



PENETRATION TEST REPORT

Network & Web Application Security Assessment

Prepared for: Northgate Logistics, Inc. · Internal + External Engagement

CLIENT

Northgate Logistics, Inc.

ENGAGEMENT TYPE

Grey-box, Internal & External

TEST WINDOW

22 Sep – 03 Oct 2026

REPORT DATE

15 Oct 2026

REPORT REF

PTL-2026-0147

CLASSIFICATION

CONFIDENTIAL

ASSESSOR

pen-test-lab · J. Brody

OVERALL RISK

HIGH

This document contains sensitive security information and is classified CONFIDENTIAL. Distribution is restricted to authorized Northgate Logistics personnel and pen-test-lab. Do not forward, copy, or store without authorization.

CONTENTS

Table of Contents

1	Executive Summary	03
2	Engagement Scope & Rules of Engagement	04
3	Methodology	05
4	Findings Summary	06
5	Detailed Findings	07
6	AI-Assisted Testing Notes	10
7	Remediation Roadmap	11
8	Appendix A – Tooling & CVSS Reference	12

Sample report. This is a demonstration deliverable produced by pen-test-lab to illustrate engagement reporting format and depth. "Northgate Logistics, Inc." and all hosts, IP ranges, and findings herein are fictional and were not drawn from any real system. All real engagements are performed only under signed written authorization and an agreed rules-of-engagement.

Executive Summary

pen-test-lab was engaged to perform a grey-box penetration test of Northgate Logistics' internal network and public-facing web application between 22 September and 03 October 2026. The objective was to identify, validate, and prioritize vulnerabilities that a motivated attacker could realistically exploit, and to provide actionable remediation guidance.

The assessment identified **12 findings**, of which **2 are Critical** and **3 are High**. Most significantly, a chained attack path allowed an unauthenticated attacker on the internal network to achieve **full domain compromise** within the test window — beginning with an exposed service and ending in local root via a known privilege-escalation flaw. The overall risk rating for the environment is **HIGH**.

2 CRITICAL	3 HIGH	4 MEDIUM	2 LOW	1 INFO
---------------	-----------	-------------	----------	-----------

Key Takeaways

- **Patch management gaps are the dominant risk.** Both Critical findings stem from missing OS and service patches for publicly documented CVEs, several over a year old.
- **A single weak point cascades.** The internal foothold required no credentials; from there, default credentials and a local kernel flaw were enough to reach domain-administrator access.
- **Perimeter hygiene needs attention.** An exposed .git directory and a database admin panel reachable from the internet together leak enough to accelerate any external attack.
- **Detection lagged.** None of the simulated attack activity generated an alert the client's team acted on during the window, indicating monitoring coverage gaps.

Bottom line for leadership: The environment is exploitable today by an attacker of moderate skill. The two Critical issues can be remediated within days through patching and credential rotation, which would remove the demonstrated path to domain compromise. Prioritize those first.

Engagement Scope & Rules of Engagement

In-Scope Targets

ASSET	RANGE / HOST	TYPE
Internal corporate network	10.10.0.0/24	Internal
Public web application	app.northgate-logistics.example	External
Public marketing site	www.northgate-logistics.example	External
VPN concentrator	203.0.113.40	External

Out of Scope

- Social engineering, phishing, and physical access testing.
- Denial-of-service and volumetric load testing.
- Third-party SaaS platforms not owned by the client.
- Production database destructive operations (read-only validation only).

Rules of Engagement

AUTHORIZATION	Signed engagement letter & RoE on file, ref PTL-2026-0147-RoE
TEST WINDOW	22 Sep – 03 Oct 2026, 09:00–18:00 ET, weekdays
APPROACH	Grey-box; standard user VPN credentials provided for internal phase
EMERGENCY CONTACT	Client SOC lead notified of all high-impact actions in advance
DATA HANDLING	No PII exfiltrated; proof-of-access limited to non-sensitive markers

All testing was conducted within the authorized window and scope. Where a finding could have been escalated further (e.g., mass data extraction), testing stopped at proof of access to avoid operational impact, as agreed in the RoE.

Methodology

The engagement followed a structured, industry-aligned process drawing on PTES, the OWASP Testing Guide, and the MITRE ATT&CK framework. Each phase fed the next; findings were validated manually to eliminate false positives before inclusion.

PHASE	ACTIVITIES	PRIMARY TOOLING
1. Reconnaissance	Passive OSINT, subdomain and asset discovery, public-footprint mapping	subfinder, amass, OSINT
2. Scanning & Enumeration	Port/service discovery, version fingerprinting, vulnerability template scans	nmap, nuclei, httpx
3. Exploitation	Manual validation and safe exploitation of confirmed weaknesses	Metasploit, sqlmap, manual
4. Post-Exploitation	Privilege escalation, lateral movement, blast-radius assessment	manual, built-in tooling
5. Reporting	CVSS scoring, ATT&CK mapping, remediation guidance	CVSS v3.1

Risk Rating Model

Each finding is scored using CVSS v3.1 and assigned a severity band. Severity reflects both the likelihood of exploitation and the business impact if exploited.

