Tungsten Intelligence

Nashville, TN | sales@tungsteni.com | 615-601-2479

Penetration Test Report

Sample Client Name: **------------------------------**

System/Application: ********************************

Engagement ID	**TI-PT-20**-*** **
Report Version	v1.0 (Sample)
Report Date	---- --, 20**
Testing Window	---- --, 20** to ---- --, 20**
Primary Contact	-----------------------------
Prepared By	Tungsten Intelligence - Offensive Security Team
Classification	Confidential (Sample / Redacted)

Intended use: This sample report illustrates structure, dashboards, and depth of detail. All client-identifying information is replaced with dashes/asterisks. Findings, screenshots, and data below are representative examples only.

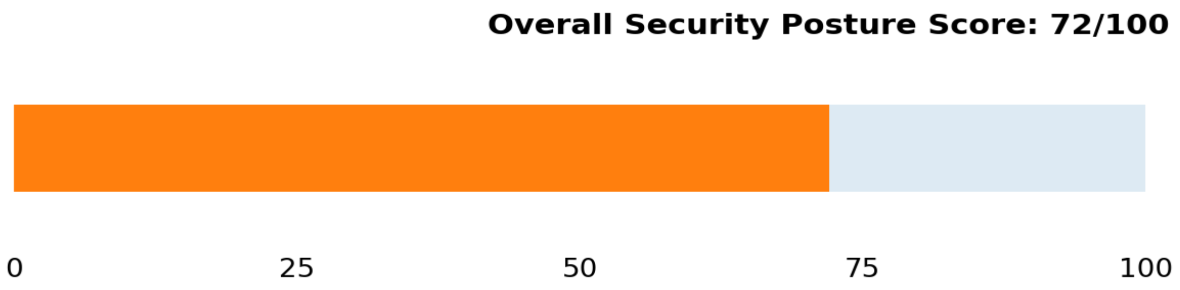
Distribution: ------------------------------

Legal notice (summary): Testing performed under written authorization. This report is provided “as-is” for the exclusive use of the intended recipient. Do not rely on this sample for security decisions.

1. Executive Summary

Tungsten Intelligence conducted a time-boxed penetration test to evaluate the security posture of ****************************** for ------------------------------. The assessment focused on identifying exploitable weaknesses, validating business impact, and providing prioritized remediation guidance.

Overall Risk Rating	Findings	Retest Included
HIGH	19	Yes



Key takeaways (sample):

- At least one **critical** issue enabled unauthorized access to sensitive data under certain conditions.
- Multiple **high** severity weaknesses increased likelihood of account takeover or privilege escalation.
- Hardening opportunities were identified across authentication, configuration, and secure SDLC controls.

Immediate actions (first 14 days): Patch/high-priority configuration changes; rotate exposed secrets; review privileged access and MFA enforcement; implement WAF rules for known exploit patterns.

2. Scope and Engagement Parameters

In-Scope Assets (Examples)	• Web Application: https://********.******.com • API Gateway: api.********.com • External IP Range: ***.***.***.0/24 • Mobile App (Optional): iOS/Android build v*.*.*
Out-of-Scope (Examples)	• Social engineering • Denial-of-Service testing • Third-party SaaS components not owned/managed by client
Testing Types	• External web application • API testing • Limited infrastructure validation • Authenticated & unauthenticated testing
Testing Approach	• Manual exploitation with targeted automation • OWASP ASVS / Top 10 alignment • MITRE ATT&CK technique mapping (where applicable)
Rules of Engagement	• Testing conducted between --:-- and --:-- (local) • Production-safe techniques prioritized • No data exfiltration beyond proof-of-access samples • Client escalation contact: ------------------------------

Assumptions: Written authorization was provided; testing accounts and representative data were available; client monitoring teams were informed of testing source IPs.

