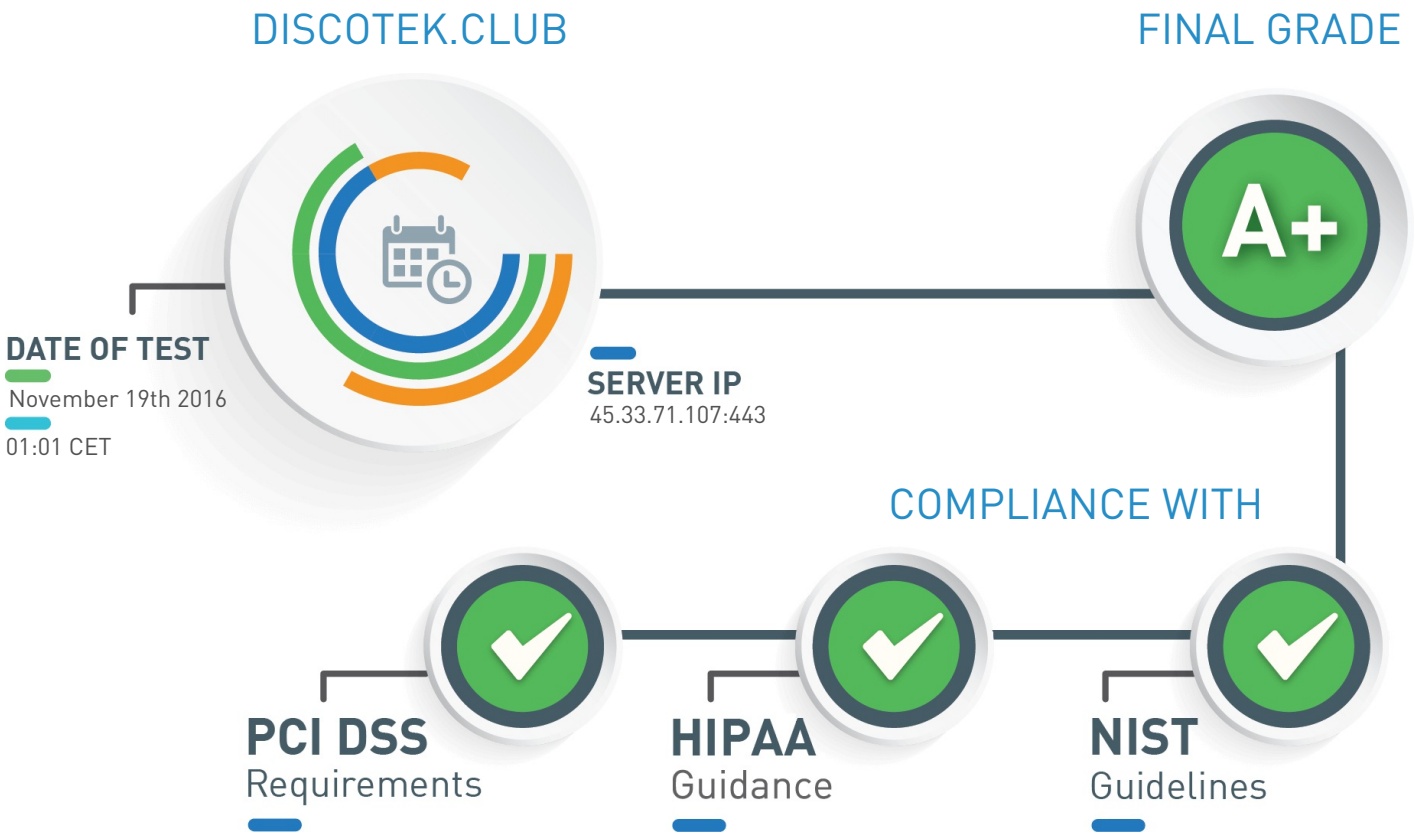
SSL Server Security Test of discotek.club

