Bug Circuit

Manual security testing · WEB CODE STORE (PVT) LTD

WEB APPLICATION

Vulnerability Assessment & Penetration Test Report

Prepared for

Northwind Store (sample client)

Target: https://northwind-store.example

Assessment type	Web application · Grey-box · Authenticated + unauthenticated
Engagement window	18–22 of the reporting month (sample)
Report version	v1.0 · Final
Classification	CONFIDENTIAL
Prepared by	Bug Circuit security team
Standards	PTES · OWASP WSTG / Top 10 (2021) · NIST SP 800-115 · CVSS v3.1

ILLUSTRATIVE SAMPLE

This document uses fictional data to demonstrate the exact format, depth and standards of a real Bug Circuit report. It is not a real customer or a real site. Your report covers your own domain with your real findings.

SECTION 1

Document Control & Confidentiality

CONFIDENTIALITY STATEMENT

This report contains proprietary and confidential information including details of security vulnerabilities. It is provided solely to the named client and authorised recipients and must be handled in accordance with the engagement agreement / NDA. Unauthorised disclosure, copying or distribution is prohibited. Findings reflect the state of the environment during the testing window only (point-in-time assessment).

VERSION HISTORY

VERSION	DATE	AUTHOR	DESCRIPTION
0.1	Day 22	Bug Circuit	Draft issued for internal QA
1.0	Day 24	Bug Circuit	Final report issued to client

DISTRIBUTION

Client security lead · Client engineering lead · Bug Circuit engagement lead. Any wider distribution must be authorised by the client point of contact.

AUTHORISATION BASIS

Testing was performed only after the client verified ownership of the in-scope domain and signed a recorded Authorization to Test defining the agreed scope and rules of engagement.

SECTION 2

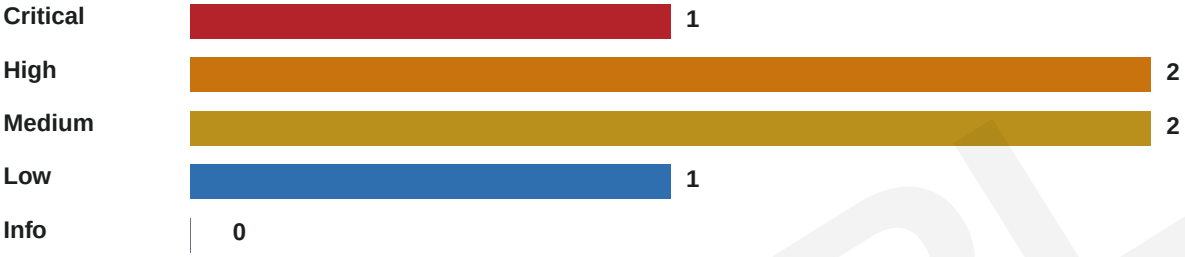
Executive Summary

Bug Circuit performed a manual vulnerability assessment and penetration test of the Northwind Store web application. The objective was to identify, safely validate and prioritise security weaknesses that a real attacker could exploit, and to provide clear, actionable remediation guidance.

Overall risk posture: ELEVATED

The assessment identified issues that, if exploited, could lead to a mass exposure of customer personal data and, in the worst case, full compromise of the application server. Two of the most serious issues are systemic access-control failures rather than isolated bugs, indicating that authorisation is not consistently enforced server-side. These should be treated as priorities for immediate remediation.

FINDINGS BY SEVERITY



WHAT THIS MEANS FOR THE BUSINESS

· Customer data at risk: an authenticated user could retrieve every customer's personal data — a reportable data breach in most jurisdictions, with regulatory and reputational cost.

· Server compromise plausible: an outdated component with a public remote-code-execution exploit exposes the site to opportunistic, automated attacks.

· Quick wins available: several medium/low issues (error handling, security headers, TLS) are low-effort fixes that materially raise the baseline.

PRIORITY RECOMMENDATIONS

1. Enforce server-side object-level authorization across all endpoints (fixes BC-01, BC-02). 2. Patch outdated components and establish a monthly update cadence (BC-03). 3. Harden configuration: generic error handling, security headers, TLS (BC-04–06).

SECTION 3

Scope & Engagement Details

IN SCOPE

· Web application: https://northwind-store.example (production-equivalent staging)
· Authenticated area using two supplied test accounts (standard customer role)
· REST API under /api/*
· TLS / HTTP configuration of the in-scope host

OUT OF SCOPE

· Denial-of-service and load/stress testing
· Third-party payment provider infrastructure
· Social engineering and physical security
· Underlying cloud provider platform

APPROACH & RULES OF ENGAGEMENT

Grey-box testing combining unauthenticated and authenticated perspectives. Testing was rate-limited and non-destructive; no customer data was exfiltrated or retained beyond the minimum needed to evidence a finding. A recorded Authorization to Test defined the window and boundaries.

