SSL-Verschlüsselung und Security-Header

Eine einfache und schnelle Kombination für mehr mobile Benutzersicherheit

Yuri Samoilov - https://www.flickr.com/photos/110751683@N02/13334048894/

Über mich

- Jan Erik Zassenhaus
- 25
- J!German-Gründer

- Joomla!-Security-Gründer

- IT-Sicherheitsbeauftragter bei Mittwald

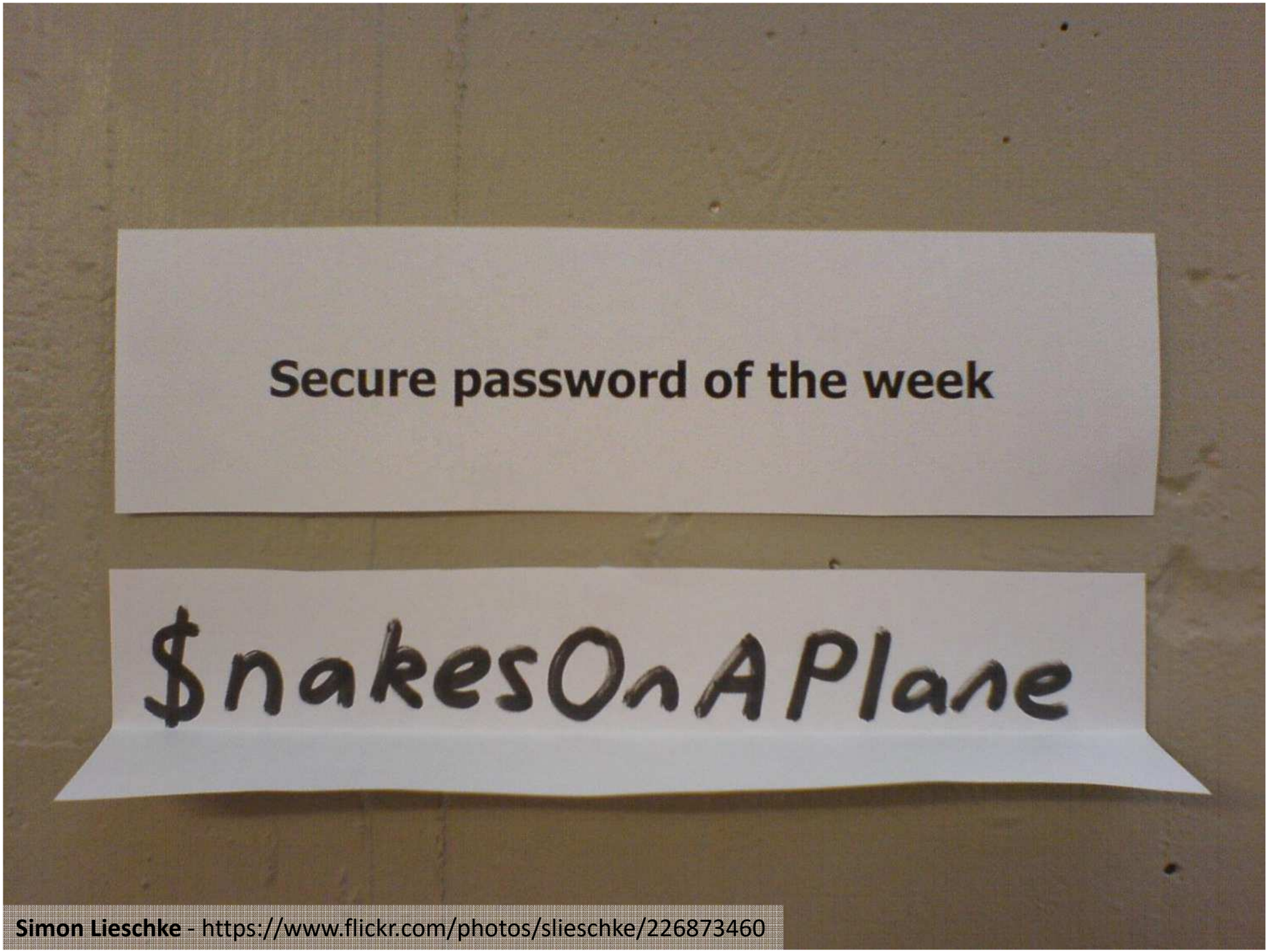
Verschlüsselung?

