Checkvanta

facebook.com

Security and configuration report

Generated on: 25/07/2026, 17:56:22 UTC

86
Overall score

Website configuration

Subscore 86

DNS

88

- **Name servers** Required
  4 name servers are configured, 4 of them reachable over IPv6.
- **IPv4 address** Required
  The domain resolves to 1 IPv4 address(es), e.g. 157.240.17.35.
- **IPv6 address** Recommended
  The domain resolves to 1 IPv6 address(es), e.g. 2a03:2880:f15b:83:face:b00c:0:25de.
- **MX records** Optional
  1 mail server(s) (MX) are configured for the domain.
- **CAA record** Recommended
  1 CAA record(s) restrict which certificate authorities may issue certificates.
- **DNSSEC** Recommended · Medium
  DNSSEC is not enabled for this domain.
  Recommendation: Enable DNSSEC at your DNS operator and publish the DS record at your registrar; fix any broken chain.

DNS servers

100

- **DNS response** Required
  The domain's nameservers deliver DNS responses.
- **Nameserver redundancy** Required
  The domain has 4 nameservers.
- **Nameservers responding** Required
  All 4 nameservers respond to queries.
- **Authoritative answers** Required
  All nameservers answer authoritatively for the zone.
- **SOA serial in sync** Recommended
  All nameservers report the same SOA serial number.
- **Open recursion** Required
  No nameserver answers recursive queries for foreign domains.
- **Public NS addresses** Required
  All nameserver addresses are publicly reachable.
- **Network dispersion** Recommended
  The nameservers are spread across 8 different networks.
- **Nameservers over IPv6** Recommended
  4 nameservers are reachable over IPv6.
- **SOA refresh** Recommended
  The SOA refresh value (14400) is within the recommended range.
- **SOA retry** Recommended
  The SOA retry value (1800) is within the recommended range.
- **SOA expire** Recommended
  The SOA expire value (604800) is within the recommended range.

- **SOA minimum TTL** Recommended
  The SOA minimum TTL value (300) is within the recommended range.
- **SOA serial format** Optional
  The SOA serial (4207849484) is a valid, increasing integer (as used by many managed-DNS providers).
- **NS match with parent** Recommended
  The zone's NS records match the delegation at the parent.
- **Glue records** Recommended
  The glue records at the parent match the nameservers' actual addresses.
- **Primary listed at parent** Recommended
  The primary nameserver (a.ns.facebook.com) is included in the parent delegation.

HTTP / Security Headers 90

- **Reachability** Required
  The site is reachable over HTTPS.
- **IPv6 reachability** Recommended
  The web server is reachable over IPv6 (2a03:2880:f15b:83:face:b00c:0:25de).
- **Same website over IPv6** Recommended · Low
  IPv6 serves substantially different content than IPv4 (only 33% text similarity).
  Recommendation: Make sure the IPv6 server serves the same content as the IPv4 server (current similarity 33%). This usually stems from a separate, unsynchronised IPv6 backend.
- **HTTPS redirect** Recommended
  Plain HTTP is redirected to HTTPS.
- **HSTS** Recommended
  Your web server sends an HSTS policy.
- **Content-Security-Policy** Recommended
  A Content-Security-Policy header is set.
- **X-Frame-Options** Recommended
  An X-Frame-Options header is set.
- **X-Content-Type-Options** Recommended
  The X-Content-Type-Options header is set to nosniff.
- **Referrer-Policy** Recommended · Low
  No Referrer-Policy header is set.
  Recommendation: Send a Referrer-Policy such as strict-origin-when-cross-origin or no-referrer.
- **HTTP compression** Optional
  HTTP compression (br) is active — a performance plus.
- **security.txt** Recommended
  A security.txt file with a contact address is published.
- **HTTP/2** Recommended
  The web server supports HTTP/2.
- **HTTP/3** Optional
  The web server advertises HTTP/3 (QUIC) via the Alt-Svc header.
- **Cookie security** Recommended · Info
  The homepage sets no cookies that could be assessed.
- **Mixed content** Required
  The page loads no resources over unencrypted HTTP.
- **Subresource integrity** Recommended · Info
  The page loads no external scripts/stylesheets where SRI would be relevant.

