Freelance with Chirag
VAPT & Application Security Consulting

CONFIDENTIAL

Web Application Penetration Test Report

Vulnerability Assessment & Penetration Testing (VAPT) of the Acme Corp customer portal — executive summary, technical findings, and remediation guidance.

Client	Acme Corp (fictional)
Engagement ID	WEB-2026-014
Assessment type	Grey-box Web Application VAPT
Report date	15 October 2026
Report version	1.0 (Final)
Prepared by	Chirag Arora — Independent VAPT Consultant
Classification	Confidential — for client distribution only

This document is a **sample** containing entirely fictional, non-sensitive data. It illustrates the structure, depth, and tone of a deliverable only.

Document Control & Confidentiality

Version history

Version	Date	Description	Author
0.1	11 Oct 2026	Draft — testing complete	Chirag Arora
0.9	14 Oct 2026	Internal QA review	Chirag Arora
1.0	15 Oct 2026	Final — issued to client	Chirag Arora

Distribution

Name	Role	Organisation
Jane Reed	CISO	Acme Corp
Sam Okoye	Head of Engineering	Acme Corp
Chirag Arora	VAPT Consultant	Freelance with Chirag

Confidentiality statement

This report contains information about the security posture of the systems in scope and is classified **Confidential**. It is intended solely for the named recipients. The findings describe weaknesses that could be exploited if disclosed; distribution should be limited to those with a legitimate need to know. All testing was conducted under written authorization and within the agreed scope.

Disclaimer

A penetration test is a point-in-time assessment based on the scope and information available during the engagement window. It cannot guarantee the identification of every vulnerability and does not certify that the systems are free of defects. Security is an ongoing process; this report reflects the state of the environment on the dates tested.

1. Executive Summary

Freelance with Chirag was engaged to perform an authorized web application penetration test of the Acme Corp customer portal. Testing was carried out against the staging environment over five business days, in a grey-box configuration using accounts provisioned by the client, and strictly within an agreed scope under written authorization.

The assessment identified **seven** vulnerabilities: one High, three Medium, and three Low severity. The most significant is an Insecure Direct Object Reference (IDOR) in the order-history API that allows an authenticated customer to read other customers' orders. No Critical issues were found. Every finding in this report was manually validated; no unconfirmed or false-positive results are included.

The underlying themes are authorization enforcement and defence in depth: several issues stem from trusting client-supplied identifiers and from missing hardening controls. These are addressable with well-understood fixes, prioritised in Section 5.

Risk snapshot

Critical	High	Medium	Low	Informational
0	1	3	3	0

Overall risk rating: **High** — driven by the cross-customer data exposure (WEB-001).

Findings summary

ID	Finding	Severity	CVSS	Status
WEB-001	IDOR in order-history API (cross-customer access)	High	8.1	Open
WEB-002	Missing rate limiting on login endpoint	Medium	5.3	Open
WEB-003	Reflected XSS in search parameter	Medium	6.1	Open
WEB-004	Session cookie missing Secure / SameSite	Medium	4.8	Open
API-004	Verbose error / stack-trace disclosure	Low	3.1	Open
WEB-006	Missing HTTP security headers	Low	2.6	Open
WEB-007	Autocomplete enabled on sensitive fields	Low	2.0	Open

2. Scope & Methodology

2.1 Scope

In-scope asset	Detail
Customer portal (web)	https://staging-portal.acme.example
Portal API	https://staging-portal.acme.example/api/v1/*
Authentication	Email/password + TOTP MFA
Test accounts	2 standard users, 1 administrator (client-provided)
Environment	Staging (production-equivalent configuration)

Out of scope: production systems, denial-of-service testing, social engineering, physical security, and third-party services not owned by the client.

2.2 Methodology

Testing followed a structured five-stage methodology aligned to the OWASP Web Security Testing Guide (WSTG) and the OWASP Top 10, combining manual testing with supporting tooling. Manual testing is emphasised so that authorization and business-logic flaws — which automated scanners routinely miss — are reliably identified.

01 Discovery & Scoping	Confirm targets, objectives, authorized boundaries, and test accounts.
02 Reconnaissance & Mapping	Enumerate the application surface, technologies, roles, and workflows.
03 Vulnerability Analysis & Exploitation	Manually test and safely validate weaknesses; capture evidence.
04 Reporting & Risk Assessment	Document findings with CVSS scoring, business impact, and remediation.
05 Retesting & Closure	Re-test remediated issues and confirm final security status.

2.3 Severity & CVSS

Each finding is rated using CVSS v3.1 base metrics and mapped to a qualitative severity. Severity reflects both technical impact and business context agreed with the client.