Brett Neilson - https://www.flickr.com/photos/brettneilson/5770214350

nolifebeforecoffee - https://www.flickr.com/photos/nolifebeforecoffee/124659356

NEIN!

Schutz der Übertragung



Simon Lieschke - https://www.flickr.com/photos/slieschke/226873460

401 (K) 2012 - https://www.flickr.com/photos/68751915@N05/6870876951

Michelangelo Carrieri - https://www.flickr.com/photos/malakhkelevra/4951863053

Zertifikate

Official U.S. Navy Page - https://www.flickr.com/photos/usnavy/5511838861

Zertifikatstypen

Paul Hocksenar - https://www.flickr.com/photos/verminc/2335148856

Selbstsigniert

```
$ openssl genrsa -out ca.key 2048
Generating RSA private key, 2048 bit long modulus
.....................................................................
.....+++
.....................................+++
e is 65537 (0x10001)
$
$ openssl req -new -key ca.key -out ca.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BD
State or Province Name (full name) [Some-State]:Dhaka
Locality Name (eg, city) []:Gulshan
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC Inc.
Organizational Unit Name (eg, section) []:NetworkServices
Common Name (e.g. server FQDN or YOUR name) []:hostname-of-the-server
Email Address []:email@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
$
```

Linux Screenshots - https://www.flickr.com/photos/xmodulo/13595105125

Dieser Verbindung wird nicht vertraut

Sie haben Firefox angewiesen, eine gesicherte Verbindung zu [redacted] aufzubauen, es kann aber nicht überprüft werden, ob die Verbindung sicher ist.

Wenn Sie normalerweise eine gesicherte Verbindung aufbauen, weist sich die Website mit einer vertrauenswürdigen Identifikation aus, um zu garantieren, dass Sie die richtige Website besuchen. Die Identifikation dieser Website dagegen kann nicht bestätigt werden.

Was sollte ich tun?

Falls Sie für gewöhnlich keine Probleme mit dieser Website haben, könnte dieser Fehler bedeuten, dass jemand die Website fälscht. Sie sollten in dem Fall nicht fortfahren.

Diese Seite verlassen

Technische Details

[redacted] verwendet ein ungültiges Sicherheitszertifikat.

Dem Zertifikat wird nicht vertraut, weil es vom Aussteller selbst signiert wurde.
Das Zertifikat gilt nur für Jan Erik Zassenhaus.

(Fehlercode: sec_error_unknown_issuer)

Ich kenne das Risiko

Wenn Sie wissen, warum dieses Problem auftritt, können Sie Firefox anweisen, der Identifikation dieser Website zu vertrauen. **Selbst wenn Sie der Website vertrauen, kann dieser Fehler bedeuten, dass jemand Ihre Verbindung manipuliert.**

Fügen Sie keine Ausnahme hinzu, außer Sie wissen, dass es einen guten Grund dafür gibt, warum diese Website keine vertrauenswürdige Identifikation verwendet.

Ausnahmen hinzufügen…

Ihre Verbindung ist nicht privat

Angreifer könnten versuchen, Ihre Informationen von [redacted] zu stehlen, z. B. Passwörter, Nachrichten oder Kreditkartendaten.

Erweiterte Informationen ausblenden

Zurück zu sicherer Website

Sie haben versucht, auf [redacted] zuzugreifen, der Server hat sich jedoch mit einem Zertifikat ausgewiesen, das von einem Aussteller herausgegeben wurde, dem das Betriebssystem des Computers nicht vertraut. Dies bedeutet möglicherweise, dass der Server seine eigenen Sicherheitsinformationen erzeugt hat, auf die Chrome als Identitätsangabe nicht vertrauen kann, oder dass ein Hacker versucht, Ihre Kommunikation abzufangen.

Weiter zu [redacted] (unsicher)

Es besteht ein Problem mit dem Sicherheitszertifikat der Website.

Das Sicherheitszertifikat dieser Website wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt.
Das Sicherheitszertifikat dieser Website wurde für eine andere Adresse der Website ausgestellt.

Die Sicherheitszertifikatprobleme deuten eventuell auf den Versuch hin, Sie auszutricksen bzw. Daten die Sie an den Server gesendet haben abzufangen.

