

Cyber Health Check Report



jte.com.sg

18 AUGUST 2026 11:58:26

Website Connection is insufficiently secured.



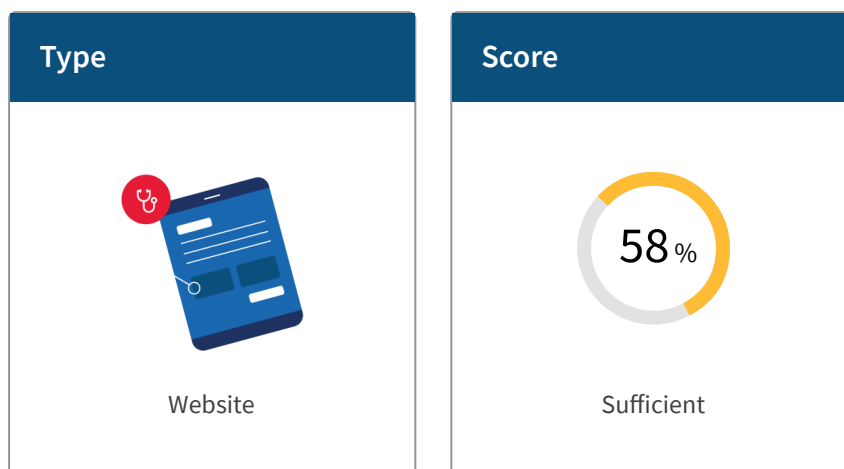
Web Domain is insufficiently or not secured.



Modern IP Addresses and Network Routing Security is partially available.



Website uses PQC to protect against quantum threats.



Disclaimer

This report is generated and provided to you subject to the Internet Hygiene Portal's Terms of Use and this Disclaimer. By utilising the Internet Health Lookup Tool, you are deemed to have consented to be bound by the Internet Hygiene Portal's Terms of Use and this Disclaimer. The Internet Hygiene Portal's Terms of Use shall prevail in the event of any inconsistency between the Internet Hygiene Portal's Terms of Use and this Disclaimer.

Achieving a sufficiently secured result in this report means that a website, e-mail service, or internet connection complies with our curated internet hygiene baseline standards. More information about the curated internet hygiene baseline standards can be found at para 22 under the 'Authorisation of Use and Disclaimer of Internet Health Lookup Tools and Reports' in the Terms of Use. The information generated in this report is non-binding and meant to be informative in nature, and are not intended to exhaustively identify or definitively reflect the scanned domain's level of cybersecurity and/or resistance against cyberattacks. Users are encouraged to seek professional advice where required.

Secure Website Connection

Try harder! Your website connection is insufficiently secured.

Improve the security of your website connection to protect the data of your visitors against eavesdropping (theft of information) and tampering (altering of data for malicious activities).

Expand the checks below for more details:

HTTP Configuration Security (HTTPS)

✔ HTTPS Existence

Scan Result:

Your website offers secure HTTPS configuration.

Web Server IP Address	185.199.111.153
HTTPS Existence	Yes

Check Description:

Hypertext Transfer Protocol Secure (HTTPS) enables secure data in transit communication between the client and the server. All your website contents should be delivered via HTTPS.

Validation:

The scanner checks if the URI instance of your website can be accessed by HTTPS protocol.

For more information:

[\[IETF\] RFC 7230 - Hypertext Transfer Protocol \(HTTP/1.1\): Message Syntax and Routing \(https URI Scheme\)](#)

[\[OWASP\] Transport Layer Protection](#)

Configuration Guides:

[\[AWS\] Enable HTTPS traffic and verifying the certificates on AWS CloudHSM](#)

[\[AWS\] Using HTTPS with Amazon CloudFront](#)

[\[AWS\] Create HTTPS listener for AWS Application Load Balancer](#)

[\[Google\] Use Hypertext Transfer Protocol Secure \(HTTPS\) on your domain](#)

[\[Microsoft\] Enabling TLS 1.2](#)

✘ HTTPS Redirection

Scan Result:

Your web server is not configured to redirect visitors from HTTP to HTTPS on the same domain.

Web Server IP Address	185.199.111.153
HTTPS Redirection	No

Impact:

Even with TLS encryption enabled, visitors can still access your website with HTTP protocol if redirection is not configured.

Recommendation:

Visitors attempting to access your website with HTTP should be automatically redirected over HTTPS. Check with your System Administrator or your hosting provider to enable HTTPS redirection on your web server or reverse proxy configuration.

Check Description:

HTTPS redirection ensures that your website can only be accessed via HTTPS protocol. Your website (1) should automatically redirect visitors from HTTP to HTTPS or (2) offer support for only HTTPS.

