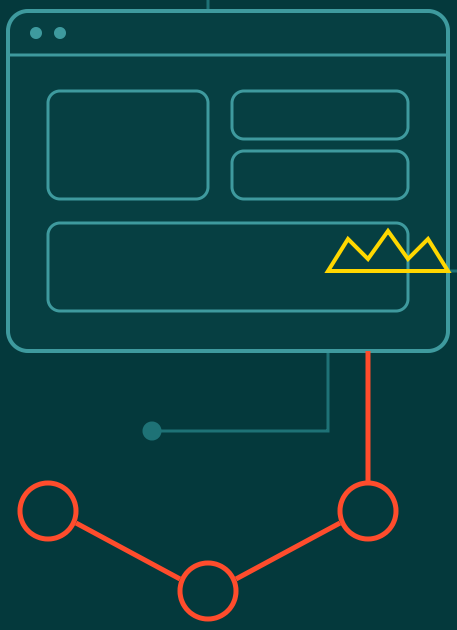
CASE STUDY

CS-2026-03

ioSENTRIX

Your Trusted Partner in Cybersecurity



SAAS PLATFORM SECURITY

Three access-control gaps, one path from no login to full platform control

A SaaS platform closes a path from no login to full admin control.

CLIENT	SERVICE	FINDINGS	VERIFIED
SaaS platform	Web application and API penetration testing	35+, including 4 Critical	**All findings closed; retested by ioSENTRIX**

AT A GLANCE

CLIENT
SaaS platform

PRODUCT
Customer-facing web platform and APIs

SERVICE
Web application and API penetration testing

SCOPE
Web application, APIs and administrative interfaces

FINDINGS
35+ in total, 4 Critical and 4 High

VERIFIED
All findings closed; retested by ioSENTRIX

TESTED BY
ioSENTRIX application security testers

EXECUTIVE SUMMARY

Three gaps chained into a full takeover, and all are now closed

A SaaS platform provider asked ioSENTRIX to test its customer-facing web application, its APIs and its administrative interfaces.

We found that an outsider could open customer dashboards without signing in, read other customers' data with any account, and create privileged users through unprotected admin APIs. The client closed every finding, and ioSENTRIX retested the fixes.

35+	4	3
findings across the platform	Critical findings, three of them chained	steps from no login to admin

Each gap was serious on its own. Together they handed an outsider the whole platform.

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

Customer dashboards opened without a login

Account dashboards sat behind predictable URLs with no authentication at all. Changing the number in the URL opened any customer's account, its data and its admin functions.

Business impact: anyone on the internet could browse customers' business data without ever creating an account.

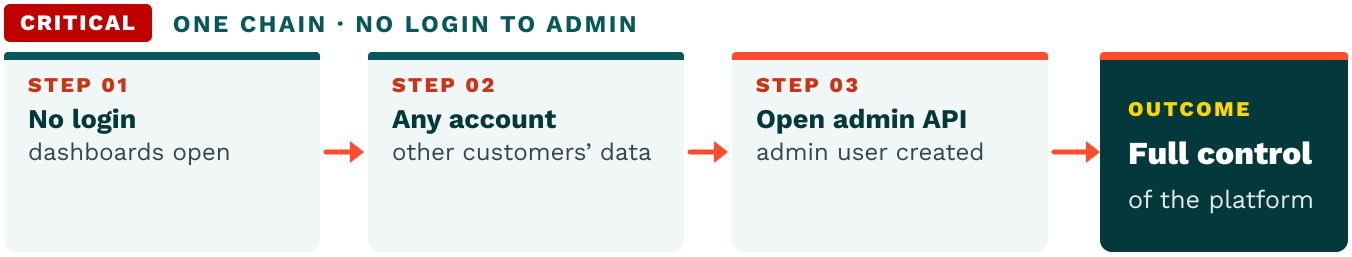
CRITICAL FINDING 2

Unprotected admin APIs let an outsider make themselves an admin

Organisation and user-management APIs answered requests without authentication. They allowed reading organisation data, listing customer groups, changing account status and creating users with elevated privileges.

Business impact: an attacker could take administrative control and change how customers' accounts operate.

Figure 1. Three Critical gaps, chained from an anonymous visitor to platform admin



HOW WE FOUND IT

Our testers treated each gap as a step rather than a separate finding, then proved the chain end to end: from an anonymous visitor to a working administrator account.

© 2026 ioSENTRIX LLC

02 Results

Figure 2. Findings by severity (35+ findings)[1]



Middle step of the chain: missing tenant checks let any signed-in user read other customers' records and billing. Also found: time-based SQL injection, stored and reflected cross-site scripting, CSRF, clickjacking and session-handling weaknesses.

WHAT CHANGED

All closed by the client; retested by ioSENTRIX

- **Authentication.** Every account URL and API now requires sign-in.
- **Authorisation.** Server-side tenant and role checks on every resource; IDs are no longer guessable.
- **Injection.** Parameterised queries throughout, and output encoding against cross-site scripting.
- **Sessions.** CSRF tokens, session invalidation, security headers and rate limits.

03 Lessons for platform teams

Authenticate every endpoint

Hidden URLs and unlinked APIs still get found (OWASP API5).[2]

Guessable IDs invite enumeration

Use non-sequential IDs, and check ownership anyway.

Test how findings combine

A chain shows the real risk better than a list of separate issues.

[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), API5 Broken Function Level Authorization. Cited as alignment guidance.

ioSENTRIX

Running a SaaS platform? See a sample web and API test report or book a strategy session on access control.

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.