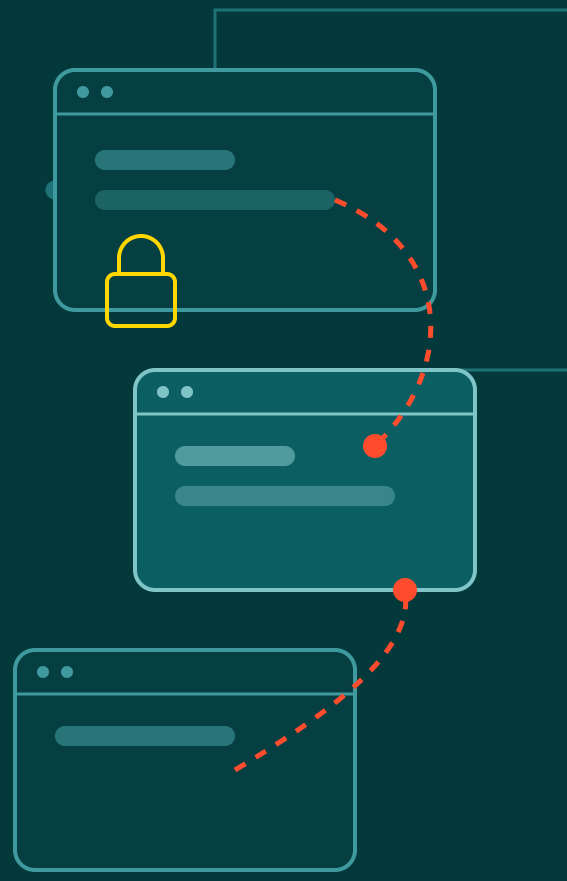
CASE STUDY

CS-2026-02

ioSENTRIX

Your Trusted Partner in Cybersecurity



SOFTWARE AND MULTI-TENANT SECURITY

When a read-only user could pull stored credentials

A read-only role reached integration secrets, and a changed record ID crossed the line between customers.

CLIENT
Software company

SERVICE
Web application and API penetration testing

ENGAGEMENT
Short engagement, 10+ findings

VERIFIED
All findings closed; retested by ioSENTRIX

AT A GLANCE

CLIENT
Software company

PRODUCT
Multi-tenant web platform and APIs

SERVICE
Web application and API penetration testing

SCOPE
Web application, backend APIs and role-based access across tenants

ACCESS
Test accounts at several permission levels

ENGAGEMENT
A short, focused engagement

VERIFIED
All findings closed; retested by ioSENTRIX

TESTED BY
ioSENTRIX application security testers

EXECUTIVE SUMMARY

A read-only role reached stored secrets, and tenant isolation failed too. Both are now fixed and retested

A software company asked ioSENTRIX to test its multi-tenant web platform and the APIs behind it. In a short, focused engagement, we found more than ten issues.

The worst let any signed-in user read other customers' records by changing one number. A second let a read-only role pull stored integration credentials. The client closed every finding, and ioSENTRIX retested the fixes.

10+	1	2
findings, 5 of them Critical or High	read-only role was enough to reach stored credentials	separate paths across the tenant boundary

The interface hid the secrets. The API handed them over.

Details in this case study are anonymised and generalised. Methods that could harm other products are withheld.

© 2026 ioSENTRIX LLC

01 What we found

CRITICAL FINDING 1

Changing one number opened another customer's records

The record endpoint checked that a user was signed in, but not which organisation the record belonged to. Record IDs were sequential and the endpoint had no rate limit, so every customer's records could be collected by a simple script.

Business impact: one customer could read another customer's confidential business data, breaking the platform's core promise of isolation.

