UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

JUNIO 2021 – NOVIEMBRE 2021

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TITULO DE INGERIERO(A) EN SISTEMAS

TEMA:

Análisis de protocolos de seguridades en las plataformas de ventas de ropa en línea del Ecuador

EGRESADA:

Daysi Jessenia Lara Palacios

TUTOR:

ING. HUGO JAVIER GUERRERO TORRES, MGS

2021

INTRODUCCIÓN

En la actualidad hay que tener en cuenta lo importante que es el tema del comercio electrónico y los protocolos de seguridad que estos proporcionan ya que durante la crisis que atraviesa el país este permite a los negocios de ventas de ropas poder realizar sus funciones utilizando las herramientas de internet como las páginas web, redes sociales, entre otros dado que, en los últimos años el número de usuarios de internet ha incrementado y esto ha abierto gradualmente las ventas en líneas que comienza a elevar sus montos anual.

Para ello hay que tener en cuenta ¿Qué es el e-commerce? ¿Cuál es el principal problema de las ventas en líneas? ¿Qué tipo de seguridad deberían tener las páginas web?, el e-commerce es el comercio electrónico como su nombre lo indica ayuda a la compra y venta por internet.

El principal problema que conlleva las ventas en líneas son las diferentes páginas web de esta modalidad ya que no brindan la seguridad adecuada de la información personal por lo que ocurren diversos peligros de ciberdelitos o suplantación de identidad y este problema hace que las personas desconfíen y no quieran emplear los servicios que dan estos portales digitales. Los usuarios poseen un miedo que llegue a ocurrir los tipos de eventos ya mencionados por aquella razón las desconfianzas a los sitios web son realmente altos, aunque en este tiempo ya diversas personan hacen uso de estas.

Los tipos de seguridad que deberían poseer estas plataformas online son los certificados SSL puesto que es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer (Capa de sockets seguros), un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.

Por esa razón se presentará a fondo este tema mediante los objetivos especificados, el marco teórico, los resultados para dar una información más específica.

DESARROLLO

En la actualidad, debido a la pandemia que está envuelta el mundo las ventas en línea o el comercio electrónico (e-commerce) ha incrementado considerablemente por este motivo la seguridad de las plataformas que ofrecen este servicio es un factor importante para que así los clientes encuentren factible y cómodo hacer uso de esta, sin necesidad de que aparezca las inseguridades de los usuarios de un posible robo.

Existe gran desconfianza al momento de realizar compras en línea, esto es producido, generalmente, por el desconocimiento de la seguridad que ofrecen los sitios web para almacenar la información privada del cliente, esto influye negativamente en las compras puesto que se han presentado noticias sobre robos por esta modalidad.

Se ha hecho necesario realizar un análisis sobre la seguridad que tienen estos sitios web, centrándose en los protocolos y versiones que se utilizan. Existen sitios web que, aunque sean de reciente diseño, utilizan versiones obsoletas de protocolos de seguridad SSL o TLS. Al utilizar una versión obsoleta de estos protocolos de seguridad se corre el riesgo de que un atacante explote algunas de sus vulnerabilidades ya conocidas y pueda acceder a información personal de un cliente o de la misma empresa.

Se espera que con estos resultados se pueda mejorar la confianza hacia este método de compra. En este estudio de caso, debido a la gran cantidad de oferta en línea de diversos productos, se han tomado como producto la venta de ropa, que corresponde al 6% de las ventas a nivel nacional (Cámara Ecuatoriana de Comercio Elecrónico, 2020) de las empresas más conocidas en el Ecuador.

Los sitios más comunes de venta de ropa en línea son:

Tabla 1 Fábricas de Ropa Ecuatorianas

Fábricas de Ropa de Ecuador	**Sitios de ventas de Ropas online**	
EMPRESA PINTO S.A	OPTIMODA	MNG
PASAMANERÍA S.A	DE PRATI	SEVERUS
PRINTEXTIL	TATY	TIENDA MIA
TECNIFARM	TENNIS S.A	TYSFASHION

Fuente: Datos tomados de la pagina (DirectorioDeFabricas, 2021)

El objetivo general de esta investigación es analizar la aplicación de protocolos de seguridad en los sitios web de venta de ropa en línea del Ecuador.

Como objetivos específicos se tienen el de identificar los posibles problemas de seguridad de diversos sitios web de venta de ropa en línea en Ecuador; verificar el uso adecuado de protocolos de seguridad SSL y/o TLS en los sitios web de compra de ropa en línea; y, evaluar los sitios web de venta de ropa en línea del Ecuador que aplican políticas de seguridad para la información de sus usuarios.

En el presente caso de estudio se realizará una investigación del tipo documental o bibliográfico, para obtener y realizar el análisis de información de un objeto de estudio. Por medio de las fuentes bibliográficas, como libros, blog, etc.

La investigación documental es una técnica de investigación cualitativa que se encarga de juntar y escoger información a través de la investigación de documentos oficiales y personales.