Es wird empfohlen, dass Sie die Webseite schließen und nicht zu dieser Website wechseln.

 Klicken Sie hier, um diese Webseite zu schließen.

 Laden dieser Website fortsetzen (nicht empfohlen).

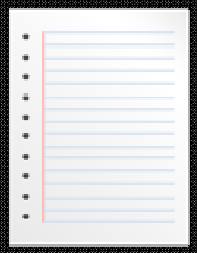
 Weitere Informationen

- Wenn Sie zu dieser durch einen Link weitergeleitet wurden, dann überprüfen Sie die Websiteadresse in der Adressleiste, um sicherzustellen, dass dies die erwartete Adresse ist.
- Wenn Sie zu Websites wie https://example.com wechseln, versuchen Sie "www" zu der Adresse hinzuzufügen (https://www.example.com).

Weitere Informationen erhalten Sie unter "Zertifikatfehler" in der Internet Explorer-Hilfe.


Ungültiges Zertifikat
Aufgrund eines Zertifikatproblems kann Opera nicht die Identität des Servers [redacted] überprüfen. Der Server könnte versuchen, Sie zu betrügen. Möchten Sie trotzdem noch den Server aufsuchen?
Zertifikat anzeigen
Trotzdem fortfahren
Abbrechen

Domainvalidiert



Datei

- admin@domain.de
- administrator@domain.de
- hostmaster@domain.de
- webmaster@domain.de
- postmaster@domain.de
- admin@www.domain.de
- administrator@www.domain.de
- hostmaster@www.domain.de
- webmaster@www.domain.de
- postmaster@www.domain.de

DNS-Änderung
(CNAME)

Unternehmensvalidiert

E-Mail

Adresse

Handelsregister o. ä.

WHOIS-Abfrage

Erweiterte Validierung

E-Mail

Adresse

Handelsregister o. ä.

