Northwind Storefront (Demo)

Web Application Penetration Test — Sample Report

RISK SCORE
89 / 100
CRITICAL RISK

1	2	3	2	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

TARGET
Northwind Storefront (Demo)
`demo.pentestme-sample.com`

SCAN
Full Web Assessment
web_application

STARTED
7/20/2026, 8:05:00 AM

COMPLETED
7/20/2026, 9:41:00 AM

Executive Summary

This security assessment of Northwind Storefront (Demo) (demo.pentestme-sample.com) identified 9 security findings. 1 critical vulnerability requires immediate attention. 2 high-severity vulnerabilities should be addressed as soon as possible. 3 medium-severity issues were also identified. 2 low-severity and 1 informational findings are included for completeness. Please review the detailed findings below and implement the recommended remediations to improve your security posture.

Methodology Coverage

OWASP Top 10 (2021) coverage based on probes that ran during this scan. Categories with findings are confirmed-tested; categories with no findings were also tested but produced no exploitable results. Coverage: **5/10** categories produced findings.

CODE	CATEGORY	FINDINGS	STATUS
A01	Broken Access Control	1	tested
A02	Cryptographic Failures	1	tested
A03	Injection	2	tested
A04	Insecure Design	0	tested · no findings
A05	Security Misconfiguration	4	tested
A06	Vulnerable and Outdated Components	1	tested
A07	Identification and Authentication Failures	0	tested · no findings
A08	Software and Data Integrity Failures	0	tested · no findings
A09	Security Logging and Monitoring Failures	0	tested · no findings
A10	Server-Side Request Forgery (SSRF)	0	tested · no findings

Findings Summary

FINDING	SEVERITY	CVSS	STATUS
SQL Injection on login endpoint EXPLOITED	CRITICAL	9.8	open
Reflected XSS in search parameter EXPLOITED	HIGH	7.1	open
IDOR on order history API EXPLOITED	HIGH	6.5	open
Content-Security-Policy and HSTS not set	MEDIUM	4.3	open
jQuery 1.12.1 with known vulnerabilities	MEDIUM	5.3	open
Weak DMARC policy (p=none)	MEDIUM	4	open
TLS 1.0/1.1 still enabled	LOW	3.7	open
Server version leaked in headers	LOW	3.1	open
Open directory listing on /uploads	INFO	–	open

Detailed Findings

CRITICAL SEVERITY (1 finding)

CRITICAL

SQL Injection on login endpoint

CVSS 9.8 | CWE CWE-89 | OWASP A03:2021 - Injection | Status open

AFFECTED URL

```
https://demo.pentestme-sample.com/login
```

VULNERABLE PARAMETER

```
email
```

ATTACK PAYLOAD

```
email=' OR 1=1-- -&password=x
```

DESCRIPTION

The login endpoint concatenates the `email` field into a SQL query without parameterisation. A crafted value bypasses authentication and permits extraction of arbitrary table data.

EVIDENCE

```
Response time and boolean-based responses confirmed injection; UNION query returned 8 columns (redacted).
```

PROOF OF CONCEPT

```
Submitting email=admin' -- to /login returns a valid session for the first admin row. A UNION-based payload extracted the users table schema (redacted).
```

REMEDIATION

Use parameterised queries / prepared statements for all database access. Apply least-privilege DB credentials and add WAF rules as defence in depth.

HIGH SEVERITY (2 findings)

HIGH

Reflected XSS in search parameter

CVSS 7.1 | CWE CWE-79 | OWASP A03:2021 - Injection | Status open

AFFECTED URL

`https://demo.pentestme-sample.com/search`

VULNERABLE PARAMETER

`q`

DESCRIPTION

The `q` parameter is reflected into the response without output encoding, allowing arbitrary script execution in the victim browser.

PROOF OF CONCEPT

`q=<script>alert(document.domain)</script> executed in a standard browser session.`

REMEDIATION

Context-aware output encoding on all reflected values; apply a strict Content-Security-Policy.

HIGH

IDOR on order history API

CVSS 6.5 | CWE CWE-639 | OWASP A01:2021 - Broken Access Control | Status open

AFFECTED URL

`https://demo.pentestme-sample.com/api/orders/{id}`

DESCRIPTION

Incrementing the numeric order id returns other customers' order records, including name and address, with no ownership check.

REMEDIATION

Enforce per-object authorisation server-side; use unguessable identifiers and verify the authenticated user owns the resource.

MEDIUM SEVERITY (3 findings)

MEDIUM

Content-Security-Policy and HSTS not set

CVSS 4.3 | CWE CWE-693 | OWASP A05:2021 - Security Misconfiguration | Status open

AFFECTED URL

`https://demo.pentestme-sample.com/`

DESCRIPTION

Responses omit Content-Security-Policy, Strict-Transport-Security and X-Content-Type-Options, increasing the impact of injection and downgrade attacks.

REMEDIATION

Add CSP, HSTS (with preload), X-Content-Type-Options: nosniff and a Referrer-Policy at the edge.

MEDIUM

jQuery 1.12.1 with known vulnerabilities

CVSS 5.3 | CWE CWE-1104 | OWASP A06:2021 - Vulnerable and Outdated Components | CVE CVE-2020-11022

Status open

AFFECTED URL

`https://demo.pentestme-sample.com/assets/jquery.min.js`

DESCRIPTION

The bundled jQuery 1.12.1 is affected by known cross-site scripting issues in HTML manipulation methods.

REMEDIATION

Upgrade to a current jQuery release (3.5+) and add automated dependency scanning to CI.

MEDIUM

Weak DMARC policy (p=none)

CVSS 4 | OWASP A05:2021 - Security Misconfiguration | Status open

AFFECTED URL

`demo.pentestme-sample.com`

DESCRIPTION

The domain publishes DMARC with p=none, so spoofed mail is neither quarantined nor rejected.

REMEDIATION

Move DMARC to p=quarantine then p=reject after monitoring aggregate reports; confirm SPF and DKIM alignment.

LOW SEVERITY (2 findings)

LOW

TLS 1.0/1.1 still enabled

CVSS 3.7 | OWASP A02:2021 - Cryptographic Failures | Status open

AFFECTED URL

`https://demo.pentestme-sample.com/`

DESCRIPTION

The server negotiates deprecated TLS 1.0/1.1 protocols.

REMEDIATION

Disable TLS 1.0/1.1; require TLS 1.2+ with modern cipher suites.

LOW

Server version leaked in headers

CVSS 3.1 | OWASP A05:2021 - Security Misconfiguration | Status open

AFFECTED URL

`https://demo.pentestme-sample.com/`

DESCRIPTION

The Server response header discloses the exact nginx version, aiding targeted attacks.

REMEDIATION

Suppress or genericise the Server header at the reverse proxy.

INFO SEVERITY (1 finding)

INFO

Open directory listing on /uploads

OWASP A05:2021 - Security Misconfiguration | Status open

AFFECTED URL

`https://demo.pentestme-sample.com/uploads/`

DESCRIPTION

The /uploads path returns an auto-generated index of files.

REMEDIATION

Disable auto-indexing (autoindex off) and restrict access to intended files.

Discovered Ports & Services

PORT / HOST	PROTOCOL	STATE	SERVICE	VERSION
443	tcp	open	https	1.24.0
80	tcp	open	http	1.24.0