SEVERITY	CVSS V3.1 RANGE	EXPECTED RESPONSE
CRITICAL	9.0 – 10.0	Remediate immediately (days)
HIGH	7.0 – 8.9	Remediate within 1–2 weeks
MEDIUM	4.0 – 6.9	Remediate within 30–60 days
LOW	0.1 – 3.9	Remediate as resources allow
INFO	0.0	Awareness / hardening

Findings Summary

The table below lists all findings in priority order. Detailed write-ups for the Critical and High findings follow in Section 5.

ID	FINDING	SEVERITY	CVSS	ATT&CK
PTL-01	Unauthenticated RCE via outdated service (CVE-2021-4034 chain)	CRITICAL	9.8	T1068
PTL-02	SQL injection in application search endpoint	CRITICAL	9.1	T1190
PTL-03	Default credentials on database admin panel	HIGH	8.6	T1078
PTL-04	Exposed .git directory on public web root	HIGH	7.5	T1592
PTL-05	Missing authentication on internal admin API	HIGH	7.4	T1133
PTL-06	Reflected cross-site scripting (XSS) in contact form	MEDIUM	6.1	T1059
PTL-07	TLS 1.0/1.1 enabled on perimeter services	MEDIUM	5.9	T1557
PTL-08	Verbose error messages leak stack traces	MEDIUM	5.3	T1592
PTL-09	SMB signing not enforced	MEDIUM	4.8	T1557
PTL-10	Missing security headers (CSP, HSTS)	LOW	3.7	T1592
PTL-11	Username enumeration via login response timing	LOW	3.1	T1589
PTL-12	Software version disclosure in HTTP banners	INFO	0.0	T1592

Detailed Findings

PTL-01 · ATT&CK T1068 · CVE-2021-4034

CRITICAL

Internal Foothold to Local Root via Privilege Escalation

CVSS 9.8 Vector AV:N/AC:L/PR:N/UI:N Affected 10.10.0.37

DESCRIPTION

An internal host exposed an unpatched service that permitted an unauthenticated attacker to gain an interactive foothold. From that low-privileged shell, the host was found vulnerable to the well-documented "PwnKit" local privilege-escalation flaw (CVE-2021-4034) in a setuid component, allowing escalation to root. The combination converts a network foothold into full control of the host.

IMPACT

Full administrative control of the affected server, which stored cached domain credentials. These were used to pivot toward domain-administrator access (see PTL-03), ultimately placing the entire Windows domain at risk.

EVIDENCE

```
# low-priv shell obtained on 10.10.0.37
whoami → svc-reports
# host missing patch for CVE-2021-4034 (pkexec)
id → uid=0(root) gid=0(root) [escalation confirmed]
```

REMEDIATION

- Apply the vendor patch for CVE-2021-4034 across all Linux hosts immediately; it has been available since January 2022.
- Patch or decommission the exposed service providing the initial foothold.
- Remove cached credentials from service accounts and enforce least privilege.

SQL Injection in Application Search Endpoint

CVSS 9.1 Vector AV:N/AC:L/PR:N/UI:N Affected /api/v2/search

DESCRIPTION

The public application's search endpoint failed to parameterize a user-supplied query parameter, allowing injection of SQL into the backend query. The flaw permitted extraction of arbitrary database contents, including the application's user table, without authentication.

IMPACT

An unauthenticated attacker could read the full application database — user records, hashed passwords, and session data — and potentially write to it. Testing was limited to read-only proof of access per the RoE; no customer data was extracted.

EVIDENCE

```
# injectable parameter confirmed (boolean + time-based)
GET /api/v2/search?q=widget' → 500 database error
# automated confirmation
sqlmap identified: parameter 'q' is injectable (UNION, time-based blind)
backend DBMS: PostgreSQL · current user: app_rw
```

REMEDIATION

- Replace string-concatenated queries with parameterized statements / prepared queries throughout the application.
- Apply least-privilege database roles; the web role should not hold write access to authentication tables.
- Add a WAF rule as defense-in-depth, not as the primary fix.

Default Credentials on Database Admin Panel

HIGH

CVSS 8.6 Vector AV:N/AC:L/PR:N/UI:N Affected 10.10.0.52:8080

DESCRIPTION

A database administration console on the internal network accepted the vendor's factory-default administrator credentials, which had never been changed. Combined with the foothold from PTL-01, this gave an attacker administrative access to a second critical system.

IMPACT

Direct administrative access to a database server holding operational data; served as the pivot point to domain-administrator credentials.

REMEDIATION

- Rotate all default credentials immediately; enforce a credential-change step in provisioning.
- Restrict admin consoles to a management VLAN; they should never be broadly reachable.
- Enable multi-factor authentication on administrative interfaces.

Exposed .git Directory on Public Web Root

HIGH

CVSS 7.5 Vector AV:N/AC:L/PR:N/UI:N Affected www root

DESCRIPTION

The public web server served the application's `.git` directory, allowing anyone to reconstruct the full source tree and commit history. The history contained a hard-coded API key in an earlier commit.

