Sample Redacted VAPT Report - Tripleplus Solutions

Tripleplus Solutions

Sample Redacted VAPT Report

Assessment Type: Web Application and API VAPT

Report Status: Sample / Redacted / Demonstration

Prepared For: Example Client Private Limited

Prepared By: Tripleplus Solutions

This document is a sample redacted report excerpt. Client name, domain, IP addresses, user IDs, tokens, screenshots, payloads and business-sensitive values have been replaced with safe placeholders.

Executive Summary

The assessment identified an access control weakness in an authenticated order detail API. A low-privilege user was able to request an object belonging to another account by changing the order identifier. This creates customer data exposure risk and should be remediated before production release or public rollout.

Assessment Scope

Application	Customer portal and backend API
Environment	Staging environment provided by client
Testing Mode	Authenticated black-box and grey-box validation
Excluded	Denial-of-service testing, social engineering and production data extraction

Finding Detail

Finding ID	VAPT-WEB-AC-001
Finding	Broken object level authorization in order detail API
Severity	High | CVSS 8.1
Affected Asset	https://portal.example-redacted.in/api/orders/{order_id}
OWASP Mapping	A01 Broken Access Control, API1 Broken Object Level Authorization
Current Status	Open, pending remediation and retest

Evidence

Authenticated low-privilege User A changed the numeric order identifier in the API request and received another user's order metadata. Customer name, address, invoice value and order references were redacted in the evidence provided to the client.

Proof of Concept

Request sent with User A session:

```
GET /api/orders/REDACTED-ID HTTP/2
```

The response returned order data not owned by User A. Session tokens, object identifiers and response body values have been removed from this sample.

Business Impact

An attacker with a valid low-privilege account could enumerate order identifiers and access sensitive customer order information. Depending on exposed fields, this may create privacy, contractual and reputational risk.

Remediation Guidance

- Enforce server-side object ownership checks on every order read and update endpoint.
- Do not rely on hidden fields, frontend controls or predictable identifiers for authorization.
- Add centralized authorization middleware where possible.
- Add regression tests for customer, staff and admin role boundaries.
- Review adjacent order, invoice, shipment and report endpoints for the same pattern.

Retest Plan

Retest should repeat the original request with the same user role, verify that cross-account access is denied, test adjacent endpoints, and confirm that logs capture authorization failures without exposing sensitive data.

Sample redacted report for buyer evaluation. This document is not a client deliverable and does not include real client data.