SECURITY ASSESSMENT ATTESTATION

Attestation of Security Testing

Reference: TP-A1B2C3D4-2026

To whom it may concern at Example Corp and their stakeholders,

This letter certifies that a third-party security assessment was conducted on the following application:

Target Application: https://demo-app.example.com

The penetration test was performed on 2026-02-10 using TurboPentest, an automated penetration testing platform operated by IntegSec. The assessment employed the following industry-standard security tools:

- Nmap (Network Scanning & Service Detection)
- Nikto2 (Web Server Analysis)
- OWASP ZAP (Automated Vulnerability Scanning)
- Nuclei (Template-Based CVE Detection)
- IntegSec PentestTools (Custom Security Checks)
- TestSSL (TLS/SSL Configuration Analysis)
- Subfinder (Subdomain Discovery & Enumeration)
- HTTPX (HTTP Probing & Technology Fingerprinting)
- FFUF (Directory & File Brute-Forcing)
- Wafw00f (WAF Detection & Identification)
- Gitleaks (Secret & Credential Scanning)
- OpenVAS/GVM (Full Vulnerability Assessment - 100,000+ NVT Checks)
- Paladin AI (Autonomous Penetration Testing)

Pentest methodology

TurboPentest follows industry-standard testing methodology: PTES + NIST SP 800-115 (overall workflow), OWASP Testing Guides (WSTG / API Security Top 10 / LLM Top 10 / MASTG depending on target type), OWASP AI Testing Guide + Generative AI Red Teaming Guide for AI/LLM testing, MITRE ATT&CK for adversary technique mapping (MITRE ATLAS for AI targets), and OWASP ASVS / MASVS verification levels and OWASP Code Review Guide methodology when source code is provided.

- **PTES** — Penetration Testing Execution Standard (overall workflow from pre-engagement through reporting)
- **NIST SP 800-115** — four-phase pentest workflow alignment (Planning / Discovery / Attack / Reporting)
- **OWASP Testing Guides** — WSTG (Web), API Security Top 10, LLM Top 10, MASTG (Mobile)
- **OWASP AI Testing Guide** — primary testing-procedure reference for AI/LLM targets (32 procedures across AITG-APP, AITG-MOD, AITG-INF, AITG-DAT)
- **OWASP Generative AI Red Teaming Guide** — offensive / red-team playbook for adversarial probing of generative AI
- **MITRE ATT&CK** — adversary technique mapping for findings
- **MITRE ATLAS** — AI/LLM-specific adversary technique IDs (AML.T####) when target is AI/LLM
- **OWASP ASVS** — verification level (L1/L2/L3) on findings when source code is provided
- **OWASP MASVS** — mobile verification level (L1/L2/R) when target is a mobile app with source provided
- **OWASP Code Review Guide** — source-code review methodology when source code is provided
- **PCI DSS Penetration Testing Guidance** — PCI SSC Information Supplement; followed when scope includes PCI cardholder data environments

The assessment covered the OWASP Top 10 vulnerability categories including injection attacks, broken authentication, cross-site scripting (XSS), security misconfigurations, server-side request forgery (SSRF), and other common web application vulnerabilities.

Findings Summary

- **Critical:** 0
- **High:** 1
- **Medium:** 3
- **Low:** 5
- **Informational:** 7

The detailed findings report has been provided separately and includes proof-of-concept exploits, CVSS scores, and remediation guidance for each finding.

Compliance Coverage

Our reporting format was built to meet the documentation requirements of the following regulatory and compliance frameworks. The full compliance mapping document - showing how findings map to each control - is published at turbopentest.com/compliance/methodology.

- **PCI DSS v4.0.1** (June 2024 errata) \u2014 Requirement 11.4 (External and internal penetration testing)
- **SOC 2 (TSC 2017 with 2022 PoF)** \u2014 Trust Services Criteria CC6.1 + CC6.6 (logical access / network access boundaries) and CC7.1 (vulnerability detection); supports CC4.1 (Monitoring activities) when the testing cadence is documented separately by the customer
- **ISO 27001:2022** \u2014 Annex A controls A.8.8 (Management of technical vulnerabilities) and A.8.29 (Security testing in development and acceptance)
- **HIPAA** - Section 164.308(a)(8) (Technical evaluation of security controls)
- **NIST SP 800-115** - Technical security testing and assessment methodology
- **OWASP WSTG** - Web Security Testing Guide coverage

> *I personally endorse the integrity of this security assessment. TurboPentest is an automated penetration testing platform operated by IntegSec, combining industry-standard tools with AI-powered analysis to deliver actionable results.*

Michel Chamberland

Michel Chamberland
CISSP, OSCP, OSCE, CEH, GIAC, CCSK
Chief Executive Officer, IntegSec
integsec.com | turbopentest.com