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



Assessment Executive Summary

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

Trusted	Yes
Common Name	discotek.club
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:discotek.club, DNS:www.discotek.club, DNS:cdn.discotek.club, DNS:cdn2.discotek.club, DNS:dev.discotek.club
Transparency	No
Extended Validation	No
OCSP Must-Staple	No
Supports OCSP Stapling	Yes
Valid From	July 16th 2016, 20:47 CEST
Valid To	July 16th 2017, 20:47 CEST

CERTIFICATE CHAIN

discotek.club

Server certificate

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	8302bf45a54e62496584dd26ac5262267a7f2d938fe6d860c3a852b149a0deee
PIN	4xE4LQuDwM7vXgFgid4cCm2bBVy4KtdnfmBvt1GdKig=
Expires in	240 days

StartCom Class 1 DV Server CA

Intermediate CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	e4a30fafb87c96bb8f9c848c42ad34e3185ecdf08f275d2804c95b5373cb5adb
PIN	Fbs+o+IxVNTHBpjNQYfX/TBnxPC+OWLYxQLEtqkrAfM=
Expires in	5,140 days

StartCom Certification Authority

Self-signed Root CA

Key Type/Size	RSA 4096 bits
Signature Algorithm	sha1WithRSAEncryption
SHA256	2a22ac9f978cd158855c4f8a7aaf44528b29b1b61a586efc12c7d30f331c7a02
PIN	5C8kvU039KouVrl52D0eZSGf4Onjo4Khs8tmyTlV3nU=
Expires in	7,243 days

CERTIFICATE CHAIN CONTINUED

discotek.club

Server certificate

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	8302bf45a54e62496584dd26ac5262267a7f2d938fe6d860c3a852b149a0deee
PIN	4xE4LQuDwM7vXgFgid4cCm2bBVy4KtdnfmBvt1GdKig=
Expires in	240 days

StartCom Class 1 DV Server CA

Intermediate CA

Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	e4a30fafb87c96bb8f9c848c42ad34e3185ecdf08f275d2804c95b5373cb5adb
PIN	Fbs+o+IxVNTHBpjNQYfX/TBnxPC+OWLYxQLEtqkrAfM=
Expires in	5,140 days

StartCom Certification Authority

Self-signed Root CA

Key Type/Size	RSA 4096 bits
Signature Algorithm	sha256WithRSAEncryption
SHA256	adc3372be57ae66359434e2932ea5e1ccf0ba0b92826f0aa68322c7d53fb53ca
PIN	5C8kvU039KouVrl52D0eZSGf4Onjo4Khs8tmyTlV3nU=
Expires in	7,243 days

Test For Compliance With PCI DSS Requirements

Reference: PCI DSS 3.1 - Requirements 2.3 and 4.1

CERTIFICATES ARE TRUSTED

All the certificates provided by the server are trusted. Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_DHE_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
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	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

DIFFIE-HELLMAN PARAMETER SIZE

Diffie-Hellman parameter size: 2048 bits Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 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

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

SERVER SUPPORTS OCSP STAPLING

The server supports OCSP stapling, which allows better verification of the certificate validation status. 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_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_DHE_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
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration

DIFFIE-HELLMAN PARAMETER SIZE

Diffie-Hellman parameter size: 2048 bits Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 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

X509 CERTIFICATES ARE IN VERSION 3

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

SERVER SUPPORTS OCSP STAPLING

The server supports OCSP stapling, which allows better verification of the certificate validation status. Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_DHE_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
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	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

DIFFIE-HELLMAN PARAMETER SIZE

Diffie-Hellman parameter size: 2048 bits Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-256 (prime256v1) (256 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

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:

TLSv1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLSv1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLSv1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	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

HTTP SITE DOES REDIRECT

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: 15638400 seconds Good configuration

SERVER DOES NOT PROVIDE HPKP

The server does not enforce HTTP Public Key Pinning which 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