RPKI 100

- **RPKI (web server)** Recommended
  The route-origin authorisation of the web server is RPKI-valid.
- **RPKI (nameservers)** Recommended
  The route-origin authorisation of the nameservers is RPKI-valid.

TLS 65

- **HTTPS reachable** Required
  An HTTPS service is reachable and completed a TLS handshake.
- **TLS versions** Required · High
  The server still offers an outdated TLS version (1.0 or 1.1).
  Recommendation: Disable TLS 1.0 and 1.1 in your web server or CDN configuration and offer only TLS 1.2 and 1.3.
- **Cipher suite** Required
  The negotiated cipher suite (TLS_AES_128_GCM_SHA256) provides forward secrecy.
- **Certificate** Required
  The certificate is trusted and valid for this host.
- **Certificate key** Required
  The certificate uses a strong ECDSA key (256 bits).
- **Certificate signature** Required
  The certificate uses a secure signature algorithm (SHA256-RSA).
- **OCSP stapling** Recommended · Low
  The server does not staple an OCSP response.
  Recommendation: Enable OCSP stapling on the web server.
- **DANE (HTTPS)** Optional · Info
  No DANE (TLSA) records are published for HTTPS — an optional bonus for the web, not a shortcoming.
- **Cipher order** Recommended
  With TLS 1.3 the server chooses from a small set of uniformly strong suites — ordering is not a concern.
- **Key exchange** Required
  The key exchange uses ECDHE with hash SHA256 — forward secrecy is provided.
- **TLS compression** Required
  TLS 1.3 has no record compression — the weakness does not apply.
- **Renegotiation** Required
  TLS 1.3 removed renegotiation entirely — no attack surface.
- **Extended Master Secret** Recommended
  TLS 1.3's key schedule supersedes Extended Master Secret — the weakness does not apply.
- **TLS 1.3 0-RTT (early data)** Optional · Low
  The server accepts TLS 1.3 0-RTT (up to 0 bytes of early data). Ensure anti-replay protection is in place.
  Recommendation: Only enable 0-RTT if your server has effective anti-replay protection and restricts early data to safe, idempotent requests. When in doubt, disable it.

Mail configuration

Subscore 86

Mail 71

- **Mail servers (MX)** Required
  The domain has 1 mail server(s) (MX).
- **SPF** Recommended · Medium
  An SPF record is published, but its policy is permissive.
  Recommendation: Publish an SPF record that lists your legitimate senders and ends in `-all` (hard fail). Keep the number of DNS lookups within the limit of ten.

- **DKIM** Recommended · Medium
  The DKIM selector exists, but the key has been revoked (empty `p=` value).
  Recommendation: Publish a DKIM key of at least 2048 bit (RSA) at `<selector>._domainkey.<domain>` and enable DKIM signing on your mail server. Revoked (empty) keys should be removed once no old mail still needs to be verified with them.
- **DMARC** Recommended
  A DMARC record with an enforcing policy (p=reject) is published.
- **BIMI** Optional · Info
  The domain does not publish a BIMI record.
  Recommendation: Optional: publish an SVG logo (SVG Tiny PS) at an HTTPS URL and a TXT record `default._bimi.<domain>` with `v=BIMI1; l=<logo URL>`. An enforcing DMARC policy (`p=quarantine` or `p=reject`) is required; some providers additionally require a paid VMC certificate.
- **MTA-STS** Recommended
  MTA-STS is set up but in “testing” mode — violations are only reported, not enforced.
- **TLS-RPT** Optional
  The domain publishes a valid TLS-RPT record.
- **MX over IPv6** Recommended
  All mail servers have an IPv6 address.
- **STARTTLS** Required
  All mail servers offer STARTTLS with a valid certificate.
- **Mail TLS version** Required
  All mail servers negotiate a modern TLS version (1.2 or 1.3).
- **DANE (SMTP)** Recommended · Low
  No DANE (TLSA) records are published for the mail servers.
  Recommendation: With DNSSEC in place, publish TLSA records at `_25._tcp.<mx>` that match each mail server's certificate, and rotate them together with the certificate.
- **Cipher suite (mail)** Recommended
  All mail servers use cipher suites with forward secrecy.
- **Mail server certificate** Required
  All mail servers present a valid certificate matching the hostname.
- **Mail server key** Required
  The certificate keys of all mail servers are sufficiently strong.
- **Mail server signature** Required
  The certificates of all mail servers use a secure signature.
- **TLS compression (mail)** Required
  No mail server has TLS compression enabled.
- **Renegotiation (mail)** Required
  All mail servers support secure renegotiation or use TLS 1.3.
- **Extended Master Secret (mail)** Recommended
  All mail servers support Extended Master Secret or use TLS 1.3.
- **Reverse DNS (PTR)** Recommended
  All checked mail server IPs have a PTR record.
- **Open relay** Required · Info
  The open-relay test could not be performed (no SMTP connection).

