Automated scan run by Tessera: 11 October 2026 at 11:10 (Rome time). The results describe the state of the site at that time.

CONFIDENTIAL — do not distribute

Security Quick Check Report

Target	**https://www.shop.example/**
HTTP status	**200**
Report ID	**example**
Test date and time	**11 October 2026 at 11:10 (Rome time)**
Prepared by	**Tessera Quick Check — automated scanning platform (no human review)**



SECURITY SCORE

Grade D · Needs work

High	0
Medium	4
Low	6
Informational	4

100 minus 25 points for each High issue, 10 for each Medium and 3 for each Low; informational findings do not count. With at least one High issue the score cannot exceed 49, with at least one Medium it cannot exceed 79.

Executive Summary

Overall risk level: MEDIUM

The site www.shop.example has no high-severity vulnerabilities. Four medium-severity issues were found, all related to configuration: the headers that protect the browser are missing (Content-Security-Policy, Strict-Transport-Security, clickjacking protection) and the server still accepts TLS 1.0 and 1.1. These are server configuration changes that can be made in a few hours without touching the application. The six low-severity issues are mostly about hardening and exposed information.

Summary written by Claude (Anthropic) based on the findings of this scan.

Severity scale

High
Directly exploitable issue with serious impact (e.g. authentication bypass, data exposure, code execution). Requires urgent action.

Medium
Exploitable under specific conditions, or a weakness in controls that significantly increases risk without being directly exploitable on its own. To be fixed in the short term.

Low
Limited practical impact on its own, typically a hardening or defence-in-depth gap. To be addressed during normal maintenance.

Informational
Observation with no direct security impact, included for completeness or awareness.

Scope and rules of engagement

Target tested: https://www.shop.example/. Test type: black-box, external, without credentials (no authenticated user session was used in this scan). Authorisation basis: control of the domain www.shop.example was verified by Tessera through a DNS TXT record published by the customer; last verified: 11 October 2026 at 10:55 (Rome time). The user also declared in the interface that they are authorised to run the test. This does not replace a letter of authorisation signed by the site owner.

In scope:

- Public surface of the site reachable from the given URL (pages, static assets, endpoints discovered by the ZAP spider)
- HTTP security headers and TLS/HTTPS configuration
- Known vulnerabilities, misconfigurations and default credentials (Nuclei)
- Application vulnerabilities detectable passively and with automated active probes (ZAP)

Out of scope:

- Authenticated areas or areas that require a user account
- Application source code
- Underlying cloud infrastructure beyond what is publicly exposed
- Social engineering, physical testing, denial of service

Methodology

This Quick Check combines passive and active checks run automatically: HTTP security header review, TLS configuration analysis (testssl.sh), detection of known vulnerabilities and misconfigurations with Nuclei, and an application scan with OWASP ZAP (spider, passive scan and active scan). Unlike a manual penetration test, this Quick Check does not include source code review or targeted testing of the application's authorisation logic: it identifies the issues that can be detected automatically from the outside, within a limited time window.

Reference standards and frameworks

CVSS v3.1 (FIRST.org)

Severity score calculated with the official formula published by FIRST, not estimated: for Nuclei findings it is taken from the template metadata when available, for ZAP findings it is assessed following the official methodology and stated openly (vector + score) in each finding. The risk level shown (High/Medium/Low) is derived from the CVSS score (High >= 7.0, Medium 4.0-6.9, Low < 4.0), not from the tool's raw severity.

CWE — Common Weakness Enumeration (MITRE)

Every finding with a security impact is classified according to the standard weakness taxonomy.

PTES — Penetration Testing Execution Standard

Report structure aligned with the sections defined by the standard: executive summary, scope and rules of engagement, methodology, detailed findings, prioritised recommendations, technical appendices.

OWASP Testing Guide (WSTG)

Methodological reference for the areas actually covered by this Quick Check (security headers, TLS/HTTPS configuration, known vulnerabilities). It does not cover the whole WSTG: business logic, authentication and session management are out of scope — see Limitations.

NIST SP 800-115

General engagement structure (planning, discovery, vulnerability testing, reporting) applied in automated form to a single scan.

Limitations — what was not tested

- No source code review: findings come exclusively from behaviour observable from the outside.
- No targeted review of authorisation logic or of the application's specific business logic (e.g. privilege escalation between roles, bypass of multi-step flows).
- No testing of authenticated areas: the scan does not use credentials or user sessions.
- No manual verification or proof of concept for individual findings: results come entirely from automated tools (ZAP, Nuclei, testssl.sh) and have not been manually confirmed by an operator.
- Nuclei limited to a curated subset of templates, not the full template corpus available.

Detailed findings

Medium 1. Strict-Transport-Security Header Not Set

CWE-319

CVSS 3.1: 4.8 (Medium) — CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N (vector assessed for this alert type, not provided natively by ZAP)

HTTP Strict Transport Security (HSTS) is not enforced: the site does not tell the browser to use HTTPS only, so a first visit can be intercepted on an untrusted network.