During redirection, website should upgrade from HTTP to HTTPS on the same domain before URL forwarding (redirecting to another domain). Proper implementation of HTTPS redirection can protect user from potential vulnerabilities, such as;

- Downgrade attacks where attackers try to force the user's web browser to use HTTP instead of HTTPS.
- SSL stripping attacks where attackers intercept HTTPS traffic and downgrade it to HTTP, potentially redirecting users to malicious website.
- Man-in-the-Middle attacks where attackers intercept user's traffic and read or modify transmitted data.

This configuration also ensures that the HSTS policy will be accepted by the user's web browser.

Validation:

The scanner checks if your web server performs redirection to HTTPS on the same domain.

Example of correct redirection sequence;

- `http://csa.gov.sg -> https://csa.gov.sg -> https://www.csa.gov.sg`
- `http://www.csa.gov.sg -> https://www.csa.gov.sg`

For more information:

[\[Mozilla\] HTTP Redirection](#)

[\[OWASP\] Transport Layer Protection](#)

[\[OWASP\] Insecure Transport](#)

Configuration Guides:

[\[AWS\] Configuring HTTP-to-HTTPS redirection for AWS Application Load Balancer](#)

[\[Google\] Setting up HTTP-to-HTTPS redirection for global external HTTP\(S\) load balancer](#)

HTTP Strict Transport Security (HSTS)

Scan Result:

Your web server is not configured with a HSTS policy.

Web Server IP Address	185.199.111.153
HSTS Options	None
Pass	No

Impact:

Setting up HTTPS Redirection is not enough as it still provides a window of opportunity for attackers to access your website without secure connection. HSTS should be implemented to completely ensure that visitors are only able to connect through HTTPS.

Recommendation:

Check with your System Administrator or your hosting provider to include the following on web server or reverse proxy configuration:

- Include HSTS with max-age $\geq$ 1yr
- Include Sub Domains as part of the response header.

Check Description:

HTTP Strict Transport Security (HSTS) is a response HTTP header that protects your website against protocol downgrade attacks. When HSTS is implemented, web browsers are informed that they should only interact with HTTPS connection. It is recommended to implement HSTS to force a secure connection.

Validation:

The scanner checks if your website offers HSTS. It checks for the existence of a "strict transport security header" with max-age $\geq$ 1yr, and the existence of "include subdomains" in your website's response header.

For more information:

[\[IETF\] RFC 6797 - HTTP Strict Transport Security \(HSTS\)](#)

[\[Mozilla\] HTTP Headers](#)

[\[OWASP\] HTTP Strict Transport Security Cheat Sheet](#)

Configuration Guides:

[\[Internet Society\] Configuring HSTS on Apache web server](#)

[\[Internet Society\] Configuring HSTS on NGINX web server](#)

[\[Internet Society\] Configuring HSTS on web server with CDN](#)

[\[AWS\] Adding security HTTP security headers on Amazon CloudFront - HSTS](#)

[\[Google\] Web security best practices - HSTS](#)

[\[Microsoft\] Configuring security headers with Azure Front Door](#)

HTTP Compression

Scan Result:

Your web server is configured to enable HTTP Compression.

Web Server IP Address	185.199.111.153
HTTP Compression	Enabled

Impact:

With HTTP Compression enabled, your website is susceptible to BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext) - attacks. BREACH attacks steal information about how data is encrypted from HTTPS-enabled web applications.

Recommendation:

Check with your System Administrator or hosting provider to:

- Disable HTTP Compression
- Provide CSRF token for sensitive information
- Limit the rate of requests

Check Description:

HTTP Compression can be used to increase website performance. With HTTP Compression enabled, web pages are compressed before sending the responses out. However, the attackers take advantage of the compression size to monitor the traffic between your website and your visitors. Hence, HTTP Compression support is not recommended, and it should be disabled.

Validation:

The scanner checks if your website's response header for "Content-Encoding" supports HTTPS Compression.

For more information:

[\[IETF\] RFC 7540 Hypertext Transfer Protocol Version 2 \(HTTP/2\) \(Use of Compression\)](#)

[\[OWASP\] Transport Layer Protection](#)

Transport Layer Security (TLS)

✓ TLS Protocols

Scan Result:

Your web server uses secure TLS protocols with strong security strength.

Web Server Address	185.199.111.153
Protocol	TLS 1.3
Strength	Strong

Web Server Address	185.199.111.153
Protocol	TLS 1.2
Strength	Sufficient

Check Description:

TLS Protocols are used to protect the data transmitted over the internet against eavesdropping. Websites should only support strong TLS Protocols to enhance secure data transmission and prevent data breaches.

Validation:

The scanner checks your web server's supported TLS Protocols and scores them based on their security strength. If no TLS Protocol is found, the system returns a bad score.

For more information:

The following TLS Protocols support are based on [NIST Special Publication 800-52 Revision 2](#).

- **Best:** TLS 1.3
- **Sufficient:** TLS 1.2
- **Bad:** TLS 1.1, TLS 1.0, SSLv

For more information:

[\[IETF\] RFC 8996 Deprecating TLS 1.0 and TLS 1.1](#)

Configuration Guides:

[\[Internet Society\] Configuring TLS 1.3 on Apache web server](#)

[\[Internet Society\] Configuring TLS 1.3 on NGINX web server](#)

[\[Internet Society\] Disabling TLS 1.0 and 1.1 on Apache web server](#)

[\[Internet Society\] Disabling TLS 1.0 and 1.1 on NGINX web server](#)

[\[Internet Society\] Disabling TLS 1.0 and 1.1 on web server with CDN](#)

[\[Microsoft\] Disabling TLS 1.0 and 1.1 for Microsoft 365](#)

TLS Cipher Suites

Scan Result:

Not all your web servers' TLS Cipher Suites use strong security strength.

Web	
Server Address	185.199.111.153
Cipher	TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA[secp256r1], TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256[secp256r1], TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA[secp256r1]
Strength	Weak
Reason	TLS_RSA_WITH_AES_256_CBC_SHA: Key exchange RSA does not meet forward secrecy requirements. Cipher mode CBC is not in the approved list. Uses SHA-1 for message authentication. TLS_RSA_WITH_AES_128_GCM_SHA256: Key exchange RSA does not meet forward secrecy requirements. TLS_RSA_WITH_AES_128_CBC_SHA: Key exchange RSA does not meet forward secrecy requirements. Cipher mode CBC is not in the approved list. Uses SHA-1 for message authentication. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA[secp256r1]: Cipher mode CBC is not in the approved list. Uses SHA-1 for message authentication. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256[secp256r1]: Cipher mode CBC is not in the approved list. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA[secp256r1]: Cipher mode CBC is not in the approved list. Uses SHA-1 for message authentication.

Impact:

Weak TLS Cipher Suites are vulnerable to attacks. It provides an opportunity for attackers to intercept/eavesdrop on the data in transit between your web servers and your visitor's browsers. Hackers can then use the data for malicious activities.

Recommendation:

It is important to use secure TLS Cipher Suites and disable the ones with weak protection. You can refer to articles under for more information to view the list of secure TLS Cipher Suites. Check with your System Administrator or your hosting provider to review your servers' TLS Cipher Suites and upgrade the weak ones if feasible.

Check Description:

TLS Cipher Suites are used along with the TLS Protocols to protect the data transmitted over the internet against eavesdropping. Websites should only support strong TLS Cipher Suites to enhance secure data transmission and prevent data breaches.

Validation:

The scanner checks your web servers' supported TLS Cipher Suites and score them based on their security strength. It also includes the check for approved Ephemeral Ciphers curves. If your servers are using Ephemeral Ciphers with insecure curves, the Ciphers would be ranked as bad.

For more information:

[\[IANA\] Transport Layer Security \(TLS\) Parameters](#)

[\[IETF\] RFC 5289 TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode \(GCM\)](#)

[\[Mozilla\] Security/Server Side TLS](#)

[\[NIST\] Special Publication 800-52 Revision 2 \(Cipher Suites\)](#)

Configuration Guides:

[\[Internet Society\] Configuring TLS cipher order on Apache web server](#)

[\[Internet Society\] Configuring TLS cipher order on NGINX web server](#)

[\[Microsoft\] Enabling TLS 1.2 support for Azure AD TLS 1.0/1.1 deprecation](#)

 TLS Compression**Scan Result:**

Your web server is configured to disable TLS Compression.

Web Server IP Address	185.199.111.153
TLS Compression	Disabled

Check Description:

TLS Compression should be disabled to protect your website against CRIME (Compression Ratio Info-leak Made Easy) attacks in which sensitive information can be recovered by an attacker.

Validation:

The scanner checks if your web server has TLS compression support.

For more information:

[\[NIST\] Special Publication 800-52 Revision 2 \(Compression Methods\)](#)

[\[OWASP\] Transport Layer Protection](#)

 Downgrade Attack Prevention**Scan Result:**

Your web server supports downgrade attack prevention.

Web Server IP Address	185.199.111.153
Downgrade Attack Prevention	Yes

Check Description:

Downgrade Attack Prevention ensures that the client and the server communicate using secure protocol versions by preventing TLS downgrade. It is one of the mitigations against [MITM \(man in the middle\) attacks](#) in which attackers can obtain the data in transit information and use it for malicious activities. TLS Signaling Cipher Suite Value (SCSV) is used to prevent downgrade attacks so it should be supported by your web server.

Validation:

The cyber health lookup tool checks if your web server supports TLS_FALLBACK_SCSV mechanism.

For more information:

[\[NIST\] Special Publication 800-52 Revision 2 \(Fallback Signaling Cipher Suite Value \(SCSV\)\)](#),

[\[OWASP\] Transport Layer Protection](#)

✓ Secure Renegotiation

Scan Result:

Secure renegotiation is enabled on your web server.

Web Server IP Address	185.199.111.153
Secure Renegotiation	Enabled

Check Description:

Renegotiation is a process where parties wish to send more data even after the session has expired and therefore requires authentication. However, renegotiation can be susceptible to [MITM \(man in the middle\) attacks](#). Only the latest protocol TLS 1.3 forbids renegotiation. To reduce the susceptibility to MITM attacks, secure renegotiation for TLS version 1.2 and below should be enabled.

Validation:

The scanner checks if the server has secure TLS renegotiation enabled.

For more information:

[\[IETF\] RFC 5746 Transport Layer Security \(TLS\) Renegotiation Indication Extension \(Server Behavior: Legacy \(Insecure\) Renegotiation\)](#),

[\[IETF\] RFC 5746 Transport Layer Security \(TLS\) Renegotiation Indication Extension \(Client Behavior: Legacy \(Insecure\) Renegotiation\)](#),

[\[NIST\] Special Publication 800-52 Revision 2 \(Renegotiation Indication\)](#)

[\[OWASP\] WSTG v4.1 Testing for Weak SSL TLS Ciphers Insufficient Transport Layer Protection](#)

✓ Client-Initiated Renegotiation

Scan Result:

Client-initiated renegotiation is disabled on your web server.

Web Server IP Address	185.199.111.153
Client Initiated Renegotiation	Disabled

Check Description:

If Client-Initiated Renegotiation is enabled, your web server can be overloaded with renegotiation requests which open a window for [Denial of Service](#).

Validation:

The scanner checks if the web server has disabled client-initiated renegotiation.

For more information:

[\[IETF\] RFC 5746 Transport Layer Security \(TLS\) Renegotiation Indication Extension \(Client Behaviour: Legacy \(Insecure\) Renegotiation\)](#)

[\[NIST\] Special Publication 800-52 Revision 2 \(Renegotiation Indication\)](#)

[\[NIST\] CVE-2011-1473](#)

[\[OWASP\] WSTG v4.1 Testing for Weak SSL TLS Ciphers Insufficient Transport Layer Protection](#)

Session Resumption

Scan Result:

Session resumption is enabled on your web server.

Web Server IP Address	185.199.111.153
Session Resumption	Enabled

Impact:

Enabling session resumption renders your web server to be susceptible to replay attacks. Replay attacks occur when a malicious actor eavesdrops on the secure network communication, intercepts it, and thereafter replays the data transmission between the web server and the visitor's browser for malicious activities.

Recommendation:

It is recommended to disable session resumption support if it is not necessary for the transactions. Otherwise, implement security controls such as frequent rotation of Session Ticket Encryption Keys, reducing session cache lifetimes, and secure handling of keys before, during, and after the usage.

Check with your System Administrator or your hosting provider regarding the removal of session resumption support or implementation of security controls for session resumption support.

Check Description:

Session resumption is a mechanism where an encrypted session between the client and the web server can be resumed. With session resumption support, the handshake between the client and your web server is significantly reduced. However, it can also open a window for replay attacks (data transmission is maliciously repeated) if not configured properly.

Validation:

The scanner checks if your web server does not support session resumption.

For more information:

[\[NIST\] Special Publication 800-52 Revision 2 \(Session Resumption and Early Data\)](#)

TLS Early Data Indication

Scan Result:

Early Data Indication is disabled on your web server.

Web Server IP Address	185.199.111.153
Early Data Indication	Disabled

Check Description:

Early Data Indication is a TLS extension for TLS 1.3 that helps to improve performance connection. However, it also opens a window for replay attacks (data transmission is maliciously repeated).

Validation:

The scanner checks if your web server does not support Early Data Indication.

For more information:

[\[NIST\] Special Publication 800-52 Revision 2 \(Session Resumption and Early Data\)](#)

[\[IETF\] RFC 8446 The Transport Layer Security \(TLS\) Protocol Version 1.3 \(0-RTT and Anti-Replay\)](#)

Certificate

Certificate Validity

Scan Result:

Your website certificates have valid dates.

Web Server Address	185.199.111.153
Serial Number	596767508172960559059046830249601362780267
Subject	CN=jte.com.sg
Issuer	CN=YR1,O=Let's Encrypt,C=US
Validity	09 Aug 2026 - 07 Nov 2026

Check Description:

Valid certificate dates prove that your website's certificate is using the latest security standards and confirm the domain control of your organisation's identity. Your website certificate dates should be valid with a maximum 1 year or less validity period based on the [National Cybersecurity Center of Excellence \(NCCoE\)](#).

Validation:

The system checks if any of your website's certificate dates has expired.

For more information:

[\[CSA\] Importance of Valid Digital Certificates](#)

[\[NIST\] Special Publication 1800-16A - Securing Web Transactions TLS Server Certificate Management \(Validity Periods\)](#)

Configuration Guides:

[\[AWS\] AWS Certificate Manager](#)

[\[Google\] Using Google-managed SSL certificates](#)

[\[Microsoft\] Adding and managing TLS/SSL certificates in Azure App Service](#)

 Public Key Algorithm**Scan Result:**

Your website certificates uses secure public key algorithms.

Web Server Address	185.199.111.153
Serial Number	596767508172960559059046830249601362780267
Subject	CN=jte.com.sg
Issuer	CN=YR1,O=Let's Encrypt,C=US
Public Key Algorithm	RSAPublicKey
Strength	Preferred

Check Description:

A website's certificate contains a public key that is used to authenticate your web server's identity. The algorithm used to sign the public key must be secure enough to be resistant to certificate forgery attacks in which attackers can spy on the data being transmitted.

Validation:

The scanner checks if all your website's certificates use secure public key algorithms.

For more information:

The following algorithms are based on [NIST Special Publication 800-131A Revision 2 \(Table 2: Approval Status of Algorithms Used for Digital Signature Generation and Verification\)](#).

Good:**RSA**

Key Size $\geq$ 2048 bits

Elliptic Curve

Key Size $\geq$ 224 bits

DSA

Key Size = (2048, 224), or (2048, 256) or (3072, 256) bits

Bad:

Other groups

 Signature Hash Algorithm**Scan Result:**

Your website certificates use secure signature hash algorithms.

Web Server IP Address	185.199.111.153
Serial Number	596767508172960559059046830249601362780267
Subject	CN=jte.com.sg
Issuer	CN=YR1,O=Let's Encrypt,C=US
Hash Algorithm	sha256
Strength	Preferred

Check Description:

Hashing is used during the creation of a digital signature to provide integrity to the certificate. The signature hash algorithm must be secure enough to be resistant to certificate forgery attacks in which attackers can spy on the data being transmitted.

Validation:

The scanner checks if all your website's certificates use secure signature hash algorithms.

For more information:

The following algorithms are based on [NIST Special Publication 800-131A Revision 2 \(Table 8: Approval Status of Hash Functions\)](#).

Good: SHA-3 family (SHA3-224, SHA3-256, SHA3-384, and SHA3-512), SHA-2 family (SHA224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256)

Bad: Other groups

 Valid Domain Name**Scan Result:**

The domain name in your website certificates matches your website's domain name.

Web Server IP Address	185.199.111.153
Correct Domain Name	Yes

Check Description:

The domain name (subject name) of a website's certificate is used to identify to which the certificate is issued. Therefore, the domain name (subject name) of your website's certificate should match your website's domain name.

Validation:

The scanner checks if your website certificates match your website's domain name.

For more information:

[\[NIST\] Special Publication 1800-16A - Securing Web Transactions TLS Server Certificate Management \(Certificate Request Reviews – Registration Authority\)](#).

[\[OWASP\] Transport Layer Protection Cheat Sheet \(Use of Correct Domain Name\)](#)

 Extended Validation (EV)**Scan Result:**

Not all your website certificates have Extended Validation (EV).

Web Server IP Address	185.199.111.153
Extended Validation	No

Impact:

EV certificates provide a stronger identity assurance to your visitors as it would validate that the website domain is duly incorporated and in good standing.

Recommendation:

You can procure EV certificates from a certificate authority or check with your hosting provider regarding the procurement process.

Check Description: Extended Validation (EV) certificates provide a higher level of verifying the entity of the certificate requestor which ensures stronger identity assurance to website visitors by providing recourse against fraudulent transactions in the website.

Validation:

The scanner checks if your website has EV certificates.

For more information:

[\[NIST\] Special Publication 1800-16A - Securing Web Transactions TLS Server Certificate Management \(Certificate Authorities\)](#)

[\[OWASP\] Transport Layer Protection Cheat Sheet \(Consider the use of Extended Certificates\)](#)

Legacy Symantec Anchor

Scan Result:

Your website certificates do not support a distrusted Symantec anchor.

Web Server IP Address	185.199.111.153
Legacy Symantec Anchor	No

Check Description:

Browser vendors are deprecating existing Symantec certificates. To comply with this requirement, your website certificates should not have a distrusted Symantec Anchor.

Validation:

The scanner checks if your website's certificate chain contains a distrusted Symantec Anchor.

For more information:

[\[NIST\] Special Publication 1800-16A - Securing Web Transactions TLS Server Certificate Management \(Crypto Agility\)](#)

[\[Google\] Distrust of Symantec Anchor](#)

[\[Mozilla\] Delaying Symantec Certificate Distrust](#)

[\[Apple\] Distrust Symantec Certificate](#)

HTTP Security Headers

X-Frame-Options

Scan Result:

Your web server does not offer X-Frame-Options.

Web Server IP Address	185.199.111.153
X-Frame-Options	None
Pass	No

Impact:

Your visitors are susceptible to clickjacking attacks wherein they are tricked to click on untrusted content.

Recommendation:

Check with your System Administrator or your hosting provider to set the following on web server or reverse proxy configuration:

Implement X-Frame-Options as part of the response header with the valid values below:

- DENY
- SAME-ORIGIN

Check Description:

X-Frame-Options is a response HTTP header that protects your website against [clickjacking](#) in which attackers deceive users with hidden links that can be used to retrieve sensitive information.

Validation:

The scanner checks if your website offers X-Frame-Options.

It checks for the existence of "X-Frame-Options" in your website's response header with the valid values below:

- DENY
- SAME-ORIGIN

For more information:

[\[Mozilla\] HTTP Headers](#)

[\[OWASP\] Secure Headers Project](#)

[\[OWASP\] HTTP Headers Cheat Sheet](#)

Configuration Guides:

[\[Internet Society\] Configure HTTP security headers on NGINX web server – X-Frame-Options](#)

[\[Internet Security\] Configuring HTTP security headers on your Apache web server – X-Frame-Options](#)

[\[AWS\] Adding security HTTP security headers on Amazon CloudFront – X-Frame-Options](#)

[\[Google\] Web security best practices – X-Frame-Options](#)

[\[Microsoft\] Configuring security headers with Azure Front Door](#)

X-Content-Type-Options

Scan Result:

Your website does not offer X-Content-Type-Options.

Web Server IP Address	185.199.111.153
X-Content-Type-Options	None
Pass	No

Impact:

Your website is susceptible to MIME-type sniffing attacks wherein malicious actors can manipulate the content rendered on your website and use it to perform malicious activities that may trick your visitors to click on malicious content.

Recommendation:

Check with your System Administrator or your hosting provider to set the following on your web server or reverse proxy configuration:

- Implement X-Content-Type-Options with the value “no sniff” as part of the response header.
- Ensure to set the correct content-type header.

Check Description:

X-Content-Type-Options is a security protects your website against [MIME-type sniffing](#) (malicious manipulation of website contents).

Validation:

The scanner checks if your website offers X-Content-Type-Options. It checks for the existence of “x-content-type-options”: "nosniff" in your website's response header.

For more information:

[\[Mozilla\] HTTP Headers](#)

[\[OWASP\] Secure Headers Project](#)

[\[OWASP\] HTTP Headers Cheat Sheet](#)

Configuration Guides:

[\[Internet Society\] Configure HTTP security headers on NGINX web server – X-Content-Type-Options](#)

[\[Internet Security\] Configuring HTTP security headers on your Apache web server – X-Content-Type-Options](#)

[\[AWS\] Adding security HTTP security headers on Amazon CloudFront – X-Content-Type-Options](#)

[\[Google\] Remediating Web Security Scanner findings – X-Content-Type-Options](#)

i Content-Security-Policy

Scan Result:

Your website does not offer Content-Security-Policy.

Web Server IP Address	185.199.111.153
Content-Security-Policy	None
Pass	No

Impact:

Your website is susceptible [to code injection](#), [XSS](#), [clickjacking](#) attacks wherein malicious actors can trick your visitors to execute malicious codes.

Recommendation:

Check with your System Administrator or your hosting provider to set Content-Security-Policy as part of the response header on your web server or reverse proxy configuration.

Check Description:

Content-Security-Policy is a response HTTP header that defends your website from [code injection](#), [XSS](#), [clickjacking](#) by informing the browsers what content sources can be trusted.

Validation:

The scanner checks if your web server has Content-Security-Policy.

It checks for the existence of "content-security-policy" in your website's response header.

For more information:

[\[Mozilla\] HTTP Headers](#)

[\[OWASP\] Secure Headers Project](#)

[\[OWASP\] HTTP Headers Cheat Sheet](#)

Configuration Guides:

[\[Internet Society\] Configure HTTP security headers on NGINX web server – Content-Security-Policy](#)

[\[AWS\] Adding security HTTP security headers on Amazon CloudFront – Content-Security-Policy](#)

[\[Google\] Web security best practices – Content-Security-Policy](#)

[\[Microsoft\] Add security headers with Azure Front Door](#)

i X-Permitted-Cross-Domain-Policies

Scan Result:

Your website does not offer X-Permitted-Cross-Domain-Policies.

Web Server IP Address	185.199.111.153
X-Permitted-Cross-Domain-Policies	None
Pass	No

Impact:

Your website's resources are susceptible to resource abuse by malicious actors for illicit purposes.

Recommendation:

Check with your System Administrator or your hosting provider to set X-Permitted-Cross-Domain-Policies as part of the response header on your web server or reverse proxy configuration.

Check Description:

X-Permitted-Cross-Domain-Policies is a response HTTP header that instructs the browsers on how requests should be handled across domains.

Validation:

The scanner checks if your website offers X-Permitted-Cross-Domain-Policies.

