

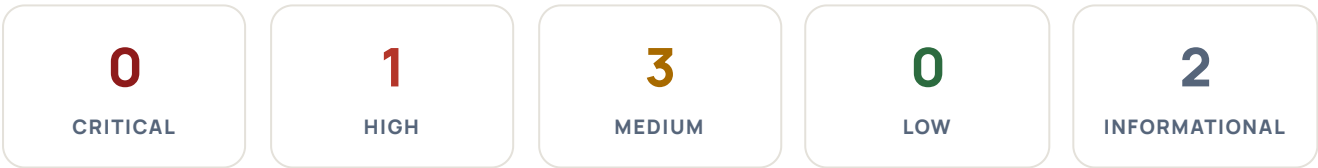
ASSESSMENT REPORT

Web Vulnerability Assessment

shop.example.com

PREPARED FOR	Example Shop Ltd (client of Northwind Web Studio)
PREPARED BY	Northwind Web Studio · using ScanBastion
DATE	21 October 2026, 09:42–09:56 UTC
SCOPE	https://shop.example.com/* (verified target · DNS TXT, 3 Oct 2026)
PROFILE	Standard
METHODS	HTTP security headers · TLS/certificate analysis · passive OWASP ZAP assessment · curated Nuclei templates (set 2026.10.2)
REPORT ID	SB-2026-10-21-4F7A

Summary



Verification status: **1 confirmed** · **3 needs review** · 0 dismissed as false positive. Counts above include unverified findings; see page 3.

Partial stage. Curated Nuclei checks: 3 of 212 templates timed out and did not complete. The affected templates are listed in Appendix B. Findings in that category may be incomplete.

The assessment found **no confirmed critical or high-severity vulnerability**. One high-severity detection (an outdated JavaScript library) is awaiting review and should be checked first. Three medium-severity configuration issues were found, of which the TLS protocol finding is confirmed. The most valuable next steps are to upgrade jQuery, disable TLS 1.0 and 1.1, add a Content-Security-Policy and set the Secure flag on the session cookie; together these are a few hours of configuration work.

Limitations

This was an external, unauthenticated, automated assessment under the Standard profile. It observed what an anonymous visitor on the internet can reach. It did not test pages behind a log-in, did not submit forms, did not send attack payloads, and did not assess business logic, infrastructure beyond HTTPS, or the organisation's processes. Automated results can include false positives and miss real issues. A report with no findings would not mean the site is free of vulnerabilities. For assurance, commission a manual penetration test. See page 8.

1. Scope and authorisation

The target shop.example.com was verified by DNS TXT record on 3 October 2026 and re-verified at the start of this scan. Authorisation to assess the domain was confirmed by the account holder (Northwind Web Studio) on behalf of the site owner. The scan covered the verified hostname only; api.example.com and other subdomains were out of scope.

2. Method

STAGE	WHAT IT DOES	REQUESTS	STATUS
HTTP security headers	Inspects response headers on 14 crawled pages	14	Completed
TLS / certificate	Negotiates TLS with varied protocol and cipher offers; validates chain	31 handshakes	Completed
Passive OWASP ZAP	Crawls public pages to depth 3 and analyses responses; no payloads	86	Completed
Curated Nuclei templates	Non-intrusive detection requests for known exposures and versions	241	Partial (3 templates timed out)

Total requests sent: 372 over 14 minutes 8 seconds, peak 2 requests/second. Scanner identified itself with a User-Agent containing ScanBastion from the published scanner address range.

3. Coverage and exclusions

- **Included:** transport security, browser-facing headers, cookie attributes, information disclosure, exposed files and panels, known-vulnerable component versions, common misconfigurations.
- **Not included in this profile:** active injection testing, authenticated areas (/account beyond the log-in page, /checkout steps 2-4), form submission, port scanning, business-logic testing.
- **Not reachable:** 2 URLs returned 403 to the scanner and were not analysed (Appendix B).

4. How to read the findings

Each finding carries three independent fields.

FIELD	MEANING
Severity	How serious the issue would be if real: Critical, High, Medium, Low, Informational. A generic rating; it does not account for this site's specific context.
Confidence	How sure the detection method is: High (observed directly), Medium (inferred, e.g. from a version string), Low (pattern match that often misfires).
Verification	Whether a person has reviewed the evidence: Confirmed, Needs review, or False positive. Set by the assessor, not by the scanner.

