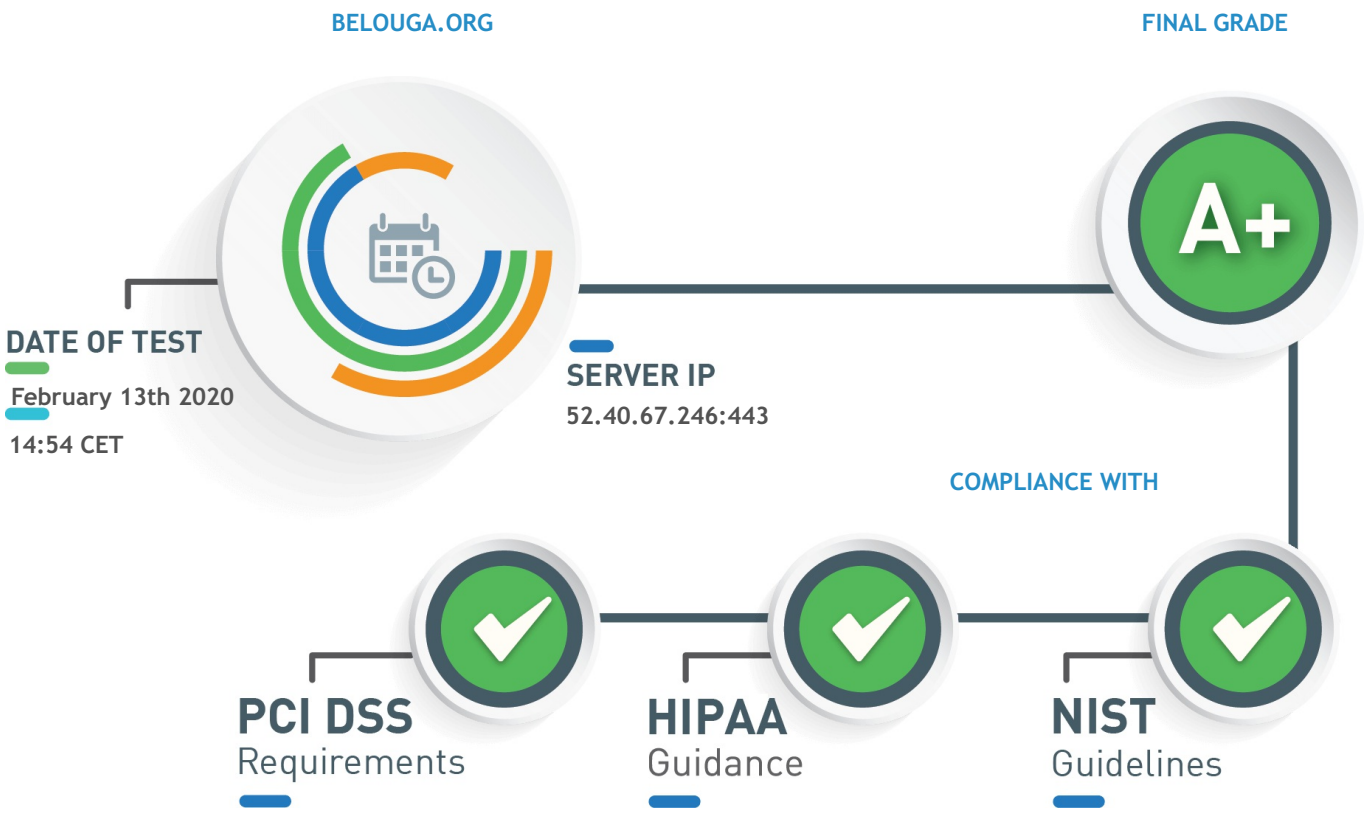
Test SSL/TLS implementation of any service on any port for compliance with PCI DSS requirements, HIPAA guidance and NIST guidelines.



Summary of belouga.org:443 (HTTPS) SSL Security Test

The server configuration supports only TLSv1.2 protocol, precluding users with older browsers from accessing your website.

Information

SSL Certificate Analysis

RSA CERTIFICATE INFORMATION

Issuer	Let's Encrypt Authority X3
Trusted	Yes
Common Name	belouga.org
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:belouga.org, DNS:www.belouga.org
Transparency	Yes
Validation Level	DV
CRL	No
OCSP	http://ocsp.int-x3.letsencrypt.org
OCSP Must-Staple	No
Supports OCSP Stapling	Yes
Valid From	January 18th 2020, 19:02 CET
Valid To	April 17th 2020, 20:02 CEST

CERTIFICATE CHAIN

DST Root CA X3

Self-signed Root CA

Key Type/Size	**RSA 2048 bits**
Signature Algorithm	**sha1WithRSAEncryption**
SHA256	**0687260331a72403d909f105e69bcf0d32e1bd2493ffc6d9206d11bcd6770739**
PIN	**Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys=**
Expires in	**595 days**

↳ Let's Encrypt Authority X3

Intermediate CA

Key Type/Size	**RSA 2048 bits**
Signature Algorithm	**sha256WithRSAEncryption**
SHA256	**25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d**
PIN	**YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=**
Expires in	**398 days**

↳ belouga.org

Server certificate

Key Type/Size	**RSA 2048 bits**

Signature Algorithm	**sha256WithRSAEncryption**
SHA256	**1825405ddd685108190a03842b38d132f58bf1728bd17b813026211e9d31f998**
PIN	**8KutBbr/zP+vOiV/YYKFL2utImPkoBndErY1TT7pyJw=**
Expires in	**64 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:

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration

SUPPORTED PROTOCOLS

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

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
P-521 (secp521r1) (521 bits)	Good configuration
P-384 (secp384r1) (384 bits)	Good configuration

X25519 (253 bits) — Good configuration

POODLE OVER TLS

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

GOLDENDOODLE

The server is not vulnerable to GOLDENDOODLE. — Not vulnerable

ZOMBIE POODLE

The server is not vulnerable to Zombie POODLE. — Not vulnerable

SLEEPING POODLE

The server is not vulnerable to Sleeping POODLE. — Not vulnerable

0-LENGTH OPENSSL

The server is not vulnerable 0-Length OpenSSL. — 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 Guidance

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:

TLSv1.2 Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_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
P-521 (secp521r1) (521 bits)	Good configuration
P-384 (secp384r1) (384 bits)	Good configuration
X25519 (253 bits)	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

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:

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration

SUPPORTED PROTOCOLS

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

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
P-521 (secp521r1) (521 bits)	Good configuration
P-384 (secp384r1) (384 bits)	Good configuration
X25519 (253 bits)	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

EXPECT-CT

Expect-CT header is properly set. Good configuration

max-age=0

CERTIFICATES DO NOT PROVIDE EV

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

NO SUPPORT OF TLSV1.3

The server does not support TLSv1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses. Misconfiguration or weakness

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:

TLSv1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLSv1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 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: Good configuration
31536000 seconds

SERVER DOES NOT PROVIDE HPKP

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

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