WHOIS-Abfrage

Anruf

Strenge Validierung

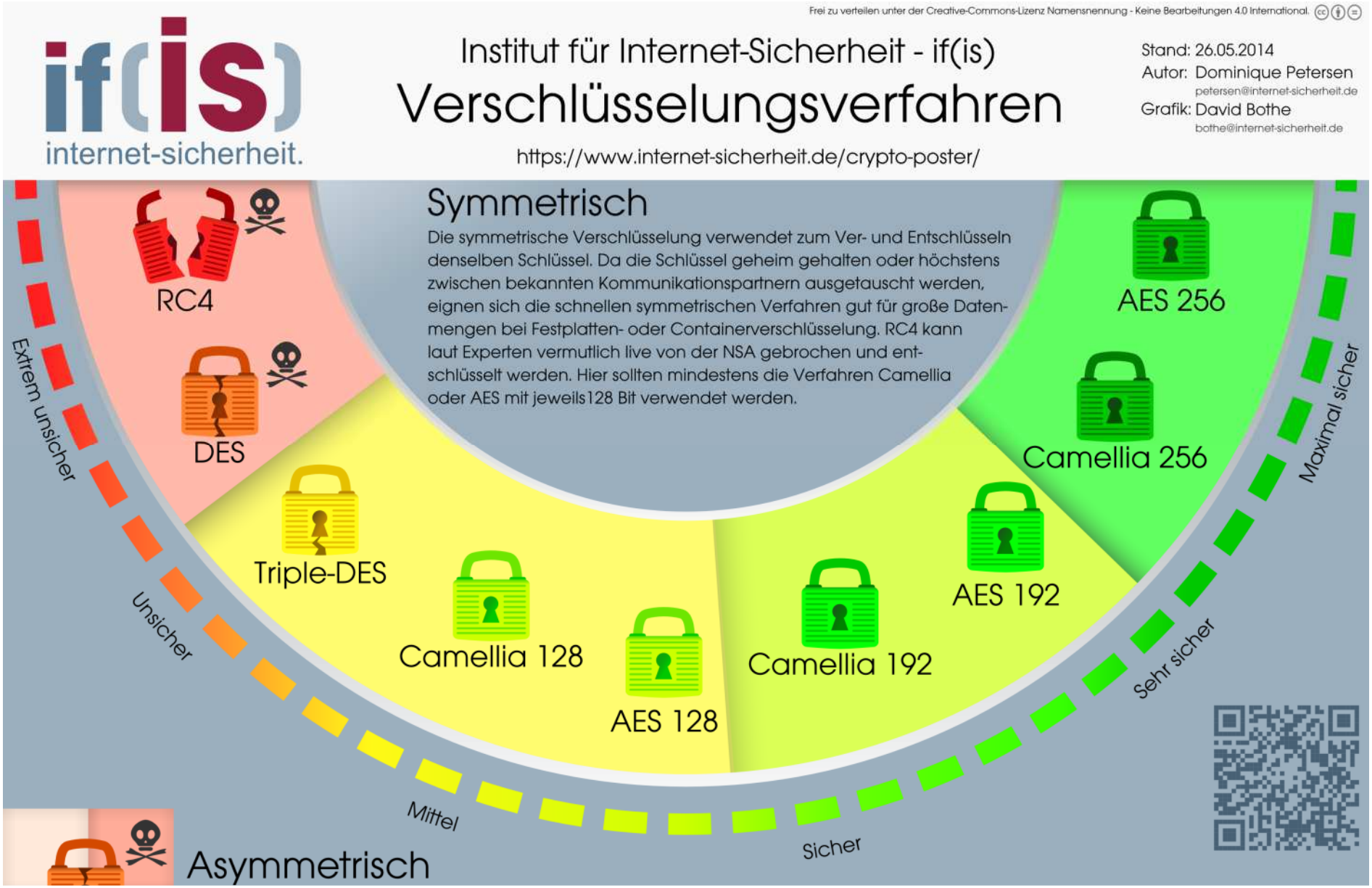
Validierungsübersicht

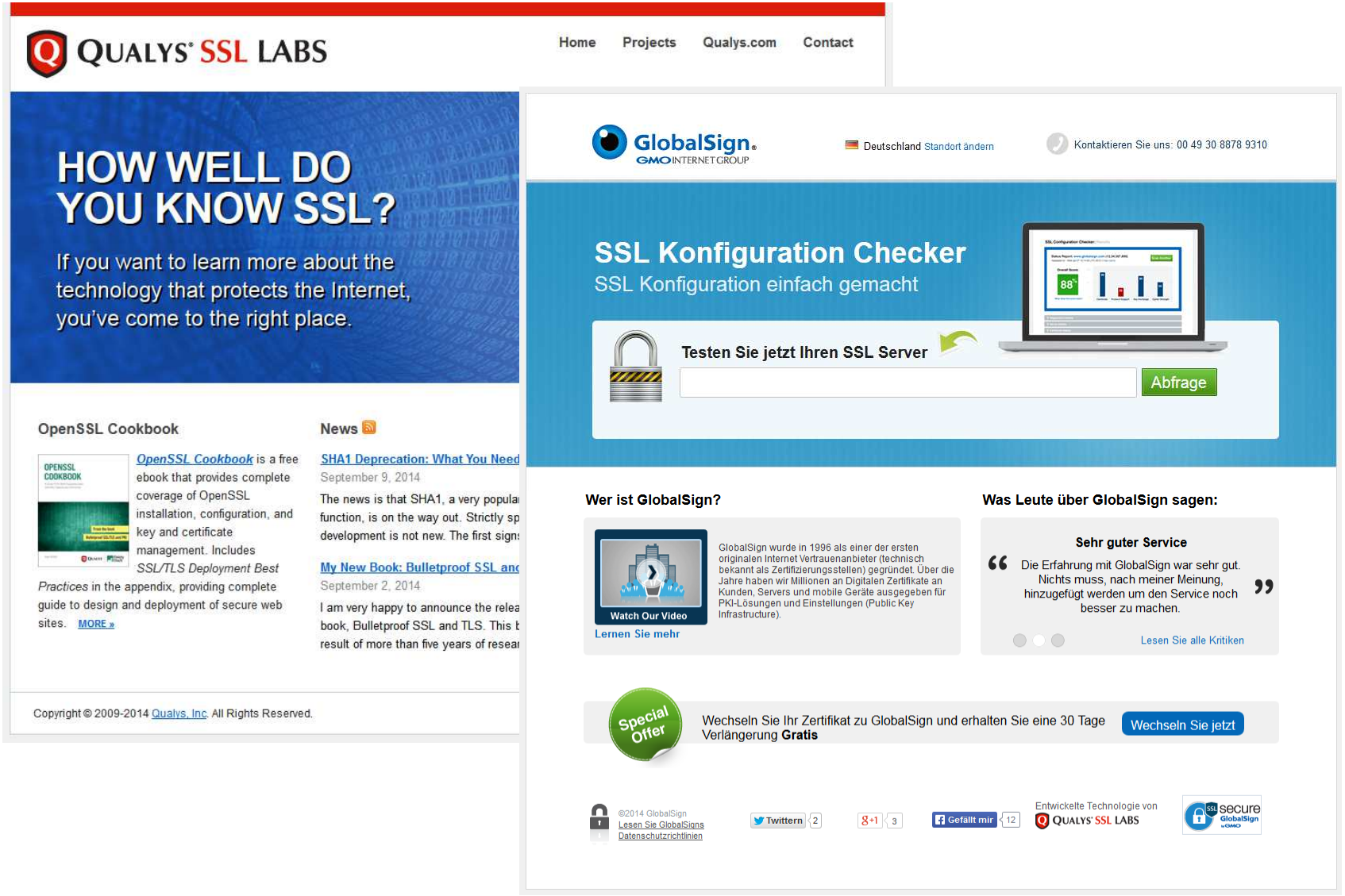
Selbstsigniert		***unbegrenzt***	**0,- €**
Domainvalidiert		**max. 4 Jahre**	**27,- €**
Unternehmensvalidiert		**max. 4 Jahre**	**94,- €**
Erweiterte Validierung		**max. 2 Jahre**	**199,- €**