3. Methodology

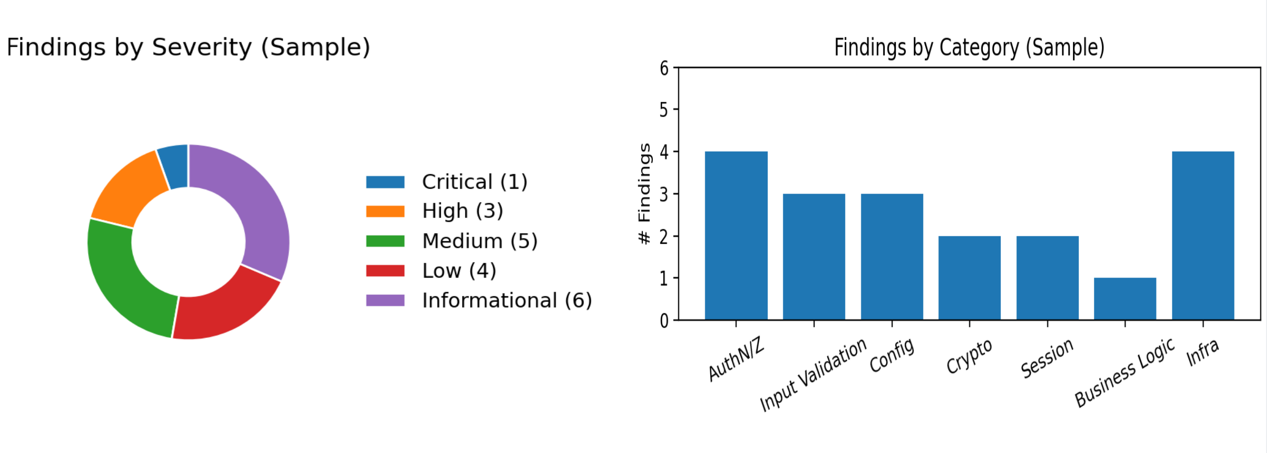
The assessment followed a mature, repeatable penetration testing lifecycle aligned to common industry practice. This sample presents the sections typically included; exact activities vary by scope and environment.

Reconnaissance & Threat Modeling	Asset discovery, attack surface mapping, and hypothesis-driven testing plan.
Vulnerability Identification	Manual review plus controlled automation to identify common and nuanced flaws.
Exploitation & Validation	Exploit development and chaining to confirm impact, including privilege escalation paths.
Post-Exploitation (Bounded)	Evidence collection limited to proof-of-access; no destructive actions.
Reporting & Remediation Support	Actionable writeups, fix guidance, and optional retest / validation.

Severity scoring (sample): CVSS v3.1 used as an input alongside exploitability, exposure, and business impact. Final severity is determined by analyst judgment and client context.

4. Findings Overview Dashboard

The dashboard below summarizes results at-a-glance. In client deliverables, this section can be expanded with environment-specific metrics (e.g., affected user counts, asset criticality, trending).



Severity	Count	Sample Notes
Critical	1	Direct compromise with minimal prerequisites.
High	3	Likely exploitation with meaningful impact.
Medium	5	Requires additional conditions or limited impact.
Low	4	Minor impact / defense-in-depth.
Informational	6	Hardening, best practice, or observation.

Top 5 themes (sample): weak authorization boundaries; missing rate limiting; insecure default configurations; inconsistent secret handling; and incomplete logging/alerting coverage.

5. Findings Summary

This section provides a catalog of identified issues. Detailed writeups follow for selected items. In the final client report, *all* findings include reproduction steps, evidence, and tailored guidance.

ID	Severity	Title	Mapping	Status
TI-PT-001	Critical	Broken Object Level Authorization (BOLA) in /api/v*/accounts/*	OWASP API1	Open
TI-PT-002	High	Password reset token predictability / insufficient entropy	OWASP A07	Open
TI-PT-003	High	Privilege escalation via misconfigured role mapping	ASVS 4.0.2	Open
TI-PT-004	High	Sensitive data exposure in application logs	OWASP A09	Open
TI-PT-005	Medium	Missing rate limiting on authentication endpoints	OWASP A04	Open
TI-PT-006	Medium	Stored XSS in administrative comment field	OWASP A03	Open
TI-PT-007	Medium	Insecure CORS policy allows broad origins	OWASP A05	Open
TI-PT-008	Low	TLS configuration supports legacy ciphers	CIS	Open
TI-PT-009	Info	Cookie flags missing on non-auth cookies	OWASP A05	Open

6. Detailed Findings (Sample)

TI-PT-001 - Broken Object Level Authorization (BOLA)

Severity	<b>Critical</b>
CVSS (v3.1)	9.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) - sample
Affected Assets	API: /api/v*/accounts/{id} - ******************************
Status	Open (Sample)

Description

An authenticated user could access or modify other users' account resources by manipulating the object identifier in API requests. Authorization checks were insufficiently enforced server-side, allowing cross-tenant data exposure in certain workflows.

Business Impact

Successful exploitation may result in unauthorized access to sensitive records, account takeover pathways, and regulatory exposure (e.g., privacy obligations) depending on data classification and tenancy model.

Evidence (sample)

- Request/response pair demonstrating access to a different accountId (redacted).
- No server-side ownership validation observed for the targeted endpoint.
- Exploit succeeded with low-privileged credentials in the sample scenario.

EVIDENCE (screenshot/redaction placeholder)

Remediation Guidance

Implement server-side object ownership checks for every resource access. Prefer centralized authorization middleware/policies. Adopt allow-list checks based on authenticated principal + tenant context. Add negative tests to CI (unit/integration) for IDOR/BOLA. Consider per-object access control lists (ACL) where applicable, and log/alert on authorization failures and anomalous access patterns.