Evidence: https://www.shop.example/ · https://www.shop.example/products (+25 more occurrences)

Recommendation: Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security with a duration of at least one year (max-age=31536000).

Detected by: OWASP ZAP

Medium 2. Deprecated protocols enabled: TLS 1.0, TLS 1.1

CWE-326

CVSS 3.1: 4.8 (Medium) — CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N (vector assessed by Tessera)

The server accepts TLS 1.0 and TLS 1.1 connections, deprecated protocols (RFC 8996) that modern browsers and compliance standards (e.g. PCI DSS) no longer accept.

Evidence: TLS 1 offered (deprecated)

Recommendation: Disable TLS 1.0 and 1.1 and keep only TLS 1.2 and 1.3.

Detected by: testssl.sh

Medium 3. Missing Anti-clickjacking Header

CWE-1021

CVSS 3.1: 4.3 (Medium) — CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N (vector assessed for this alert type, not provided natively by ZAP)

The response does not protect against 'ClickJacking' attacks: the page can be loaded in an iframe on another site, which can trick the user into clicking on hidden elements.

Evidence: https://www.shop.example/ · https://www.shop.example/account/login · https://www.shop.example/cart (+16 more occurrences)

Recommendation: Set the X-Frame-Options header to DENY or SAMEORIGIN, or use the frame-ancestors directive of the Content-Security-Policy header.

Detected by: OWASP ZAP

Medium 4. Content Security Policy (CSP) Header Not Set

CWE-693

CVSS 3.1: 4.2 (Medium) — CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N (vector assessed for this alert type, not provided natively by ZAP)

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. Without CSP the browser runs any script present in the page.

Evidence: https://www.shop.example/ · https://www.shop.example/products · https://www.shop.example/cart · https://www.shop.example/contact (+19 more occurrences)

Recommendation: Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, starting from a restrictive policy (default-src 'self') and adding only the origins you need.

Detected by: OWASP ZAP

Low 5. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

CWE-497

CVSS 3.1: 3.7 (Low) — CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N (vector assessed for this alert type, not provided natively by ZAP)

The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers (PHP/8.1.2). Access to such information may help an attacker find known vulnerabilities in that version.

Evidence: https://www.shop.example/ · https://www.shop.example/products (+22 more occurrences)

Recommendation: Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers (in PHP: expose_php = Off).

Detected by: OWASP ZAP

Low 6. HTTPS Content Available via HTTP

CWE-311

CVSS 3.1: 3.7 (Low) — CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N (vector assessed for this alert type, not provided natively by ZAP)

Content which was initially accessed via HTTPS is also accessible via HTTP without a redirect: anyone using the plain-text connection exposes their data to interception.

Evidence: http://www.shop.example/

Recommendation: Ensure that your web server, application server, load balancer, etc. is configured to only serve such content via HTTPS, with a permanent (301) redirect from HTTP, and enable HSTS.

Detected by: OWASP ZAP

Low

7. CBC ciphers enabled (potential exposure to LUCKY13)

CWE-327

CVSS 3.1: 3.7 (Low) — CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N (vector assessed by Tessera)

The server offers CBC-mode cipher suites. testssl.sh reports potential exposure to LUCKY13 (CVE-2013-0169), a timing attack that is hard to exploit on modern implementations, but the presence of CBC is considered a hardening gap.

Evidence: LUCKY13 (CVE-2013-0169), experimental potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches

Recommendation: Prefer AEAD suites (AES-GCM, ChaCha20-Poly1305) with forward secrecy and remove CBC suites if the clients you need to support allow it; make sure the TLS library is up to date.

Detected by: testssl.sh

Low

8. Cookie without SameSite Attribute

CWE-1275

CVSS 3.1: 3.1 (Low) — CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N (vector assessed for this alert type, not provided natively by ZAP)

A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request, making cross-site request forgery attacks easier.

Evidence: https://www.shop.example/ · https://www.shop.example/account/login

Recommendation: Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Detected by: OWASP ZAP

Low

9. X-Content-Type-Options Header Missing

CWE-693

CVSS 3.1: 3.1 (Low) — CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N (vector assessed for this alert type, not provided natively by ZAP)

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff': some browsers may interpret a file as a different type from the one declared.

Evidence: https://www.shop.example/ · https://www.shop.example/static/app.js · https://www.shop.example/static/style.css (+28 more occurrences)

Recommendation: Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all responses.

Detected by: OWASP ZAP

Low

10. Cookie No HttpOnly Flag

CWE-1004

CVSS 3.1: 3.1 (Low) — CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N (vector assessed for this alert type, not provided natively by ZAP)

A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page, for example through an XSS vulnerability, the cookie will be accessible.