IMPACT

Source disclosure accelerates discovery of other flaws (such as PTL-02) and leaked a credential that was still valid against a third-party service.

REMEDIATION

- Block access to `.git` and other VCS metadata at the web server; never deploy the repository to the web root.
- Rotate the leaked API key and audit it for misuse.
- Adopt a build/deploy pipeline that ships only built artifacts, not the working tree.

Missing Authentication on Internal Admin API

CVSS **7.4** Vector **AV:N/AC:L/PR:L/UI:N** Affected **10.10.0.44/admin**

DESCRIPTION

An internal administrative API exposed privileged operations (user creation, config changes) without requiring authentication to any user on the internal network.

IMPACT

Any internal host, including a compromised workstation, could alter application configuration and create privileged accounts.

REMEDIATION

- Require authenticated, role-checked access on every administrative route.
- Default-deny on API gateways; whitelist only intended endpoints.
- Log and alert on privileged API calls.

Medium, Low, and Informational findings (PTL-06 through PTL-12) are documented in full in the client's accompanying findings workbook, summarized in Section 4 above. Write-ups follow the same structure: description, impact, evidence, and remediation.

AI-Assisted Testing Notes

This engagement used pen-test-lab's AI-assisted workflow during the reconnaissance and triage phases. The approach pairs an LLM-driven orchestration layer with human operator judgment — the model accelerates breadth, the operator owns every exploitation decision.

Where AI was applied

PHASE	AI CONTRIBUTION	HUMAN VERIFICATION
Reconnaissance	Parallel subdomain, parameter, and tech-stack enumeration; deduplicated and ranked the attack surface	Operator reviewed and scoped the target list
Triage	Correlated scanner output against CVE data; flagged 7 high-value candidates from ~200 raw signals	Each candidate manually confirmed; false positives discarded
Payload shaping	Suggested context-aware test payloads tuned to the detected PostgreSQL + framework stack	Operator validated and executed all payloads manually

Human-in-the-loop guarantee. No vulnerability was exploited, and no change was made to any target, without explicit operator sign-off. AI expanded coverage and cut triage time; it did not act autonomously against client systems. Every finding in this report was manually validated.

Measured benefit

- Reconnaissance coverage of the external surface completed in roughly a third of the time of a manual-only pass.
- False-positive rate on flagged findings reduced through stack-aware correlation before human review.
- Operator time reallocated from enumeration to deeper manual exploitation of the two Critical findings.

Remediation Roadmap

Recommended sequencing, ordered by risk reduction per unit of effort. Completing the "Immediate" tier removes the demonstrated path to domain compromise.

Immediate (0–7 days)

ACTION	ADDRESSES
Patch CVE-2021-4034 across all Linux hosts	PTL - 01
Parameterize the vulnerable search query; restrict DB role	PTL - 02
Rotate all default and leaked credentials	PTL - 03, PTL - 04

Short term (1–4 weeks)

ACTION	ADDRESSES
Enforce authentication on internal admin API & consoles	PTL - 05
Block VCS metadata at the web server; fix deploy pipeline	PTL - 04
Remediate reflected XSS; add output encoding	PTL - 06

Hardening (1–3 months)

ACTION	ADDRESSES
Disable TLS 1.0/1.1; enforce SMB signing	PTL - 07, PTL - 09
Add security headers (CSP, HSTS); suppress verbose errors & banners	PTL - 08, PTL - 10, PTL - 12
Review monitoring/alerting coverage against tested ATT&CK techniques	Detection gap

Retest. pen-test-lab recommends a focused retest of all Critical and High findings once remediation is complete, to confirm closure and validate that fixes did not introduce new issues. A retest is included within 60 days of this report.

Tooling & CVSS Reference

Tooling Used

CATEGORY	TOOLS
Reconnaissance	subfinder, amass, httpx
Scanning	nmap, nuclei
Web testing	Burp Suite, sqlmap, manual
Exploitation	Metasploit Framework, manual
AI orchestration	pen-test-lab AI-assisted recon pipeline

CVSS v3.1 Severity Bands

BAND	SCORE	MEANING
CRITICAL	9.0–10.0	Trivial to exploit, severe impact
HIGH	7.0–8.9	Realistic exploitation, significant impact
MEDIUM	4.0–6.9	Conditional exploitation or moderate impact
LOW	0.1–3.9	Limited impact or difficult to exploit
INFO	0.0	No direct risk; hardening opportunity

Confidentiality & authorization. This report is the confidential property of Northgate Logistics, Inc. and pen-test-lab. It documents a point-in-time assessment; security posture may change as the environment evolves. All testing was authorized in writing and conducted within the agreed scope and rules of engagement. pen-test-lab performs security testing only against systems whose owners have granted explicit permission.

pen-test-lab.com · jimmy@pen-test-lab.com · Buffalo, NY · Report PTL-2026-0147