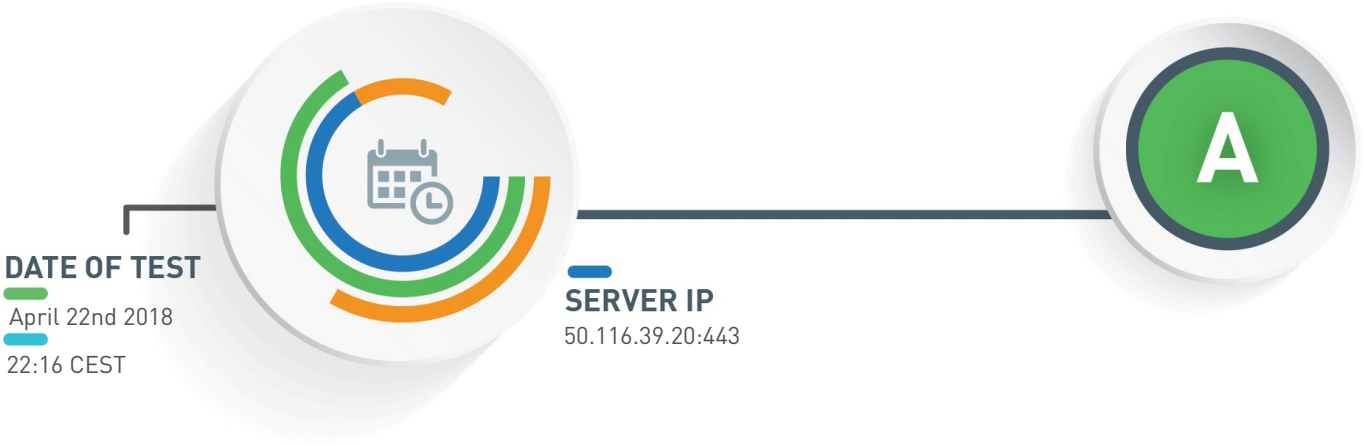
SSL/TLS Server Test of 50.116.39.20:443 (HTTPS)

Test SSL/TLS implementation of any service on any port for compliance with PCI DSS requirements, HIPAA guidance and NIST guidelines.

50.116.39.20

FINAL GRADE



DATE OF TEST
April 22nd 2018
22:16 CEST

SERVER IP
50.116.39.20:443

Assessment Executive Summary

TEST HIGHLIGHTS

The server's certificate is untrusted.	Non-compliant with PCI DSS requirements
The server configuration has a good protocol compatibility, allowing users with older browsers to access your website.	Information
The server prefers cipher suites supporting Perfect-Forward-Secrecy.	Good configuration
The server provides HTTP Strict Transport Security.	Good configuration

SSL Certificate Overview

RSA CERTIFICATE INFORMATION

Issuer	-
Trusted	No
Untrusted Reasons	The certificate is self-signed The certificate has been signed by an unknown Certificate Authority (CA)
Common Name	50.116.39.20
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Transparency	No
Validation Level	No
OCSP Must-Staple	No
Supports OCSP Stapling	No
Valid From	April 20th 2018, 00:25 CEST
Valid To	April 18th 2023, 23:25 CET

CERTIFICATE CHAIN

50.116.39.20 — Self-signed | Server certificate

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	e997faaf009787fc4297a6fbef74136cd6f101536065b7e332cf808fe7818915
PIN	leJV6K4D+Z8H9Z9MalpjwvW0M6NzEDUI0gEuF+pEc8s=
Expires in	1,822 days

Test For Compliance With PCI DSS Requirements

Reference: PCI DSS 3.1 - Requirements 2.3 and 4.1

CERTIFICATES ARE UNTRUSTED

The RSA certificate provided by the server could not be trusted. — Non-compliant with PCI DSS requirements

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration

TLSV1.1

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.1	Good configuration
TLSv1.2	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-384 (secp384r1) (384 bits)	Good configuration

POODLE OVER TLS

The server is not vulnerable to POODLE over TLS. — Not vulnerable

CVE-2016-2107

The server is not vulnerable to OpenSSL padding-oracle flaw (CVE-2016-2107). — Not vulnerable

SERVER DOES NOT SUPPORT CLIENT-INITIATED INSECURE RENEGOTIATION

The server does not support client-initiated insecure renegotiation. — Good configuration

ROBOT

The server is not vulnerable to ROBOT (Return Of Bleichenbacher's Oracle Threat) vulnerability. — Not vulnerable

HEARTBLEED

The server version of OpenSSL is not vulnerable to Heartbleed attack. Not vulnerable

CVE-2014-0224

The server is not vulnerable to CVE-2014-0224 (OpenSSL CCS flaw). Not vulnerable

Test For Compliance With HIPAA

Reference: HIPAA of 1996, Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

X509 CERTIFICATES ARE IN VERSION 3

All the X509 certificates provided by the server are in version 3.