SECTION 4

Methodology & Approach

The engagement followed recognised industry standards so results are rigorous, repeatable and auditable. Automated tooling is used only to accelerate discovery; every reported finding is manually validated by a human engineer to eliminate false positives.

STANDARDS & FRAMEWORKS

· PTES (Penetration Testing Execution Standard) — overall engagement lifecycle
· OWASP Web Security Testing Guide (WSTG v4.2) — per-test methodology and test IDs
· OWASP Top 10 (2021) — risk categorisation of each finding
· NIST SP 800-115 — process backbone (planning, discovery, attack, reporting)
· MITRE ATT&CK — mapping of the attack narrative to real adversary techniques
· CVSS v3.1 — severity scoring

ASSESSMENT PHASES

1 · Reconnaissance	Passive OSINT: subdomains, technologies, DNS and email posture.
2 · Enumeration	Mapping endpoints, parameters, roles and the authentication surface.
3 · Vulnerability analysis	Manual + tool-assisted identification of weaknesses against WSTG.
4 · Exploitation	Safe, controlled validation to confirm real, exploitable impact.
5 · Post-exploitation	Assessing reachable data / privilege, mapped to MITRE ATT&CK.
6 · Reporting	Risk-rated findings, evidence and prioritised remediation.

SECTION 5

Risk Rating Methodology

Each finding is scored with CVSS v3.1, which produces a base score from 0.0 to 10.0 and a transparent vector string capturing exploitability (Attack Vector, Complexity, Privileges, User Interaction, Scope) and impact (Confidentiality, Integrity, Availability). Scores map to the qualitative severity bands below. Business context may adjust the final priority.

SEVERITY	CVSS v3.1 BASE SCORE
CRITICAL	9.0 – 10.0
HIGH	7.0 – 8.9
MEDIUM	4.0 – 6.9
LOW	0.1 – 3.9
INFO	0.0

Finding status taxonomy: Open (present at time of test) · Fixed (validated closed on retest) · Risk Accepted (client-acknowledged). All findings in this sample are Open.

SECTION 6

Findings Summary

The table below lists all findings in priority order. Full technical detail for each follows in Section 7.

ID	FINDING	SEVERITY	CVSS	OWASP
BC-01	Insecure Direct Object Reference (IDOR) in order history API	CRITICAL	**8.6**	A01:2021
BC-02	Unauthenticated administrative data-export endpoint	HIGH	**7.5**	A01:2021
BC-03	Outdated third-party component with a known RCE vulnerability	HIGH	**8.8**	A06:2021
BC-04	Verbose error handling discloses stack traces and stack fingerprint	MEDIUM	**5.3**	A05:2021
BC-05	Missing HTTP security headers (CSP, HSTS, frame protection)	MEDIUM	**4.3**	A05:2021
BC-06	TLS configuration permits deprecated protocol and weak ciphers	LOW	**3.7**	A02:2021

SECTION 7.1

BC-01 — Insecure Direct Object Reference (IDOR) in order history API

CRITICAL

CVSS 8.6

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

A01:2021 Broken Access Control · WSTG-ATHZ-04 · CWE-639 Authorization Bypass Through User-Controlled Key

AFFECTED ASSET

`https://northwind-store.example/api/orders/{id}`

DESCRIPTION & ROOT CAUSE

The order-detail endpoint returns an order based solely on the numeric identifier supplied in the URL, without verifying that the order belongs to the authenticated user. Any logged-in customer can enumerate sequential IDs and retrieve arbitrary orders.

BUSINESS IMPACT

A single authenticated customer can harvest the personal data (name, email, postal address, phone, purchase history) of the entire customer base — a mass personal-data breach with direct GDPR / privacy-regulation exposure and reputational damage.

LIKELIHOOD

High — trivially exploitable by changing a number in the address bar; requires only a valid low-privilege account and no special tooling.

EVIDENCE (REDACTED PROOF OF CONCEPT)

```
GET /api/orders/10432   Authorization: Bearer <victimA>   ->  200 OK  (belongs to victimB)
{ "orderId": 10432, "customer": "REDACTED", "email": "r*****@*****.com", "address": "REDACTED" }
Sequential enumeration of 10000..10500 returned 431 distinct customer records.
```

RECOMMENDATION

Enforce an object-level authorization check on every request: the order's owner_id must equal the authenticated principal's id. Return 404 (not 403) for non-owned objects to prevent ID enumeration. Adopt a deny-by-default access-control layer and add automated authorization tests.

