Vulnerability Assessment

By Lucio Rodrigues

Scenario

You have recently been brought on as a cybersecurity analyst for a mid-sized logistics and supply chain company. The company relies heavily on an internal web application that manages real-time freight tracking, inventory updates, and vendor communications.

The application is hosted on a cloud-based virtual machine that has remained publicly accessible via HTTP since its deployment. As cyber threats increase globally, you've been asked to assess this exposure and deliver a risk-based report highlighting the vulnerabilities and proposing mitigation strategies.

Date

May 1st, 2025 - August 1st, 2025 (3 Months)

System Description

The logistics application is hosted on an Ubuntu 22.04 virtual machine using an Apache web server stack. The backend runs PostgreSQL and Django. While the server supports IPv6, it is currently only using IPv4.

The system uses HTTP with no enforced SSL/TLS and logs show irregular access from various foreign IP addresses. No web application firewall (WAF) is in place. User accounts are authenticated through a custom-built login module with no MFA.

Scope

This assessment focuses on the security of external access controls, web application exposure, and data transmission practices. The analysis follows the **NIST SP 800-30 Revision 1** framework and includes risk identification, threat modeling, and remediation planning for externally facing systems.

Purpose

The system manages high-value logistics data, including route details, vendor agreements, and real-time fleet status. Unauthorised access could lead to shipment delays, reputational damage, or even corporate espionage. The goal of this report is to identify current vulnerabilities and present actionable recommendations to reduce risk.

Risk Assessment

Threat Source	Threat Event	Likelihood	Severity	Risk
Hacktivist groups	Modify or leak sensitive tracking data to disrupt supply chain	3	3	9
Malicious insiders	Tamper with delivery schedules or redirect resources	2	3	6
Unsecured endpoints	Data interception due to unencrypted transmission	3	2	6
Competitor surveillance	Extract fleet movement patterns and vendor deals through scraping	2	2	4
Anonymous actors	Inject malicious scripts via input forms to access backend	2	3	6

Approach

Threat sources were categorised based on access vectors and motivation. Open access via HTTP and exposed application forms significantly increase the system's attack surface. High likelihood and severity scores were assigned to hacktivist threats due to geopolitical instability affecting logistics globally.

Internal threats were considered based on recent employee turnover. Technical assessment tools such as Nmap, Nikto, and OWASP ZAP were used to confirm exposure points.

Remediation Strategy

- **Enforce TLS** for all web traffic to prevent data interception.
- **Implement a Web Application Firewall (WAF)** to filter malicious traffic.
- **Restrict external access** using VPN or allowlisting known IPs.
- **Enforce Multi-Factor Authentication (MFA)** for all administrative accounts.
- **Refactor authentication module** to align with OWASP top 10 best practices.
- **Regularly patch server and application components** to fix known CVEs.
- **Enable logging and anomaly detection** to flag suspicious activity in real time.
- **Conduct periodic access reviews** for all user roles and permissions.