Einfach Sicherer?


@MacLemon

0x59


bettercrypto·org

Überwachung

Spionage

Industriespionage

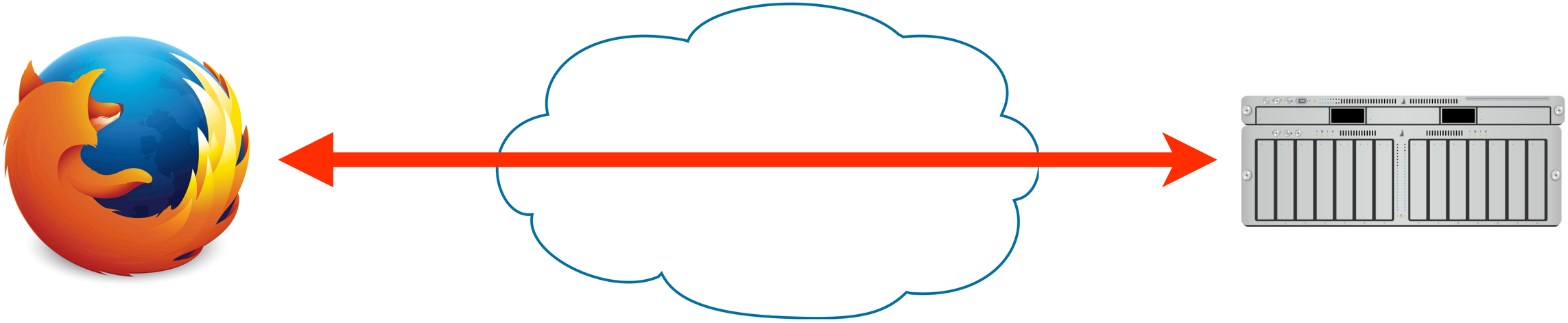
Alle sind betroffen

Webseiten

Webseiten

Webseiten

http

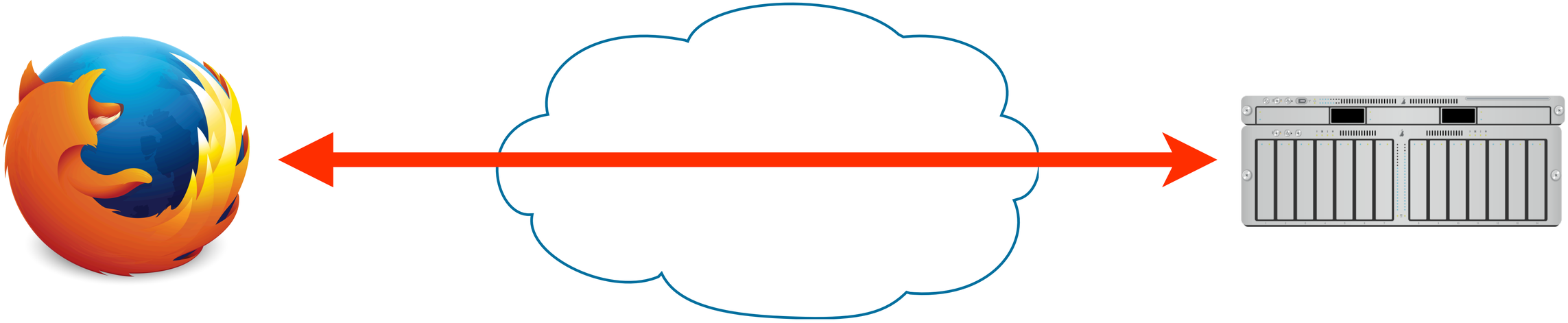


WLAN

Internet Provider

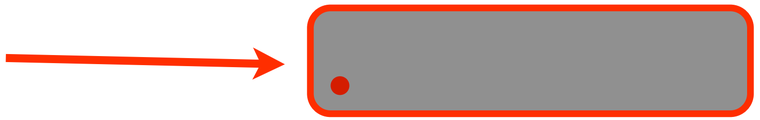
Mobilfunkbetreiber

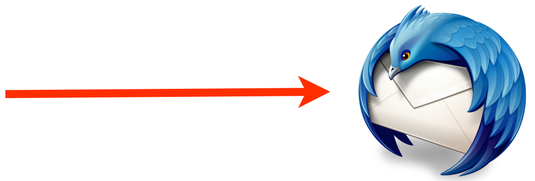
Internet



Email

smtp
submission
imap
pop



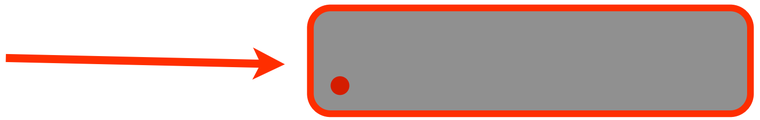


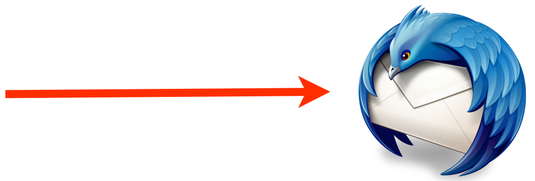
WLAN

Internet Provider

Mobilfunkbetreiber

Internet





Gemeinsamkeiten?