References: CWE-639 · OWASP WSTG-ATHZ-04 · OWASP API Security Top 10: API1:2023 BOLA

SECTION 7.2

BC-02 — Unauthenticated administrative data-export endpoint

HIGH

CVSS 7.5

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A01:2021 Broken Access Control · WSTG-ATHN-01 · CWE-306 Missing Authentication for Critical Function

AFFECTED ASSET

`https://northwind-store.example/admin/export/customers.csv`

DESCRIPTION & ROOT CAUSE

The administrative CSV-export route is hidden from the UI but the endpoint itself performs no server-side session or role check. Requesting the URL directly, with no authentication, returns the full customer list.

BUSINESS IMPACT

Anyone who discovers or guesses the path downloads the entire customer database. Hiding a link is not an access control; unlinked endpoints are routinely found by crawlers and attackers.

LIKELIHOOD

Medium — requires knowledge/guessing of the path, but the export is fully unauthenticated once found.

EVIDENCE (REDACTED PROOF OF CONCEPT)

```
GET /admin/export/customers.csv   (no session cookie)   ->  200 OK
Content-Type: text/csv  ·  3,4XX rows returned
```

RECOMMENDATION

Apply the same server-side authentication and admin-role authorization to the endpoint as the rest of /admin. Authorize the request, not the button that links to it. Add an automated test asserting the route returns 401/403 without a valid admin session.

References: CWE-306 · OWASP WSTG-ATHN-01 · A01:2021

SECTION 7.3

BC-03 — Outdated third-party component with a known RCE vulnerability

HIGH

CVSS 8.8

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A06:2021 Vulnerable and Outdated Components · WSTG-CONF-11 · CWE-1104 Use of Unmaintained Third Party Components

AFFECTED ASSET

`northwind-store.example — contact-form plugin v4.1.2`

DESCRIPTION & ROOT CAUSE

The application runs a contact-form component two major versions behind the current release. The installed version carries a publicly documented, exploited-in-the-wild vulnerability permitting arbitrary file upload leading to remote code execution.

BUSINESS IMPACT

Automated botnets scan for exactly this component and version. Left unpatched it is among the most probable routes to full server compromise — attacker code executing in your environment, pivot to the database, and persistence.

LIKELIHOOD

High — a public exploit exists and mass-scanning for the vulnerable version is ongoing.

EVIDENCE (REDACTED PROOF OF CONCEPT)

```
Detected version: 4.1.2   (fixed in 4.3.0)
Fingerprint: /wp-content/plugins/REDACTED/readme.txt  ->  "Stable tag: 4.1.2"
Public exploit / advisory reference withheld from sample.
```

RECOMMENDATION

Update the component to the latest supported release immediately, then establish a monthly patch-review cadence and a software bill of materials (SBOM). Remove unused plugins/dependencies to reduce attack surface. Subscribe to the vendor's security advisories.

References: CWE-1104 · OWASP WSTG-CONF-11 · A06:2021

SECTION 7.4

BC-04 — Verbose error handling discloses stack traces and stack fingerprint

MEDIUM

CVSS 5.3

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

A05:2021 Security Misconfiguration · WSTG-ERRH-01 · CWE-209 Generation of Error Message Containing Sensitive Information

AFFECTED ASSET

`https://northwind-store.example/checkout (error path)`

DESCRIPTION & ROOT CAUSE

Submitting malformed input to the checkout flow returns an unhandled exception page containing a full stack trace, the framework and language version, and absolute server file paths.

BUSINESS IMPACT

Provides an attacker a precise map of the technology stack and versions to target, may leak secrets embedded in code paths, and undermines customer confidence when surfaced in the UI.

LIKELIHOOD

Medium — reachable by any user submitting unexpected input; no authentication required.

EVIDENCE (REDACTED PROOF OF CONCEPT)

```
POST /checkout   (malformed JSON body)   ->  500 Internal Server Error
Response body includes: "at /var/www/REDACTED/app/services/REDACTED:214"  and framework version
banner.
```

RECOMMENDATION

Return a generic, branded error page to users and log full detail server-side only. Disable debug/verbose mode in production. Add a global exception handler that never echoes internal detail to the client.

