PENETRATION TEST REPORT

API Penetration Test Report

CLIENT	Acme Fintech
ENGAGEMENT ID	demo-api
TESTER	Komal Prasad
TARGET	https://api.acmepay.example
START DATE	2026-08-03
END DATE	2026-08-06
MODULE	API Pentest
OWASP FRAMEWORK	OWASP API Security Top 10 — 2023

HIGH 1 MEDIUM 1 LOW 1

Table of Contents

1. Executive Summary

During the engagement, a total of **3** findings were identified against https://api.acmepay.example: 1 high, 1 medium and 1 low.

The most significant issue is **Broken Object Level Authorization on /v1/transactions/{id}** (High, CVSS 8.1), which should be remediated as a priority.

The overall risk is assessed as **High**. Remediation of the high-severity findings should be scheduled promptly.

Detailed technical findings, evidence, and remediation guidance are provided in the following sections. All testing was performed with appropriate authorization.

Severity Breakdown

Severity	Count	CVSS Range
Critical	0	9.0 – 10.0
High	1	7.0 – 8.9
Medium	1	4.0 – 6.9
Low	1	0.1 – 3.9
Info	0	0.0
TOTAL	**3**	

2. Engagement Overview

Client	Acme Fintech
Engagement ID	demo-api
Tester	Komal Prasad
Start Date	2026-08-03
End Date	2026-08-06
Target	https://api.acmepay.example
Module	API Pentest
OWASP Framework	OWASP API Security Top 10 — 2023

3. Scope & Methodology

In-Scope

- https://api.acmepay.example
- https://api.acmepay.example/docs/
- https://api.acmepay.example/api/

Out of Scope

- https://api.acmepay.example/admin-panel/

Testing Checklist

Step	Status
API discovery & inventory (versions, endpoints, shadow APIs)	Complete
Authentication testing (tokens, sessions, MFA, OAuth flows)	Complete
Authorization testing (BOLA / IDOR across roles)	Complete
Object property level authorization (mass assignment)	Complete
Function level authorization (admin vs user routes)	Complete
Input validation & injection (SQLi, NoSQLi, XSS, SSTI, SSRF)	Complete
Rate limiting & resource consumption testing	Complete
Business flow / abuse-case testing	Complete
JWT & token security (alg confusion, weak secrets, expiry)	Pending
GraphQL / gRPC / WebSocket specific testing	Pending
Security misconfiguration (CORS, headers, error handling)	Pending
Retesting of confirmed findings	Pending

4. Findings Summary

ID	Title	Severity	CVSS	Status
F-001	Broken Object Level Authorization on /v1/transactions/{id}	High	8.1	open
F-002	Unrestricted resource consumption on /v2/ledger	Medium	7.5	open
F-003	Verbose error disclosure leaks stack traces	Low	5.3	open

5. Detailed Findings

F-001 — Broken Object Level Authorization on /v1/transactions/{id} *[High]*

Category	API1:2023 — Broken Object Level Authorization (BOLA)
Severity	High
CVSS v3.1	8.1 · CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
Status	open
Affected Endpoint	/v1/transactions/{id}
HTTP Method	GET
Parameter / Body field	id
Auth Required?	JWT

DESCRIPTION

Transaction endpoint returns full transaction data for any ID regardless of the authenticated user's ownership of the record.

EVIDENCE / PROOF OF CONCEPT

GET /v1/transactions/884211 with a token for user 501 returned user 502's transaction with card PAN.

IMPACT

Complete transaction and PII disclosure across the customer base.

REMEDIATION

Validate object ownership on every object-level read/write; use opaque identifiers.

REFERENCES

- https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/

F-002 — Unrestricted resource consumption on /v2/ledger [Medium]

Category	API4:2023 — Unrestricted Resource Consumption
Severity	Medium
CVSS v3.1	7.5 · CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Status	open
Affected Endpoint	/v2/ledger
HTTP Method	GET
Parameter / Body field	page_size
Auth Required?	no

DESCRIPTION

Ledger endpoint honors page_size up to 100000 with no rate limiting, enabling resource exhaustion and inflated cloud costs.

EVIDENCE / PROOF OF CONCEPT

page_size=100000 returned in 14s; 50 concurrent requests saturated the pod.

IMPACT

Denial of service for all API consumers and elevated infrastructure costs.

REMEDIATION

Cap pagination, enforce per-client rate limits and payload quotas.

F-003 — Verbose error disclosure leaks stack traces [Low]

Category	API8:2023 — Security Misconfiguration
Severity	Low
CVSS v3.1	5.3 · CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Status	open
Affected Endpoint	/v1/login
HTTP Method	POST
Parameter / Body field	body
Auth Required?	no

DESCRIPTION

Malformed JSON requests return 500 responses containing full Django debug tracebacks with internal paths and dependency versions.

EVIDENCE / PROOF OF CONCEPT

POST /v1/login with invalid body returned <pre>traceback…django/core/handlers…</pre>

IMPACT

Information disclosure that aids reconnaissance and version-based attacks.

REMEDIATION

Return generic errors in production; log details server-side only.

6. Conclusion & Recommendations

The engagement identified 3 finding(s). All findings should be tracked to closure with defined owners and target dates. High and critical findings should be remediated before the application is exposed to untrusted users. A retest should be scheduled once fixes are deployed.

Remediation Priority

Severity	Recommended Timeline
Critical	Immediate (within days)
High	Short term (within 2 weeks)
Medium	Near term (next release)
Low	Scheduled (next cycle)
Info	Informational

Appendix A — OWASP Category Reference

OWASP API Security Top 10 — 2023

Code	Category
API1:2023	Broken Object Level Authorization (BOLA)
API2:2023	Broken Authentication
API3:2023	Broken Object Property Level Authorization (BOPLA)
API4:2023	Unrestricted Resource Consumption
API5:2023	Broken Function Level Authorization
API6:2023	Unrestricted Access to Sensitive Business Flows
API7:2023	Server Side Request Forgery (SSRF)
API8:2023	Security Misconfiguration
API9:2023	Improper Inventory Management
API10:2023	Unsafe Consumption of APIs