SSL Report: simplexpay.com (66.94.100.240)

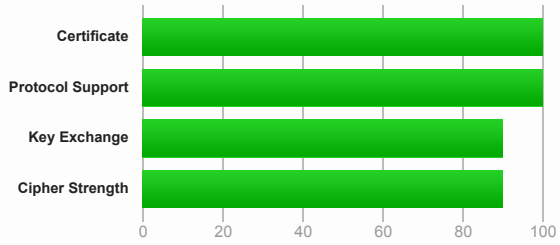
Assessed on: Wed, 25 Dec 2024 00:27:23 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating

A+



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.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	www.simplexpay.com Fingerprint SHA256: cb645a8da1816da36d0ef4c3e0a785dd16afb5dd17d03f70785d9f7b0ef230dd Pin SHA256: G9HJqtv2wxp8/jpitlagRy60vIT67PkZ6sAYluUXiaE=
Common names	www.simplexpay.com
Alternative names	cpanel.simplexpay.com ftp.simplexpay.com mail.simplexpay.com simplexpay.com webmail.simplexpay.com www.simplexpay.com
Serial Number	044f9e00d9ea11c72fbe0f6a649d1a36e349
Valid from	Mon, 16 Dec 2024 04:47:15 UTC
Valid until	Sun, 16 Mar 2025 04:47:14 UTC (expires in 2 months and 19 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R11 AIA: http://r11.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r11.o.lencr.org
Revocation status	Good (not revoked)

DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	2 (2668 bytes)
Chain issues	None

#2

Subject	R11 Fingerprint SHA256: 591e9ce6c863d3a079e9fabe1478c7339a26b21269dde795211361024ae31a44 Pin SHA256: bdrBhpj38ffhxpubzkINl0rG+UyossdhcBYj+Zx2fcc=
Valid until	Fri, 12 Mar 2027 23:59:59 UTC (expires in 2 years and 2 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

Certification Paths

Mozilla | Apple | Android | Java | Windows

Path #1: Trusted

1	Sent by server	www.simplexpay.com Fingerprint SHA256: cb645a8da1816da36d0ef4c3e0a785dd16afb5dd17d03f70785d9f7b0ef230dd Pin SHA256: G9HJqtv2wxp8/jpitlagRy60vIT67PkZ6sAYluUXiaE= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	R11 Fingerprint SHA256: 591e9ce6c863d3a079e9fabe1478c7339a26b21269dde795211361024ae31a44 Pin SHA256: bdrBhpj38ffhxpubzkINl0rG+UyossdhcBYj+Zx2fcc= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	ISRG Root X1 Self-signed Fingerprint SHA256: 96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA

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

Server Key and Certificate #1

Subject	vps.methacortex.com Fingerprint SHA256: a42147af9d9d010a60b2bde1023da89c00565778bd927e6d670c600e48ba592a Pin SHA256: QfG2sN/sNpTlyXm7kpA+vyTvAk/S/nTacW10eCjzkAk=
Common names	vps.methacortex.com
Alternative names	vps.methacortex.com MISMATCH
Serial Number	0339f77be8fa48356b67acf3330600e5b6ab
Valid from	Fri, 06 Dec 2024 17:59:58 UTC
Valid until	Thu, 06 Mar 2025 17:59:57 UTC (expires in 2 months and 9 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R11 AIA: http://r11.i.lencr.org/

Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r11.o.lencr.org
Revocation status	Good (not revoked)
Trusted	No **NOT TRUSTED** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	2 (2562 bytes)
Chain issues	None

#2

Subject	R11 Fingerprint SHA256: 591e9ce6c863d3a079e9fabe1478c7339a26b21269dde795211361024ae31a44 Pin SHA256: bdrBhpj38ffhxpubzkINl0rG+UyossdhcBYj+Zx2fcc=
Valid until	Fri, 12 Mar 2027 23:59:59 UTC (expires in 2 years and 2 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

Certification Paths

Mozilla | Apple | Android | Java | Windows

Path #1: Not trusted (invalid certificate [Fingerprint SHA256: a42147af9d9d010a60b2bde1023da89c00565778bd927e6d670c600e48ba592a])

