-25 @ 14:31:06	Xfce	1996	2015-02-28	C	GTK+	GPL, LGPL, BSD license	✓	!	!	!
2	http://lxqt.org/ / 2017-12-30 @ 03:31:11	LXQt	2014-05-07	2017-01-02	C, C++	Qt	GPL, LGPL	✓	!	!	!
3	http://trinitydesktop.org/ (1 failure) / 2017-12-30 @ 03:31:21	Trinity Desktop Environment (TDE)	2010-04-29	2016-11-07	C++	Qt	GPL (and other)	!	?	!	?
4	http://artemis-project.github.io/ / 2017-12-30 @ 03:24:23	Artemis	?	?	?	?	?	!	!	!	?
5	http://cinnamon-spices.linuxmint.com/ / 2017-12-30 @ 03:24:39	Cinnamon	2011	2017-07-02	C, JavaScript, Python	GTK+	GPL	!	!	!	?
6	http://lxde.org/ / 2017-12-30 @ 03:30:34	LXDE (Lightweight X11 Desktop Environment)	2006	2016-02-20	C	GTK+	GPL, LGPL	!	!	!	?

Performed Checks

No Tracking	Encryption to Website	Encryption to Mailserver	Protection Against Other Attacks
Third Parties Known Trackers Server Locations	HTTPS/STARTTLS available? Certificate: validity / key size Insecure protocols: SSLv3… Known vulnerabilities: Heartbleed…		Information leak Referer-Policy Security-Header
	HSTS HPKP HTTPS redirection		

Ranking und Detailed Results



Change order

Public Ranking

		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/	!	!	!	✗	✗
		!	!	!	✗	✗
		!	✗	!	?	✗
		!	✗	!	?	✗
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/	!	✗	!	!	✗

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 E
All web servers are located in Germany.

Check whether mail server is located in E
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.

vents the browser from disclosing the URL of the . Without a referrer policy most browsers send a ontent is retrieved from third parties or when you king on a link. This may disclose sensitive informa-

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).

