smaoin

badssl.com

DNS: Google Cloud DNS · 104.154.89.105
NS: ns-cloud-c1.googledomains.com, ns-cloud-c2.googledomains.com, ns-cloud-c3.googledomains.com, ns-cloud-c4.googledomains.com

Scanned 20 November 2026 · 17:12 UTC

EXECUTIVE SUMMARY

SECURITY SCORE



OPTIMISATION



12 of 29 checks passed

8 issues found that need your attention. 9 advisory items noted below for extra hardening.

SAMPLE

WHAT THIS REPORT COVERS

- Malware / phishing blocklist (Safe Browsing)
- HTTPS redirect
- SSL certificate validity + expiry
- TLS protocol version (1.0/1.1 vs 1.2/1.3)
- Security headers (graded A+ to F)
- HSTS strength + HTTP TRACE
- Cross-origin isolation + security.txt
- Server / technology information leakage
- Cookie security flags
- DNS CAA records
- DNSSEC
- HSTS preload list
- Mixed content (HTTP on HTTPS page)
- Subresource Integrity (SRI)
- Open redirect
- Clickjacking protection
- CORS policy exposure
- SPF / DKIM / DMARC / MTA-STS email auth
- MX records
- PageSpeed: performance
- PageSpeed: accessibility
- PageSpeed: SEO
- PageSpeed: best practices
- Technical SEO & AI readiness
- Privacy policy
- Cookie consent
- Contact & business details
- Accessibility statement

SCOPE OF THIS ASSESSMENT

An external, unauthenticated assessment: public URL, DNS and HTTP-header checks plus a homepage Lighthouse analysis. It sends a few harmless test requests (open redirect, CORS and HTTP TRACE), but it does not crawl every page, log in, or attempt any exploitation or penetration testing. Findings that reference cookies, redirects, CORS or mixed content relate to the home page unless stated otherwise.

PRIORITISED ACTION PLAN

Hand the items below to your developer or web host, most serious first. Each includes a recommended remediation or example configuration — validate it against your own environment before deploying. Some changes (DMARC enforcement, CSP, HSTS preload, SPF) can disrupt email or break a site if applied without testing.

1. **SPF Record** · High
   Add an SPF TXT record to your DNS listing only your mail providers — e.g. v=spf1 include:<your provider> ~all (for Google Workspace, include:_spf.google.com; for Microsoft 365, include:spf.protection.outlook.com). Validate it against your actual senders before publishing.

2. **Security Headers** · High
   Add the missing response headers in your web server config or application middleware. Exact values are listed in the header table below.

3. **DMARC Record** · High
   Add a DMARC TXT record at _dmarc.[yourdomain]. Start in monitoring mode — v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com — then, once the aggregate reports confirm your legitimate mail passes SPF/DKIM alignment, tighten to p=quarantine and finally p=reject. Deploying enforcement first can interrupt legitimate email.

4. **Privacy policy** · High
   If your site collects any personal data - even just a contact form - UK GDPR expects a privacy policy that's easy to find, usually linked in the footer.

5. **Clickjacking Protection** · High
   Add X-Frame-Options: SAMEORIGIN to block your pages from being embedded in third-party iframes. Alternatively — or additionally — add frame-ancestors 'self' to your Content-Security-Policy header, which is the modern W3C-recommended approach.

6. **Mixed Content** · High
   Replace all http:// URLs in your HTML with https:// equivalents. Browsers block or warn on mixed content, and some browsers will block the page entirely. Check embedded fonts, scripts, images, and iframes.

7. **PageSpeed: Accessibility** · Medium
   Fix accessibility issues: add alt text to images, ensure sufficient colour contrast, and use semantic HTML.

8. **Information Leakage** · Low
   Hide software names and version numbers in these response headers, because they help attackers target known vulnerabilities. Remove the version from the Server header: in Apache, ServerTokens Prod and ServerSignature Off; in nginx, server_tokens off; in IIS, removeServerHeader='true' under requestFiltering in web.config. A generic name such as Apache can remain.

Worth doing next. These aren't failures, but they're the advisories most worth acting on.

9. **DKIM Record**
   In Google Workspace's domain settings, turn on DKIM signing and publish the records it gives you. Without it, your mail isn't signed as your domain, so DMARC relies on SPF alone.