Good configuration

CERTIFICATES ARE SELF-SIGNED

The RSA certificate provided by the server is self-signed.

Non-compliant with HIPAA guidance

CERTIFICATES DO NOT PROVIDE REVOCATION INFORMATION

The RSA certificate provided is missing OCSP URI and crlDistributionPoints extension, making impossible to verify if it has been revoked.

Non-compliant with HIPAA guidance

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.1	Good configuration
TLSv1.2	Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration

TLSV1.1

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-384 (secp384r1) (384 bits)	Good configuration

TLSV1.1 SUPPORTED

The server supports TLSv1.1 which is mandatory to comply with HIPAA guidance.

Good configuration

TLSV1.2 SUPPORTED

The server supports TLSv1.2 which is the only SSL/TLS protocol that currently has no known flaws or exploitable weaknesses.

Good configuration

EC_POINT_FORMAT EXTENSION

The server supports the EC_POINT_FORMAT TLS extension.

Good configuration

Test For Compliance With NIST Guidelines

Reference: NIST Special Publication 800-52 Revision 1 - Section 3

NIST Update to Current Use and Deprecation of TDEA abrogates 3DES authorized in the NIST guidelines. — Information

X509 CERTIFICATES ARE IN VERSION 3

All the X509 certificates provided by the server are in version 3. — Good configuration

CERTIFICATES ARE SELF-SIGNED

The RSA certificate provided by the server is self-signed. — Non-compliant with NIST guidelines

CERTIFICATES DO NOT PROVIDE REVOCATION INFORMATION

The RSA certificate provided is missing OCSP URI and crlDistributionPoints extension, making impossible to verify if it has been revoked.

Non-compliant with NIST guidelines

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration

TLSV1.1

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.1	Good configuration
TLSv1.2	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-384 (secp384r1) (384 bits) — Good configuration

TLSV1.1 SUPPORTED

The server supports TLSv1.1 which is mandatory to comply with NIST guidelines. — Good configuration

TLSV1.2 SUPPORTED

The server supports TLSv1.2 which is the only SSL/TLS protocol that currently has no known flaws or exploitable weaknesses.

Good configuration

EC_POINT_FORMAT EXTENSION

The server supports the EC_POINT_FORMAT TLS extension.

Good configuration

Test For Industry Best-Practices

DNSCAA

This domain does not have a Certification Authority Authorization (CAA) record.

Information

CERTIFICATES DO NOT PROVIDE EV

The RSA certificate provided is NOT an Extended Validation (EV) certificate.

Information

SERVER HAS CIPHER PREFERENCE

The server enforces cipher suites preference.

Good configuration

SERVER PREFERRED CIPHER SUITES

Preferred cipher suite for each protocol supported (except SSLv2). Expected configuration are ciphers allowed by PCI DSS and enabling PFS:

TLSv1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLSv1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Good configuration

Good configuration

SERVER PREFERS CIPHER SUITES PROVIDING PFS

For TLS family of protocols, the server prefers cipher suite(s) providing Perfect Forward Secrecy (PFS).

Good configuration

ALWAYS-ON SSL

The HTTP version of the website redirects to the HTTPS version.

Good configuration

SERVER PROVIDES HSTS WITH LONG DURATION

The server provides HTTP Strict Transport Security for more than 6 months:

15768000 seconds

Good configuration

SERVER DOES NOT PROVIDE HPKP

The server does not enforce HTTP Public Key Pinning that helps preventing man-in-the-middle attacks.

Information

TLS_FALLBACK_SCSV

The server supports TLS_FALLBACK_SCSV extension for protocol downgrade attack prevention.

Good configuration

SERVER DOES NOT SUPPORT CLIENT-INITIATED SECURE RENEGOTIATION

The server does not support client-initiated secure renegotiation.

Good configuration

SERVER-INITIATED SECURE RENEGOTIATION

The server supports secure server-initiated renegotiation.

Good configuration

SERVER DOES NOT SUPPORT TLS COMPRESSION

TLS compression is not supported by the server.

Good configuration