Blacklist 100

- **Spamhaus ZEN** Required
  Not listed on Spamhaus ZEN (zen.spamhaus.org).
- **Spamhaus DBL** Required
  Not listed on Spamhaus DBL (dbl.spamhaus.org).

- **Barracuda** Required
  Not listed on Barracuda (b.barracudacentral.org).
- **SpamCop** Required
  Not listed on SpamCop (bl.spamcop.net).
- **PSBL** Required
  Not listed on PSBL (psbl.surriel.com).
- **0SPAM** Required
  Not listed on 0SPAM (bl.0spam.org).
- **BLOCKLIST.DE** Required
  Not listed on BLOCKLIST.DE (bl.blocklist.de).
- **SURBL multi** Recommended
  Not listed on SURBL multi (multi.surbl.org).
- **SEM FRESH** Recommended
  Not listed on SEM FRESH (fresh.spameatingmonkey.net).
- **SEM Blacklist** Recommended
  Not listed on SEM Blacklist (bl.spameatingmonkey.net).
- **SEM Backscatter** Recommended
  Not listed on SEM Backscatter (backscatter.spameatingmonkey.net).
- **SPFBL** Recommended
  Not listed on SPFBL (dnsbl.spfbl.net).
- **GBUdb Truncate** Recommended
  Not listed on GBUdb Truncate (truncate.gbudb.net).
- **SpamRATS RATS-Spam** Recommended
  Not listed on SpamRATS RATS-Spam (spam.spamrats.com).
- **SpamRATS RATS-Dyna** Recommended
  Not listed on SpamRATS RATS-Dyna (dyna.spamrats.com).
- **SpamRATS RATS-NoPtr** Recommended
  Not listed on SpamRATS RATS-NoPtr (noptr.spamrats.com).
- **JustSpam** Recommended
  Not listed on JustSpam (dnsbl.justspam.org).
- **Fabel Spamsources** Recommended
  Not listed on Fabel Spamsources (spamsources.fabel.dk).
- **s5h.net** Recommended
  Not listed on s5h.net (all.s5h.net).
- **DroneBL** Recommended
  Not listed on DroneBL (dnsbl.dronebl.org).
- **InterServer RBL** Recommended
  Not listed on InterServer RBL (rbl.interserver.net).
- **Mailspike** Recommended
  Not listed on Mailspike (z.mailspike.net).
- **UCEPROTECT Level 1** Recommended
  Not listed on UCEPROTECT Level 1 (dnsbl-1.uceprotect.net).
- **UCEPROTECT Level 2** Optional
  Not listed on UCEPROTECT Level 2 (dnsbl-2.uceprotect.net).
- **UCEPROTECT Level 3** Optional
  Not listed on UCEPROTECT Level 3 (dnsbl-3.uceprotect.net).

RPKI (mail) 95

- **RPKI (mail servers)** Recommended · Low
  No RPKI authorisation (ROA) exists for the IP addresses of the mail servers.
  Recommendation: Publish a ROA (Route Origin Authorisation) for the IP prefixes of the mail servers with your network operator or RIR, authorising the correct announcing ASN and maximum prefix length. For an "invalid" result, check the ASN and max prefix length in the existing ROA.