SAMPLE

SECURITY

Malware & Phishing Blocklist

PASS

What this means

Google Safe Browsing powers the malware/phishing warnings in Chrome, Safari and Firefox. If your site (or a script it loads) is listed, browsers show every visitor a full-page red warning and search rankings collapse — usually the result of a compromise or a bad third-party script.

Result

Not flagged on Google Safe Browsing

Google's Safe Browsing service does not list this site for malware, phishing, or unwanted software.

HTTPS Redirect

PASS

What this means

Ensures all visitors are served over the encrypted HTTPS connection. Without a redirect, browsers show a 'Not Secure' warning and search engines may rank the site lower.

Result

HTTP redirects to HTTPS

Final URL: https://badssl.com/

SSL Certificate

PASS

What this means

The certificate encrypts traffic between your server and visitors. An expired or missing certificate blocks access entirely with a full-page browser warning.

Result

SSL certificate valid — 38 days remaining

*Expires: 28 December 2026 (38 days) · Issued to: *.badssl.com · Issued by: Let's Encrypt*

TLS Version

PASS

What this means

The TLS protocol version secures the connection itself. TLS 1.2 and 1.3 are current; TLS 1.0 and 1.1 are deprecated — they carry known protocol weaknesses and are rejected by every modern browser. A server that still accepts them should disable them; one that offers only them is unreachable by current browsers.

Result

Modern TLS only — TLS 1.2, deprecated TLS 1.0/1.1 refused

The server negotiates TLS 1.2/1.3 and rejects deprecated TLS 1.0/1.1.

SAMPLE

✕ Security Headers

F

What this means

HTTP response headers that instruct browsers to enforce security policies — preventing clickjacking, content injection, MIME sniffing, and data leakage. Graded A+ to F by how many of the six are present, in the style of SecurityHeaders.com.

Result

Grade F — 6 header(s) missing

Header	Status	Current value / Recommended
HSTS (Strict-Transport-Security)	✕ Missing	*Strict-Transport-Security: max-age=31536000; includeSubDomains; preload*
Content Security Policy (CSP)	✕ Missing	*Content-Security-Policy: default-src 'self' — then tighten per-resource*
X-Frame-Options	✕ Missing	*X-Frame-Options: SAMEORIGIN*
X-Content-Type-Options	✕ Missing	*X-Content-Type-Options: nosniff*
Referrer-Policy	✕ Missing	*Referrer-Policy: strict-origin-when-cross-origin*
Permissions-Policy	✕ Missing	*Permissions-Policy: geolocation=(), microphone=(), camera=()*

⚠ **Information leakage detected**

Server: nginx/1.10.3; (Ubuntu)

Remove or replace these headers to avoid exposing your technology stack.

⚠ **Recommended fix**

Add the missing response headers in your web server config or application middleware. Exact values are listed in the header table below.

SAMPLE

Information Leakage

FAIL

What this means

Response headers such as Server, X-Powered-By, and X-Generator can expose your web server software, language runtime, and CMS — giving attackers a precise target for known CVEs. For example, 'Server: Apache/2.4.51' or 'X-Powered-By: PHP/8.3.0' immediately narrows the field of viable exploits.

Result

1 header reveals technology stack information

Server: nginx/1.10.3, (Ubuntu)

Recommended fix

Hide software names and version numbers in these response headers, because they help attackers target known vulnerabilities. Remove the version from the Server header: in Apache, ServerTokens Prod and ServerSignature Off; in nginx, server_tokens off; in IIS, removeServerHeader='true' under requestFiltering in web.config. A generic name such as Apache can remain.

Cookie Security

N/A

What this means

Cookies that store session tokens or authentication state must carry the Secure flag (HTTPS-only), HttpOnly (inaccessible to JavaScript), and SameSite=Lax or Strict (prevents cross-site request forgery). Missing flags allow session hijacking and CSRF attacks.

Result

No cookies set on home page

No Set-Cookie headers were returned, so there are no cookie security flags to assess.

DNS CAA Records

ADVISORY

What this means

Certification Authority Authorisation (CAA) DNS records restrict which certificate authorities are allowed to issue SSL certificates for your domain. Without them, any CA in the world can issue a cert — enabling rogue or misissued certificates.

Result

No DNS CAA records found

Any certificate authority can issue a certificate for this domain.

Recommended fix

Add CAA records to restrict which CAs can issue SSL certificates for your domain. Example: "0 issue \"letsencrypt.org\"" or "0 issue \"sectigo.com\"". This prevents rogue CAs from issuing fraudulent certificates.