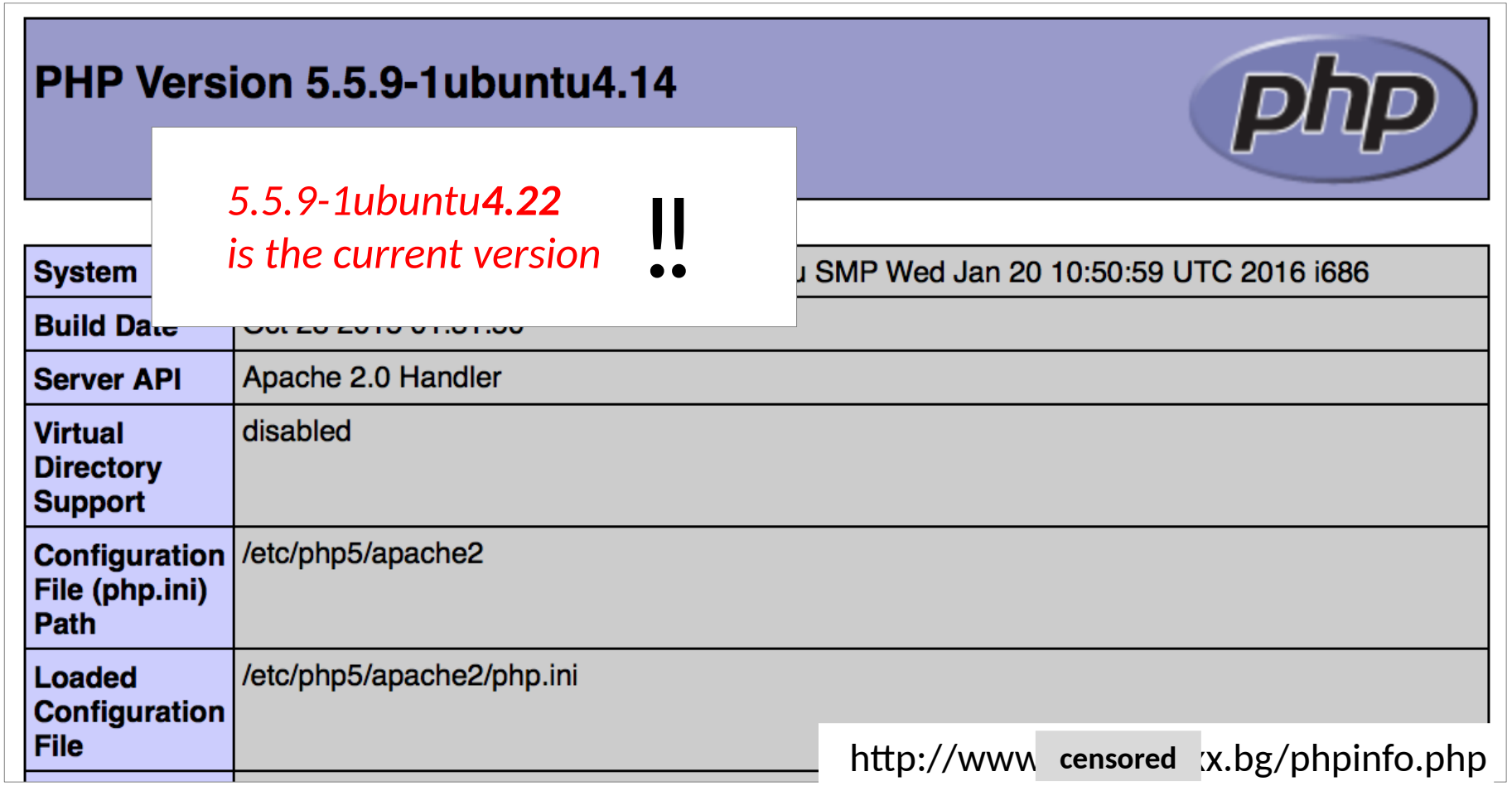
Potential scan errors: We may miss security problems on sites that redirect multiple times. We may also miss security problems on sites that issue multi-

Detailed Results

Typical information leaks

phpinfo.php *test.php* *backup.sql* *server-info* *server-status*

.git *.svn* *server.key* *<domain>.key* ...



phpinfo.php *test.php* *backup.sql* *server-info* *server-status*

.git *.svn* *server.key* *<domain>.key* ...

First complaint in November 2017.

Legal implications

Are we allowed to scan without permission?