Findings marked **Needs review** are the scanner's detections, not yet confirmed by the assessor. They should be checked before being treated as vulnerabilities.

5. Findings overview

#	SEVERITY	FINDING	AFFECTED	CONFIDENCE	VERIFICATION	SOURCE
1	HIGH	Outdated jQuery 1.12.4 detected	/assets/js/vendor.min.js	Medium	Needs review	Nuclei
2	MEDIUM	TLS 1.0 and 1.1 accepted	shop.example.com:443	High	Confirmed	TLS
3	MEDIUM	Content-Security-Policy not set	/ and 11 pages	High	Needs review	Headers, ZAP
4	MEDIUM	Session cookie missing Secure flag	/account	High	Needs review	Headers, ZAP
5	INFO	Server version disclosed in header	all pages	High	Confirmed	Headers
6	INFO	Third-party script without Subresource Integrity	/ and 11 pages	High	Needs review	ZAP

6. Recommended order of work

PRIORITY	ACTION	CLEARs	EFFORT
1	Verify whether the site calls jQuery functions covered by the published advisories; upgrade to jQuery 3.x regardless and test dependent plugins	#1	2–4 h incl. testing
2	Set minimum TLS version to 1.2 in the web server or CDN	#2	15 min
3	Set Secure; HttpOnly; SameSite=Lax on the session cookie in the application config	#4	30 min
4	Introduce a Content-Security-Policy in report-only mode, then enforce	#3, partly #6	1–2 days elapsed, 2–3 h work
5	Remove the Server version token; add integrity to the analytics script or self-host it	#5, #6	30 min

Effort estimates are indicative, for a developer familiar with the stack. After the changes, rescan with the same profile to confirm; a comparison against this report (ID SB-2026-10-21-4F7A) will be generated automatically.

7. Rescan and verification plan

After the changes above are deployed, rescan the target with the same profile. The rescan report compares against this one (ID SB-2026-10-21-4F7A): findings that no longer reproduce are listed as resolved, unchanged findings keep their verification decisions, and anything new is flagged as new. Decisions recorded in the verification log carry forward, so a finding dismissed as a false positive here is not raised again as new.

Recommended cadence for a site of this kind: a Quick scan after every deployment, a Standard scan monthly, and a manual review of any High or Critical detection within two working days of it appearing.

FINDING 1 OF 6

HIGH Outdated jQuery 1.12.4 detected

CONFIDENCE Medium	VERIFICATION Needs review	SOURCE Nuclei · tech/jquery-version
----------------------	------------------------------	--

Affected

https://shop.example.com/assets/js/vendor.min.js (loaded by 12 pages)

What this means

The page loads a jQuery version with published cross-site scripting advisories (CVE-2015-9251, CVE-2019-11358, CVE-2020-11022, CVE-2020-11023). Whether the site is exploitable depends on how it uses the affected functions (for example passing untrusted HTML to `.html()` or `$()`). The version number alone is not proof of exploitability, which is why confidence is Medium.

Evidence

```
GET /assets/js/vendor.min.js HTTP/1.1 → 200 OK · 91,204 bytes
/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license */
```

Remediation

Upgrade to a supported jQuery 3.x release and test dependent plugins (the theme's slider and the cart widget were observed using jQuery). If an immediate upgrade is not possible, review whether untrusted input ever reaches the affected functions, and add a Content-Security-Policy (finding 3) to reduce the impact of any cross-site scripting. Rescan to verify.

First seen 21 Oct 2026 · References: jQuery 3.5 release notes; NVD entries for the CVEs above.

FINDING 2 OF 6

MEDIUM TLS 1.0 and 1.1 accepted

CONFIDENCE

High

VERIFICATION

Confirmed · 21 Oct, N. Okafor

SOURCE

TLS analysis

Affected

shop.example.com:443

What this means

The server completed handshakes using TLS 1.0 and TLS 1.1 as well as TLS 1.2 and 1.3. These versions are deprecated (RFC 8996) and rejected by current browsers; an attacker able to interfere with a connection from an older client may force a downgrade to a weaker protocol.

