SSL/TLS Security Assessment of 185.67.36.64

Test SSL/TLS implementation of any service on any port for compliance with industry best-practices, NIST guidelines and PCI DSS requirements.

185.67.36.64

FINAL GRADE

F

DATE OF TEST

September 9th 2016

09:11 CEST

SERVER IP

185.67.36.64:25

Assessment Executive Summary

The tested service does not seem to be an HTTPS service — Information

The server prefers cipher suites supporting Perfect-Forward-Secrecy — Good configuration

Consider reviewing the set of supported cipher suites — Non-compliant with PCI DSS requirements; Non-compliant with NIST guidelines

The certificate is untrusted — Non-compliant with PCI DSS requirements

The server is vulnerable to OpenSSL padding-oracle flaw (CVE-2016-2107), consider upgrading OpenSSL — Non-compliant with PCI DSS requirements

SSL Certificate Overview

RSA CERTIFICATE INFORMATION

Trusted	No
Untrusted Reasons	The certificate doesn't match hostname
Common Name	posteo.de
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:www.posteo.de, DNS:mout03.posteo.de, DNS:mout04.posteo.de, DNS:mx01.posteo.de, DNS:m.posteo.de, DNS:mout02.posteo.de, DNS:cdn.posteo.de, DNS:mx04.posteo.de, DNS:mout01.posteo.de, DNS:api.posteo.de, DNS:mx03.posteo.de, DNS:autodiscover.posteo.de, DNS:lists.posteo.de, DNS:mx02.posteo.de, DNS:posteo.de
Transparency	No
Extended Validation	Yes
Valid From	January 22nd 2016, 01:00 CET
Valid To	January 22nd 2017, 00:59 CET

CERTIFICATE CHAIN

posteo.de

Extended Validation Server certificate

Key Type/Size	**RSA 2048 bits**
Signature Algorithm	**sha256WithRSAEncryption**
SHA256	**14afddf132890075f3220f8c308213cdaa6747f0f669deff944dc0221ae5bfc2**
PIN	**YHg6IF6c81F7j83apmWtrzgANaHRN1gjRXGqMNGm5C0=**
Expires in	**135 days**

↥ GeoTrust EV SSL CA - G4

Intermediate CA

Key Type/Size	**RSA 2048 bits**
Signature Algorithm	**sha256WithRSAEncryption**
SHA256	**f9cce53a2c02bfdd9b421931d8556b782c6ecd2333ff1759e7a701722351de47**
PIN	**owrR9U9FWDWtrFF+myoRIu75JwU4sJwzvhCNLZoY37g=**
Expires in	**2,608 days**

↥ GeoTrust Primary Certification Authority

Self-signed Root CA

Key Type/Size	**RSA 2048 bits**
Signature Algorithm	**sha1WithRSAEncryption**
SHA256	**a0fa1c76fd1acf62c1445b319370caaaa24a2d1086e3857bad214cc0f57a8dc1**
PIN	**SQVGZiOrQXi+kqxcvWWE96HhfydlLVqFr4lQTqI5qqo=**
Expires in	**7,251 days**

Test For Compliance With NIST Guidelines

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

DIFFIE-HELLMAN PARAMETER SIZE

The size of your Diffie-Hellman (DH) parameter:

2048 bits	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)	Good configuration

SUPPORTED PROTOCOLS

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

TLSv1.0	Good configuration
TLSv1.1	Good configuration
TLSv1.2	Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	Non-compliant with NIST guidelines
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_SEED_CBC_SHA	Non-compliant with NIST guidelines
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	Non-compliant with NIST guidelines
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	Non-compliant with NIST guidelines
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_SEED_CBC_SHA	Non-compliant with NIST guidelines
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	Non-compliant with NIST guidelines

TLS_ECDHE_RSA_WITH_RC4_128_SHA	Non-compliant with NIST guidelines
TLS_RSA_WITH_RC4_128_SHA	Non-compliant with NIST guidelines
TLS_RSA_WITH_RC4_128_MD5	Non-compliant with NIST guidelines

MISSING MANDATORY CIPHERS

The support of these ciphers is mandatory according to NIST:

TLS_RSA_WITH_3DES_EDE_CBC_SHA	Non-compliant with NIST guidelines

SERVER DOES NOT SUPPORT OCSP STAPLING

The server does not support OCSP stapling. Its support allows better verification of the certificate validation status.

Non-compliant with NIST guidelines

Test For Compliance With PCI DSS Requirements

Reference: PCI DSS 3.1 - Requirements 2.3 and 4.1

CERTIFICATE IS UNTRUSTED

The RSA certificate provided could not be trusted.

Non-compliant with PCI DSS requirements

DIFFIE-HELLMAN PARAMETER SIZE

The size of your Diffie-Hellman (DH) parameter:

2048 bits	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 bits)	Good configuration

SUPPORTED PROTOCOLS

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

TLSv1.0	Deprecated. Dropped in June 2018
TLSv1.1	Good configuration
TLSv1.2	Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_SEED_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_SEED_CBC_SHA	Good configuration
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_RC4_128_SHA	Non-compliant with PCI DSS requirements
TLS_RSA_WITH_RC4_128_SHA	Non-compliant with PCI DSS requirements
TLS_RSA_WITH_RC4_128_MD5	Non-compliant with PCI DSS requirements

POODLE

The server is not vulnerable to POODLE over TLS.

Not vulnerable

CVE-2016-2107

The server is vulnerable to OpenSSL padding-oracle flaw (CVE-2016-2107), consider upgrading OpenSSL.

Non-compliant with PCI DSS requirements

SERVER DOES NOT SUPPORT CLIENT-INITIATED INSECURE RENEGOTIATION

The server does not support client-initiated insecure renegotiation.

Good configuration

HEARTBLEED

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

Not vulnerable

Test For Industry Best-Practices

CERTIFICATE IS EV

All the server certificates provide Extended Validation (EV).

Good configuration

SERVER SUPPORTS TLSV1.2

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

Good configuration

SERVER PREFERS PFS ENABLED CIPHER SUITES

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

Good configuration

SERVER SUPPORTS TLS FALLBACK SCSV EXTENSION

The server supports TLS_FALLBACK_SCSV extension for protocol downgrade attack prevention.

Good configuration

SERVER SUPPORTS CLIENT-INITIATED SECURE RENEGOTIATION

The server supports client-initiated secure renegotiation which may be unsafe and allow Denial of Service attacks.

Misconfiguration or weakness

SECURE RENEGOCIATION SUPPORTED

The server supports secure server-initiated renegotiation.

Good configuration

TLS COMPRESSION SUPPORT

TLS compression is supported by the server which may allow CRIME attack. We advise to disable this feature.

Misconfiguration or weakness

SERVER PREFERRED CIPHER SUITES

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

TLSv1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLSv1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration