WebCheckApp

Website Security Scanner

google.com

Deep Scan Report — 27 categories scanned

Scanned: 03 Apr 2026, 19:30 UTC

Generated: 04 Apr 2026, 00:30 UTC

webcheckapp.com

72
/100

B-

OVERALL GRADE

12 critical | 25 warnings | 70 passed

12 issues require immediate attention.

SSL & HTTPS	58
Security Headers	36
DNS & Email Security	83
Performance & SEO	75
Content & CMS	100
Exposed Files	100

Executive Summary

We performed a comprehensive security analysis of **google.com** across 20 categories. The website received an overall score of **72/100** (grade **B-**), with 12 critical issues, 25 warnings, and 70 passed checks.

Overall assessment: google.com has a reasonable security foundation but there is room for improvement. Several issues were identified that could expose the website or its users to unnecessary risk. We recommend addressing the critical issues first, followed by the warnings.

✓ **Strong areas:** DNS & Email Security, TLS / Cipher, OWASP Top 10, Robots & Sitemap.

⚠ **Needs improvement:** Performance & SEO, Email Security.

✗ **Weak areas:** Branding & Social, Cookie Compliance, Security Headers, Accessibility.

OWASP Top 10 Analysis (Score: 81/100)

The OWASP Top 10 is the globally recognized standard for web application security risks. Below is how google.com scores against each of the ten categories.

✓ A01:2021 – Broken Access Control Low Risk

No broken access control issues detected. Access restrictions appear properly configured.

⚠ A02:2021 – Cryptographic Failures Medium Risk

Issues found: SSL/TLS configuration has weaknesses.

□□ Enable HTTPS with strong TLS 1.2+ configuration. Set HSTS header with a long max-age. Remove all mixed content. Use secure cipher suites only.

✗ A03:2021 – Injection Critical Risk

Issues found: Content-Security-Policy is missing or weak (XSS protection reduced); X-Content-Type-Options header missing (MIME sniffing risk); URL parameters are reflected in HTML response (potential XSS).

□□ Implement a strict Content-Security-Policy. Set X-Content-Type-Options: nosniff. Sanitize and encode all user input. Use parameterized queries for database access.

⚠ A04:2021 – Insecure Design Medium Risk

Issues found: No visible rate limiting headers detected (may still be present server-side).

□□ Add X-Frame-Options or CSP frame-ancestors to prevent clickjacking. Disable GraphQL introspection in production. Implement rate limiting on all endpoints.

✓ A05:2021 – Security Misconfiguration Low Risk

No security misconfigurations detected. Server headers and file access are properly restricted.

✓ A06:2021 – Vulnerable and Outdated Components Low Risk

No known vulnerable components detected in the visible technology stack.

✓ A07:2021 – Identification and Authentication Failures Low Risk

Authentication-related configurations appear secure. No user enumeration or credential exposure detected.

⚠ A08:2021 – Software and Data Integrity Failures Medium Risk

Issues found: Cross-Origin-Opener-Policy (COOP) header not set; Cross-Origin-Embedder-Policy (COEP) header not set.

□□ Add Subresource Integrity (SRI) hashes to all external scripts and stylesheets. Set COOP and COEP headers for cross-origin isolation.

✓ A09:2021 – Security Logging and Monitoring Failures Low Risk

Security monitoring indicators are in place. A security.txt file is present for vulnerability reporting.

✓ A10:2021 – Server-Side Request Forgery (SSRF) Low Risk

No SSRF indicators detected. No open redirects or exposed internal endpoints found.

⚠ Critical Issues (12)

These issues pose an immediate security risk and should be addressed as a priority.

HTTP redirects to HTTPS SSL & HTTPS

HTTP requests are not being redirected to HTTPS.

Configure a permanent (301) redirect from HTTP to HTTPS.

HSTS header configured SSL & HTTPS

No Strict-Transport-Security (HSTS) header found.

Add: Strict-Transport-Security: max-age=31536000; includeSubDomains

No weak cipher suites SSL & HTTPS

Server accepts weak cipher suite(s): RC4, 3DES, EXPORT, NULL. These ciphers have known cryptographic weaknesses.

Restrict your cipher list in your server config: Nginx: ssl_ciphers ECDH+AESGCM:ECDH+AES256:ECDH+AES128:!aNULL:!MD5:!3DES:!RC4; Apache: SSLCipherSuite HIGH:!aNULL:!MD5:!3DES:!RC4 Then reload your server.

A03:2021 – Injection OWASP Top 10

Issues found: Content-Security-Policy is missing or weak (XSS protection reduced); X-Content-Type-Options header missing (MIME sniffing risk); URL parameters are reflected in HTML response (potential XSS).

Implement a strict Content-Security-Policy. Set X-Content-Type-Options: nosniff. Sanitize and encode all user input. Use parameterized queries for database access.

X-Content-Type-Options Security Headers

X-Content-Type-Options header is missing.

Add X-Content-Type-Options: nosniff to prevent browsers from MIME-sniffing responses.

Referrer-Policy Security Headers

No Referrer-Policy header found.

Add Referrer-Policy: strict-origin-when-cross-origin to control how much referrer info is sent.

Response compression enabled Performance & SEO

No gzip or Brotli compression detected.

Enable gzip or Brotli compression on your web server. This typically reduces HTML/CSS/JS size by 60-80%.

Viewport meta tag Accessibility

No viewport meta tag found.

Add <meta name="viewport" content="width=device-width, initial-scale=1"> to your <head>.

Single H1 heading Accessibility

No H1 heading found on the page.

Add a single <h1> tag that describes the main topic of the page.

Parameter 'q' reflected in response Input Reflection

The parameter 'q' is reflected inside a script block — high XSS risk.

Encode all user input before rendering in HTML. Use context-aware output encoding (HTML entities, JavaScript escaping, URL encoding).

No cookie consent with tracking cookies Cookie Compliance

Tracking cookies are set without a visible cookie consent mechanism. This violates GDPR/ePrivacy requirements.

Implement a cookie consent banner that blocks non-essential cookies until the user gives explicit consent.

1 tracking cookie(s) set before consent Cookie Compliance

The following tracking cookies are set on initial load: __Secure-ENID. Under GDPR, tracking cookies require explicit consent before being placed.

- [ ] Defer all tracking scripts and cookies until the user has given explicit consent via the cookie banner.

Warnings (25)

These items are not immediately critical but should be reviewed to strengthen your security posture.

DKIM record configured DNS & Email Security

No DKIM record found for common selectors. DKIM cryptographically signs outgoing emails, making them verifiable and preventing tampering in transit.

□□ Configure DKIM in your email provider (Google Workspace, Microsoft 365, etc.) and publish the TXT record they provide at {selector}._domainkey.google.com

DNSSEC DNS & Email Security

DNSSEC could not be confirmed via this check. Verify with your domain registrar.

□□ Enable DNSSEC through your domain registrar to protect against DNS cache poisoning.

A02:2021 – Cryptographic Failures OWASP Top 10

Issues found: SSL/TLS configuration has weaknesses.

□□ Enable HTTPS with strong TLS 1.2+ configuration. Set HSTS header with a long max-age. Remove all mixed content. Use secure cipher suites only.

A04:2021 – Insecure Design OWASP Top 10

Issues found: No visible rate limiting headers detected (may still be present server-side).

□□ Add X-Frame-Options or CSP frame-ancestors to prevent clickjacking. Disable GraphQL introspection in production. Implement rate limiting on all endpoints.

A08:2021 – Software and Data Integrity Failures OWASP Top 10

Issues found: Cross-Origin-Opener-Policy (COOP) header not set; Cross-Origin-Embedder-Policy (COEP) header not set.

□□ Add Subresource Integrity (SRI) hashes to all external scripts and stylesheets. Set COOP and COEP headers for cross-origin isolation.

Crawlers not fully blocked Robots & Sitemap

robots.txt appears to block all crawlers (Disallow: /). This will prevent search engine indexing.

□□ If this is a production site, remove or restrict the broad Disallow: / rule to allow indexing.

Content-Security-Policy Security Headers

Only a Content-Security-Policy-Report-Only header was found. This monitors violations but does NOT prevent attacks.

□□ Promote your CSP from Report-Only to enforced by renaming the header to Content-Security-Policy.

Permissions-Policy Security Headers

No Permissions-Policy header found.

□□ Add a Permissions-Policy header to restrict browser features like camera, microphone, and geolocation.

Cross-Origin-Opener-Policy Security Headers

No Cross-Origin-Opener-Policy (COOP) header found.

□□ Add Cross-Origin-Opener-Policy: same-origin to isolate your browsing context and protect against cross-origin attacks and Spectre-like vulnerabilities.

Cross-Origin-Embedder-Policy Security Headers

No Cross-Origin-Embedder-Policy (COEP) header found.

□□ Add Cross-Origin-Embedder-Policy: require-corp to enable advanced browser isolation features (required for SharedArrayBuffer and high-resolution timers).

Apple Touch Icon Branding & Social

No Apple Touch Icon found.

□□ Add <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png"> for iOS home screen support.

Web App Manifest Branding & Social

No Web App Manifest found.

Add a manifest.json (or site.webmanifest) with name, icons, and theme_color for PWA support.

Open Graph title Branding & Social

No og:title meta tag found.

Add <meta property="og:title" content="..."> for proper social media previews on Facebook, LinkedIn, and WhatsApp.

Open Graph description Branding & Social

No og:description meta tag found.

Add <meta property="og:description" content="..."> for social media link previews.

Open Graph image Branding & Social

No og:image meta tag found.

Add <meta property="og:image" content="..."> with a 1200×630px image for social sharing previews.

Twitter/X Card Branding & Social

No twitter:card meta tag found.

Add <meta name="twitter:card" content="summary_large_image"> for rich link previews on X/Twitter.

Theme color Branding & Social

No theme-color meta tag found.

Add <meta name="theme-color" content="#yourcolor"> to brand the browser address bar on mobile.

security.txt present Performance & SEO

No security.txt file found at /.well-known/security.txt or /security.txt.

Create a security.txt file (RFC 9116) at /.well-known/security.txt to provide security researchers with a responsible disclosure contact.

Meta description Accessibility

No meta description found.

Add <meta name="description" content="..."> to improve SEO and accessibility.

Form labels Accessibility

1 of 1 form inputs may be missing accessible labels.

Associate each <input> with a <label for="..."> or use aria-label/aria-labelledby.

SPF uses soft fail (~all) Email Security

SPF record uses ~all (soft fail) instead of -all (hard fail). Spoofed emails may still be delivered.

Change SPF policy from ~all to -all once you have confirmed all legitimate mail sources are included.

No DANE/TLSA record Email Security

No DANE TLSA record found. DANE provides additional verification for TLS certificates on mail servers.

URL path reflected in error page Input Reflection

The requested URL path is reflected in the error page response. This could be exploited for XSS if output is not properly encoded.

Ensure error pages use proper HTML encoding for all dynamic content including the requested URL.

No cookie prefix used Session Security

Session cookies do not use the __Host- or __Secure- prefix. These prefixes provide additional protection against cookie overwriting.

Consider using __Host- prefix for session cookies (requires Secure flag, no Domain, Path=/).

1 cookie(s) with expiry > 1 year Cookie Compliance

1 cookie(s) have an expiration longer than 1 year. GDPR guidance suggests cookies should not persist longer than necessary.

Reduce cookie lifetimes to the minimum necessary period. Analytics cookies should typically expire within 6-13 months.

✓ Passed Checks (70)

These checks were all successfully validated. Keep up the good work.

✓	SPF record configured	DNS & Email Security
✓	DMARC record configured	DNS & Email Security
✓	CAA record configured	DNS & Email Security
✓	MTA-STS (email transport security)	DNS & Email Security
✓	IPv6 support	DNS & Email Security
✓	HTTPS / SSL enabled	SSL & HTTPS
✓	SSL certificate valid	SSL & HTTPS
✓	TLS 1.0 and 1.1 disabled	SSL & HTTPS
✓	TLS 1.3 supported	TLS / Cipher
✓	TLS 1.2 supported	TLS / Cipher
✓	TLS 1.1 disabled	TLS / Cipher
✓	TLS 1.0 disabled	TLS / Cipher
✓	Perfect Forward Secrecy (PFS)	TLS / Cipher
✓	A01:2021 – Broken Access Control	OWASP Top 10
✓	A05:2021 – Security Misconfiguration	OWASP Top 10
✓	A06:2021 – Vulnerable and Outdated Components	OWASP Top 10
✓	A07:2021 – Identification and Authentication Failures	OWASP Top 10
✓	A09:2021 – Security Logging and Monitoring Failures	OWASP Top 10
✓	A10:2021 – Server-Side Request Forgery (SSRF)	OWASP Top 10
✓	robots.txt present	Robots & Sitemap
✓	Sitemap referenced in robots.txt	Robots & Sitemap
✓	Sitemap accessible	Robots & Sitemap
✓	security.txt present	Robots & Sitemap
✓	No mixed content detected	Content & CMS
✓	CMS admin panel not publicly accessible	Content & CMS
✓	CMS version not exposed	Content & CMS
✓	Subresource Integrity (SRI)	Content & CMS
✓	No open redirect	Content & CMS
✓	Directory listing disabled	Content & CMS
✓	Server version not disclosed	Security Headers
✓	X-Frame-Options	Security Headers
✓	Cookie security flags	Security Headers
✓	X-XSS-Protection (deprecated)	Security Headers
✓	Favicon	Branding & Social
✓	Fast server response time (TTFB)	Performance & SEO
✓	robots.txt present	Performance & SEO

✓	XML sitemap present	Performance & SEO
✓	API/docs endpoints	API Security
✓	GraphQL introspection	API Security
✓	WordPress user enumeration	API Security
✓	OPTIONS method does not expose allowed methods	HTTP Methods
✓	TRACE method is disabled	HTTP Methods
✓	PUT method rejects arbitrary uploads	HTTP Methods
✓	HTML lang attribute	Accessibility
✓	Page title	Accessibility
✓	Image alt attributes	Accessibility
✓	.env file exposed	Exposed Files
✓	.git directory exposed	Exposed Files
✓	phpinfo() page exposed	Exposed Files
✓	Database backup file exposed	Exposed Files
✓	WordPress config backup exposed	Exposed Files
✓	.htpasswd file exposed	Exposed Files
✓	web.config not exposed	Exposed Files
✓	.git/config not exposed	Exposed Files
✓	composer.lock not exposed	Exposed Files
✓	Apache server-status not exposed	Exposed Files
✓	DMARC policy is reject	Email Security
✓	MX records configured	Email Security
✓	SMTP banner not exposing version	Email Security
✓	No common sensitive paths found	Directory Discovery
✓	404 error page is clean	Error Disclosure
✓	Server error pages are clean	Error Disclosure
✓	No version information in error responses	Error Disclosure
✓	Forms submit to same origin	Input Reflection
✓	Session cookies have Secure flag	Session Security
✓	Session cookies have HttpOnly flag	Session Security
✓	Session cookies have SameSite flag	Session Security
✓	No session cookies on homepage	Session Security
✓	Only 2 cookie(s) on initial load	Cookie Compliance
✓	Subdomain takeover	Subdomain Takeover

Category Details

Branding & Social 15/100

Apple Touch Icon

No Apple Touch Icon found.

Add <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-icon.png"> for iOS home screen support.

Web App Manifest

No Web App Manifest found.

Add a manifest.json (or site.webmanifest) with name, icons, and theme_color for PWA support.

Open Graph title

No og:title meta tag found.

Add <meta property="og:title" content="..."> for proper social media previews on Facebook, LinkedIn, and WhatsApp.

Open Graph description

No og:description meta tag found.

Add <meta property="og:description" content="..."> for social media link previews.

Open Graph image

No og:image meta tag found.

Add <meta property="og:image" content="..."> with a 1200×630px image for social sharing previews.

Twitter/X Card

No twitter:card meta tag found.

Add <meta name="twitter:card" content="summary_large_image"> for rich link previews on X/Twitter.

Theme color

No theme-color meta tag found.

Add <meta name="theme-color" content="#yourcolor"> to brand the browser address bar on mobile.

Cookie Compliance 25/100

No cookie consent with tracking cookies

Tracking cookies are set without a visible cookie consent mechanism. This violates GDPR/ePrivacy requirements.

Implement a cookie consent banner that blocks non-essential cookies until the user gives explicit consent.

1 tracking cookie(s) set before consent

The following tracking cookies are set on initial load: __Secure-ENID. Under GDPR, tracking cookies require explicit consent before being placed.

Defer all tracking scripts and cookies until the user has given explicit consent via the cookie banner.

1 cookie(s) with expiry > 1 year

1 cookie(s) have an expiration longer than 1 year. GDPR guidance suggests cookies should not persist longer than necessary.

Reduce cookie lifetimes to the minimum necessary period. Analytics cookies should typically expire within 6-13 months.

Security Headers 36/100

Content-Security-Policy

Only a Content-Security-Policy-Report-Only header was found. This monitors violations but does NOT prevent attacks.

□□ Promote your CSP from Report-Only to enforced by renaming the header to Content-Security-Policy.

X-Content-Type-Options

X-Content-Type-Options header is missing.

□□ Add X-Content-Type-Options: nosniff to prevent browsers from MIME-sniffing responses.

Referrer-Policy

No Referrer-Policy header found.

□□ Add Referrer-Policy: strict-origin-when-cross-origin to control how much referrer info is sent.

Permissions-Policy

No Permissions-Policy header found.

□□ Add a Permissions-Policy header to restrict browser features like camera, microphone, and geolocation.

Cross-Origin-Opener-Policy

No Cross-Origin-Opener-Policy (COOP) header found.

□□ Add Cross-Origin-Opener-Policy: same-origin to isolate your browsing context and protect against cross-origin attacks and Spectre-like vulnerabilities.

Cross-Origin-Embedder-Policy

No Cross-Origin-Embedder-Policy (COEP) header found.

□□ Add Cross-Origin-Embedder-Policy: require-corp to enable advanced browser isolation features (required for SharedArrayBuffer and high-resolution timers).

Accessibility 50/100

Viewport meta tag

No viewport meta tag found.

□□ Add <meta name="viewport" content="width=device-width, initial-scale=1"> to your <head>.

Meta description

No meta description found.

□□ Add <meta name="description" content="..."> to improve SEO and accessibility.

Single H1 heading

No H1 heading found on the page.

□□ Add a single <h1> tag that describes the main topic of the page.

Form labels

1 of 1 form inputs may be missing accessible labels.

□□ Associate each <input> with a <label for="..."> or use aria-label/aria-labelledby.

Input Reflection 50/100

Parameter 'q' reflected in response

The parameter 'q' is reflected inside a script block — high XSS risk.

Encode all user input before rendering in HTML. Use context-aware output encoding (HTML entities, JavaScript escaping, URL encoding).

URL path reflected in error page

The requested URL path is reflected in the error page response. This could be exploited for XSS if output is not properly encoded.

Ensure error pages use proper HTML encoding for all dynamic content including the requested URL.

SSL & HTTPS 58/100

HTTP redirects to HTTPS

HTTP requests are not being redirected to HTTPS.

Configure a permanent (301) redirect from HTTP to HTTPS.

HSTS header configured

No Strict-Transport-Security (HSTS) header found.

Add: Strict-Transport-Security: max-age=31536000; includeSubDomains

No weak cipher suites

Server accepts weak cipher suite(s): RC4, 3DES, EXPORT, NULL. These ciphers have known cryptographic weaknesses.

Restrict your cipher list in your server config: Nginx: ssl_ciphers ECDH+AESGCM:ECDH+AES256:ECDH+AES128:!aNULL:!MD5:!3DES:!RC4; Apache: SSLCipherSuite HIGH:!aNULL:!MD5:!3DES:!RC4 Then reload your server.

Performance & SEO 75/100

Response compression enabled

No gzip or Brotli compression detected.

Enable gzip or Brotli compression on your web server. This typically reduces HTML/CSS/JS size by 60-80%.

security.txt present

No security.txt file found at /.well-known/security.txt or /security.txt.

Create a security.txt file (RFC 9116) at /.well-known/security.txt to provide security researchers with a responsible disclosure contact.

Email Security 75/100

SPF uses soft fail (~all)

SPF record uses ~all (soft fail) instead of -all (hard fail). Spoofed emails may still be delivered.

Change SPF policy from ~all to -all once you have confirmed all legitimate mail sources are included.

No DANE/TLSA record

No DANE TLSA record found. DANE provides additional verification for TLS certificates on mail servers.

Robots & Sitemap 80/100

Crawlers not fully blocked

robots.txt appears to block all crawlers (Disallow: /). This will prevent search engine indexing.

If this is a production site, remove or restrict the broad Disallow: / rule to allow indexing.

DNS & Email Security 83/100

DKIM record configured

No DKIM record found for common selectors. DKIM cryptographically signs outgoing emails, making them verifiable and preventing tampering in transit.

Configure DKIM in your email provider (Google Workspace, Microsoft 365, etc.) and publish the TXT record they provide at {selector}._domainkey.google.com

DNSSEC

DNSSEC could not be confirmed via this check. Verify with your domain registrar.

Enable DNSSEC through your domain registrar to protect against DNS cache poisoning.

TLS / Cipher 100/100

✓ All checks passed

Content & CMS 100/100

✓ All checks passed

API Security 100/100

✓ All checks passed

HTTP Methods 100/100

✓ All checks passed

Exposed Files 100/100

✓ All checks passed

Directory Discovery 100/100

✓ All checks passed

Error Disclosure 100/100

✓ All checks passed

Subdomain Takeover 100/100

✓ All checks passed

Session Security 175/100

No cookie prefix used

Session cookies do not use the __Host- or __Secure- prefix. These prefixes provide additional protection against cookie overwriting.

Consider using __Host- prefix for session cookies (requires Secure flag, no Domain, Path=/).