SAMPLE

DNSSEC

ADVISORY

What this means

DNS Security Extensions (DNSSEC) cryptographically sign DNS responses so resolvers can verify they haven't been tampered with. Without DNSSEC, attackers can perform DNS cache poisoning — silently redirecting visitors to fraudulent servers.

Result

DNSSEC not enabled

No DS record at the parent zone and no DNSKEY at the domain apex.

Recommended fix

Enable DNSSEC through your DNS provider or registrar. DNSSEC cryptographically signs your DNS records, preventing cache-poisoning and spoofing attacks that redirect visitors or intercept email.

HSTS Preload

ADVISORY

What this means

HSTS (HTTP Strict Transport Security) forces browsers to always use HTTPS. Being on the preload list goes further — browsers enforce HTTPS even on the very first visit, before they've seen your HSTS header. This eliminates SSL-stripping attacks on the initial request.

Result

Not on the HSTS preload list

This domain is not currently submitted to the browser HSTS preload list.

Recommended fix

Submit your domain at https://hstspreload.org/ after ensuring your HSTS header includes includeSubDomains and preload directives with a max-age of at least 31536000 (1 year). Preloading guarantees HTTPS even on the very first visit, before any HSTS header is seen.

Mixed Content

FAIL

What this means

A page loaded over HTTPS must not load any resources (images, scripts, stylesheets, iframes) over plain HTTP. Mixed content downgrades the security of the encrypted connection, and modern browsers block or warn on mixed active content.

Result

6 mixed-content references found

http://http.badssl.com/
http://http-textarea.badssl.com/
http://http-password.badssl.com/
http://http-login.badssl.com/
http://http-dynamic-login.badssl.com/
http://http-credit-card.badssl.com/

Recommended fix

Replace all http:// URLs in your HTML with https:// equivalents. Browsers block or warn on mixed content, and some browsers will block the page entirely. Check embedded fonts, scripts, images, and iframes.

SAMPLE

Subresource Integrity (SRI)

N/A

What this means

Scripts and stylesheets loaded from CDNs or third-party hosts should carry an integrity attribute containing a cryptographic hash of the expected file content. Without it, a compromised CDN could serve malicious code to every visitor without detection.

Result

No third-party resources require SRI

All external scripts and stylesheets are either served from your own domain, already have integrity attributes, or are from providers that don't support static SRI hashes.

Open Redirect

PASS

What this means

An open redirect lets an attacker craft a link to your site that automatically forwards the visitor to a malicious URL — making phishing attacks far more convincing because the initial link appears legitimate. Common parameters tested: ?url=, ?redirect=, ?next=, ?return=, ?returnUrl= and others.

Result

No open redirect detected on common parameters

Tested: ?url=, ?redirect=, ?next=, ?return=, ?returnUrl=, ?return_url=, ?goto=, ?target=, ?dest=, ?destination=

Clickjacking Protection

FAIL

What this means

Clickjacking tricks users into clicking hidden elements by overlaying your site inside an invisible iframe on a malicious page. X-Frame-Options or the CSP frame-ancestors directive prevents your pages from being embedded in third-party frames entirely.

Result

No effective clickjacking protection

Neither X-Frame-Options nor CSP frame-ancestors is set

Recommended fix

Add X-Frame-Options: SAMEORIGIN to block your pages from being embedded in third-party iframes. Alternatively — or additionally — add frame-ancestors 'self' to your Content-Security-Policy header, which is the modern W3C-recommended approach.

CORS Policy

PASS

What this means

Cross-Origin Resource Sharing (CORS) controls which other websites may read responses from your site in a browser. Reflecting any origin — especially while allowing credentials — lets a malicious site read your logged-in users' data. It should be restricted to an explicit list of trusted origins.

Result

No cross-origin resource sharing exposure

The home page does not return an Access-Control-Allow-Origin header to an untrusted origin.

SAMPLE

HSTS Strength

N/A

What this means

Beyond simply being present, a Strict-Transport-Security header should last at least a year (max-age ≥ 31536000) and cover subdomains (includeSubDomains). A short or subdomain-less HSTS leaves gaps that SSL-stripping attacks can exploit.

Result

HSTS strength not assessed — no HSTS header

The Strict-Transport-Security header is not set, so there is no max-age or includeSubDomains to grade here. Its absence is already reflected in the Security Headers result above.

