CASE STUDY #2

Chained Authorization Weaknesses Leading to Cross-Tenant Data Exposure

Multi-Tenant SaaS Web Application & Partner API Security Assessment

SAAS PLATFORM MULTI-TENANT CROSS-TENANT EXPOSURE

⬡ ENGAGEMENT AT A GLANCE

1	5+	1-2 wks	100%
Critical Vulnerabilities	High & Medium Findings	Engagement Duration	Manual Validation Rate

⬡ CLIENT BACKGROUND

A fast-growing SaaS provider approached IVASTA Security after onboarding several enterprise customers. As part of their sales process, they were required to provide independent penetration testing validation of both their web application and partner-facing API.

The client had implemented automated scanning tools and internal security checks but sought assurance that their multi-tenant architecture and access controls could withstand real-world adversarial testing. Their primary concern was whether newly introduced features and API integrations introduced hidden authorization or data isolation weaknesses.

⬡ SCOPE OF ENGAGEMENT

The assessment covered all major surfaces of the client's SaaS platform and partner API:

- Authenticated and unauthenticated testing of the web application
- Full API security assessment
- Multi-tenant access control validation
- Role and permission boundary analysis
- Business workflow testing
- Token and session management validation

A manual, adversarial testing approach was applied throughout — no automation-only shortcuts.

⬡ METHODOLOGY

APPROACH	KEY FOCUS AREAS
▸ Cross-tenant access validation ▸ Horizontal and vertical privilege escalation attempts	▸ Token replay and modification testing ▸ Chaining medium-severity issues across endpoints

▸ Object reference manipulation ▸ API parameter tampering	▸ Authorization gap exploitation chains ▸ Determining meaningful cross-tenant impact

⬡ KEY FINDINGS

The assessment uncovered a critical cross-tenant data exposure scenario enabled through chained authorization weaknesses — an attack path invisible to automated scanning tools.

FINDING 01 | CRITICAL

Cross-Tenant Data Exposure via Authorization Chaining

- Individual endpoints appeared to enforce access controls, but inconsistencies between the web application layer and backend API validation introduced exploitable gaps
- Cross-endpoint interaction and parameter manipulation used to enumerate sensitive internal identifiers
- Exploitation of inconsistent authorization logic between application and API layers
- Leveraging a medium-severity IDOR-like issue as a pivot point for escalation
- Final impact: Unauthorized access to data belonging to other tenants and bypass of intended permission boundaries

⚠ IMPACT SUMMARY

No single vulnerability alone resulted in critical impact. However, when chained together, the weaknesses enabled unauthorized cross-tenant data access — a severe risk for a SaaS provider operating in an enterprise environment. Automated scanners did not detect the complete attack path.

⬡ ADDITIONAL FINDINGS

HIGH SEVERITY

- Inconsistent rate limiting across API endpoints
- Weak token invalidation mechanisms
- Excessive data exposure in API responses

MEDIUM SEVERITY

- Improper input validation in business workflows
- Missing secondary validation on sensitive operations
- Attack surface expansion via configuration gaps

While not immediately catastrophic, these weaknesses contributed to expanding the attack surface and increasing exploitation feasibility.

⬡ RETESTING & VALIDATION

Following remediation, IVASTA Security conducted a structured retest to validate that all identified vulnerabilities were fully resolved and properly implemented.

✓	✓	✓	✓
Authorization checks consistently enforced	**Tenant isolation** properly implemented	**API validation** aligned with frontend	**Token handling** securely managed

The retesting phase confirmed that the previously identified critical attack chain was fully mitigated.

⬡ DELIVERABLES & OUTCOME

📄 **Detailed Technical Report** — Full documentation of findings with clear reproduction steps and evidence

🎯 **Risk-Prioritized Remediation Guidance** — Actionable fixes with business impact analysis tailored to the client environment

🔄 **Formal Retest Validation Report** — Structured confirmation that the critical attack chain and all high-severity issues were resolved

🏆 **Digital Security Validation Certificate** — Used during enterprise customer security reviews to demonstrate independent third-party validation

⬡ BUSINESS IMPACT

The engagement significantly reduced the risk of cross-tenant data exposure and strengthened the integrity of the client's multi-tenant architecture.

The client considered the assessment critical in supporting their continued enterprise growth.

- Increased enterprise customer confidence through independent validation
- Strengthened API security posture across all tenant boundaries
- Reduced regulatory and reputational risk for enterprise deployments
- Improved overall application resilience and authorization architecture

Ready to find out what attackers could do to your systems?

hello@ivasta-security.com | ivasta-security.com