Alt

Klartext

Und nun?

lrefpuyüffryhat

Verschlüsselung

Transport-Verschlüsselung

Vertraulichkeit

2 Integrität

3 Authentizität

4 Nichtabstreitbarkeit

Transportverschlüsselung

TLS 1.2

TLS 1.1

TLS 1.0

~~*SSLv3*~~

~~*SSLv2*~~

Ihre Webseite

Ihr Mailserver

Testen

Webserver testen

https://ssllabs.com/ssltest

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Domain name: Submit

Do not show the results on the boards

Recently Seen

metronets.com	Err
slack.com	
owncloud.jonaskim.de	

Recent Best-Rated

londoners.ro	A+
openmailbox.org	A
pop.openmailbox.org	A

Recent Worst-Rated

client.investia.ca	F
outlook.com	F
webmin.studiotwo.com	Trust

SSL Report: nsa.gov (23.39.50.161)

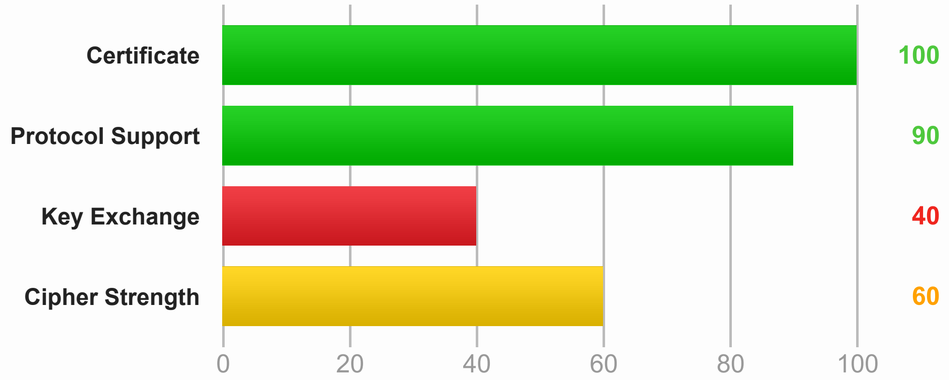
Assessed on: Sat Sep 20 20:37:28 UTC 2014 | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

C



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

Certificate uses SHA1. When renewing, ensure you upgrade to SHA256. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

 https://isitchristmas.com

NEIN

SSL Report: isitchristmas.com (54.235.64.112)

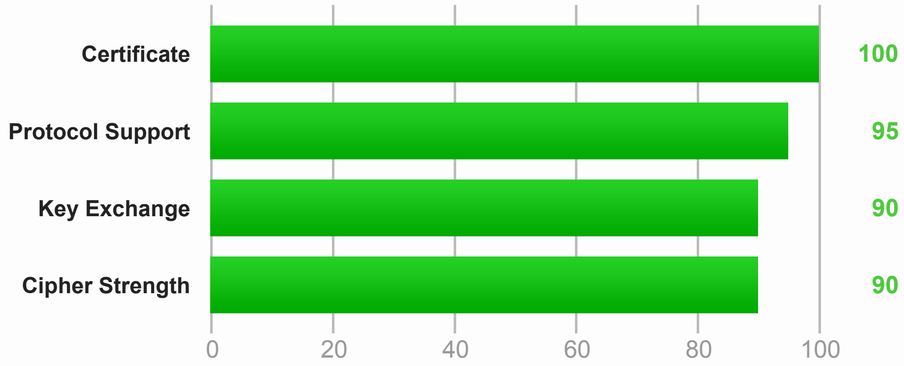
Assessed on: Mon Jul 28 06:42:17 UTC 2014 | Clear cache

Scan Another »

Summary

Overall Rating

A+



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

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

This server is not vulnerable to the Heartbleed attack.

