SAMPLE · REDACTED

API Vulnerability Assessment & Penetration Testing

Summary Report — sample deliverable

Prepared by Virtue Software Technologies Private Limited (VirtuesTech)

This is a redacted sample. Client identity, endpoints, and evidence from a real engagement have been removed to illustrate report structure and depth only.

1 · Assessment Overview

VirtuesTech conducted an API Vulnerability Assessment and Penetration Testing (VAPT) engagement for [redacted] over a two-week period. The assessment evaluated the security posture of the client's API against current industry best practices, conducted in accordance with **NIST SP 800-115**, the **OWASP API Security Testing** methodology, and VirtuesTech's testing methodology.

Phases: Planning (goals and rules of engagement) → Discovery (scanning and enumeration) → Attack (exploitation and validation) → Reporting (findings, evidence, and strengths).

2 · Scope

Item	Detail
Assessment type	API Vulnerability Assessment & Penetration Test
Targets	[redacted]
User roles tested	Organization Admin, Organization Member
Exclusions (client request)	Denial of Service (DoS); Phishing / Social Engineering

3 · Finding Severity Ratings

Severity	CVSS v3	Definition (abridged)
CRITICAL	9.0–10.0	Straightforward exploitation, usually system compromise. Patch immediately.
HIGH	7.0–8.9	More difficult, but can elevate privileges or cause data loss/downtime. Patch as soon as possible.
MEDIUM	4.0–6.9	Exploitable with extra steps. Patch after high-priority issues.
LOW	0.1–3.9	Non-exploitable but reduces attack surface. Patch in next maintenance window.
INFO	N/A	Observations, strong controls, and documentation notes.

4 · Vulnerability Summary & Report Card

Illustrative distribution from a representative engagement:

0	3	1	6	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

ID	Severity	Finding	Remediation (summary)
PT-001	HIGH	Prompt injection in AI processing endpoint	Validate/isolate user instructions before the model; separate system and user content.
PT-002	HIGH	Unrestricted file upload	Enforce allow-list of extensions, MIME types, and content signatures.
PT-003	HIGH	Double-extension upload bypass via null byte	Server-side filename/extension/MIME/signature validation; allow-list approach.
PT-004	MEDIUM	No rate limiting on OTP verification	Rate limiting, CAPTCHA, IP throttling, OTP expiry enforcement.
PT-005–010	LOW	Input validation, password history, information disclosure	Strict server-side validation; suppress server identification; password-history checks.
PT-011–012	INFO	Confirm-password field, missing security headers	Add confirm-password validation and the full security-header set.

5 · Security Rating

An overall grade is assigned from the count and severity of findings. In this representative engagement the application graded **A** — a limited number of High-severity issues, with the primary risks in AI prompt handling and file-upload security.

Example finding (redacted)

Each finding in a VirtuesTech report carries a description, demonstrated impact, affected component, evidence, and specific remediation. One finding is reproduced below with client-specific detail removed.

PT-001 — Potential Prompt Injection in AI Processing Endpoint

HIGH

DESCRIPTION

An AI-backed endpoint accepted a user-controlled parameter ([redacted]) that was passed into the model prompt. By supplying crafted instructions within that parameter, an attacker could override the intended function and force the model to follow arbitrary instructions. The application exhibited behavior indicating insufficient isolation between user input and system instructions.

IMPACT

An attacker can manipulate the model to ignore intended application logic and produce attacker-controlled responses — potentially disclosing internal prompts, hidden instructions, or sensitive information where the AI is integrated with additional tools or knowledge bases.

AFFECTED COMPONENT

[redacted]

EVIDENCE

[redacted]

REMEDIATION

Implement prompt-injection guards: validate and control user instructions before they reach the model, and establish clear boundaries between system prompts and user-controlled content to prevent behavior manipulation.

> This showcases why AI products need AI-aware testing: prompt injection is invisible to a conventional API scanner, and sits outside the OWASP API Top 10 that most tools check. VirtuesTech treats AI endpoints as their own attack surface.

What a full report also includes

Executive summary for leadership · every finding with reproduction steps and evidence · remediation grouped by affected functionality · retest verification once fixes are applied (findings updated to "remediated and retested") · and an annual-cadence recommendation.

> **Retest closes the loop.** In the engagement this sample is drawn from, the client remediated the findings and a follow-up retest returned a clean scan. We report to fix, not just to file.

This is a redacted sample deliverable. To discuss a scoped assessment for your own API, contact info@virtuestech.com.