Como método de investigación se ha decidido optar por el método descriptivo puesto que nos permite describir las características de los protocolos de seguridad que nos mostrará los resultados de las plataformas de ventas de ropas escogidas para la comprobación de certificados SSL de los sitios web ya que es importante conocer que la pagina esté protegida, por ejemplo:

El mensaje "*NO SSL CERTIFICATION."* indica que la conexión a tu sitio web o servidor no está asegurada con un certificado SSL. Puede ser que no hayas instalado ninguno, o que la instalación no sea válida o sea defectuosa (IONOS, 2021).

En este caso, se debe revisar la instalación del certificado SSL tan pronto como sea posible o instalar una nueva versión, es decir, realizar una nueva solicitud (IONOS, 2021).

El test de SSL muestra si se ha instalado correctamente el certificado que se está utilizando o si existe alguna posible brecha de seguridad. (IONOS, 2021).

Como también puede aparecer el mensaje *"CERTIFICATE IS INSTALLED CORRECTLY"* significa que tu certificado SSL funciona de la manera prevista y que, por lo tanto, es válido. Toda la información sobre el certificado la encontrarás en "Información sobre el certificado" (IONOS, 2021).

En el apartado "Estado del certificado" también se indica la validez del certificado (IONOS, 2021).

A pesar de que un certificado sea válido y funcione correctamente, esto no significa necesariamente que el intercambio de datos de tu página web esté protegido contra todas las amenazas conocidas. (IONOS, 2021).

Políticas de seguridad

Las políticas de seguridad informática son declaraciones formales de las reglas que debemos cumplir las personas que tenemos acceso a los activos de tecnología e información de una organización. (Carisio, s.f.)

Protocolos HTTPS

Actualmente gracias a los grandes avances tecnológicos las ventas online se disparan, para lograr una campaña exitosa y que los clientes compren de forma segura, por ello los e-commerce deben estar listos e implantar los protocolos web como el HTTPS". (Consulting, 2020)

¿Qué es el protocolo https y en qué consiste?

En la barra de dirección de los navegadores se encontrará un icono de un candado cerrado. Dicho símbolo indica al usuario la conexión entre su equipo y el servidor que proporciona la página, está asegurada mediante un sistema de encriptación. (Consulting, 2020)

Este protocolo de seguridad permite una conexión segura entre el servidor y usuario que no puede ser obstruida por personas no autorizadas. (Consulting, 2020)

Certificado SSL consiste en tres capas de protección:

- Encriptación: los datos entre el navegador del cliente y el sitio web se protegen con una fuerte codificación. Si un hacker los roba o intercepta, encontrará complicado descifrarlos. (Consulting, 2020)
- Integridad de datos: la información no puede verse alterada o corrompida durante la transmisión, sin que se detecten errores. (Consulting, 2020)

- Autenticación: el proceso de verificación de conexión con el sitio web deseado. (Consulting, 2020)

Ventajas del protocolo de seguridad https:

Especialmente indicado para páginas dedicadas al ecommerce, la inclusión del protocolo de protección aporta tres grandes beneficios a los dueños de estos sitios web y a los navegantes (Consulting, 2020):

- Seguridad: el protocolo proporciona seguridad para el sitio web de la empresa u organización, garantizando que los datos entre la página y los usuarios se verifican y codifican. (Consulting, 2020)
- Confianza: los usuarios que acceden a sitios web mediante https se sienten más confiados a la hora de navegar y comprar en páginas con este protocolo. (Consulting, 2020).

Certificados SSL

"Es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer, un protocolo de seguridad que crea un enlace cifrado entre un servidor y un navegador web". (Lab, 2019)

¿Cómo funcionan los certificados SSL?

Los certificados SSL funcionan garantizando que los datos transferidos entre usuarios y sitios web, o entre dos sistemas, sean imposibles de leer. (Lab, 2019)

Utiliza algoritmos de cifrado para cifrar los datos en tránsito, lo que evita que los hackers la información que se envía a través de la conexión. Estos datos incluyen información potencialmente confidencial, como nombres, direcciones u otros detalles financieros. (Lab, 2019)

Ilustración 1 Función de los Certificados SSL

Fuente: Imágenes extraída de la página DigiCert *(DigiCert, 2021)*

1. El protocolo SSL comienza a actuar después de establecerse la conexión TCP e inicia lo que se denomina el protocolo de enlace de SSL. (DigiCert, 2021)
2. El servidor envía su certificado al usuario junto con una serie de especificaciones, como la versión de SSL/TLS y los métodos de cifrado que se utilizarán. (DigiCert, 2021)
3. El usuario comprueba la validez del certificado, selecciona el nivel de cifrado más alto admitido por ambas partes e inicia una sesión segura con estos métodos. Hay una amplia variedad de series de métodos, con diferentes puntos fuertes. (DigiCert, 2021)
4. Para garantizar la integridad y la autenticidad de todos los mensajes que se transfieren, los protocolos SSL y TLS también incluyen un proceso de autenticación que utiliza códigos de autenticación de mensajes (MAC, Message Authentication Code) (DigiCert, 2021). Todo esto parece largo y complicado, pero en realidad se efectúa casi de manera instantánea. (DigiCert, 2021)

