TRINETRIX INTELLIGENCE

SEE BEYOND. SECURE EVERYTHING.

Web Application VAPT Report

Sanitized sample showing report structure, evidence standards and remediation detail.

SAMPLE ONLY / FICTIONAL ASSETS / NO CUSTOMER DATA

This document demonstrates a typical deliverable. Findings, identifiers, domains, screenshots and business context are fictional.

// EXECUTIVE SUMMARY

A decision-ready view of technical exposure

The assessment identified one critical and two high-risk weaknesses in the fictional application. The most important theme was inconsistent server-side authorization across administrative and customer workflows.

ASSESSMENT	Authenticated grey-box web application test
SAMPLE TARGET	portal.example.test (fictional)
TESTING STANDARD	OWASP WSTG, ASVS and CWE mapping
OVERALL POSTURE	Material risk requiring prioritized remediation
RETEST STATUS	Included after fixes are submitted

SEVERITY	COUNT	PRIMARY THEME	RECOMMENDED ACTION
Critical	1	Authorization bypass	Restrict administrative actions server-side
High	2	Session and data exposure	Harden trust boundaries and secrets handling
Medium	3	Defense in depth	Resolve during the next engineering cycle
Low	2	Hardening	Track through standard maintenance

Priority remediation sequence

1. Enforce role and object authorization in a centralized server-side policy layer.
2. Revoke exposed secrets and move credential access to short-lived workload identities.
3. Invalidate active sessions after security-sensitive account changes.
4. Add negative authorization tests to the release pipeline.

// FINDING TNX-SAMPLE-001

Administrative action accessible to a standard user

A standard account could submit a crafted request to an administrative endpoint and change another user's account status.

SEVERITY	Critical / CVSS 3.1: 9.1
CATEGORY	Broken access control / CWE-862
AFFECTED ASSET	https://portal.example.test/api/admin/users/{id}
STATUS	Open - remediation required

Business impact

An authenticated customer could suspend or reactivate unrelated accounts. In a real environment this may disrupt service, support fraud or enable further privilege escalation.

Proof of concept

The tester authenticated as a standard user, captured the account-update request, replaced the target identifier with an unrelated user and changed the requested status. The server returned HTTP 200 and the change was visible to the affected account.

Root cause

The route checked that a session existed but did not enforce the administrative role or verify that the caller was authorized to act on the target object.

Remediation

Apply deny-by-default authorization at the route and service layers. Resolve the caller's permissions server-side, validate authorization against the target resource, and add tests covering standard, support and administrator roles.

// FINDING TNX-SAMPLE-002

Long-lived cloud credential exposed in application configuration

A deployable application artifact contained a cloud access key with read access to a fictional storage environment.

SEVERITY	High / CVSS 3.1: 8.1
CATEGORY	Hard-coded credentials / CWE-798
AFFECTED ASSET	Fictional application release artifact
STATUS	Retest pending

Evidence captured

The key was recovered during static analysis and validated only against the explicitly authorized test resource. No customer or production data was accessed.

Risk

Anyone obtaining the artifact could reuse the credential outside the application. Long-lived credentials are difficult to contain and can remain valid after the application is removed.

Remediation

Revoke the credential, review its access history, remove secrets from build inputs, and use short-lived workload identity or a managed secret service. Add secret scanning to source control and build pipelines.

Retest plan

Confirm the original key is revoked, inspect a new build for residual secrets, and verify the replacement identity has the minimum permissions required.

// CLOSURE EVIDENCE

What a completed retest records

A retest does more than repeat one request. It verifies the original exploit, adjacent paths and whether the underlying security control now behaves consistently.

ORIGINAL EXPLOIT	No longer reproducible
RELATED ROLE CHECKS	Validated across representative roles
REGRESSION COVERAGE	Recommended tests supplied to engineering
RESIDUAL RISK	Documented where architectural work remains
CERTIFICATE	Issued only when agreed closure criteria are met

What the full client report also includes

Executive risk themes, complete scope and limitations, test methodology, every confirmed finding, request and response evidence, screenshots where useful, CVSS vectors, standards mapping, root-cause analysis, remediation guidance, debrief notes and updated closure status.

Need a report tailored to your environment?
admin@trinetrixintelligence.com
+91 88494 40989
www.trinetrixintelligence.com