Verschlüsselungsstärke

Lin Mei - https://www.flickr.com/photos/leomei/2651904068

Cipher


Frei zu verteilen unter der Creative-Commons-Lizenz Namensnennung - Keine Bearbeitungen 4.0 International.
if(is)
internet-sicherheit.
Institut für Internet-Sicherheit - if(is)
Verschlüsselungsverfahren
https://www.internet-sicherheit.de/crypto-poster/
Stand: 26.05.2014
Autor: Dominique Petersen
petersen@internet-sicherheit.de
Grafik: David Bothe
bothe@internet-sicherheit.de
Symmetrisch
Die symmetrische Verschlüsselung verwendet zum Ver- und Entschlüsseln denselben Schlüssel. Da die Schlüssel geheim gehalten oder höchstens zwischen bekannten Kommunikationspartnern ausgetauscht werden, eignen sich die schnellen symmetrischen Verfahren gut für große Datenmengen bei Festplatten- oder Containerverschlüsselung. RC4 kann laut Experten vermutlich live von der NSA gebrochen und entschlüsselt werden. Hier sollten mindestens die Verfahren Camellia oder AES mit jeweils128 Bit verwendet werden.
RC4
DES
Triple-DES
Camellia 128
AES 128
Camellia 192
AES 192
Camellia 256
AES 256
Extrem unsicher
Unsicher
Mittel
Sicher
Sehr sicher
Maximal sicher
Asymmetrisch


QUALYS SSL LABS
Home
Projects
Qualys.com
Contact
HOW WELL DO YOU KNOW SSL?
If you want to learn more about the technology that protects the Internet, you've come to the right place.
OpenSSL Cookbook
OpenSSL Cookbook is a free ebook that provides complete coverage of OpenSSL installation, configuration, and key and certificate management. Includes SSL/TLS Deployment Best Practices in the appendix, providing complete guide to design and deployment of secure web sites. MORE »
News
SHA1 Deprecation: What You Need
September 9, 2014
The news is that SHA1, a very popular function, is on the way out. Strictly speaking development is not new. The first signs
My New Book: Bulletproof SSL and
September 2, 2014
I am very happy to announce the release book, Bulletproof SSL and TLS. This b result of more than five years of resear
Copyright © 2009-2014 Qualys, Inc. All Rights Reserved.
GlobalSign
GMO INTERNET GROUP
Deutschland Standort ändern
Kontaktieren Sie uns: 00 49 30 8878 9310
SSL Konfiguration Checker
SSL Konfiguration einfach gemacht
Testen Sie jetzt Ihren SSL Server
Abfrage
Wer ist GlobalSign?
Watch Our Video
Lernen Sie mehr
GlobalSign wurde in 1996 als einer der ersten originalen Internet Vertrauenanbieter (technisch bekannt als Zertifizierungsstellen) gegründet. Über die Jahre haben wir Millionen an Digitalen Zertifikate an Kunden, Servers und mobile Geräte ausgegeben für PKI-Lösungen und Einstellungen (Public Key Infrastructure).
Was Leute über GlobalSign sagen:
Sehr guter Service
Die Erfahrung mit GlobalSign war sehr gut. Nichts muss, nach meiner Meinung, hinzugefügt werden um den Service noch besser zu machen.
Lesen Sie alle Kritiken
Special Offer
Wechseln Sie Ihr Zertifikat zu GlobalSign und erhalten Sie eine 30 Tage Verlängerung Gratis
Wechseln Sie jetzt
©2014 GlobalSign
Lesen Sie GlobalSigns Datenschutzrichtlinien
Twittern 2
+1 3
Gefällt mir 12
Entwickelte Technologie von QUALYS SSL LABS
secure GlobalSign