It checks for the existence of "x-permitted-cross-domain-policies" in your website's response header.

For more information:

[\[Mozilla\] HTTP Headers](#)

[\[OWASP\] Secure Headers Project](#)

[\[OWASP\] HTTP Headers Cheat Sheet](#)

Referrer-Policy

Scan Result:

Your website does not offer Referrer-Policy.

Web Server IP Address	185.199.111.153
Referrer-Policy	None
Pass	No

Impact:

Without Referrer-Policy configured, sensitive information on your website could be leaked and the privacy of your visitors might be affected.

Recommendation:

Check with your System Administrator or your hosting provider to implement Referrer-Policy as part of the response header on your web server or reverse proxy configuration.

Check Description:

Referrer-Policy is a response HTTP header that prevents the leaking of internal URLs via the Referrer header.

Validation:

The scanner checks if your website offers Referrer Policy.

It checks for the existence of "referrer-policy" in your website's response header.

For more information:

[\[Mozilla\] HTTP Headers](#)

[\[OWASP\] Secure Headers Project](#)

[\[OWASP\] HTTP Headers Cheat Sheet](#)

Configuration Guides:

[\[Internet Society\] Configure HTTP security headers on NGINX web server – Referrer-Policy](#)

[\[Internet Society\] Configuring HTTP security headers on your Apache web server – Referrer-Policy](#)

[\[Google\] Remediating Web Security Scanner findings – Referrer-Policy](#)

Web Domain Security

Try harder! Your web domain is insufficiently or not secure because it is not signed and validated with Domain Name System Security Extensions (DNSSEC).

Implement DNSSEC to protect your visitors from DNS spoofing (redirection to malicious websites).

Expand the checks below for more details:

DNSSEC

DNSSEC Validity

Scan Result:

Your web domain's DNSSEC is either not signed or invalid.

Domain	jte.com.sg				
Root DNSSEC Status	Unsigned				
DNSSEC Category	UnsignedAtParent				
Root Reason	No DS found at parent for the child zone.				
Root Failure At	jte.com.sg (com.sg)				
Chain Details	Chain No	Domain	Record Type	Signature Status	Zone Status
	1.	jte.com.sg	Parent	—	—

Impact:

Without DNSSEC, your visitors are vulnerable to DNS spoofing (redirection to malicious websites).

Recommendation:

In order for your domain to implement DNSSEC properly, it must be DNSSEC signed, and your domain registrar and hosting provider must support DNSSEC. To help improve your website's credibility, check with your Domain Registrar and/or DNS Hosting Provider regarding your domain's DNSSEC support.

Check Description:

DNS Security Extensions (DNSSEC) adds an authentication layer to your DNS to guarantee that your visitors are directed to your website, preventing DNS spoofing or redirection to malicious websites. A domain's DNSSEC status has to be signed and validated to be secured.

Validation:

The scanner checks the DNSSEC status of your web domain.

Valid DNSSEC Status:

- **Secure DNSSEC (signed and validated)** indicates that the zone has been signed and the DS record has been published and configured correctly.

Invalid DNSSEC Status:

- **Indeterminate DNSSEC** indicates an unknown status. The verification is unable to determine if there is a DNSSEC Resource Record.
- **Unsigned DNSSEC** indicates that the DNSSEC is not fully deployed. It could be caused by a partial deployment of DS Record. Zone owners need to upload their DS Record to the registrar for it to be considered fully deployed.
- **Bogus DNSSEC** may indicate an attack, but it could also be caused by a configuration error by your domain provider.

For more information:

[\[CSA\] Technical Advisory on DNSSEC](#)

[\[ICANN\] What is DNSSEC?](#)

[\[IETF\] RFC 4035 - Protocol Modifications for the DNS Security Extensions \(Determining Security Status of Data\)](#)

[\[NIST\] Special Publication 800-81-2 - Secure Domain Name System \(DNS\) Deployment Guide \(9.7.1 Recording and Communicating Results of Signature Verification\)](#)

Configuration Guides:

[\[Internet Society\] Configuring DNSSEC for web server using either Apache or NGINX](#)

[\[AWS\] Configuring DNSSEC for a domain](#)

[\[AWS\] Configuring DNSSEC signing and validation with Amazon Route 53](#)

[\[Google\] Setting up DNSSEC Security for Google Domains](#)

[\[Microsoft\] Overview of DNSSEC](#)

Modern IP Address and Network Security

Your web server supports some modern IP standards. However, one or more checks did not fully pass.

Having IPv6 and valid RPKI (ROA) information help improve routing security and long-term reachability. While your current configuration is sufficient for operation, completing the remaining items will improve reliability and security.

Expand the checks below for more details.

IPv6

IPv6 Existence

Scan Result:

Your web server has no IPv6 support.

Domain	jte.com.sg
IPv6 Address	None

Impact:

Your website might have limited device accessibility in the future.