Por qué necesita un certificado SSL

Los sitios web necesitan certificados SSL para mantener la seguridad de los datos del usuario, verificar la propiedad del sitio web, evitar que los atacantes creen una versión falsa del sitio y para transmitir confianza a los usuarios. (Lab, 2019)

Si un sitio web solicita a los usuarios que inicien sesión, ingresen datos personales, como sus números de tarjeta de crédito, o vean información confidencial, como información financiera, entonces es esencial mantener la confidencialidad de los datos. (Lab, 2019)

Los certificados SSL ayudan a mantener la privacidad de las interacciones en línea y garantizan a los usuarios que el sitio web es auténtico y que es seguro compartir información privada mediante él. (Lab, 2019)

Las herramientas a utilizar en el caso de estudio son Qualys certview y Site24x7 ya que van a ayudar con el proceso de análisis de las plataformas digitales de prueba para dar a conocer si estas poseen o no un protocolo de seguridad.

Qualys Certview

CertView genera grados de instancia de certificado utilizando la metodología sencilla de SSL Labs que permite a los administradores evaluar configuraciones SSL de servidor que a menudo se pasan por alto sin tener que convertirse en expertos en SSL. (INC, 2018)

También le permite corregir rápidamente conjuntos de cifrado, protocolos y parámetros de intercambio de claves en los puntos finales subyacentes. (INC, 2018).

CertView supervisa continuamente certificados en toda la empresa, para garantizarlos se renueven antes de que caduquen, lo que detiene las interrupciones relacionadas con los

certificados, mejorando la disponibilidad, tanto en las instalaciones locales como en las instancias en la nube. (INC, 2018)

- Resalta visualmente los certificados vencidos y vencidos para que pueda acceder a la información que desea rápidamente. (INC, 2018)
- Proporciona una descripción general rápida de cuántos certificados necesitan atención inmediata a través de simples widgets del tablero. (INC, 2018)

Site24x7

El servicio de Site24x7 es una solución práctica, escalable y es operativa rápidamente. La facilidad para su parametrización y uso diario nos da una información muy útil de la disponibilidad de nuestros servicios. (Casas, 2021)

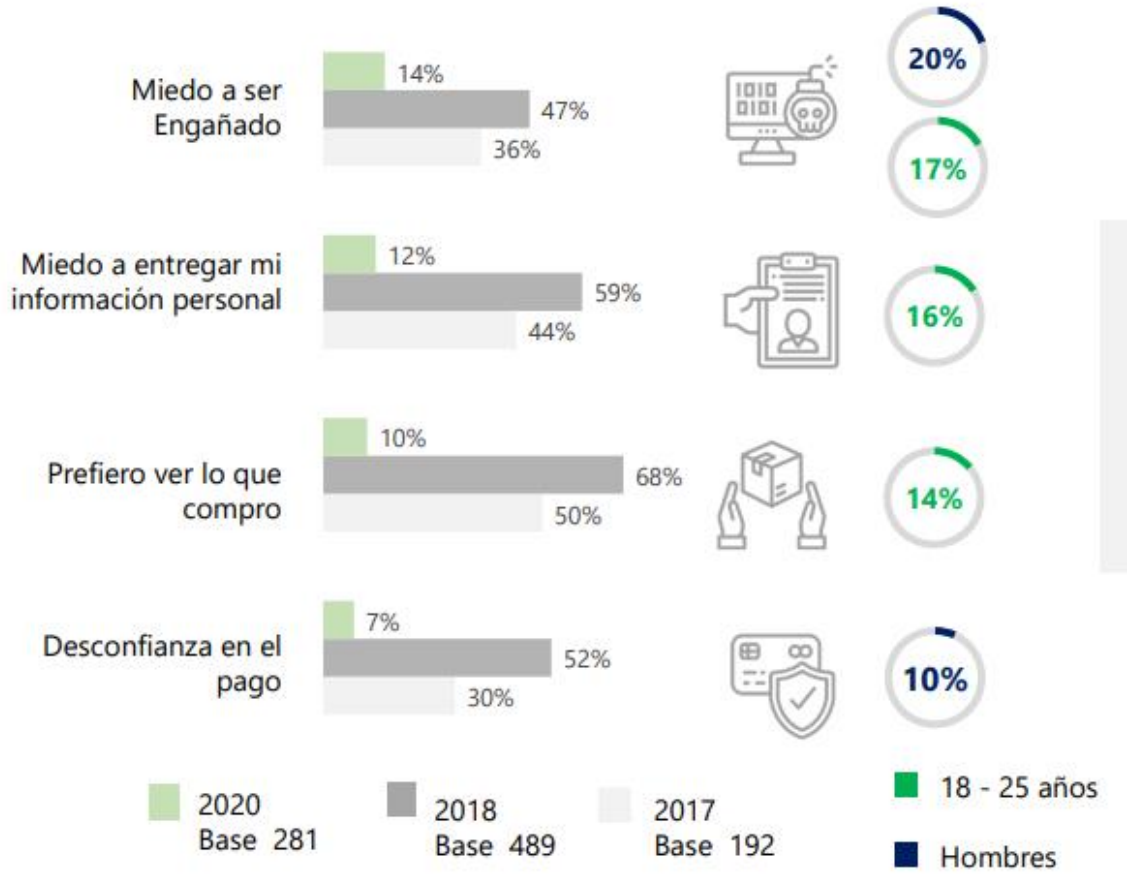
Además, el uso de la App nos permite tener monitorizados y en alerta de cualquier incidencia de nuestros servicios de forma remota. (Casas, 2021).