1	Sent by server	vps.methacortex.com Fingerprint SHA256: a42147af9d9d010a60b2bde1023da89c00565778bd927e6d670c600e48ba592a Pin SHA256: QfG2sN/sNpTlyXm7kpA+vyTvAk/S/nTacW10eCjzkAk= RSA 2048 bits (e 65537) / SHA256withRSA
2	Sent by server	R11 Fingerprint SHA256: 591e9ce6c863d3a079e9fabe1478c7339a26b21269dde795211361024ae31a44 Pin SHA256: bdrBhpj38ffhxpubzkINl0rG+UyossdhcBYj+Zx2fcc= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	ISRG Root X1 Self-signed Fingerprint SHA256: 96bcec06264976f37460779acf28c5a7cfe8a3c0aae11a8ffcee05c0bddf08c6 Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M= RSA 4096 bits (e 65537) / SHA256withRSA

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes*
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

(*) Experimental: Server negotiated using No-SNI

Cipher Suites

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
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 **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)	FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS **WEAK**	128

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Chrome 80 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Firefox 73 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 11.0.3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 12.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.1.1c R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	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 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 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 12.1.1 / iOS 12.3.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS

 # Not simulated clients (Protocol mismatch)

Android 2.3.7 No SNI [2]	Protocol mismatch (not simulated)
Android 4.0.4	Protocol mismatch (not simulated)
Android 4.1.1	Protocol mismatch (not simulated)
Android 4.2.2	Protocol mismatch (not simulated)
Android 4.3	Protocol mismatch (not simulated)
Baidu Jan 2015	Protocol mismatch (not simulated)
IE 6 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)
IE 7 / Vista	Protocol mismatch (not simulated)
IE 8 / XP No FS [1] No SNI [2]	Protocol mismatch (not simulated)
IE 8-10 / Win 7 R	Protocol mismatch (not simulated)
IE 10 / Win Phone 8.0	Protocol mismatch (not simulated)
Java 6u45 No SNI [2]	Protocol mismatch (not simulated)
Java 7u25	Protocol mismatch (not simulated)
OpenSSL 0.9.8y	Protocol mismatch (not simulated)
Safari 5.1.9 / OS X 10.6.8	Protocol mismatch (not simulated)
Safari 6.0.4 / OS X 10.8.4 R	Protocol mismatch (not simulated)

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

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

(3) 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).

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

Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc027
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc027

OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc027
Sleeping POODLE	No (more info) TLS 1.2 : 0xc027
Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
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	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes http/1.1
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=31536000
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
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	No
Supported Named Groups	secp256r1, secp521r1, secp384r1, secp256k1 (server preferred order)
SSL 2 handshake compatibility	Yes

HTTP Requests

1 **https://simplexpay.com/** (HTTP/1.1 302 Found)

Server	nginx/1.26.1
Date	Wed, 25 Dec 2024 00:26:39 GMT
Content-Type	text/html; charset=UTF-8
Transfer-Encoding	chunked
Connection	close
Cache-Control	private, must-revalidate
pragma	no-cache
expires	-1
Set-Cookie	XSRF-TOKEN=eyJpdiI6IjR4WHA1TG9ZbEU0YkU3OGRXOXgyQkE9PSIsInZhbHVlIjoi-U1NDK0RGOWFpUXVDWWV6V2RVMkFkU0k5MFMvVGdRc05YVDZyZldDMmwvMytScSt-CazM1V0RjQWZjUFNjbTVDVndBRXhPd3gxaHpWaW9hcDNRR3VEU0EwN1pUdmNvajdqe-FFjOHNqUWxLa2dvN1RZTEdPSTlBdlhKTEo0ejIwdTAiLCJtYWMiOiJhZTY1OGIw-YTk5NTc0OWQ0YjFlYTQ0ZmNjMGZkODc5NDE2Y2Y0MGFlMThjNDY2MjJjNWQ4MDY4O-