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

SSL Report: ecb.europa.eu (184.25.151.166)

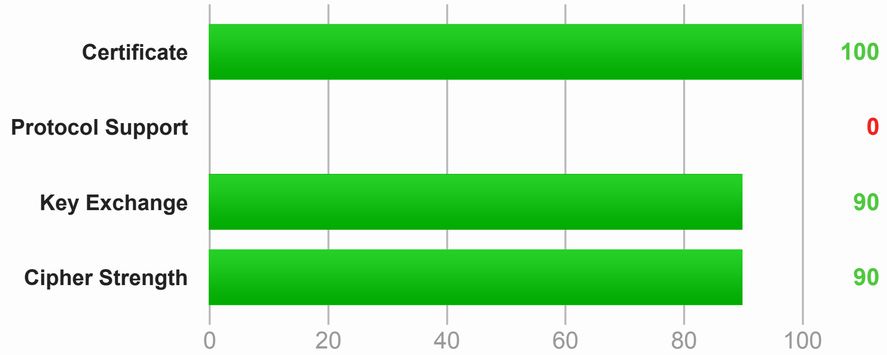
Assessed on: Sat Sep 20 20:51:40 UTC 2014 | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

F



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

This server supports SSL 2, which is obsolete and insecure. Grade set to F.

Certificate uses SHA1. When renewing, ensure you upgrade to SHA256. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

SSL Report: adv.at (5.254.185.81)

Assessed on: Mon Oct 06 01:25:12 UTC 2014 | **HIDDEN** | Clear cache

Scan Another »

Assessment failed: No secure protocols supported

Known Problems

There are some errors that we cannot fix properly in the current version. They will be addressed in the next generation version, which is currently being developed.

- **No secure protocols supported** - if you get this message, but you know that the site supports SSL, wait until the cache expires on its own, then try again, making sure the hostname you enter uses the "www" prefix (e.g., "www.ssllabs.com", not just "ssllabs.com").
- **no more data allowed for version 1 certificate** - the certificate is invalid; it is declared as version 1, but uses extensions, which were introduced in version 3. Browsers might ignore this problem, but our parser is strict and refuses to proceed. We'll try to find a different parser to avoid this problem.
- **Failed to obtain certificate** and **Internal Error** - errors of this type will often be reported for servers that use connection rate limits or block connections in response to unusual traffic. Problems of this type are very difficult to diagnose. If you have access to the server being tested, before reporting a problem to us, please check that there is no rate limiting or IDS in place.
- **NetScaler issues** - some NetScaler versions appear to reject SSL handshakes that do not include certain suites or handshakes that use a few suites. If the test is failing and there is a NetScaler load balancer in place, that's most likely the reason.
- **Unexpected failure** - our tests are designed to fail when unusual results are observed. This usually happens when there are multiple TLS servers

Email

https://starttls.info/

Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the blog.

Enter a hostname, IP- or e-mail address

Test it!

This site is a beta. | Read about this. | Check the stats.

Developed by Einar Otto Stangvik.

Results for: nsa.gov

Mail server	Result
emvm-gh1-uea09.nsa.gov	Grade: D (42.8%)

Certificate

- The certificate is not valid for the server's hostname.

There are validity issues for the certificate. Certificates are seldom verified for SMTP servers, so this doesn't mean that STARTTLS won't be used.

Generally speaking it's a bad practice not to have a valid certificate, and an even worse practice not to verify them. Any attempted encrypted communication is left all but wide open to Man-in-the-Middle attacks.

Protocol

- Supports SSLV3.
- Supports TLSV1.

Key exchange

- Anonymous Diffie-Hellman is accepted. This is suspectible to Man-in-the-Middle attacks.
- Key size is 2048 bits; that's good.

Cipher

- Weakest accepted cipher: 0.
- Strongest accepted cipher: 256.

emvm-gh1-uea08.nsa.gov	Grade: D (44.3%)

Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the blog.

Results for: ubermorgen.com

Mail server	Result
ubermorgen.com	Grade: A (93.4%)

Certificate

- No remarks.

Protocol

- Supports SSLV3.
- Supports TLSV1.
- Supports TLSV1.1.
- Supports TLSV1.2.

Key exchange

- Key size is 4096 bits; that's very good.

Cipher

- Weakest accepted cipher: 128.
- Strongest accepted cipher: 256.

Does your mail server support STARTTLS?

If you care about privacy, it should. Read more in the blog.

Results for: parlament.gv.at

Mail server	Result
mta3.parlament.gv.at	STARTTLS not supported!
mta2.parlament.gv.at	STARTTLS not supported!

Click the score for details.

Test another!

