CONFIDENTIAL

STACKED NERDS

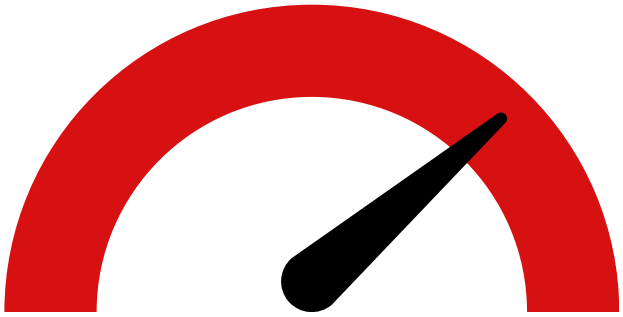
VULN & RISK ANALYSIS

JANUARY 2026

Prepared by
STACKED NERDS

Prepared for
ABC CORP

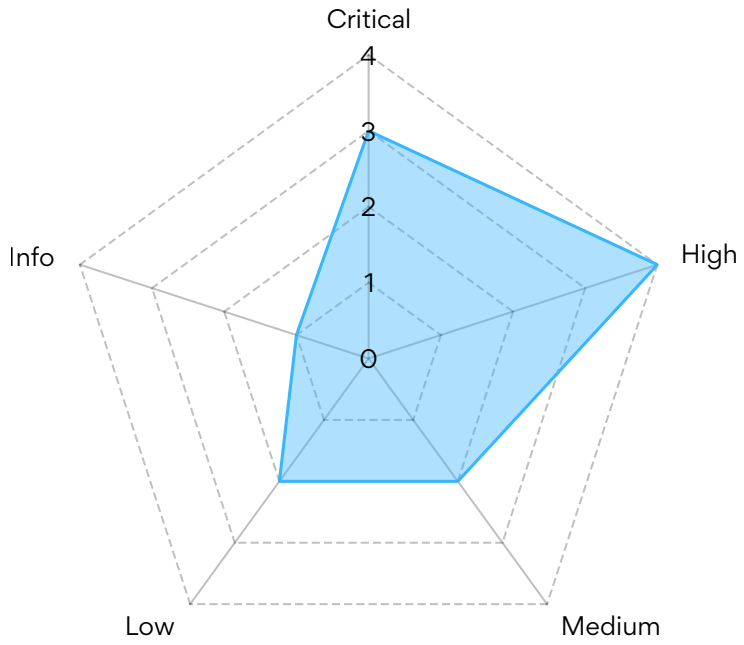
SUMMARY



CRITICAL

Assessment Overview

We conducted a non-invasive external security assessment of ABC CORP public infrastructure. While the core application functionality is stable, our scan detected **critical misconfigurations** in the deployment pipeline. These vulnerabilities currently expose sensitive internal data and API endpoints to the public internet, bypassing standard authentication layers.



Business Impact

⚠️ **Data Leakage**	Exposed .env files allow attackers to clone customer databases
⚖️ **Compliance Risk**	Current encryption gaps violate GDPR & DPDP standards.
🛑 **Service Disruption**	Lack of rate-limiting makes the API vulnerable to DDoS attacks.
📉 **Brand Reputation**	Publicly visible exploits can lead to loss of client trust.

PRIORITY VULN ANALYSIS

#01 EXPOSED ENVIRONMENT SECRETS

CRITICAL

The Issue

The application's .env configuration file is publicly accessible via the web root. This file typically contains sensitive credentials.

Business Risk

Attackers can scrape database passwords, AWS keys, and API tokens, leading to a total infrastructure compromise.

FIX: Block access to all "dotfiles" (.*) in your Nginx or Apache configuration immediately.

```
DB_HOST=192.168.1.45
DB_USER=admin_prod
DB_PASS=Sup3rS3cr3tP@ssw0rd!
AWS_ACCESS_KEY=AKIAIOSFODNN7EXAMPLE
STRIPE_SECRET=sk_live_51M3p...
DEBUG=true
```

#02 EXPOSED .GIT REPOSITORY

CRITICAL

The Issue

The /.git folder is exposed. This allows anyone to download the entire source code history, including previous commits.

Business Risk

Competitors can reverse-engineer your proprietary logic. Hackers can analyze old code to find hidden security flaws.

FIX: Remove .git folders from production builds or deny access to the /.git path in the Ingress controller.

```
Index of /.git/
----------------------------------
[DIR] HEAD
[DIR] config
[DIR] description
[DIR] hooks/
[DIR] info/
[DIR] objects/
[DIR] refs/
----------------------------------
```

Additional Identified Threats (Summary)

Severity	Vulnerability	Potential Impact
CRITICAL	Log4j Remote Code Execution	Full server takeover via logging exploit.
HIGH	Spring Boot Actuator Exposed	Leaks internal memory and heap dump data.
HIGH	Reflected XSS (Search Bar)	Allows attackers to hijack user sessions.
HIGH	Unrestricted File Upload	Users can upload malicious .php/.exe files.

THE PATH FORWARD

Manual patching is temporary. We propose implementing an **Automated Security Pipeline** to fix these issues and prevent future vulnerabilities.

❌ CURRENT STATE (MANUAL)

❌Developers accidentally commit secrets (.env)
❌Vulnerabilities found only after deployment
❌Inconsistent security headers across servers
❌High risk of data breach & compliance fines

✅ THE STACKED NERDS WAY

✅ Pre-Commit Scanning : Blocks secrets before upload
✅ Automated CI/CD : Scans every PR for bugs
✅ Hardened Ingress : Headers fixed globally
✅ Continuous Compliance : Auto-generated reports

PROPOSED ENGAGEMENT : THE DEVSECOPS PIPELINE

1. SECRET DETECTION

Implementation of Secrets pipeline to block API keys and passwords from entering your codebase.

2. DAST INTEGRATION

Automated DAST scans running in your GitHub/GitLab pipeline to catch XSS and SQLi daily.

3. CONTAINER SECURITY

Scanning of Docker images to ensure no vulnerable base images are deployed.

4. INFRASTRUCTURE HARDENING

Updating Nginx/Kong Ingress configurations to seal all exposed ports and headers.

READY TO SECURE YOUR INFRASTRUCTURE?

BOOK REMEDIATION CALL

Email : Stacked@stackednerds.tech