HTTP TRACE Method

PASS

What this means

The HTTP TRACE method echoes the request back to the client. When left enabled it allows Cross-Site Tracing (XST), which can expose cookies and authentication headers that are otherwise protected. It should be disabled.

Result

HTTP TRACE method is disabled

The server did not honour a TRACE request (HTTP 405).

Cross-Origin Isolation

ADVISORY

What this means

The Cross-Origin-Opener/Embedder/Resource-Policy headers isolate your pages from other origins, defending against cross-window attacks and speculative-execution (Spectre-class) side-channel leaks. Modern defence-in-depth that most sites don't yet set.

Result

No cross-origin isolation headers

Cross-Origin-Opener-Policy is not set.

Recommended fix

Add Cross-Origin-Opener-Policy: same-origin (optionally with COEP/CORP) to defend against cross-window and speculative-execution (Spectre-class) side-channel leaks. Modern defence-in-depth — most sites don't set it yet.

SAMPLE

security.txt

ADVISORY

What this means

A /.well-known/security.txt file (RFC 9116) publishes how to report a security issue to you. It's a low-effort trust signal that shows you take security seriously and gives researchers a responsible way to reach you.

Result

No security.txt file

No valid /.well-known/security.txt found for badssl.com.

Recommended fix

Publish a security.txt (RFC 9116) at /.well-known/security.txt with a Contact: line, so anyone who finds a vulnerability knows how to report it responsibly. Low effort, good trust signal.

EMAIL AUTHENTICATION

SPF Record

FAIL

What this means

A DNS TXT record that lists which mail servers are authorised to send email from your domain. Without it, any server can impersonate your address and your emails are far more likely to land in spam.

Result

No SPF record found

No TXT record starting with 'v=spf1' was found for this domain.

Recommended fix

Add an SPF TXT record to your DNS listing only your mail providers — e.g. v=spf1 include:<your provider> ~all (for Google Workspace, include:_spf.google.com; for Microsoft 365, include:spf.protection.outlook.com). Validate it against your actual senders before publishing.

DKIM Record

ADVISORY

What this means

A cryptographic signature attached to every outgoing email, proving it was genuinely sent from your domain and hasn't been altered in transit. Now required by Google and Yahoo for bulk senders.

Result

DKIM not set up for Google Workspace on this domain

Your email runs on Google Workspace, which signs with google._domainkey.badssl.com. None is published. Another sending service could still sign with its own selector.

Recommended fix

In Google Workspace's domain settings, turn on DKIM signing and publish the records it gives you. Without it, your mail isn't signed as your domain, so DMARC relies on SPF alone.

SAMPLE

✕ DMARC Record

FAIL

What this means

A DNS policy telling receiving mail servers what to do with emails that fail SPF or DKIM — reject, quarantine, or allow. Set to reject or quarantine, it protects your domain from being spoofed in phishing attacks. With a reporting address, it also delivers daily reports on email usage.

Result

No DMARC record found

No TXT record found at _dmarc.badssl.com

Recommended fix

Add a DMARC TXT record at _dmarc.[yourdomain]. Start in monitoring mode — v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com — then, once the aggregate reports confirm your legitimate mail passes SPF/DKIM alignment, tighten to p=quarantine and finally p=reject. Deploying enforcement first can interrupt legitimate email.

⚠ MTA-STS

ADVISORY

What this means

MTA-STS (RFC 8461) instructs sending mail servers to deliver email to your domain over TLS only, and to validate the certificate. Without it, email in transit between mail servers can be intercepted or downgraded to plain text by a network attacker.

Result

MTA-STS not configured

No _mta-sts.badssl.com TXT record found.

Recommended fix

MTA-STS (RFC 8461) instructs sending mail servers to use TLS when delivering email to your domain. Add a _mta-sts TXT record and publish a policy file at https://mta-sts.badssl.com/.well-known/mta-sts.txt with mode: enforce to prevent email interception in transit.

✓ MX Records

PASS

What this means

MX records say which servers receive email for your domain. If there are none, the domain doesn't accept mail — which is fine if intentional, but SPF, DKIM and DMARC still matter because they stop attackers spoofing email that appears to come FROM your domain.

Result

5 MX records found — the domain receives email

5 gmr-smtp-in.l.google.com
10 alt1.gmr-smtp-in.l.google.com
20 alt2.gmr-smtp-in.l.google.com
30 alt3.gmr-smtp-in.l.google.com
40 alt4.gmr-smtp-in.l.google.com

SAMPLE

HOW WE SCORE

Your security score is a severity-weighted average, not a simple pass count. Each check carries a weight reflecting its real-world risk, so a broken padlock counts far more than a missing “nice to have” header.

