bright defense

Demo Corp

PENETRATION TESTING FINDINGS REPORT

Date: August 2, 2026

Project: DEMO-CORP-2026-001

Version: 1.0

BUSINESS CONFIDENTIAL

Bright Defense Penetration Testing Report
Table of Contents

Table of Contents 2
Confidentiality Statement 3
Disclaimer 3
Contact Information 3
Assessment Overview 4
Assessment Components 5
External Penetration Test 5
Finding Severity Ratings 6
Risk Factors 6
Likelihood 2
Impact 2
Scope 7
Scope Exclusions 7
Client Allowances 7
Executive Summary 8
Scope and Time Limitations 8
External Testing Summary 8
Key Strengths and Weaknesses 8
Vulnerability Summary and Report Card 9
External Penetration Test Findings 9
Technical Findings 10
External Penetration Test Findings 10
Finding EPT-001: Deprecated Encryption Protocols 10
Finding EPT-002: Self-Signed TLS Certificate 11
Finding EPT-003: Missing HTTP Security Headers 12
Finding EPT-004: Effective Perimeter Management 13
Additional Scans and Reports 14

Copyright © Bright Defense

Bright Defense Confidentiality Statement, Disclaimer, and Contact Information

Confidentiality Statement

This document is the exclusive property of Demo Corp and Bright Defense. It contains proprietary and confidential information. Reproduction, distribution, disclosure, or use, in whole or in part, requires written authorization from both Demo Corp and Bright Defense. Demo Corp may share this document with authorized auditors, legal advisers, or compliance partners operating under appropriate nondisclosure agreements.

Disclaimer

A penetration test represents security conditions during a defined assessment period. The findings and recommendations reflect the information available during testing and may not account for changes made after the engagement ended.
Time-limited assessments cannot evaluate every system, control, or possible attack path. Bright Defense prioritized testing based on the agreed scope, observed exposure, and likely attack techniques. Periodic reassessments are recommended to confirm that remediation remains effective and newly introduced risks are addressed

Contact Information

Name	Title	Contact Information
Demo Corp		
Jordan Lee	Chief Technology Officer	jordan.lee@democorp.com
Bright Defense		
Alex Morgan	Principal Penetration Tester	alex.morgan@brightdefense.com

Copyright © Bright Defense

Assessment Overview

From August 18, 2026, to August 22, 2026, Demo Corp engaged Bright Defense to assess the security posture of its external infrastructure against current security practices and common attack techniques. The engagement consisted of external network penetration testing. Testing followed guidance from NIST SP 800-115, the OWASP Web Security Testing Guide, the Penetration Testing Execution Standard, and Bright Defense testing procedures.

The penetration testing process included the following phases:

- **Planning:** Confirm assessment objectives, authorized targets, testing limitations, communication procedures, and rules of engagement.
- **Discovery:** Conduct reconnaissance, scanning, and service enumeration to locate exposed systems, weaknesses, and potential attack paths.
- **Attack:** Safely validate suspected vulnerabilities through controlled exploitation and assess the access or impact an attacker could achieve.
- **Reporting:** Document validated findings, supporting evidence, risk ratings, affected assets, unsuccessful attempts, and remediation recommendations.
- **Retesting:** Reassess remediated findings when requested to confirm that corrective actions have resolved the reported vulnerabilities.

Copyright © Bright Defense

Assessment Components

External Penetration Test

An external penetration test simulates an attacker targeting internet-facing systems without internal access. Bright Defense uses reconnaissance, scanning, enumeration, and controlled exploitation to identify and validate weaknesses that could expose sensitive systems or data.

Copyright © Bright Defense

Finding Severity Ratings and Risk Factors

Confidentiality Statement

The following ratings classify findings by severity, exploitability, and potential impact.

Severity	CVSS v3 Score	Definition
Critical	9.0–10.0	Easily exploitable and may result in full system compromise. Immediate remediation is required.
High	7.0–8.9	May provide elevated access, expose data, or disrupt operations. Prompt remediation is recommended.
Medium	4.0–6.9	Requires specific conditions or additional attack steps. Remediate after higher-risk findings.
Low	0.1–3.9	Presents limited direct risk but may weaken the overall security posture.
Informational	N/A	No direct vulnerability exists. The finding records observations or positive security controls.

Risk Factors

Risk is determined using likelihood and impact.

Likelihood

Likelihood measures how easily a vulnerability could be exploited based on attack complexity, available tools, required access, and environmental conditions.

Impact

Likelihood measures how easily a vulnerability could be exploited based on attack complexity, available tools, required access, and environmental conditions.

Copyright © Bright Defense

Project Scope

Assessment	Details
External Penetration Test	**203.0.113.10**

Scope Exclusions

The penetration testing process included the following phases:

- Denial-of-service testing
- Phishing or social engineering

Client Allowances

Demo Corp did not provide credentials, allowlisting, or internal access during the engagement.

Copyright © Bright Defense

Executive Summary

Bright Defense assessed Demo Corp's external security posture from **August 18, 2026**, to **August 22, 2026**. Testing identified several low-risk weaknesses but no critical or high-risk vulnerabilities.

Scope and Time Limitations

Denial-of-service and social engineering testing were excluded. Testing was limited to the approved systems and assessment period.

External Testing Summary

Bright Defense reviewed exposed services, performed vulnerability scanning, and checked publicly available information for possible attack paths.

The assessment identified deprecated TLS protocols, a self-signed certificate, and missing HTTP security headers. No exploitable perimeter vulnerability or exposed credential access was confirmed.

Key Strengths

- Small external attack surface
- No successful password-spraying attacks
- No exposed credentials provided access
- No critical or high-risk findings

Key Weaknesses

- Deprecated TLS protocols
- Self-signed certificate
- Missing HTTP security headers

Copyright © Bright Defense

Vulnerability Summary and Report Card

The assessment identified three low-severity findings. No critical, high, or medium-severity vulnerabilities were confirmed.

External Penetration Test Findings

Critical	High	Medium	Low
0	0	0	3

Finding	Severity	Recommendation
EPT-001: Deprecated TLS Protocols	Low	Disable outdated TLS versions and use TLS 1.2 or TLS 1.3.
EPT-002: Self-Signed TLS Certificate	Low	Replace it with a certificate issued by a trusted authority
EPT-003: Missing HTTP Security Headers	Low	Configure the recommended HTTP security headers.

Copyright © Bright Defense

Technical Findings

External Penetration Test Findings

Finding EPT-001: Deprecated TLS Protocol Supported (Low)

Attribut	Details
Description	The assessed system supports TLS 1.1, which is deprecated and no longer considered secure.
Risk	**Likelihood:** Low. Exploitation requires specific conditions. **Impact**: Moderate. Weak encryption may expose sensitive communications.
Affected System	203.0.113.10
Evidence	Testing confirmed that the server accepted TLS 1.1 connections.

Remediation

Disable TLS 1.0 and TLS 1.1. Configure the server to support only TLS 1.2 and TLS 1.3.

Copyright © Bright Defense