SSL testen

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > google.de > 74.125.239.119

SSL Report: google.de (74.125.239.119)

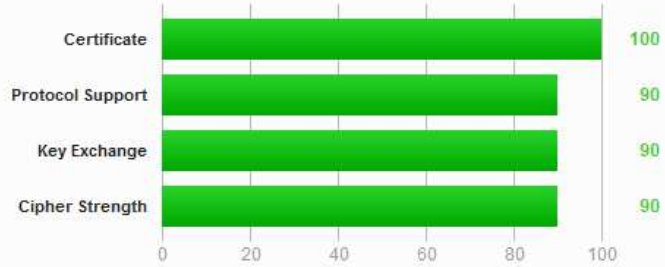
Assessed on: Wed Sep 10 11:48:30 UTC 2014 | HIDDEN | Clear cache

Scan Another »

Summary

Overall Rating

A



Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, OpenSSL Cookbook and known issues.

This server is not vulnerable to the Heartbleed attack.

Experimental: This server is not vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224).

Authentication

Server Key and Certificate #1

Common names	www.google.de
Alternative names	www.google.de
Prefix handling	Not valid for "google.de" CONFUSING
Valid from	Wed Aug 27 11:10:49 UTC 2014
Valid until	Tue Nov 25 00:00:00 UTC 2014 (expires in 2 months and 15 days)
Key	RSA 2048 bits

GlobalSign
GMO INTERNET GROUP

Deutschland Standort ändern

Home > Ergebnisse abfragen > Ihre Auswertung

SSL Konfiguration Checker: Ihre Auswertung

Scannen

Die Auswertung:

Stufe **A**

Was bedeutet diese Auswertung ?

Entwickelte Technologie von QUALYS SSL LABS

www.google.de (74.125.239.119)

Bewertet am 10.9.2014 13:44:23

Zwischenspeicher leeren

[X]

Wiederaufnahme der Sitzung auf dem Server is nicht aktiviert

Der Benutzer kann langsame Leistungen erleben

Wie kann ich dieses Problem beheben?

[X]

Der Server hat den HTTP Strict-Transport-Security nicht aktiviert

Benutzer könnten durch Man-in-the-middle Attacken belichtet werden

Wie kann ich dieses Problem beheben?

Security-Header

417

Expectation Failed

Tomomi - https://www.flickr.com/photos/girliemac/6508023679

Strict-Transport-Security

Header always set Strict-Transport-Security

"max-age=31536000"

"max-age=31536000; includeSubDomains"

Ihre Verbindung ist nicht privat

Angreifer könnten versuchen, Ihre Informationen von **www.google.de** zu stehlen, z. B. Passwörter, Nachrichten oder Kreditkartendaten.

Erweiterte Informationen ausblenden

Neu laden

www.google.de schützt Ihre Informationen in der Regel durch Verschlüsselung. Als Chrome dieses Mal versuchte, eine Verbindung zu www.google.de herzustellen, gab die Website ungewöhnliche und falsche Anmeldedaten zurück. Entweder versucht ein Angreifer, sich als www.google.de auszugeben, oder die Verbindung wurde durch eine WLAN-Anmeldeseite unterbrochen. Da Chrome die Verbindung vor dem Austausch von Daten unterbrochen hat, sind Ihre Informationen weiterhin sicher.

www.google.de kann zurzeit nicht aufgerufen werden, da die Website HSTS verwendet. Netzwerkfehler und Angriffe sind in der Regel nur vorübergehend, sodass die Seite wahrscheinlich später wieder funktioniert.