Utilizamos Site24x7 para mantener al público informado sobre el estado de nuestros servicios. Site24x7 nos brinda visibilidad de todos los parámetros de rendimiento críticos de nuestros recursos y nos ayuda a estar al tanto de los problemas. (Anema, 2021)

La facilidad de uso, el conjunto de funciones, los precios asequibles, y un excelente soporte son factores que nos impresionaron con Site24x7. (Anema, 2021).

Barreras para comprar en línea

Ilustración 2 Barreras de compras en línea

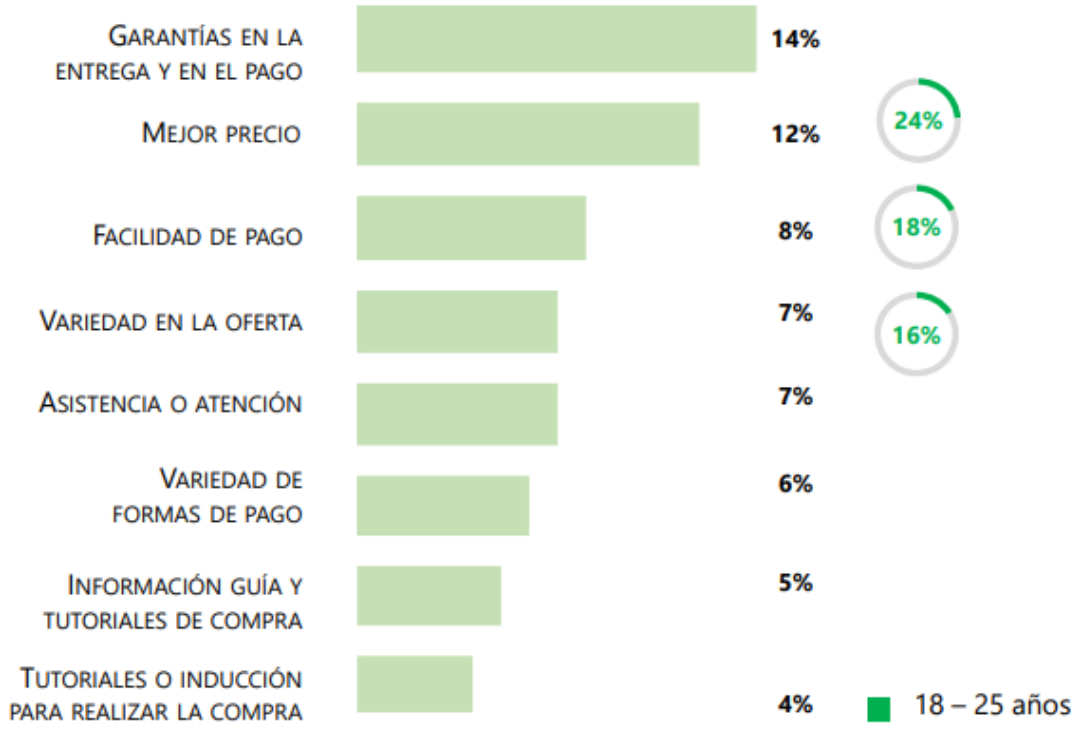


Fuente: Estudio de Comportamiento de transacciones no presenciales en Ecuador PDF (CECE (Cámara Ecuatoriana de Comercio Elecrónico), 2020)

La desconfianza de ser víctima de engaño o fraude con el pago, ha disminuido respecto a las mediciones previas. Sin embargo, continúa liderando las barreras de acercamiento a las compras online. (CECE (Cámara Ecuatoriana de Comercio Elecrónico), 2020)

Motivaciones para comprar en línea

Ilustración 3 Motivaciones para comprar en línea



Fuente: Estudio de Comportamiento de transacciones no presenciales en Ecuador PDF (CECE (Cámara Ecuatoriana de Comercio Elecrónico), 2020)

Contar con respaldo del E-commerce para realizar la transacción y precios atractivos son los estímulos que más incentivarían la compra. (CECE (Cámara Ecuatoriana de Comercio Elecrónico), 2020)

Para realizar las siguientes preguntas las páginas web seleccionadas como una pequeña muestra se realizó una prueba con la aplicación SSL Server Test del sitio web Qualys. La herramienta utilizada es la técnica de observación ya que con ella se pudo ver los diferentes grados y versiones de los certificados SSL de cada plataforma.

Para demostrar se los resultados de la investigación se decidió establecer una matriz comparativa con las características de los protocolos de seguridad más conocidas para proceder a elaborar la tabla y grafico para obtener los resultados que se muestran a continuación.