		TUwZDJlN2FlIiwidGFnIjoiIn0%3D; expires=Wed, 25 Dec 2024 02:26:39 GMT; Max-Age=7200; path=/; samesite=lax
	Set-Cookie	simplexpay_session=eyJpdiI6InJuc1Y1QmxyYnN4OXhlVnh3cTZmcXc9PSIsInZhbHVlIjoi-RVEvSXlNVUVFK0dWSGlFSTZJTVp3czZjZ2RERytkMXE0Wi9UNzNNU3FuMTdJUWVK-WEdlU2FXUiswZE4xOE9kSjRMQUtWNnlQS05YemhKdUFjcmhSMC9nb3lVYjM2QlNUWEv-VXg5Vm1zSDRRWFVaN2s2QUNDSUFGSHVmRmpMZWwiLCJtYWMiOiJlMWUzYzU5Mm-NkOGFkMjBkOWU0NTlkODA5ZDYxN2Y1OTY1ZjA0MDMxMzNhYzVlMTg0YzIzMTNh-NGE1NTgwN2MxIiwidGFnIjoiIn0%3D; expires=Wed, 25 Dec 2024 02:26:39 GMT; Max-Age=7200; path=/; httponly; samesite=lax
	Location	https://simplexpay.com/login
	X-Cache	HIT from Backend
	Strict-Transport-Security	max-age=31536000
	X-XSS-Protection	1; mode=block
	X-Content-Type-Options	nosniff

2 **https://simplexpay.com/login** (HTTP/1.1 200 OK)

	Server	nginx/1.26.1
	Date	Wed, 25 Dec 2024 00:26:40 GMT
	Content-Type	text/html; charset=UTF-8
	Transfer-Encoding	chunked
	Connection	close
	Vary	Accept-Encoding
	Cache-Control	private, must-revalidate
	pragma	no-cache
	expires	-1
2	**Set-Cookie**	XSRF-TOKEN=eyJpdiI6IkE5K25ZUUZDbElSU1l4WFlteGJKR3c9PSIsInZhbHVlIjoiekFmN-Fk5M1JycDdUeDVZSnJGOG9ENmF0UzdwUEE1cUxNYUw3MlEyZDBWNTBSRGFsZ1ovb-TR5dWNJUzQwR3VZdGhwWjlwWTJpdTNGOEhSU3dlbEU2T3pOU3lxMk42WGo4TVl6Yz-FNUFJDQzZVT0hOcERURVJtYWdnSGJScjZsWGsiLCJtYWMiOiI1ZTQwNjNhODkzNDVjZ-TA2YzUxN2RjOTYyMzE3ODgzNjI4ZGYxN2Y2MjNhOTc0MDRhNDlmMzRmZTk0NjEwYTRiI-iwidGFnIjoiIn0%3D; expires=Wed, 25 Dec 2024 02:26:40 GMT; Max-Age=7200; path=/; samesite=lax
	Set-Cookie	simplexpay_session=eyJpdiI6ImUxU1pUb3F1WW5FTzhzbnl4VWtFQUE9PSIsInZhbHVlIjoi-UVBPRDBhWVFDMWE0aE5aSEFDcW9ORGtrc2dCcmFVRG9jdmFvZ1BHdmt5RmRXbm-dueTV2RjVNclVMcjliQnh4SW9kR2FnTUlpRERmcklyRGZVQTJPb0NRMkgrYmc3dVlJcER-CaitEU0lFY0ZDZlF4TjRNakJtT2JWSDh1cytNTHciLCJtYWMiOiJjNTU5YTI2NmUzNzMx-Yzc1NjcxMGRkMjIzODg5ZWYyNzI5OTM2NmZhMzdmMTA1NGJkOGE2YmY0ZTQzMDky-MjQzIiwidGFnIjoiIn0%3D; expires=Wed, 25 Dec 2024 02:26:40 GMT; Max-Age=7200; path=/; httponly; samesite=lax
	X-Cache	HIT from Backend
	Strict-Transport-Security	max-age=31536000
	X-XSS-Protection	1; mode=block
	X-Content-Type-Options	nosniff

Miscellaneous

Test date	Wed, 25 Dec 2024 00:26:28 UTC
Test duration	54.977 seconds
HTTP status code	200
HTTP server signature	nginx/1.26.1
Server hostname	vmi853444.contaboserver.net