CRITICAL	Breaks the site for visitors — no HTTPS, or an invalid certificate. A failure here caps the whole score at “Fair”, however good everything else is.
HIGH	A real, exploitable weakness — spoofable email, weak security headers, session-cookie, TLS or clickjacking gaps.
MEDIUM	Hardening that meaningfully reduces risk but isn't directly exploitable on its own.
LOW	Minor hygiene and information-disclosure items — worth tidying, low impact.

Advisories (amber) are flagged for attention but are not failures — things that are valid today but could be hardened (e.g. a certificate that's valid but expiring soon, or optional DNS hardening). They gently lower the score (about half a check's weight) so a perfect 100 means nothing is outstanding — but they never count as an issue or cap the score.

What the number means. 90+ is Excellent, 75+ Good, 50+ Fair, 25+ Poor, below that Critical risk. This report focuses on security; performance and SEO are a separate concern and don't affect this score.

SAMPLE

Mobile Performance — Lighthouse lab metrics

Good

Lab data from a single Lighthouse run, not field Core Web Vitals. The current Core Web Vitals are LCP, CLS and INP measured from real users; the rest below (FCP, TBT, Speed Index, TTFB) are Lighthouse lab metrics.

Largest Contentful Paint	1.2 s
First Contentful Paint	1.2 s
Cumulative Layout Shift	0
Total Blocking Time	0 ms
Speed Index	3.3 s
Time to First Byte	0 ms

Performance

PASS

What this means

How fast your page loads on a mobile device. Scores below 70 indicate slow load times that hurt conversions, increase bounce rates, and can damage search rankings. Google factors page experience, including Core Web Vitals, into its ranking systems — though good scores alone don't guarantee higher rankings.

Score

Performance score: 99/100

Score guide: 0–49 Critical | 50–89 Needs work | 90–100 Passing

Diagnostics

Issues that may affect performance, quality, or correctness:

0 — Network dependency tree

Avoid chaining critical requests by reducing the length of chains, reducing the download size of resources, or deferring the download of unnecessary resources to improve page load

0 — Render-blocking requests

Est savings of 430 ms

Requests are blocking the page's initial render, which may delay LCP. Deferring or inlining can move these network requests out of the critical path.

Resource	Size / Savings	Time Saving
https://badssl.com/funky/funky.css	2 KiB	451 ms
https://badssl.com/github-ribbon.css	5 KiB	451 ms
https://badssl.com/funky/funky.js	1 KiB	451 ms
https://badssl.com/index.css	4 KiB	151 ms
https://badssl.com/index.js	4 KiB	451 ms

50 — Image elements do not have explicit width and height

Set an explicit width and height on image elements to reduce layout shifts and improve CLS. Learn how to set image dimensions

SAMPLE

Resource
https://badssl.com/front-page-icons/chrome.svg

Passed checks

Use efficient cache lifetimes · Layout shift culprits · Document request latency · Optimize DOM size · Duplicated JavaScript · Font display · Forced reflow · Improve image delivery · Legacy JavaScript · 3rd parties · Optimize viewport for mobile · Time to Interactive · Max Potential First Input Delay · Minify CSS · Minify JavaScript · Reduce unused CSS · Reduce unused JavaScript · Avoids enormous network payloads · JavaScript execution time · Minimizes main-thread work · Avoid multiple page redirects · Initial server response time was short

Accessibility

NEEDS WORK

What this means

How usable your site is for people with disabilities — screen-reader compatibility, keyboard navigation, and descriptive alt text (decorative images may correctly use an empty alt=""). WCAG 2.1 AA asks for a contrast ratio of 4.5:1 for normal text and 3:1 for large text (18pt+ or 14pt bold). Automated testing flags potential barriers and a low score is worth investigating — but automated tools cannot establish WCAG 2.1 AA or Equality Act 2010 conformance; only a manual audit can.

Score

Accessibility score: 72/100

Score guide: 0–49 Critical · 50–89 Needs work · 90–100 Passing

Diagnostics

Issues that may affect performance, quality, or correctness:

0

<html> element does not have a [lang] attribute

If a page doesn't specify a lang attribute, a screen reader assumes that the page is in the default language that the user chose when setting up the screen reader. If the page isn't actually in the default language, then the screen reader might not announce the page's text correctly. Learn more about the lang attribute.