Los parámetros utilizados para la elaborar de la matriz comparativa son:

Utilizar certificado SSL/TLS, al hacer uso de estos certificados los clientes se sentirán más seguros.

La Encriptación ayudara a cifrar la información proporcionada por el usuario.

Las Políticas de seguridad son los acuerdos que indica la empresa para mejorar la experiencia de compra en los sitios web.

Los Protocolos HTTPS emplean combinaciones de dos protocolos de comunicación HTTP y SSL/TLS que hace que cualquier tipo de información que se transmita en la red sea cifrada y nadie pueda acceder a ella, únicamente navegador y servidor web. (Acibeiro, 2021).

La Seguridad de las páginas web el protocolo proporciona seguridad para el sitio web de la empresa u organización, garantizando que los datos entre la página y los usuarios se verifican y codifican. (Consulting, 2020).

La Confianza los usuarios que acceden a sitios web mediante https se sienten más confiados a la hora de navegar y comprar en páginas con este protocolo". (Consulting, 2020).

Tabla 2 Comprobación de características de protocolos de seguridad

SSL Server Test del sitio web Qualys						
Parámetros		Optimoda	Tennis S.A	TATY	Tysfashion	De Prati
1	Utilizan certificados TLS/SSL	X	X	X	X	X
2	Encripta información	X	X			X
3	Política de seguridad	X			X	X
4	Protocolo HTTPS		X	X	X	X
5	Seguridad de los sitios web				X	X
6	Confianza del usuario					X

Elaborado por Daysi Lara, X indica que cumple el parámetro

CONCLUSIONES

En el análisis de la muestra de los sitios web dedicados a la venta de ropa, se obtuvo que el 40% de los clientes no aceptan las políticas de seguridad del sitio por temor a que la información proporcionada sea mal utilizada.

El 40% de la muestra investigada demostraba problemas de vulnerabilidad y en los protocolos de seguridad por lo que es necesario que cuenten con planes o herramientas para hacerle frente a posibles ataques informáticos y que la información personal de los usuarios no sea expuesta.

Mediante la investigación realizada se pudo determinar que en el 100% de los sitios analizados, el protocolo utilizado es el HTTPS, que es un protocolo de comunicación segura y confiable y por tanto se pueden utilizar certificados SSL/TLS, de esta manera se garantizar que estos sitios pueden comprobar la autenticidad de la información en sus plataformas.

Las herramientas utilizadas para este estudio proporcionan la información suficiente acerca de las seguridades y vulnerabilidades, aunque es muy recomendable utilizar varias para poder contrastar la información de cada una de ellas, ya que se ha visto pequeñas diferencias en los resultados de estas herramientas

Para garantizar que el cliente o usuario confié en estos sitios web de venta de ropa en línea es necesario que estos sitios se mantengan actualizados constantemente, tanto en tecnología como en protocolos y otros sistemas de seguridad. De esta manera se creará todo un entorno de confianza para usar este tipo de plataformas digitales.

REFERENCIAS

Acibeiro, M. (06 de 07 de 2021). *godaddy*. Obtenido de godaddy: https://es.godaddy.com/blog/diferencia-entre-http-y-https/

Anema, R. (2021). *Site24x7*. Obtenido de Site24x7: https://www.site24x7.com/

Cámara Ecuatoriana de Comercio Elecrónico. (2020). Estudio de transacciones electronicas en Ecuador durante el Covid19. *Estudio de eCommerce en el Ecuador*.

Carisio, E. (s.f.). *MediaCloud*. Obtenido de MediaCloud: https://blog.mdcloud.es/politicas-de-seguridad-informatica-y-su-aplicacion-en-la-empresa/

Casas, C. (2021). *Site24x7*. Obtenido de Industrias Preciber.

CECE (Cámara Ecuatoriana de Comercio Elecrónico). (2020). Estudio de Comportamiento de transacciones no presenciales en Ecuador. *Estudios de eCommerce en Ecuador*, 31-32.

Consulting, S. T. (10 de Diciembre de 2020). *tecsens*. Obtenido de tecsens: https://www.tecsens.com/por-que-es-necesario-el-protocolo-https/

De Prati . (2020). *De Prati* . Obtenido de De Prati : https://www.deprati.com.ec/

DigiCert. (2021). *DigiCert*. Obtenido de DigiCert: https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https

DirectorioDeFabricas. (19 de Febrero de 2021). *Directorio De Fabricas*. Obtenido de Directorio De Fabricas: https://www.directoriodefabricas.com/ecuador/fabricantes-de-ropa-en-ecuador.html

El Universo. (26 de Febrero de 2021). *Cómo la pandemia cambió los hábitos de compras en línea en Ecuador y provocó que nazcan proyectos de 'e-commerce' colaborativos*.