References: CWE-209 · OWASP WSTG-ERRH-01 · A05:2021

SECTION 7.5

BC-05 — Missing HTTP security headers (CSP, HSTS, frame protection)

MEDIUM

CVSS 4.3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

A05:2021 Security Misconfiguration · WSTG-CONF-07 · CWE-693 Protection Mechanism Failure

AFFECTED ASSET

`northwind-store.example — all HTTP responses`

DESCRIPTION & ROOT CAUSE

Responses omit Content-Security-Policy, Strict-Transport-Security, and X-Frame-Options / frame-ancestors, and set cookies without consistent Secure/HttpOnly/SameSite attributes.

BUSINESS IMPACT

Increases the blast radius of any cross-site scripting flaw, permits clickjacking via framing, allows protocol-downgrade attacks, and weakens session-cookie protection.

LIKELIHOOD

Medium — the headers are absent by default; exploitation depends on a paired flaw or user interaction.

EVIDENCE (REDACTED PROOF OF CONCEPT)

```
Response headers: Content-Security-Policy (absent) · Strict-Transport-Security (absent) · X-Frame-Options (absent)
Set-Cookie: session=...  (no Secure, no SameSite)
```

RECOMMENDATION

Add a restrictive Content-Security-Policy, HSTS (with preload once verified), and frame-ancestors ‘none’. Set Secure, HttpOnly and SameSite on all session cookies. Exact header values are provided in Appendix B.

References: CWE-693 · OWASP WSTG-CONF-07 · A05:2021

SECTION 7.6

BC-06 — TLS configuration permits deprecated protocol and weak ciphers

LOW

CVSS 3.7

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

A02:2021 Cryptographic Failures · WSTG-CRYP-01 · CWE-327 Use of a Broken or Risky Cryptographic Algorithm

AFFECTED ASSET

`northwind-store.example:443`

DESCRIPTION & ROOT CAUSE

The server still negotiates TLS 1.0 and offers a small set of weak cipher suites alongside modern ones.

BUSINESS IMPACT

Modern browsers will not use the weak options, but their presence lowers the overall security posture and fails common compliance checklists that enterprise customers may run against you.

LIKELIHOOD

Low — practical exploitation is difficult on current clients; largely a hardening / compliance gap.

EVIDENCE (REDACTED PROOF OF CONCEPT)

```
Enabled protocols: TLS 1.0, TLS 1.2, TLS 1.3
Weak cipher suites offered: 2 (CBC-mode legacy)
```

RECOMMENDATION

Disable TLS 1.0/1.1 and the legacy CBC cipher suites; serve TLS 1.2 and 1.3 only with a modern cipher list.

References: CWE-327 · OWASP WSTG-CRYP-01 · A02:2021

SECTION 8

Remediation Roadmap

Recommended sequencing to reduce risk fastest. Effort is indicative.

Immediate (0–7 days)

- BC-01 · Enforce object-level authorization on the orders API
- BC-02 · Add authentication to the admin export endpoint
- BC-03 · Patch the outdated component with the public RCE

Short term (1–4 weeks)

- BC-04 · Generic error handling; disable production debug
- BC-05 · Add CSP, HSTS, frame protection and secure cookies

Ongoing / strategic

- BC-06 · Tighten TLS configuration
- Establish monthly patching + SBOM
- Add automated authorization tests to CI
- Schedule a re-test to validate fixes

SECTION 9

Conclusion

The Northwind Store application carries elevated risk driven primarily by inconsistent server-side authorization and an outdated, publicly-exploitable component. None of the critical issues require sophisticated attacker capability, so remediation should begin immediately. Encouragingly, the most serious problems share a single root cause — authorization enforced in the UI rather than the server — so a focused fix closes several findings at once. After remediation we recommend a re-test to validate closure, and adoption of a regular testing cadence as the application evolves.

APPENDIX

Reference Material

A · STANDARDS MAPPED IN THIS REPORT

PTES · OWASP WSTG v4.2 · OWASP Top 10 (2021) · OWASP API Security Top 10 · NIST SP 800-115 · MITRE ATT&CK · CVSS v3.1 · CWE.

B · RECOMMENDED SECURITY HEADERS (EXAMPLE)

```
Content-Security-Policy: default-src 'self'; object-src 'none'; frame-ancestors 'none'
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
X-Frame-Options: DENY   ·   X-Content-Type-Options: nosniff
Set-Cookie: session=...; Secure; HttpOnly; SameSite=Lax
```

C · GLOSSARY

IDOR — Insecure Direct Object Reference · RCE — Remote Code Execution · CVSS — Common Vulnerability Scoring System · CWE — Common Weakness Enumeration · WSTG — Web Security Testing Guide · TLS — Transport Layer Security.

This is an illustrative sample produced by Bug Circuit to demonstrate report format and depth. Fictional data throughout.