38%

https://starttls.info/stats

CC: NSA

Konkurrenz

Katzen

＼(=^‥^)


bettercrypto·org

Keinen Klartext herschenken

Applied Crypto Hardening

Praktischer Crypto Guide

Management

System Administration


PDF

Umfang

Server Tests

Webserver

Mailserver

Schlüssel

Verfahren

Zufallszahlen

VPN

SSH

PGP/GnuPG

Instant Messaging

Datenbanken

Praktische Einstellungen

Kopieren/Einsetzen

Beteiligung

Review

Overview

This whitepaper arose out of the need for system administrators to have an updated, solid, well researched and thought-through guide for configuring SSL, PGP, SSH and other cryptographic tools in the post-Snowden age. Triggered by the NSA leaks in the summer of 2013, many system administrators and IT security specialists saw the need to strengthen their encryption settings. This guide is specifically written for these system administrators.

Initiated by Aaron Kaplan (CERT.at) and Adi Kriegisch (VRVis), a group of specialists, cryptographers and sysadmins from CERTs, academia and the private sector joined forces to write such a concise, short guide.

This project aims at creating a simple, copy & paste-able HOWTO for secure crypto settings of the

Get the paper

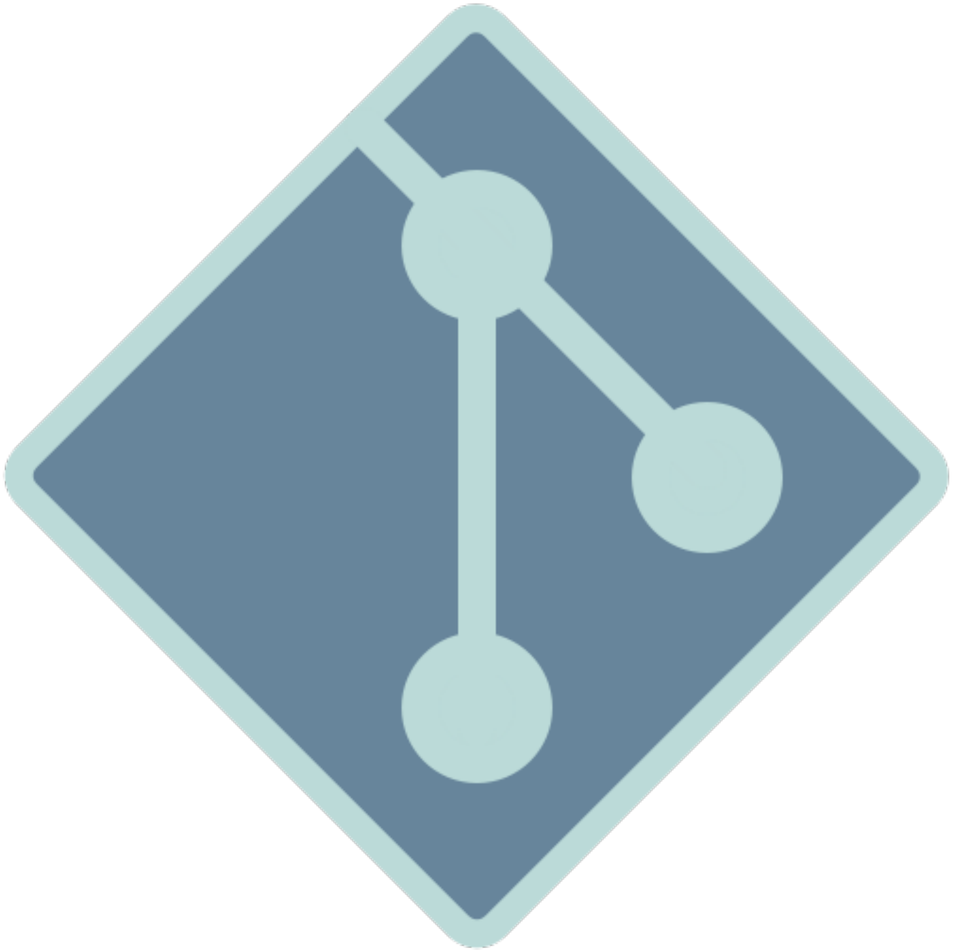
Draft status

Applied Crypto Hardening PDF

Join the discussion

Public mailing list

Get the sources




bettercrypto·org

Handlungsbedar F

Gute Verschlüsselung
muß Standard sein

Fragen?

Gute Verschlüsselung muß Standard sein

Hausübung

https://SSLLabs.com Web

https://StartTLS.info Mail

Weitere Informationen

https://BetterCrypto.org

https://MacLemon.at

https://CryptoParty.at

Pepi Zawodsky
@MacLemon
https://MacLemon.at/