INC, Q. (13 de ABRIL de 2018). *Qualys CertView*. Obtenido de Qualys CertView: https://www.qualys.com/certview/data-enriched/

IONOS. (2021). *IONOS by 1&1*. Obtenido de IONOS by 1&1: https://www.ionos.es/tools/ssl-checker

Lab, K. (2019). *Kaspersky*. Obtenido de Kaspersky: https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate

Optimoda. (2019). *Optimoda* . Obtenido de Optimoda : http://www.optimoda.com.ec/

Site24x7. (2021). *Site24x7*. Obtenido de Site24x7: https://www.site24x7.com/

TATY. (2020). *TATY* . Obtenido de TATY : https://www.taty.com.ec/

Tennis S.A . (2020). *Tennis S.A* . Obtenido de Tennis S.A : https://www.tennis.com.ec/informacion/acerca-de-tennis

Tysfashion. (2021). *Tysfashion*. Obtenido de Tysfashion: https://www.tysfashion.com/

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > www.optimoda.com.ec

SSL Report: www.optimoda.com.ec

Assessed on: Fri, 01 Oct 2021 20:25:47 UTC | Hide | Clear cache

Scan Another >>

	Server	Test time	Grade
1	100.24.208.97 staticip2.multiscreensite.com Ready	Fri, 01 Oct 2021 20:23:47 UTC **Duration:** 60.18 sec	A+
2	35.172.94.1 staticip.multiscreensite.com Ready	Fri, 01 Oct 2021 20:24:47 UTC **Duration:** 59.445 sec	A+

SSL Report v2.1.8

Certificate #1: RSA 4096 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	www.optimoda.com.ec Fingerprint SHA256: a0c80f2353913b9acf405e743d045ec7828197fd30d39bacbc09a1b0feb37768 Pin SHA256: hi19+xnNhVDdimDzt+cpNjPCOQmlNYTSa6VOldBa3YY=
Common names	www.optimoda.com.ec
Alternative names	www.optimoda.com.ec
Serial Number	04f681e82deb243ecf9377ace1196257803a
Valid from	Tue, 31 Aug 2021 11:50:36 UTC
Valid until	Mon, 29 Nov 2021 11:50:35 UTC (expires in 1 month and 8 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (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
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)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV 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	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes h2 http/1.1
NPN	No
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=31536000; preload

Configuration

Protocols

TLS 1.3	Yes
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 1.3 (suites in server-preferred order)

TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256P

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS	256

(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)

Strict Transport Security (HSTS)	**Yes** max-age=31536000; preload
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
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1, x448, secp521r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	Yes
0-RTT enabled	No

HTTP Requests

1 https://www.optimoda.com.ec/ (HTTP/1.1 200)

Miscellaneous

Test date	Wed, 20 Oct 2021 22:21:08 UTC
Test duration	60.327 seconds
HTTP status code	200
HTTP server signature	nginx
Server hostname	staticip2.multiscreensite.com

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > www.tennis.com.ec

SSL Report: www.tennis.com.ec

Assessed on: Fri, 01 Oct 2021 20:55:52 UTC | Hide | Clear cache

Scan Another >>

	Server	Test time	Grade
1	143.204.128.62 server-143-204-128-62.sfo5.r.cloudfront.net Ready	Fri, 01 Oct 2021 20:30:15 UTC Duration: 433.701 sec	A
2	143.204.128.110 server-143-204-128-110.sfo5.r.cloudfront.net Ready	Fri, 01 Oct 2021 20:37:29 UTC Duration: 415.997 sec	A
3	143.204.128.101 server-143-204-128-101.sfo5.r.cloudfront.net Ready	Fri, 01 Oct 2021 20:44:25 UTC Duration: 331.494 sec	A
4	143.204.128.35 server-143-204-128-35.sfo5.r.cloudfront.net Ready	Fri, 01 Oct 2021 20:49:56 UTC Duration: 355.913 sec	A

S

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	www.tennis.com.ec Fingerprint SHA256: 1d94b654a94abbf3bd70bc97ee9c499c363620ed2046087c8aa483f6ff8991a1 Pin SHA256: rgxKTonn82vq0+WPKMaCwT5DnSVmDY1DzmHy3rkLbs=
Common names	www.tennis.com.ec
Alternative names	www.tennis.com.ec
Serial Number	03228c3ca763360c3b906960ee3755c33c8e
Valid from	Fri, 08 Oct 2021 08:49:23 UTC
Valid until	Thu, 06 Jan 2022 08:49:22 UTC (expires in 2 months and 16 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: tennis.com.ec issue: letsencrypt.org flags:0 issue: digicert.com flags:0 issue: globalsign.com flags:0 issue: comodoca.com flags:0
Trusted	Yes Mozilla Apple Android Java Windows

Configuration

Protocols

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

Cipher Suites

# TLS 1.3 (suites in server-preferred order)	
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256

# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (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
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	**Yes, TLS_FALLBACK_SCSV 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	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes h2 http/1.1
NPN	No
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	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	x25519, secp256r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 https://www.tennis.com.ec/ (HTTP/1.1 200 OK)

Miscellaneous

Test date	Wed, 20 Oct 2021 22:45:42 UTC
Test duration	162.291 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	server-99-84-224-213.sfo5.r.cloudfront.net

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > www.taty.com.ec

SSL Report: www.taty.com.ec (3.208.229.80)

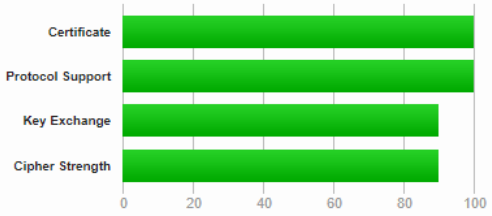
Assessed on: Fri, 01 Oct 2021 21:01:19 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A



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

This server supports TLS 1.3.