Severity	CVSS base	Expected response
Critical	9.0 – 10.0	Immediate action; fix within days
High	7.0 – 8.9	Prioritised remediation; fix within 2–4 weeks
Medium	4.0 – 6.9	Planned remediation; fix within the quarter
Low	0.1 – 3.9	Address during normal maintenance
Informational	0.0	Best-practice hardening; no direct risk

3. Detailed Findings

Each finding below includes a description, affected component, CVSS vector, business impact, reproduction steps, and remediation guidance. Three representative findings are detailed in full in this sample.

WEB-001 · Insecure Direct Object Reference (IDOR) — High · CVSS 8.1

Affected component	CWE	CVSS vector
GET /api/v1/orders/{orderId}	CWE-639: Authorization Bypass Through User-Controlled Key	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

DESCRIPTION

The order-history endpoint returns an order based on an `orderId` supplied by the client, without verifying that the order belongs to the authenticated user. Because identifiers are sequential integers, an attacker can enumerate values to read other customers' orders, including names, addresses, and purchase history.

BUSINESS IMPACT

Unauthorized disclosure of personal data across customer accounts (a tenancy/authorization breach). This carries privacy, regulatory, and reputational consequences and is the highest-risk issue identified.

REPRODUCTION STEPS

```
1. Log in as a standard user and open an order you own.
2. Capture the request: GET /api/v1/orders/10482
3. Change the identifier: GET /api/v1/orders/10483
4. Observe another customer's order returned (HTTP 200, no ownership check).
```

REMEDIATION

Enforce server-side authorization on every object access: confirm the authenticated principal owns, or is explicitly permitted to view, the requested resource before returning data. Prefer indirect references scoped to the session, deny by default, and add automated authorization tests covering horizontal access.

WEB-003 · Reflected Cross-Site Scripting (XSS) — Medium · CVSS 6.1

Affected component	CWE	CVSS vector
GET /search?q=	CWE-79: Improper Neutralization of Input During Web Page Generation	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

DESCRIPTION

The search page reflects the q parameter into the HTML response without contextual output encoding, allowing injection of arbitrary script that executes in the victim's browser when they follow a crafted link.

BUSINESS IMPACT

An attacker can run script in a victim's session context — stealing session tokens, performing actions as the user, or defacing page content. Delivery typically requires a crafted link (phishing).

REPRODUCTION STEPS

```
1. Browse to: /search?q=test
2. Replace the value with: /search?q=alert(document.domain)
3. Observe the script execute, confirming unencoded reflection.
```

REMEDIATION

Apply context-aware output encoding on all user-controlled data rendered into responses, validate input server-side, and deploy a restrictive Content-Security-Policy as defence in depth.

WEB-002 · Missing Rate Limiting on Authentication — Medium · CVSS 5.3

Affected component	CWE	CVSS vector
POST /api/v1/login	CWE-307: Improper Restriction of Excessive Authentication Attempts	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

DESCRIPTION

The login endpoint does not throttle or lock out repeated failed authentication attempts, permitting high-volume credential guessing (brute-force and credential-stuffing) against accounts.

BUSINESS IMPACT

Increases the likelihood of account takeover, particularly for accounts with weak or reused passwords, and enables large-scale credential-stuffing attacks.

REPRODUCTION STEPS

```
1. Submit repeated POST /api/v1/login requests with invalid passwords.
2. Observe that 100+ attempts succeed without throttling, CAPTCHA, or lockout.
```

REMEDIATION

Introduce progressive rate limiting and temporary lockout per account and per source, add anomaly detection and alerting, and consider CAPTCHA or step-up challenges after repeated failures.

4. Remediation Priorities

The following order balances risk reduction against implementation effort. Addressing the authorization issues first removes the highest business risk.

Priority	Finding	Action	Effort
1	`WEB-001`	Enforce server-side object ownership checks	Low
2	`WEB-003`	Context-encode output; add CSP	Low–Med
3	`WEB-002`	Add rate limiting + lockout on auth endpoints	Low
4	`WEB-004`	Set Secure/HttpOnly/SameSite on session cookies	Low
5	`WEB-006`	Add standard security headers	Low
6	`API-004`	Return generic errors; log details server-side	Low
7	`WEB-007`	Disable autocomplete on sensitive fields	Low

5. Retesting & Closure

A remediation re-test is included in this engagement. Once fixes are deployed to staging, each finding is re-tested to confirm it is fully resolved and that no regression or related issue has been introduced. A short closure report is then issued recording the final status of every finding and the resulting security posture.

Milestone	Target date	Owner
Remediation complete (client)	Within 4 weeks	Acme Engineering
Re-test window	1–2 days	Chirag Arora
Closure report issued	On re-test completion	Chirag Arora

End of sample report. All names, systems, and findings in this document are fictional and for illustration only. A real engagement report is tailored to your environment and scope. — Freelance with Chirag · Chirag Arora