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

TL;DR: yes

Ethical implications

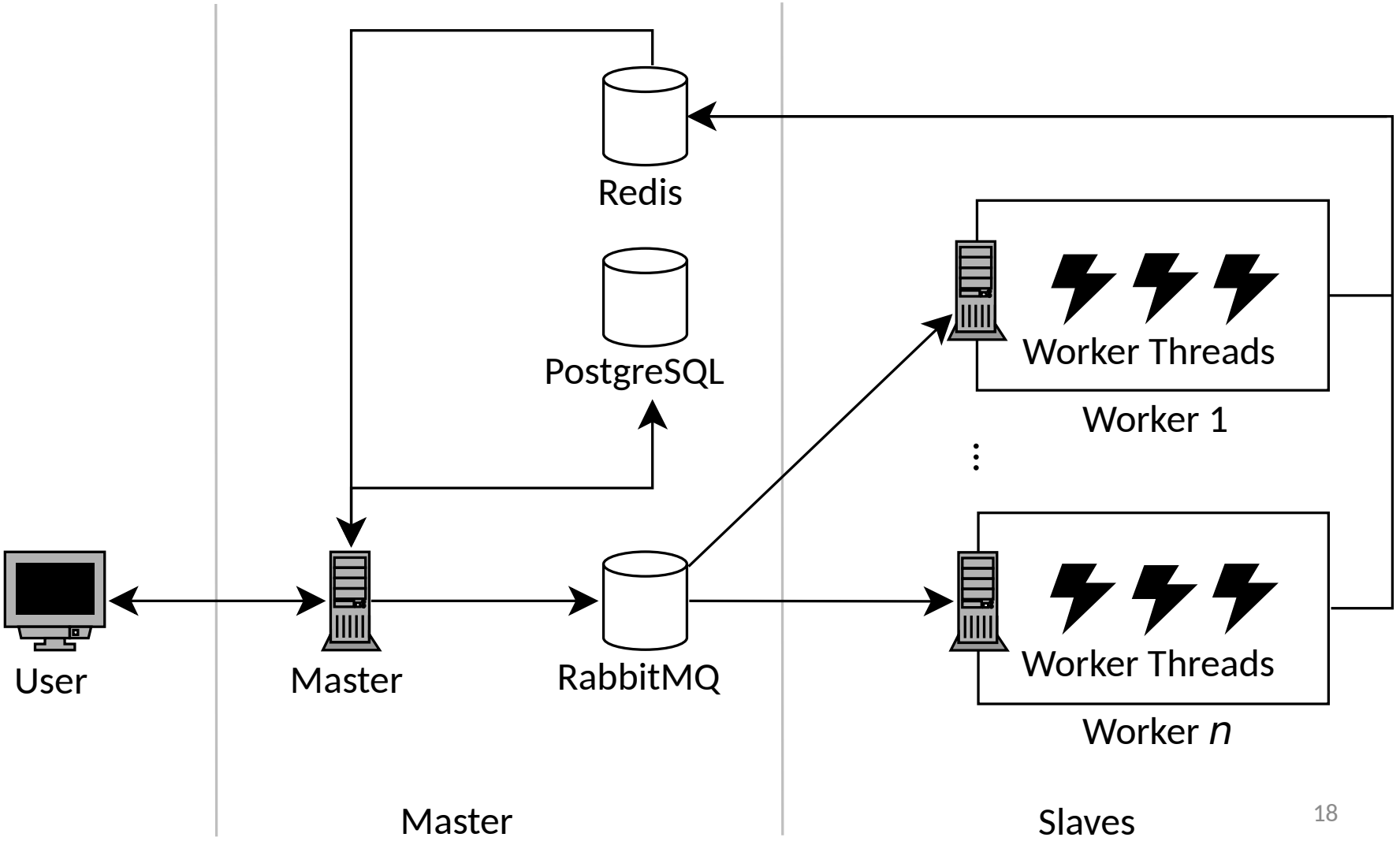
PrivacyScore is a Dual-Use-Tool.

- Certain results are **harder to acquire**
- **Rate limiting** as DoS protection
- **Blacklisting** on demand