References

- OWASP API Security Top 10 (API1: Broken Object Level Authorization)
- OWASP ASVS: V4 Access Control (selected requirements)

6. Detailed Findings (Sample) - Continued

TI-PT-002 - Password Reset Token Predictability

Severity	<b>High</b>
CVSS (v3.1)	8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N) - sample
Affected Assets	Auth service: ******************************
Status	Open (Sample)

Description

Password reset tokens were generated using a predictable pattern and/or insufficient randomness in the sample scenario. An attacker could potentially enumerate valid tokens for targeted accounts within a short time window.

Business Impact

Token prediction can enable unauthorized password resets and account takeover, especially when combined with user enumeration and weak rate limiting.

Evidence (sample)

- Token length/format suggests non-cryptographic randomness (redacted).
- Multiple tokens observed to share a prefix/time-derived component in sample collection.
- Reset endpoint lacked robust throttling and anomaly detection in sample configuration.

EVIDENCE (token sample/redaction placeholder)

Remediation Guidance

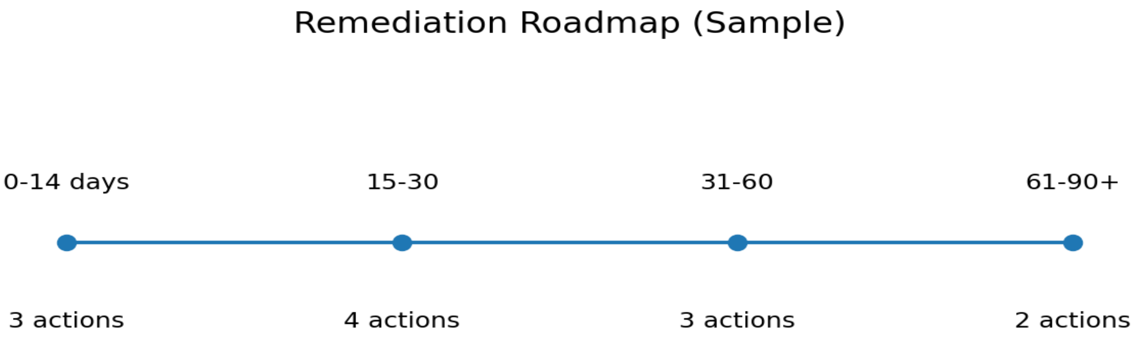
Generate reset tokens using a cryptographically secure RNG with sufficient entropy (e.g., 128 bits+), store only hashed tokens server-side, enforce short expirations, and bind tokens to user + purpose + device context where possible. Add rate limiting, monitoring, and CAPTCHA/step-up controls for anomalous reset patterns.

References

- OWASP Cheat Sheet: Forgot Password
- NIST SP 800-63B (selected guidance on tokens/authentication)

7. Remediation Roadmap (Sample)

A phased plan to reduce risk quickly and sustain improvements. In full client reports, each action maps to findings, owners, due dates, and validation criteria.



Phase	Priority Actions (Examples)
0-14 days	• Remediate critical/high findings affecting authz and reset flows • Rotate exposed secrets and invalidate tokens • Enable MFA for privileged accounts • Add emergency WAF/rate limit rules
15-30 days	• Centralize authorization policy checks • Harden logging with sensitive-data scrubbing • Add security tests to CI for key abuse cases
31-60 days	• Implement least privilege for service accounts • Improve secrets management (vault, rotation) • Expand monitoring/alerting use-cases
61-90+ days	• Programmatic threat modeling cadence • Secure SDLC maturity (SAST/DAST, dependency scanning) • Quarterly regression testing / continuous validation

8. Appendices (Sample)

A. Severity Definitions

Severity	Definition (Sample)
Critical	Immediate risk of system compromise or material data exposure; likely exploitation; minimal prerequisites.
High	Significant impact with reasonable exploitation path; may enable account takeover, privilege escalation, or sensitive
Medium	Meaningful weakness requiring additional conditions; limited blast radius; or compensated by other controls.
Low	Minor impact or defense-in-depth; exploitation unlikely or limited.
Informational	Observation, best practice, or hardening recommendation.

B. Tooling (Examples)

Common tools may include: Burp Suite Professional, Nmap, nuclei, custom scripts, Postman, cloud-native logging/query tools, and manual code review (if scoped). Exact tooling is tailored per engagement.

C. Deliverables (Typical)

- Executive report (PDF) with dashboards and prioritized actions
- Technical findings report with evidence and reproduction steps
- Remediation workshop (optional)
- Retest / validation memo (optional) with closure status

D. Client Evidence Handling

Evidence is minimized and redacted. Sensitive data is not retained beyond agreed timelines. Artifacts are transferred via approved secure channels (e.g., encrypted portal or client-managed repository).