Element	CSS Selector
html	html

0

Image elements do not have [alt] attributes

Informative elements should aim for short, descriptive alternate text. Decorative elements can be ignored with an empty alt attribute. Learn more about the alt attribute.

Element	CSS Selector
div.group > h2#chrome > span.emoji > img.chrome-icon	div.group > h2#chrome > span.emoji > img.chro...

0

Document does not have a main landmark.

One main landmark helps screen reader users navigate a web page. Learn more about landmarks.

Element	CSS Selector
html	html

Passed checks

[aria-hidden="true"] is not present on the document <body> · Background and foreground colors have a sufficient contrast ratio · Document has a <title> element · Heading elements appear in a sequentially-descending order · Links have a discernible name · [user-scalable="no"] is not used in the <meta name="viewport"> element and the [maximum-scale] attribute is not less than 5. · Touch targets have sufficient size and spacing.

Recommended fix

Fix accessibility issues: add alt text to images, ensure sufficient colour contrast, and use semantic HTML.

SAMPLE

SEO

NEEDS WORK

What this means

Technical on-page factors that affect how search engines discover, crawl, and index your content — meta descriptions, canonical URLs, structured headings, mobile-friendliness, and crawlability.

Score

SEO score: 83/100

Score guide: 0–49 Critical · 50–89 Needs work · 90–100 Passing

Diagnostics

Issues that may affect performance, quality, or correctness:

0

Document does not have a meta description

Meta descriptions may be included in search results to concisely summarize page content. Learn more about the meta description.

0

Image elements do not have [alt] attributes

Informative elements should aim for short, descriptive alternate text. Decorative elements can be ignored with an empty alt attribute. Learn more about the alt attribute.

Element	CSS Selector
div.group > h2#chrome > span.emoji > img.chrome-icon	div.group > h2#chrome > span.emoji > img.chro...

Passed checks

Page isn't blocked from indexing · Document has a <title> element · Page has successful HTTP status code · Links have descriptive text · Links are crawlable · robots.txt is valid · Document has a valid hreflang

Best Practices

PASS

What this means

Adherence to modern web standards — HTTPS everywhere, no deprecated APIs, no browser console errors, correct image aspect ratios, and third-party libraries free of known vulnerabilities.

Score

Best Practices score: 100/100

Score guide: 0–49 Critical · 50–89 Needs work · 90–100 Passing

Passed checks

Uses HTTPS · Avoids requesting the geolocation permission on page load · Avoids requesting the notification permission on page load · Allows users to paste into input fields · Displays images with correct aspect ratio · Serves images with appropriate resolution · Page has the HTML doctype · Properly defines charset · Avoids deprecated APIs · Avoids third-party cookies · No browser errors logged to the console · Page has valid source maps · No issues in the Issues panel in Chrome Devtools

Technical SEO & AI Readiness

3 / 16 passed

How well search engines and AI assistants can find, crawl, and understand your site — the on-page tags, discoverability files, and structured data that decide whether you show up and how you're described. Each item below is a specific, checkable fix.

SAMPLE

Page title ADVISORY

Title present but short (10 characters)

"badssl.com"

Recommended fix

Aim for roughly 50–60 characters so the title is descriptive enough to earn the click and fills the space search engines show.

Meta description ADVISORY

No meta description

The homepage has no <meta name="description">.

Recommended fix

Add a compelling ~140–160 character meta description. It doesn't directly affect ranking, but it's the snippet under your link in search results and drives click-through.

Headings FAIL

No <h1> heading

The homepage has no top-level <h1> heading.

Recommended fix

Add a single <h1> that states what the page is about. It anchors the page topic for search engines and assistive technology.

Structured data ADVISORY

No structured data (JSON-LD)

No <script type="application/ld+json"> blocks were found.

Recommended fix

Add JSON-LD structured data (e.g. Organization, LocalBusiness, WebSite, BreadcrumbList). It helps you earn rich results and gives AI assistants clearer signals about your business — though it doesn't guarantee they will cite you.

Canonical URL ADVISORY

No canonical URL

The homepage has no <link rel="canonical">.

Recommended fix

Add a self-referential <link rel="canonical"> so search engines know which URL is authoritative and don't split ranking across duplicates (with/without trailing slash, query strings, etc.).

Language ADVISORY

No lang attribute

The <html> element has no lang attribute.