NET::ERR_CERT_COMMON_NAME_INVALID

Dieser Verbindung wird nicht vertraut

Sie haben Firefox angewiesen, eine gesicherte Verbindung zu **www.paypal.com** aufzubauen, es kann aber nicht überprüft werden, ob die Verbindung sicher ist.

Wenn Sie normalerweise eine gesicherte Verbindung aufbauen, weist sich die Website mit einer vertrauenswürdigen Identifikation aus, um zu garantieren, dass Sie die richtige Website besuchen. Die Identifikation dieser Website dagegen kann nicht bestätigt werden.

Was sollte ich tun?

Falls Sie für gewöhnlich keine Probleme mit dieser Website haben, könnte dieser Fehler bedeuten, dass jemand die Website fälscht. Sie sollten in dem Fall nicht fortfahren.

Diese Seite verlassen

Technische Details

www.paypal.com verwendet ein ungültiges Sicherheitszertifikat.

Das Zertifikat gilt nur für folgende Namen:
www.ssllabs.com, ssllabs.com

(Fehlercode: ssl_error_bad_cert_domain)

Header always set X-Frame-Options

"deny" oder "sameorigin"

X-Frame-Options

Response Header

https://webmail.mittwald.de/

```
Date: Wed, 10 Sep 2014 16:06:14 GMT
Server: HTTPD
Expires: -1
x-dns-prefetch-control: off
Cache-Control: no-cache, no-store, must-revalidate, pre-check=0, post-check=0, max-age=0
Pragma: no-cache
X-Frame-Options: sameorigin
Strict-Transport-Security: max-age=31536000
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Permitted-Cross-Domain-Policies: master-only
Last-Modified: Wed, 10 Sep 2014 16:06:14 GMT
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1800
Keep-Alive: timeout=5, max=93
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

200 OK
```

Security Headers for https://webmail.mittwald.de

Using user-agent for Chrome 30.0-MacOSX

Result	Category	Name	Actual Value	Our Recommendation	Show All Details
✔ Correct	Framing	X-Frame-Options	sameorigin	Use 'sameorigin'	Details
⚠ Warning	Transport	Strict-Transport-Security	max-age=31536000	Use 'max-age=31536000; includeSubDomains'	Details
✔ Correct	Content	X-Content-Type-Options	nosniff	Use 'nosniff'	Details
✔ Correct	Content	Content-Type	text/html; charset=UTF-8	Use 'text/html;charset=utf-8'	Details
✔ Correct	XSS	X-XSS-Protection	1; mode=block	Use '1; mode=block'	Details
✔ Correct	Cookies	Set-Cookie	L3u2AFeWA_L0TAE8e8TW...=/; secure; HttpOnly	Use 'secure; httponly;'	Details
✔ Correct	Caching	Cache-Control	no-cache, no-store, ...t-check=0, max-age=0	Use 'no-cache, no-store, must-revalidate'	Details
✔ Correct	Caching	Pragma	no-cache	Use 'no-cache'	Details
✔ Correct	Caching	Expires	-1	Use '-1'	Details
✔ Correct	Access Control	X-Permitted-Cross-Domain-Policies	master-only	Use 'master-only'	Details
⚠ Missing	Content Security Policy	Content-Security-Policy		Try Content-Security-Policy-Report-Only to start. Include default-src 'self', avoid 'unsafe-inline' and 'unsafe-eval'	Details

Other Headers

Name	Value
Date	Wed, 10 Sep 2014 16:09:32 GMT
X-DNS-Prefetch-Control	off
Connection	Keep-Alive
Last-Modified	Wed, 10 Sep 2014 16:09:32 GMT
Keep-Alive	timeout=5, max=100
Vary	Accept-Encoding
Server	HTTPD

Dennis Skley - https://www.flickr.com/photos/dskley/13796815083

Bettina Braun - https://www.flickr.com/photos/bettina-braun/277386361