Evidence

```
ClientHello max=TLS1.0 → ServerHello TLS1.0 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ClientHello max=TLS1.1 → ServerHello TLS1.1 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ClientHello max=TLS1.3 → ServerHello TLS1.3 TLS_AES_256_GCM_SHA384 (preferred)
```

Remediation

Set the minimum protocol version to TLS 1.2 in the web server (nginx: ssl_protocols TLSv1.2 TLSv1.3;) or in the CDN's edge TLS settings if TLS is terminated there. Rescan to verify.

FINDING 3 OF 6

MEDIUM Content-Security-Policy not set

CONFIDENCE

High

VERIFICATION

Needs review

SOURCE

Headers · ZAP 10038

Affected: / and 11 other crawled pages. **What this means:** no Content-Security-Policy header is sent, so if a cross-site scripting bug exists anywhere on the site (see finding 1) the browser will not restrict what injected script can do. The header is absent rather than weak, which is unambiguous. **Remediation:** deploy a policy in Content-Security-Policy-Report-Only mode first, starting from default-src 'self'; frame-ancestors 'none'; base-uri 'self'; form-action 'self', add the analytics and payment origins the site legitimately uses, then enforce.

```
GET / HTTP/1.1 → 200 OK
content-type: text/html; charset=UTF-8
(no content-security-policy header)
x-frame-options: SAMEORIGIN
```

FINDING 4 OF 6

MEDIUM Session cookie missing Secure flag

CONFIDENCE
High

VERIFICATION
Needs review

SOURCE
Headers · ZAP 10011

Affected: /account. **What this means:** the response sets PHPSESSID without the Secure attribute. Because the site is also reachable over plain HTTP (it redirects, but only after the first request), the browser may send the session cookie in clear text. **Remediation:** set Secure, HttpOnly and SameSite=Lax on the session cookie (PHP: session.cookie_secure=1) and add Strict-Transport-Security.

```
GET /account HTTP/1.1 → 200 OK
set-cookie: PHPSESSID=...; path=/; HttpOnly
```

Informational findings

#	FINDING	EVIDENCE	SUGGESTION
5	Server version disclosed	server: nginx/1.18.0	Set server_tokens off;. Low impact; removes a hint for attackers.
6	Third-party script without SRI	cdn.example-analytics.net/tag.js	Add integrity and crossorigin, or self-host. Depends on the provider publishing versioned files.

Appendix A. Verification log

FINDING	DECISION	BY	NOTE
#2 TLS 1.0/1.1	Confirmed	N. Okafor, 21 Oct 2026	Reproduced with openssl s_client -tls1
#5 Server version	Confirmed	N. Okafor, 21 Oct 2026	Visible in every response

8. Limitations of this assessment

- This is an automated, external, unauthenticated scan. It is **not a penetration test** and does not replace one.
- Automated detections can be **false positives**; findings marked Needs review have not been confirmed. Automated scans also **miss** issues, in particular anything behind a log-in, business-logic flaws and novel bugs in custom code.
- Coverage is limited to the Standard profile, the curated template set 2026.10.2, and pages reachable by the crawler. One stage completed partially (Appendix B).
- Results reflect the site at the time of the scan. Configuration and content change; rescan after changes and on a regular schedule.
- Severity ratings are generic. The assessor's recommended order of work (page 3) reflects context the scanner cannot know.

Appendix B. Stage detail

ITEM	DETAIL
Nuclei templates timed out	http/exposures/backups/zip-backup-files.yaml · http/misconfiguration/directory-listing-deep.yaml · http/technologies/wordpress-plugins/enum.yaml
URLs returning 403 to scanner	/wp-admin/ · /xmlrpc.php
Pages crawled	14 (depth 3, same host only)
Scanner source	Published ScanBastion scanner address range · User-Agent: Mozilla/5.0 (compatible; ScanBastion/1.0; +https://scanbastion.com/responsible-scanning)
Template set	Curated set 2026.10.2 (212 templates enabled; intrusive, dos, fuzz and bruteforce tags excluded)

Assessor: N. Okafor, Northwind Web Studio

Generated by ScanBastion · Report ID SB-2026-10-21-4F7A

This sample report is published by ScanBastion to show the planned report format. The target, organisations, people and findings are fictional. The format is planned for the first release and may change.