Recommended fix

Set <html lang="en-GB"> (or your primary language). It helps search engines serve the right regional results and lets screen readers pronounce content correctly.

SAMPLE

✕ **Image alt text** FAIL

Only 0% of images have alt text (1 missing)

1 of 1 <img> elements have no alt attribute.

> **Recommended fix**
>
> Add descriptive alt text to your images (alt="" for decorative ones). Missing alt text fails WCAG, hurts screen-reader users, and forfeits image-search visibility.

✓ **Mobile viewport** PASS

Mobile viewport configured

⚠ **robots.txt** ADVISORY

robots.txt present but no sitemap reference

robots.txt was found but doesn't reference a sitemap.

> **Recommended fix**
>
> Add a “Sitemap: https://.../sitemap.xml” line to robots.txt so crawlers reliably discover all your pages.

⚠ **XML sitemap** ADVISORY

No sitemap.xml

No sitemap found at /sitemap.xml (HTTP 404).

> **Recommended fix**
>
> Publish an XML sitemap at /sitemap.xml listing your important pages, and reference it from robots.txt. It helps search engines find and index everything, especially newer pages.

✓ **Favicon** PASS

Favicon declared

✓ **404 handling** PASS

Missing pages return HTTP 404

⚠ **Open Graph** ADVISORY

No Open Graph tags

No og:title / og:description / og:image were found.

> **Recommended fix**
>
> Add Open Graph tags so links to your site show a proper title, description, and image when shared on LinkedIn, Facebook, WhatsApp, Slack, etc. — a big lift to click-through.

⚠ **Twitter/X cards** ADVISORY

No Twitter/X card tags

No <meta name="twitter:card"> was found.

> **Recommended fix**
>
> Add twitter:card (usually summary_large_image) plus twitter:title/description/image so links shared on X render a rich card. It falls back to Open Graph, so this is a small top-up.

SAMPLE

llms.txt ADVISORY

No llms.txt (optional)

No /llms.txt file was found.

Recommended fix

Optional and experimental: /llms.txt is an emerging community convention (now with a v2 proposal) that some sites publish to offer AI assistants (ChatGPT, Claude, Perplexity) a curated map of key pages. Support is not standardised and it is not required — treat it as a low-effort experiment, not a ranking or citation guarantee.

Search Console / Bing ADVISORY

No search-engine verification found

No Google or Bing ownership-verification signal (meta tag, DNS TXT, or site-auth file) was detected.

Recommended fix

If you haven't already, claim your site in Google Search Console and Bing Webmaster Tools — both free. It's how you see the searches you appear for, submit your sitemap, and get told about indexing or mobile problems. (We can only see the public verification marker, not your account, so treat this as a prompt, not a verdict.)

SAMPLE

Website Compliance & Trust Readiness

1 to address · 2 to review · 1 present

The externally-visible basics a buyer's due-diligence or security questionnaire looks at first. This is a readiness indicator, not a certification or legal advice: it covers the technical, website-visible basics only — not the policy, training and governance parts of a questionnaire, and not the technical controls of a formal scheme such as Cyber Essentials.

✕ **Privacy policy** FAIL

No privacy policy link found

We couldn't find a homepage link mentioning "privacy".

Recommended fix

If your site collects any personal data - even just a contact form - UK GDPR expects a privacy policy that's easy to find, usually linked in the footer.

✓ **Cookie consent** PASS

No consent banner required

⚠ **Contact / business details** ADVISORY

No obvious contact details

We couldn't find a contact link, email or phone on the homepage.

Recommended fix

Buyers and regulators expect a way to reach you. Show a contact link, business email or phone - and, for a limited company, your registered company details.

⚠ **Accessibility statement** ADVISORY

No accessibility statement found

We couldn't find a homepage link mentioning "accessibility".

Recommended fix

An accessibility statement is best practice (and required for public-sector sites). It shows you've considered users with disabilities.

SAMPLE

NEXT STEPS

This report can be handed to your developer or web host. Each failing section above includes a recommended header value, DNS record, or configuration change — these are examples to validate against your own environment before applying, as some (DMARC enforcement, CSP, HSTS preload) can disrupt email or break a site if rolled out without testing. Most items take under an hour to resolve with access to your hosting panel or DNS settings.

If you'd like Smaoin to review the findings and advise on next steps, get in touch:

hello@smaoin.co.uk · smaoin.co.uk