Evidence: https://www.shop.example/account/login

Recommendation: Ensure that the HttpOnly flag is set for all cookies that do not need to be read by JavaScript, starting with the session cookie.

Detected by: OWASP ZAP

Informational

11. Information Disclosure - Suspicious Comments

CWE-615

The response appears to contain suspicious comments which may help an attacker (for example development notes or references to internal functions).

Evidence: https://www.shop.example/static/app.js (+1 more occurrence)

Recommendation: Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

Detected by: OWASP ZAP

Informational

12. Storable and Cacheable Content

CWE-524

The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server.

Evidence: https://www.shop.example/products · https://www.shop.example/contact (+7 more occurrences)

Recommendation: Validate that the response does not contain sensitive, personal or user-specific information. If it does, use Cache-Control: no-store, private.

Detected by: OWASP ZAP

Informational

13. Re-examine Cache-control Directives

CWE-525

The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content that may be personal.

Evidence: https://www.shop.example/account · https://www.shop.example/cart (+2 more occurrences)

Recommendation: For pages with personal data set Cache-Control: no-store; for static assets set an explicit cache duration.

Detected by: OWASP ZAP

Informational

14. Loosely Scoped Cookie

CWE-565

Cookies can be scoped by domain or path. The cookie is scoped to a parent domain, so other subdomains can receive and change it.

Evidence: https://www.shop.example/account/login

Recommendation: Always scope cookies to a FQDN (Fully Qualified Domain Name).

Detected by: OWASP ZAP

Positive findings

- TLS grade: B (testssl, experimental). The grade does not take HSTS or CBC ciphers into account: see the TLS findings and the Strict-Transport-Security header.
- TLS 1.3 supported.
- Forward secrecy with AEAD ciphers available.
- Certificate chain of trust valid.
- No exposure to Heartbleed, ROBOT, POODLE, SWEET32, FREAK, DROWN and the other known TLS vulnerabilities checked by testssl.sh.
- No known vulnerabilities found by Nuclei.

Prioritised recommendations

P1 — Protect the HTTPS connection

- Enable Strict-Transport-Security and a permanent redirect from HTTP to HTTPS.
- Disable TLS 1.0 and 1.1, keeping only TLS 1.2 and 1.3.

P2 — Add the security headers

- Introduce a Content-Security-Policy, starting in report-only mode so that existing features keep working.
- Set X-Frame-Options (or frame-ancestors) and X-Content-Type-Options: nosniff.

P3 — Reduce exposed information and harden cookies

- Turn off the X-Powered-By header (expose_php = Off).
- Set SameSite on session cookies and review the cache directives of personal pages.

Technical appendix — Security headers

Content-Security-Policy	**Missing**
Strict-Transport-Security	**Missing**
X-Frame-Options	**Missing**
X-Content-Type-Options	**Missing**

Note: X-Powered-By: PHP/8.1.2

Technical appendix — TLS (testssl.sh, full output)

```
 Start 2026-10-11 09:02:14        -->> 203.0.113.10:443 (www.shop.example) <<--

 rDNS (203.0.113.10):           --
 Service detected:       HTTP

 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      offered (deprecated)
 TLS 1.1    offered (deprecated)
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final

 Testing cipher categories

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            offered
 Strong encryption (AEAD ciphers) with no FS       not offered
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)

 Testing server defaults (Server Hello)

 Certificate Validity (UTC)   78 >= 60 days (2026-09-12 00:00 --> 2026-12-28 23:59)
 Chain of trust               Ok
 OCSP stapling                not offered

 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)               not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                      not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
 ROBOT                                    not vulnerable (OK)
 Secure Renegotiation (RFC 5746)          supported (OK)
 CRIME, TLS (CVE-2012-4929)               not vulnerable (OK)
 POODLE, SSL (CVE-2014-3566)              not vulnerable (OK), no SSLv3 support
 SWEET32 (CVE-2016-2183, CVE-2016-6329)   not vulnerable (OK)
 FREAK (CVE-2015-0204)                    not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)     not vulnerable on this host and port (OK)
 LOGJAM (CVE-2015-4000), experimental     not vulnerable (OK): no DH key detected with <= TLS 1.2
 BEAST (CVE-2011-3389)                    TLS1: ECDHE-RSA-AES128-SHA
                                          VULNERABLE -- but also supports higher protocols  TLSv1.1
TLSv1.2 (likely mitigated)
 LUCKY13 (CVE-2013-0169), experimental    potentially VULNERABLE, uses cipher block chaining (CBC)
ciphers with TLS. Check patches
 RC4 (CVE-2013-2566, CVE-2015-2808)       no RC4 ciphers detected (OK)

 Rating (experimental)

 Overall Grade                B
 Grade cap reasons            Grade capped to B. TLS 1.1 offered
                              Grade capped to B. TLS 1.0 offered

 Done 2026-10-11 09:03:31 [  79s] -->> 203.0.113.10:443 (www.shop.example) <<--
```