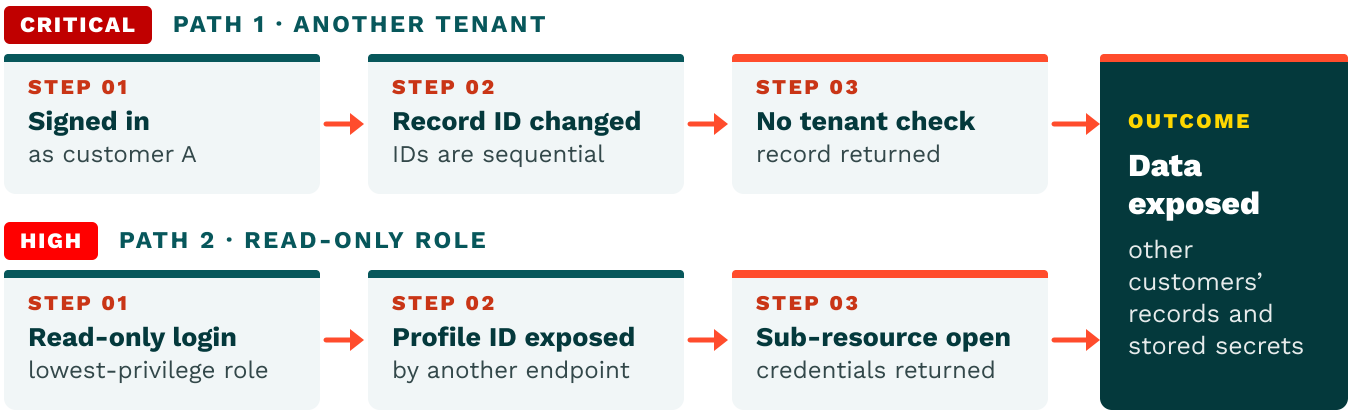
HIGH FINDING 2

A read-only role could pull stored credentials

Access was checked on parent objects but not on their sub-resources. A user with the platform's lowest, read-only role could request authentication settings directly and receive HTTP Basic credentials and OAuth client secrets in plain text. Webhook secrets and one-time-password seeds leaked the same way.

Business impact: stolen credentials would let an attacker act as a customer's own service accounts on the systems those credentials unlock.

Figure 1. Two paths across a boundary the platform was built to enforce



HOW WE FOUND IT

Our testers held accounts at several permission levels, then replayed each API call under every role and against other customers' records to compare what each was allowed to see.

© 2026 ioSENTRIX LLC

02 Results

Figure 2. Findings by severity (10+ findings)[1]



Beyond the signature findings: settings and schedules exposed to restricted roles, an internal ID leak that enabled the credential chain, a missing function-level check, no rate limit on search, and weak input validation.

WHAT CHANGED

All closed by the client; retested by ioSENTRIX

- **Tenant checks.** Every record endpoint now verifies the organisation, with rate limiting.
- **Role checks.** Permissions are enforced on every sub-resource, not inferred from parents.
- **Secrets.** Credentials, webhook secrets and seeds are no longer returned in plain text.
- **Hardening.** Search is rate-limited and inputs are validated server-side.

03 Lessons for software teams

Check the tenant on every request

Being signed in is not permission to see a record (OWASP API1).[2]

Authorise sub-resources too

A role allowed to see a profile is not allowed to see its secrets.

Hiding is not access control

If the API returns a value, the user has it, whatever the interface shows.

[1] Severity rated on a five-level likelihood and impact matrix based on NIST SP 800-30 Rev. 1.

[2] OWASP API Security Top 10 (2023): API1 Broken Object Level Authorization, API5 Broken Function Level Authorization. Cited as alignment guidance.

ioSENTRIX

Running a multi-tenant platform? See a sample API test report or book a strategy session on tenant isolation.

iosentrix.com/contact-us

contact@iosentrix.com

+1 (888) 958-0554

13800 Coppermine Rd, Suite 190
Herndon, VA 20171

CREST-accredited · ISO/IEC 27001 certified · SOC 2 Type 2 attested

© 2026 ioSENTRIX LLC. General information only. Client details anonymised.