Certificate #1: EC 384 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	www.taty.com.ec Fingerprint SHA256: 34cc25f051c3b3e90879eaa8a1d29c5cf0b94f79afcb8c3ba615a84760e0a585 Pin SHA256: boCAw4U57KX0E+UKySDSSMb3FQOMnj2T+VcZODC7RHs=
Common names	www.taty.com.ec
Alternative names	www.taty.com.ec
Serial Number	041f07aa426b129aebcb9ed8edc90221db0f
Valid from	Fri, 06 Aug 2021 15:18:45 UTC
Valid until	Thu, 04 Nov 2021 15:18:43 UTC (expires in 14 days, 16 hours)
Key	EC 384 bits
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.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	3 (3834 bytes)
Chain issues	None

#2

Subject	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=
Valid until	Mon, 15 Sep 2025 16:00:00 UTC (expires in 3 years and 10 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

#3

Subject	ISRG Root X1 Fingerprint SHA256: 6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf7ff1c24f Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M=
Valid until	Mon, 30 Sep 2024 18:14:03 UTC (expires in 2 years and 11 months)
Key	RSA 4096 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Configuration

Protocols

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

Cipher Suites

 # TLS 1.3 (suites in server-preferred order)

TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc073) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc072) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 (0xc0af) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xc0ad) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384 (0xc05d) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xc0ae) ECDH x25519 (eq. 3072 bits RSA) FS	128

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (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
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 : 0xc023
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc023
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc023
Sleeping POODLE	No (more info) TLS 1.2 : 0xc023
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV 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	**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)	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
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	x25519, secp256r1, x448, secp521r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 https://www.taty.com.ec/ (HTTP/1.1 200 OK)

Miscellaneous

Test date	Wed, 20 Oct 2021 22:49:04 UTC
Test duration	66.176 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	ec2-3-208-229-80.compute-1.amazonaws.com

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > www.tysfashion.com

SSL Report: www.tysfashion.com (185.230.60.102)

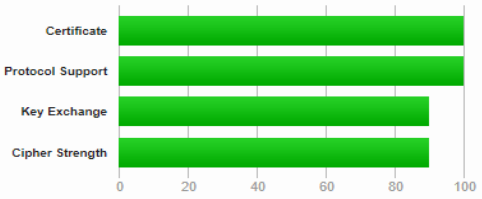
Assessed on: Fri, 01 Oct 2021 21:06:49 UTC | Hide | Clear cache

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.

This server supports TLS 1.3.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	tysfashion.com Fingerprint SHA256: 7b46ff5657e21bea3ed69130b2f64b7e957abfb08c171239b46930b0f1db891a Pin SHA256: PJBrFQIA4+jDbfVAy5WQ3fD7NSDatmjlpHCySHjOI4=
Common names	tysfashion.com
Alternative names	tysfashion.com www.tysfashion.com
Serial Number	1b2625041aaa0fd456b5791435b3c52e
Valid from	Mon, 20 Sep 2021 00:00:00 UTC
Valid until	Sun, 19 Dec 2021 23:59:59 UTC (expires in 1 month and 29 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Sectigo RSA Domain Validation Secure Server CA AIA: http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.sectigo.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 (4446 bytes)
Chain issues	None

#2

Subject	Sectigo RSA Domain Validation Secure Server CA Fingerprint SHA256: 7fa4ff68ec04a99d7528d5085f94907f4d1dd1c5381bacdc832ed5c960214676 Pin SHA256: 4a6cPehI7OG6cuDZka5NDZ7FR8a60d3auda+sKfg4Ng=
Valid until	Tue, 31 Dec 2030 23:59:59 UTC (expires in 9 years and 2 months)
Key	RSA 2048 bits (e 65537)
Issuer	USERTrust RSA Certification Authority
Signature algorithm	SHA384withRSA

#3

Subject	USERTrust RSA Certification Authority Fingerprint SHA256: 68b9c761219a5b1f01317844746665db61bbdb109e00f05ca9f74244ee5f5f52b Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4=
Valid until	Sun, 31 Dec 2028 23:59:59 UTC (expires in 7 years and 2 months)
Key	RSA 4096 bits (e 65537)
Issuer	AAA Certificate Services
Signature algorithm	SHA384withRSA

Configuration

Protocols

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

Cipher Suites

 # TLS 1.3 (suites in server-preferred order)

TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH x25519 (eq. 3072 bits RSA) FS **WEAK**	112
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (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
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 : 0xc013
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc013
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc013
Sleeping POODLE	No (more info) TLS 1.2 : 0xc013
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV 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	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1
Session resumption (caching)	No (IDs empty)
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** TOO SHORT (less than 180 days) max-age=120