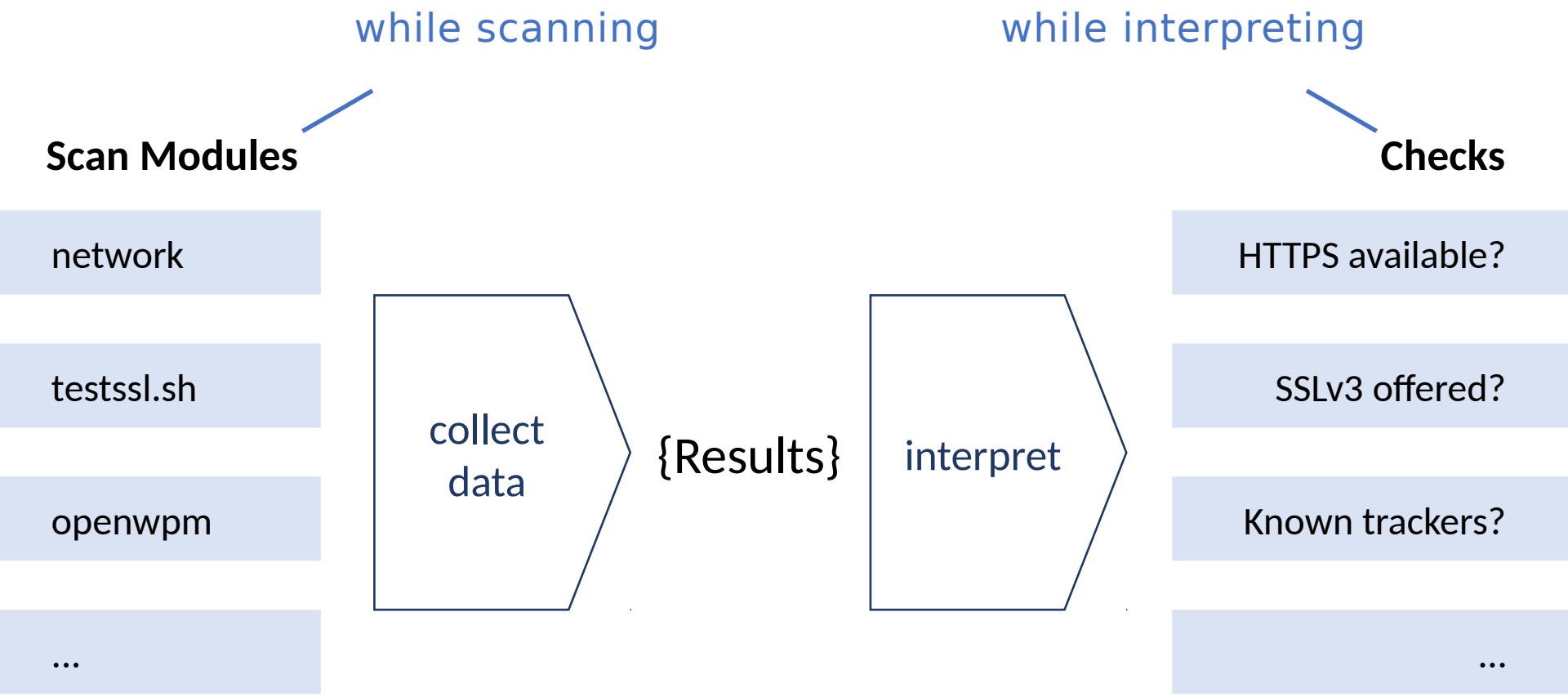
Technical Details

Distributed infrastructure of virtual machines

(currently approx. 30 VMs)



