SSL Report: api.aspnet4you.com (13.65.39.165)
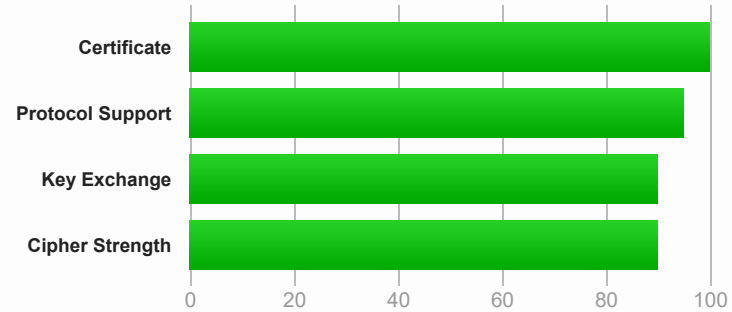
Assessed on: Mon, 25 Dec 2017 16:16:49 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A

Certificate	
Protocol Support	
Key Exchange	
Cipher Strength	

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

This site works only in browsers with SNI support.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject   api.aspnet4you.com
Fingerprint SHA256: 701174d78ab1f51c2979005cc4fa7ae6762855f7bbb0ed24a2188016bd21987b
Pin SHA256: D9iIqsZy4rEH4vooRSawWXjBh+a3GsS7f8BvL/o3Jis=

Server Key and Certificate #1

Common names	api.aspnet4you.com
Alternative names	api.aspnet4you.com azure.aspnet4you.com www.aspnet4you.com
Serial Number	0088d720c48517c82b6018aae2e5487a30
Valid from	Mon, 25 Dec 2017 00:00:00 UTC
Valid until	Thu, 24 Dec 2020 23:59:59 UTC (expires in 2 years and 11 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	COMODO RSA Domain Validation Secure Server CA AIA: http://crt.comodoca.com/COMODORSADomainValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl OCSP: http://ocsp.comodoca.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	3 (4354 bytes)
Chain issues	None

#2

Subject	COMODO RSA Domain Validation Secure Server CA Fingerprint SHA256: 02ab57e4e67a0cb48dd2ff34830e8ac40f4476fb08ca6be3f5cd846f646840f0 Pin SHA256: klO23nT2ehFDXCfx3eHTDRESMz3asj1muO+4aIdjiuY=
Valid until	Sun, 11 Feb 2029 23:59:59 UTC (expires in 11 years and 1 month)
Key	RSA 2048 bits (e 65537)
Issuer	COMODO RSA Certification Authority

Additional Certificates (if supplied)

Signature algorithm	SHA384withRSA

#3

Subject	COMODO RSA Certification Authority
	Fingerprint SHA256: 4f32d5dc00f715250abcc486511e37f501a899deb3bf7ea8adbbd3aef1c412da
	Pin SHA256: grX4Ta9HpZx6tSHkmCrvpApTQGo67CYDnvprLg5yRME=
Valid until	Sat, 30 May 2020 10:48:38 UTC (expires in 2 years and 5 months)
Key	RSA 4096 bits (e 65537)
Issuer	AddTrust External CA Root
Signature algorithm	SHA384withRSA

Certification Paths ➕

<div align="center">

Click here to expand

</div>

Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI ➕

<div align="center">

Click here to expand

</div>

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes

Protocols

SSL 3	No
SSL 2	No

For TLS 1.3 tests, we currently support draft version 18.

Cipher Suites

TLS 1.2 (suites in server-preferred order)   ⊟

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (`0xc02f`)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (`0xc028`)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (`0xc027`)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (`0xc014`)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (`0xc013`)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (`0x9d`)		256
TLS_RSA_WITH_AES_128_GCM_SHA256 (`0x9c`)		128
TLS_RSA_WITH_AES_256_CBC_SHA256 (`0x3d`)		256
TLS_RSA_WITH_AES_128_CBC_SHA256 (`0x3c`)		128
TLS_RSA_WITH_AES_256_CBC_SHA (`0x35`)		256
TLS_RSA_WITH_AES_128_CBC_SHA (`0x2f`)		128

TLS 1.1 (suites in server-preferred order)   ⊞

TLS 1.0 (suites in server-preferred order)   ⊞

Handshake Simulation

[Android 2.3.7](#) No SNI [2]	Incorrect certificate because this client doesn't support SNI				
	RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA				
[Android 4.0.4](#)	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
[Android 4.1.1](#)	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
[Android 4.2.2](#)	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
[Android 4.3](#)	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS

Handshake Simulation

Client	Certificate	Protocol	Cipher Suite	Key Exchange	
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 57 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 53 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 8 / XP No FS [1] No SNI [2]	Server closed connection				
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Edge 13 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Java 6u45 No SNI [2]	Incorrect certificate because this client doesn't support SNI				
	RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA				
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Java 8u31	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS		

Handshake Simulation

Client	Cert	Protocol	Cipher Suite	Key Exchange	FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS

Not simulated clients (Protocol mismatch) ⊟

| IE 6 / XP No FS [1] No SNI [2] | | Protocol mismatch (not simulated) |

(1) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

(2) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(3) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(4) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

Protocol Details

	No, server keys and hostname not seen elsewhere with SSLv2
DROWN	**(1) For a better understanding of this test, please read this longer explanation**
	(2) Key usage data kindly provided by the Censys network search engine; original DROWN website here
	(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete

Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side ([more info](#)) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported ([more info](#))
POODLE (TLS)	No ([more info](#))
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported ([more info](#))
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No ([more info](#))
Ticketbleed (vulnerability)	No ([more info](#))
OpenSSL CCS vuln. (CVE-2014-0224)	No ([more info](#))
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No ([more info](#))
ROBOT (vulnerability)	No ([more info](#))
Forward Secrecy	With modern browsers ([more info](#))
ALPN	No
NPN	No
Session resumption (caching)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No ([more info](#))
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No ([more info](#))
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No

Protocol Details

Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	**Yes**
Supported Named Groups	secp256r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	Yes

HTTP Requests ⊞

1	**https://api.aspnet4you.com/**	(HTTP/1.1 200 OK)

Miscellaneous

Test date	Mon, 25 Dec 2017 16:15:17 UTC
Test duration	91.699 seconds
HTTP status code	200
HTTP server signature	Microsoft-IIS/10.0
Server hostname	-

SSL Report v1.30.5

Terms and Conditions