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	x25519, secp256r1, secp384r1, secp521r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No

HTTP Requests

1 https://www.tysfashion.com/ (HTTP/1.1 200 OK)

Miscellaneous

Test date	Wed, 20 Oct 2021 22:53:34 UTC
Test duration	102.736 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	unallocated.60.wixsite.com

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > www.deprati.com.ec

SSL Report: www.deprati.com.ec

Assessed on: Fri, 01 Oct 2021 21:13:13 UTC | Hide | Clear cache

Scan Another >>

	Server	Test time	Grade
1	104.17.176.182 Ready	Fri, 01 Oct 2021 21:09:45 UTC **Duration:** 103.931 sec	B
2	104.17.177.182 Ready	Fri, 01 Oct 2021 21:11:29 UTC **Duration:** 104.46 sec	B

SSL Report v2.1.8

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	sni.cloudflaressl.com Fingerprint SHA256: 0832550bf1726dcf064e6988c3a229985ee5edaf807d2eb3b4ec65f4880ffeff Pin SHA256: PfigY0La7hUEQYUqIOQwUEz7hS9EbA6nDCcfaclg6c=
Common names	sni.cloudflaressl.com
Alternative names	deprati.com.ec *.deprati.com.ec sni.cloudflaressl.com
Serial Number	0208c5c13888201a716416883a95c595
Valid from	Thu, 08 Jul 2021 00:00:00 UTC
Valid until	Thu, 07 Jul 2022 23:59:59 UTC (expires in 8 months and 17 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Cloudflare Inc RSA CA-2 AIA: http://cacerts.digicert.com/CloudflareIncRSACA-2.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/CloudflareIncRSACA-2.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	2 (2921 bytes)
Chain issues	None

#2

Subject	Cloudflare Inc RSA CA-2 Fingerprint SHA256: aec863898f284d6cd4c6a3f6c3e6523480a359c33daf66fad3381849b6bb018b Pin SHA256: hS5jJ4P+iQUErBkvoWBQOd1T7VOAYlOVegvv1MzpxA=
Valid until	Tue, 31 Dec 2024 23:59:59 UTC (expires in 3 years and 2 months)
Key	RSA 2048 bits (e 65537)
Issuer	Baltimore CyberTrust Root
Signature algorithm	SHA256withRSA

Certificate #2: EC 256 bits (SHA256withECDSA)

Server Key and Certificate #1

Subject	sni.cloudflaressl.com Fingerprint SHA256: 47b837d27caa05873184e7064430ec954f04146c2df813162614608adf226422 Pin SHA256: SjO2FCBzN2SrQO6fQQBvN9GLkqc8Ftr8kLlZ3CNnfaAM=
Common names	sni.cloudflaressl.com
Alternative names	deprati.com.ec *.deprati.com.ec sni.cloudflaressl.com
Serial Number	0e2501c0092199c3eb2f656849cb685a
Valid from	Thu, 08 Jul 2021 00:00:00 UTC
Valid until	Thu, 07 Jul 2022 23:59:59 UTC (expires in 8 months and 17 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	Cloudflare Inc ECC CA-3 AIA: http://cacerts.digicert.com/CloudflareIncECCCA-3.crt
Signature algorithm	SHA256withECDSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/CloudflareIncECCCA-3.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	2 (2322 bytes)
Chain issues	None

#2

Subject	Cloudflare Inc ECC CA-3 Fingerprint SHA256: 3abbe63daf756c5016b6b85f52015fd8e6acbe277c5087b127a60563a841ed8a Pin SHA256: FEzVOUp4dF3gI0ZVPRJhFbSJVXR+uQmMH65xhs1glH4=
Valid until	Tue, 31 Dec 2024 23:59:59 UTC (expires in 3 years and 2 months)
Key	EC 256 bits
Issuer	Baltimore CyberTrust Root
Signature algorithm	SHA256withRSA

Configuration

Protocols

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

Cipher Suites

TLS 1.3 (server has no preference)

TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH x25519 (eq. 3072 bits RSA) FS	128
OLD_TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc14) ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
OLD_TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc13) ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (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
Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	Unknown (more info)
GOLDENDOODLE	Unknown (more info)
OpenSSL 0-Length	Unknown (more info)
Sleeping POODLE	Unknown (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV 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	Yes h2 http/1.1
NPN	Yes h2 http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	**Yes**

OCSP stapling	Yes
Strict Transport Security (HSTS)	Yes max-age=31536000 ; includeSubDomains
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	x25519, secp256r1, secp384r1, secp521r1 (server preferred order)
SSL 2 handshake compatibility	Yes
0-RTT enabled	No

HTTP Requests

1 https://www.deprati.com.ec/ (HTTP/1.1 200 OK)

Miscellaneous

Test date	Wed, 20 Oct 2021 22:56:29 UTC
Test duration	103.115 seconds
HTTP status code	200
HTTP server signature	cloudflare
Server hostname	-