Recommendation:

1. Check from your hosting provider if they support IPv6. If it is not supported, you may look for a hosting provider that supports IPv6.
2. If your hosting provider supports IPv6, obtain an IPv6 address for your web server and name server from your hosting provider.

Check Description:

IPv6 is the latest version of the Internet Protocol which will eventually replace IPv4. In order for other devices to discover your website over IPv6, a DNS record type AAAA is pointed to your web server's IPv6 address.

Validation:

The scanner checks if your web server has at least one AAAA DNS record type.

For more information:

[\[ICANN\] What is IPv6?](#)

[\[IETF\] RFC 3596 - DNS Extensions to Support IP Version 6 \(New resource record definition and domain\).](#)

[\[Internet Society\] IPv6](#)

[\[NIST\] Special Publication 800-119 - Guidelines for the Secure Deployment of IPv6 \(3.7.2 DNS Specification Overview\)](#)

Configuration Guides:

[\[Internet Society\] – Configuring IPv6 on your Apache web server](#)

[\[Internet Society\] – Configuring IPv6 on your NGINX web server](#)

[\[Internet Society\] – Configuring IPv6 on web server with CDN](#)

[\[AWS\] Designing an IPv6 AWS Cloud network](#)

[\[Microsoft\] Configuring IPv6 in Windows](#)

🚫 IPv6 Reachability

The check was not performed because its parent check has a failed result.

IPv6 Address	None
--------------	------

Check Description:

IPv6 is the latest version of the Internet Protocol which will eventually replace IPv4. Having IPv6 correctly configured enables your web servers to be able to connect to devices that support it.

Validation:

IPv6 Existence is a pre-requisite for this check. If IPv6 Existence is passed, the scanner checks if your web servers are reachable over IPv6.

For more information:

[\[ICANN\] What is IPv6?](#)

[\[IETF\] RFC 3596 - DNS Extensions to Support IP Version 6 \(New resource record definition and domain\)](#)

[\[Internet Society\] IPv6](#)

[\[NIST\] Special Publication 800-119 - Guidelines for the Secure Deployment of IPv6 \(3.7.2 DNS Specification Overview\)](#)

RPKI

📘 RPKI (ROA) Validation

Scan Result:

Your web domain RPKI (ROA) is published.

Domain	jte.com.sg
Detected Origin ASN	AS54113
Detected BGP Prefix	185.199.110.0/24, 185.199.111.0/24, 185.199.108.0/24, 185.199.109.0/24
ROA Status	Valid

Check Description:

RPKI (ROA) is a security framework that allows network operators to verify that an Autonomous System is authorized to announce a specific IP prefix. This helps prevent route hijacking and accidental misconfigurations on the global internet.

Validation:

The cyber health lookup tool retrieves your domain's DNS records, maps the IP address to its announcing ASN and prefix, and checks this information against published RPKI (ROA) data. The validation confirms whether the detected prefix and origin ASN are covered by a valid ROA.

For more information:

[What is RPKI ROA?](#)

Post-Quantum Cryptography

Great job! Your web server uses post-quantum cryptography to secure the TLS connection, providing protection against quantum-enabled threats and helping ensure quantum-resilient communications as quantum computing evolves. Expand below for more information.

PQC

i Post-Quantum Cryptography

Scan Result:

Your web server employs PQC or hybrid cryptography in its TLS key exchange, providing protection against both classical and quantum-enabled attacks.

Domain	jte.com.sg
Matched Key Exchange	X25519MLKEM768
Matched Signature	None

Check Description:

Post-quantum cryptography (PQC) refers to cryptographic algorithms designed to be resistant to attacks by both classical and quantum computers, enabling secure key exchange and digital signatures even in the presence of powerful quantum computing capabilities. Adopting PQC helps protect TLS communications against quantum threats and supports long-term confidentiality and authentication.

Validation:

The Cyber Health Lookup tool analyses the TLS handshake of your web server to determine whether the key exchange uses post-quantum or hybrid (classical + PQC) cryptography. Although digital signatures are also assessed and are important for overall quantum-safe security, the PQC scan result is based solely on the key exchange component.

If the Digital Signature is matched:

Your web server uses post-quantum or hybrid cryptographic signatures for TLS authentication, helping to protect server identity against both classical and quantum-enabled attacks.

If the Digital Signature is not matched:

Your web server relies on conventional cryptographic signatures for TLS authentication and does not use post-quantum cryptography (PQC). In the absence of PQC, a future quantum-capable adversary could potentially forge valid digital signatures, enabling server impersonation or fraudulent certificate issuance. Consider adopting post-quantum or hybrid signature algorithms in your digital certificates to strengthen quantum resilience. Adoption of PQC signature algorithms remains limited due to certificate ecosystem readiness and integration challenges, though deployment is expected to grow as support improves.

For more information:

[\[NIST\] What is Post-Quantum Cryptography?](#)