Scan Modules and Checks



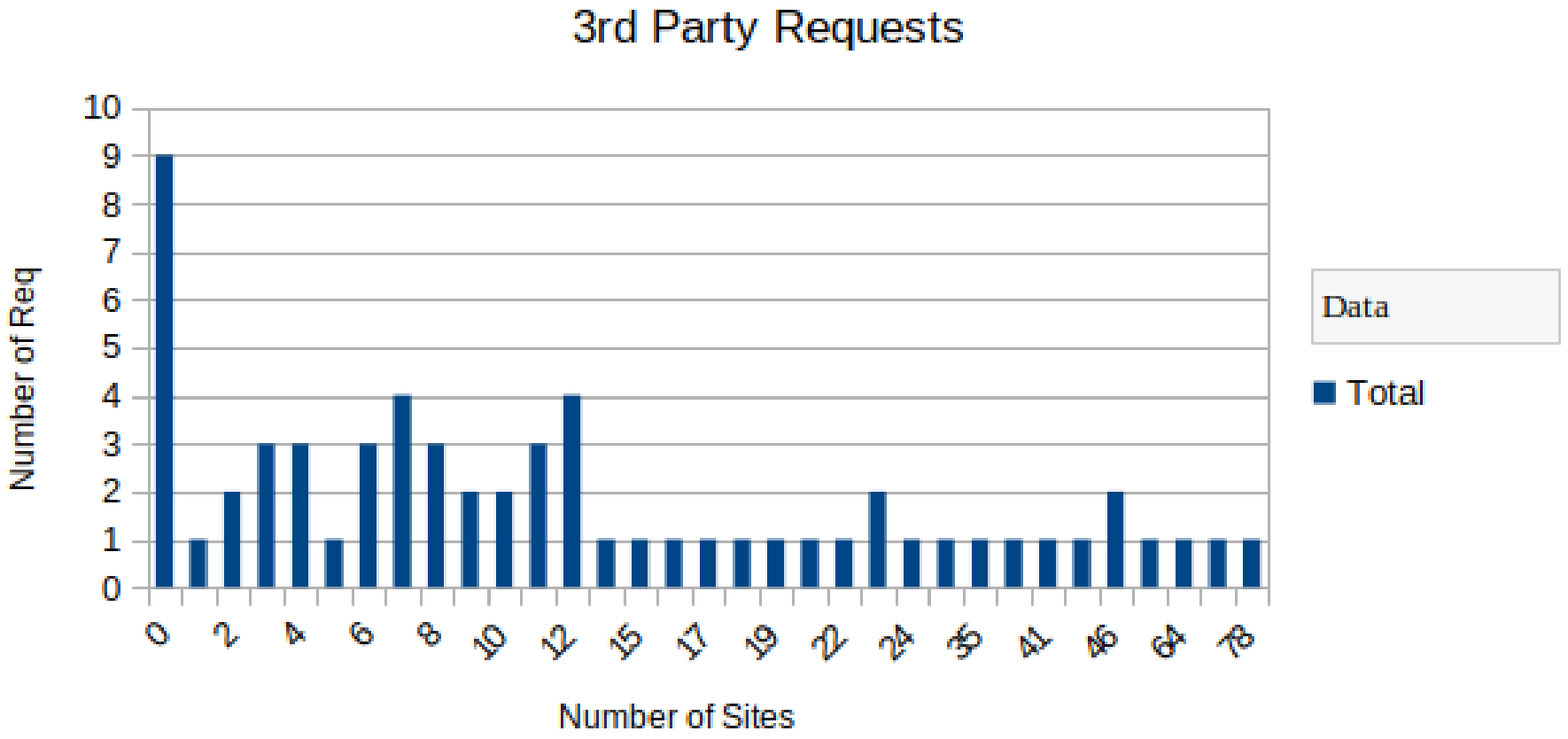
openwpm: Firefox ESR + Selenium

Stats

URL	3rd P Req	3rd P C	Trackers
https://eclipse.org/	78	1	0
https://www.libreoffice.org/	75	1	0
https://www.oreilly.com/	64	11	5
https://www.python-fosdem.org/	48	0	0
https://training.linuxfoundation.org/free-linux-training/	46	9	4
https://grafana.com/grafana	46	3	0
https://summerofcode.withgoogle.com/	45	4	1
https://www.owasp.org/index.php/Main_Page	41	4	1
https://www.openstack.org/	39	12	5

URL	3rd P Req	3rd P C	Trackers
https://www.openstack.org/	39	12	5
https://www.oreilly.com/	64	11	5
https://training.linuxfoundation.org/free-linux-training/	46	9	4
https://xenproject.org/	23	8	2
https://summerofcode.withgoogle.com/	45	4	1
https://www.owasp.org/index.php/Main_Page	41	4	1
https://www.automotivelinux.org/	26	4	1
https://grafana.com/grafana	46	3	0
https://micropython.org/	19	3	1

Median	9.5
Mean	15.69
Variance	331.92
Standard Deviation	18.21



PrivacyScore.org: Surveying security and privacy properties of Web sites

BETA

TODOs

Edit lists, private lists, user management, …

Ranking templates, usable interpretations,

OCSP, OCSP stapling, browser fingerprinting, webapp versions

Abuse handling, containment, …

Send lists **Send bugs** **Send ideas!** **Send patches!!1**

mueller@informatik.uni-hamburg.de

Follow us @privascore